GTA 90-01-011

JOINT FORWARD OPERATIONS BASE (JFOB) PROTECTION HANDBOOK

SIXTH EDITION - OCTOBER 2011

Distribution Restriction Statement on inside Front Cover

FOR OFFICIAL USE ONLY

Joint Forward Operations Base (JFOB) Protection Handbook

This is the Sixth Edition of the JFOB Handbook, originally published in 2005, and supersedes the Fifth Edition.

Digital copies of this handbook are available by request at ERDC-JAT@usace.army.mil. Digital copies are also available from the Joint Staff Antiterrorism Enterprise Portal at https://atep.dtic.mil and the Reimer Digital Library at http://www.train.army.mil or http://www.adtdl.army.mil. Printed copies are available from the nearest Army Training Support Center.

Preface to the Sixth Edition

Scope. The Joint Forward Operations Base (JFOB) Protection Handbook describes protective measures for Forward Operations Bases (FOB) outside the continental United States. Guidance is presented for generic FOB size and construction with respect to mass casualty threats including rockets, artillery, and mortar (RAM), direct-fire munitions, and vehicle- and personborne improvised explosive devices (VBIED and PBIED). The handbook's sixth edition (JFOB6) details courses of action (COA), "best practices" and lessons learned that allow engineer, security, and reaction forces input to FOB operational planning and command decisions.

Purpose. This publication identifies tactics, techniques and procedures (TTP) for FOB protection, construction, structural retrofits, threat analysis, and risk management. Findings are supported by applicable doctrine and validated blast mitigation techniques. JFOB6 does not supersede any command authority and protective recommendations must always be mission consistent. The JFOB Handbook was originally prepared for the Office of the Secretary of Defense (OSD).

Administrative Notes. JFOB6 is endorsed by the Joint Staff (J3) Deputy Directorate for Antiterrorism/Homeland Defense, Antiterrorism/Force Protection Division. JFOB6 replaces its predecessor, the Joint Forward Operations Base (JFOB) Survivability and Protective Construction Handbook, Fifth Edition (GTA 90-01-011). Distribution is authorized to U.S. Government agencies and their contractors.

Availability. Document requests should be directed to erdc-jat@usace.army.mil. Graphic Training Aid (GTA 90-01-011) copies are available through the U.S. Army Training Support Center (http://www.atsc.army.mil/). Electronic copies are available from the Reimer Digital Library (http://www.adtdl.army.mil/) and Army Knowledge Online (http://www.us.army.mil/).

This page intentionally blank

TABLE OF CONTENTS

This page intentionally blank

Chapter 1
Forward Operations Base Protection

The current operational environment is characterized by uncertainty, complexity, rapid change, and persistent conflict. Operational demands placed on US military forces are high and will continue so for the foreseeable future. Understanding the operational environment is fundamental to protecting joint forces and operations. This environment requires deployed military units and forward-based activities to protect themselves against threats designed to interrupt, interfere, or impair the effectiveness of joint operations.

Commanders, responsible for protection of forward operations bases (FOB), should have a thorough understanding of threats, vulnerabilities, potential consequences of threat actions, and the methods and resources available for preserving mission capability, and protecting personnel and equipment. FOB commanders typically focus on threats that disrupt operations or cause the greatest number of casualties and decrease force effectiveness.

This chapter discusses the concept of joint security, the role and types of FOBs, command and control, FOB planning, protection concepts, priorities and strategies, FOB construction standards and available engineer resources.

Joint Security Concept

Current national security and military strategies utilize flexible expeditionary forces deployed to forward-based joint operations. The joint security concept requires commanders to protect bases, airfields, seaports, sustainment activities, and lines of communication located within the commander's area of operations. Figure 1-1 depicts a notional organizational structure for joint security operations.

As part of the joint security concept, the Joint Force Commander (JFC) establishes joint security areas (JSA) and command relationships. A JSA is a specific surface area designated to facilitate protection of bases. Regional political considerations and sensitivities will influence whether a JSA is established. JSA sizes may vary considerably depending on the size of the area of operations, mission essential assets, logistic support requirements, and threat. The JFC may retain control of joint security operations or designate area commanders with joint security responsibilities. The JFC also assesses host nation (HN) contributions to base security.

A base cluster is a collection of bases within a JSA, geographically grouped for mutual protection and ease of command and control. The JFC designates a base cluster and the base cluster commander. A base cluster contains no fixed number, but two to seven bases is typical.

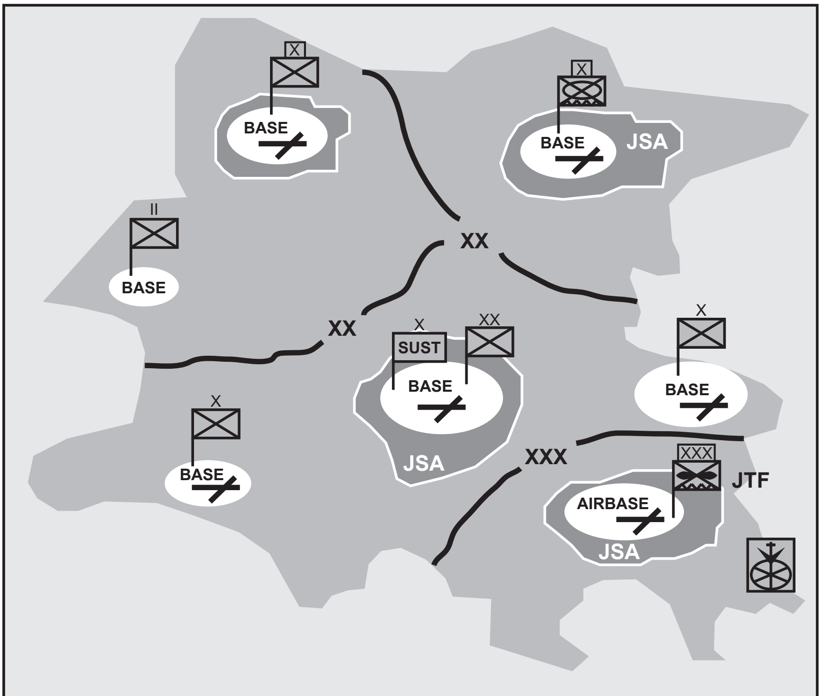


Figure 1-1. Notional Organizational Structure for Joint Security Operations (JP 3-10, *Joint Security Operations in Theater*)

Providing for security of bases/base clusters, units, activities, and lines of communication is complicated by the location, distance between supporting bases, and security environment. Security operations must be properly planned, prepared, and executed to prevent or mitigate hostile actions. In order to facilitate joint security operations, the typical command relationship is one in which the base/base cluster commander establishes tactical control (TACON) over dedicated security forces. This relationship is essential when the force is attached or assigned from a different component command.

Forward Operations Bases

A FOB is an evolving base that extends and maintains the operational reach of joint forces, providing a secure location from which to conduct and sustain military operations. FOBs are not permanent but may develop many of the same functions and facilities over time. A FOB may be either Joint or single-Service. A FOB can contain one or more units from one or more Services; units from allied, coalition, and contingency partners; HN units; and various type US agency and department teams. The FOB commander may be US or from an allied, coalition, or contingency partner nation.

Single-Service FOB. A single-Service FOB supports one Service and the FOB's primary mission is controlled by that Service. FOB commanders are normally designated by the Service component commander.

Joint FOB. A Joint FOB supports two or more Service components. The JFC assigns command authority to a Service component and that component designates a FOB commander.

Allied or Coalition FOB. An allied or coalition FOB may support a specific allied or coalition contingent force or multiple contingent forces and may include US forces. The commander is designated from one of the allied or coalition contingent forces.

The area commander establishes FOB boundaries in coordination with base or cluster commanders. A FOB boundary is not necessarily the base perimeter and should be established based upon the planning factors of mission, enemy, terrain and weather, troops and support available and civil considerations (METT-T[C]), while balancing the need of base defense forces to control key terrain. Base boundaries may be dynamic and require ongoing coordination due to changing METT-T[C].

FOBs vary in size from small combat outposts to large complexes. FOBs can be located in urban or rural areas, on former military bases, in former government or public facilities, on critical supply routes, or on rivers. Typically, a FOB is established adjacent to a regional distribution hub, such as a large civilian or military airfield, rail terminal, or highway junction. During protracted operations, FOBs may be expanded and upgraded to perform many sustainment and support operations.

Command and Control

The FOB commander is responsible for base defense and security operations (see Appendix A). This responsibility is not limited to the base boundary but may extend to the surrounding region. Normally, FOB commanders exercise TACON over defense forces providing interior security within base boundaries and coordinate efforts with ground or HN forces providing exterior security, if available. If a dedicated security force is attached to the FOB from a different component command then the FOB commander will establish TACON over that force.

Tenant units normally secure their own facilities. However, the FOB commander may use all available assets to establish the required level of security. The commander may, for the purposes of base protection, exercise TACON over tenant and transient units from other Services or functional components that are assigned or attached to the base. Unity of command is essential to this concept of FOB protection. Commanders at all levels (assigned, attached or TACON) have the responsibility to ensure that base protection, security, and defense procedures and policies are executed in accordance with the FOB commander's requirements.

Unity of command overcomes the challenges created when different units from different commands with different missions are assigned to support FOB protection. The FOB commander facilitates unity of command by establishing command relationships early, ideally prior to a unit being assigned or attached to the FOB. FOB commanders define areas of responsibility both for interior security and for the surrounding area that influences the FOB.

Planning

FOB planners must consider varying threats, uncertainty in mission duration, and likely troop strength fluctuations. FOBs are vulnerable to surveillance and threats such as improvised explosive devices (IED), rockets, artillery, and mortars (RAM), snipers, and surface-to-air missiles. Planners must also contend with frequent repositioning of forces, while simultaneously determining site selection, FOB size, layout, and defensive posture.

Effective FOBs hinge on proper planning, coordination, and oversight. These tasks must be addressed early in the development process to avoid later difficulties. Early identification of security and protection requirements is essential to FOB planning. Attention to these requirements ensures that site location and layout are compatible with security operations, mission accomplishment, and enhanced survivability. Early development of these requirements also reduces construction and manpower demands.

Effective FOB planning requires a multi-disciplined approach with participants from various organizations who provide expertise in areas such as civil engineering, design, environmental, safety, preventive medicine, antiterrorism, security and real estate. At a minimum, effective FOB planning requires a partnership between security forces and engineers.

Planning provides a framework for locating, designing, constructing, and eventually closing FOBs. Planners must constantly assess, revise, and coordinate their efforts. The process is not absolute, is rarely performed in sequence, and is dependent on mission and operational variables. These include: political, military, economic, social, information, and infrastructure. Example considerations for operational variables are described in Table 1-1.

Table 1-1. Example FOB Assessment Using Operational Variables
(Source: Data from EP 500-1-2, *Field Force Engineering*)

Operational Variable	Planning Considerations
Political	• Political circumstances permitting or denying access to key ports of entry or critical sustainment facilities • Alternative access routes • The effect of laws, agreements, or positions of partners that might prevent the shipment of construction, hazardous, or other materials across borders • Political considerations that might affect real estate acquisition or FOB planning and operations
Military	• An adversary's capability to employ explosive hazards or other obstacles and the capability to challenge traditional survivability standards • Existing military installations and other infrastructure • An understanding of capabilities in a joint, interagency, and multinational context
Economic	• Production or availability of key materials and construction resources • Potential for new or improved production facilities that might be added
Social	• Specific cultural or religious buildings or installations • Potential impact of language barriers or unique local dialects on the availability of labor and engineer resources • Ability to provide culturally related building requirements
Information	• Physical deficiencies in the supporting architecture (including electrical power) or nodes • Provisions for humanitarian projects or services
Infrastructure	• Deficiencies in basic infrastructure • Access to existing infrastructure and the ability to build, deconstruct, or transfer infrastructure for base camps • Opportunities for improvements to existing infrastructure and specific new projects

Protection Concepts

FOB protection is the preservation of the effectiveness and survivability of personnel, equipment, facilities, information, and infrastructure. For that reason, FOB commanders typically focus on protecting against threats that cause the greatest number of casualties or disrupt operations. FOB protection is a continuous process that relies on innovation and adaptability and involves the simultaneous application of several protection concepts. Figure 1-2 conceptualizes five broad protection concepts involved in FOB protection:

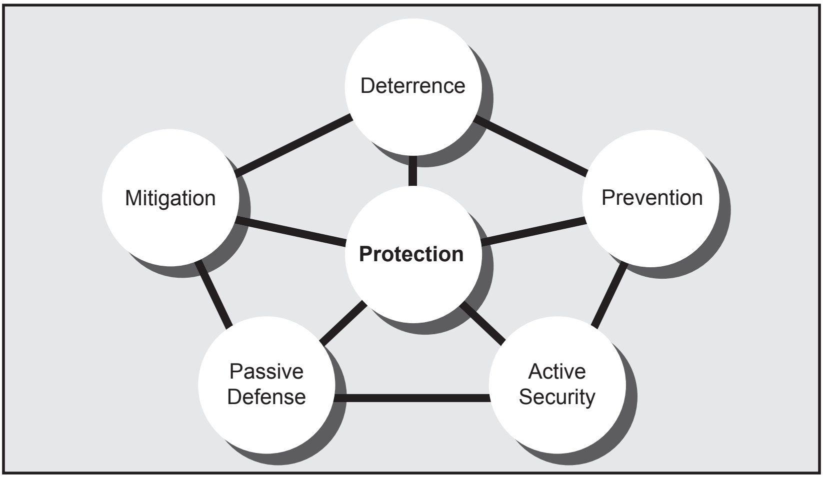


Figure 1-2. Forms of Protection (FM 3-37, *Protection*)

Deterrence. Deterrence involves motivating the enemy to avoid attacking the FOB. Deterrence examples include measures to prevent enemy surveillance, the presence of trained, properly-equipped troops and/or well-armed vehicles, a hardened FOB perimeter, and other factors such as random operational measures that disrupt routine patterns and give the appearance of greater security.

Prevention. Prevention involves the ability to neutralize, delay, or reduce the likelihood of an imminent attack. Prevention does not typically represent an offensive, preemptive capability, but employs other measures such as information security, operations security, and civil and public affairs.

Active Security. Active security includes dynamic activities that detect, interdict, avert, disrupt, neutralize, or destroy threats and hazards. Examples include access control equipment, perimeter sensor systems, aggressive patrolling and a quick reaction force to respond to an attack.

Passive Defense. Passive defense is passive measures taken to protect against the effects of a threat action. Passive defense includes establishment of standoff, construction of a perimeter barrier system, sidewall and overhead cover protection of inhabited structures, survivability positions, and camouflage, concealment and dispersion of critical assets.

Mitigation. Mitigation measures typically involve actions that reduce vulnerabilities and attack consequences by improving deterrence, active security, and passive defense. Mitigation includes incident response and consequence management activities.

Protection Priorities

FOB commanders should develop protection priorities based on threat, vulnerability and risk. Using the protection concepts discussed earlier, a detailed plan should be developed to support protection efforts and incrementally increase FOB protection. An integrated, layered, defense-in-depth plan includes the establishment of perimeter security measures and standoff; access control measures and entry control points; and structures designed to protect personnel and other assets from threat weapons effects. The protection sequence shown in Figure 1-3 is intended to assist in prioritizing FOB protection efforts. The sequence is intended only as a guide and is not a substitute for detailed mission analysis and course of action development. Each situation may require additional sequences or tactics, techniques, and procedures (TTP) to achieve the desired protection.

Protection Strategies

This Handbook is scoped to address threats commonly encountered in current contingency operations and provides protection strategies based on commonly used TTP, best practices and lessons learned. Protection strategies discussed throughout this Handbook are summarized below. For each listed threat, tables 1-2 through 1-6 discuss the protective strategy that can be employed and the associated chapter containing additional information. These strategies are not all inclusive and focus primarily on threats that would likely produce mass casualties or significantly disrupt operations.

Table 1-2. Vehicle-borne Improvised Explosive Device (VBIED) Protection Strategies

Protection Strategy	Reference Chapter
Provide sufficient standoff	4
Provide perimeter barriers and walls capable of stopping vehicles and reducing detonation effects	5
Establish access control procedures and entry control structures to deter, detect, deny, and protect against VBIEDs	6
Provide guard towers and fighting positions to help identify, engage, and defeat VBIEDs	11
Provide personnel bunkers and/or retrofit existing structures for blast protection	8, 11

Sequence	Task	Protection
Establish a permiter at a sufficient standoff	Install concertina/razor wire; man perimeter with personnel dug in or in fighting vehicles	Minimal
	Add obscurations at perimeter using netting or opaque screens	
	Add tall barriers to the perimeter such as soil-filled bins or soil-backed concrete T-walls	
	Provide a double-wall perimeter with an outer low wall and an inner-high wall separated by a minimum 30-foot clear zone; use sensor, lighting and observation towers	Increased
Establish access control procedures and entry control facilities	Provide an entry control point with an approach zone comprised of barriers forming a serpentine approach; provide access control zone with armed personnel in fighting positions and an armored vehicle control gate	Minimal
	Add dedicated and protected vehicle and pedestrian search areas and vehicle barriers	
	Add response zone with armed response force, overwatch position and a final denial gate	
	Provide bunkers for increased protection of security personnel	
	Construct a full entry control facility; provide a load transfer yard for material delivery; deny entry to all vehicles inside the FOB; provide a protected parking area	Increased
Enhance personnel protection	Disperse personnel so there are no large gatherings in one place at the same time	Minimal
	Provide personnel bunkers at various locations on the FOB	
	Add full height sidewall protection for tents and modular housing units	
	Retrofit existing buildings	
	Compartmentalize structures	
	Add detonation screens and overhead cover for high occupancy facilities	Increased

Figure 1-3. Sequential Priority of Protection Effort. Protection increases (moving from minimal to increased; top to bottom) as additional tasks within each sequence re accomplished.

Table 1-3. Person-borne Improvised Explosive Device (PBIED) Protection Strategies

Protection Strategy	Reference Chapter
Provide perimeter barriers / walls capable of stopping personnel	4, 5
Establish access control procedures to deter, detect, deny, and protect against PBIEDs	6
Provide guard towers and fighting positions to help identify, engage and defeat PBIEDs.	11
Provide security systems (lighting and sensors) to assist in detecting and assessing PBIEDs	10
Compartmentalize high occupancy facilities to limit PBIED effects	8

Table 1-4 RAM Protection Strategies

Protection Strategy	Reference Chapter
Provide personnel bunkers for blast and fragment protection	11
Provide full-height sidewall protection for “soft” structures	7
Compartmentalize high-occupancy facilities to limit RAM effects	8
Provide overhead protection to detonate and defeat incoming RAM	9

Table 1-5. Rocket-propelled grenades (RPG) Protection Strategies

Protection Strategy	Reference Chapter
Provide detonation screens and barriers/walls to stop RPG penetration	7
Provide netting or other screens to obscure targets inside the FOB and prevent targeting	5
Provide bunkers with detonation screens or thick walls to prevent RPG penetration	11

Table 1-6. Small-Arms Fire and Sniper Protection Strategies

Protection Strategy	Reference Chapter
Provide netting or other screens and perimeter walls to prevent targeting	5, 7
Provide guard towers and fighting positions to engage and defeat small arms attack	11
Provide full height sidewall protection for “soft” structures to stop ballastic penetration	7
Provide bunkers forsmall arms protection	11

Construction Standards

FOB construction standards affect protection planning efforts and are established at the combatant commander level in coordination with Service components. Construction standards for theater facilities optimize the engineering effort and concentrate on assuring adequate health, safety, and mission requirements. Joint Publication 3-34, *Joint Engineer Operations,* describes two broad categories of construction based on the anticipated length of operation: contingency (up to 2 years) and enduring (2 to 10 years or more). Within these two categories are five possible standards: organic, initial, temporary, semi-permanent, and permanent. These standards are detailed in Figure 1-5 and Table 1-7, which highlight the base development continuum and base camp standards. Master planners use these standards in the development of FOBs and to assist with the transition to more permanent facilities as an operation develops. While the Figure 1-5 timeline provides a conceptual framework, each situation is different and may require adaptations. Ultimately, the combatant commander determines exact construction types based on location, material availability, and other factors. Construction standards are guidelines and other planning factors must also be considered. Each theater of operations has unique construction standards. Examples are the USCENTCOM Sand Book and the USAREUR Red Book.

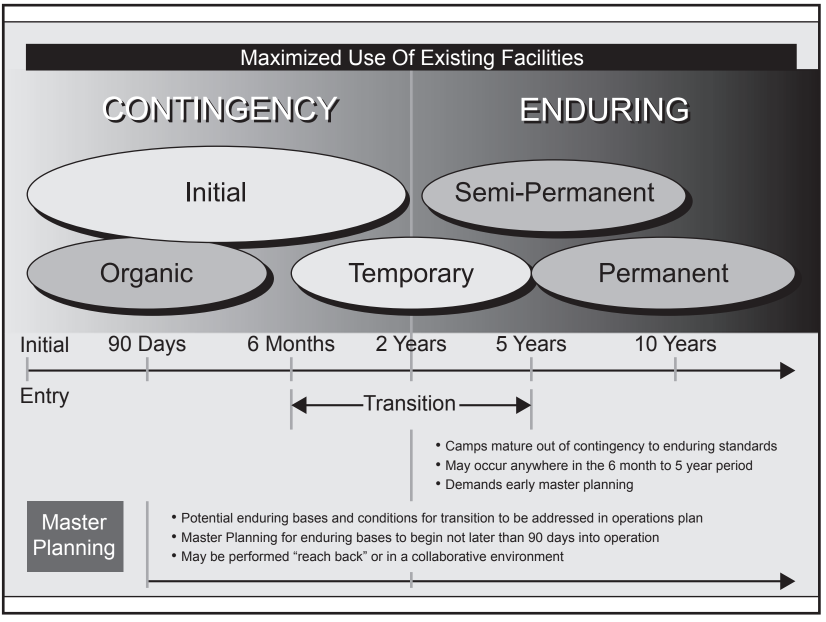


Figure 1-5. Base Development Continuum
(JP 3-34, *Joint Engineer Operations*)

Table 1-7. Base Camp Standards
(JP 3-34, *Joint Engineer Operations*)

Duration	Characteristics
Organic (up to 6 months)	• Use unit equipment and capabilities • Minimal engineer support or construction effort
Initial (up to 2 years)	• Unit equipment augmented with additional assets • Limited military engineer or contractor support and some new construction effort
Temporary (up to 5 years - bridges the gap between contin-gency and enduring phases)	• High degree of engineer support • New construction or repair of existing facilities • Crosses the gap into the enduring phase
Semi-permanent (2-10 years)	• Design effort exceeds military engineer unit capabilities • Most work is beyond the scope of construction for military engineers • Designed and built for moderate energy efficiency, maintenance, and life-cycle management
Permanent (5-10 years or more)	• Significant design effort required • Completely beyond the scope of construction for military engineer units • Designed and built for a high degree of energy efficiency, maintenance, and life-cycle management

Planning and Construction Resources

Each Service has core engineering units and capabilities that can be used for FOB planning and construction. The engineering capabilities of each Service component may support other components or contingency partners to meet engineering requirements. Labor, material, infrastructure, and services specifically adapted to the local environment are often supplied by contracts with HN and civilian contractors. This capabilities mixture may change during an operation and require management across Service lines to ensure appropriate engineering support.

Army Engineers. US Army engineers perform combat, general, and geospatial engineering operations. Engineer units at the brigade combat team level and below focus their efforts on combat engineering. Engineers at division level and above reinforce the combat engineering capability at the brigade level with general engineering capabilities. Some capabilities that are categorized as engineering by other Services reside in other branches of the Army including explosive ordnance disposal [EOD] and chemical, biological, radiological, and nuclear (CBRN) capabilities.

Navy Engineers. Navy engineers, organized under the naval construction force, commonly known as Seabees, have rapidly deployable units of various sizes and configurations. Seabees provide advanced base construction to include airfields, LOC upgrade and maintenance, battle damage repair, underwater and amphibious construction, and logistic facilities construction. Navy engineers also provide engineering support to the Marines and can function as a major subordinate command to a Marine Air-Ground Task Force (MAGTF).

Marine Corps Engineers. Marine Corps engineers are primarily tasked for combat and general engineering in support of MAGTFs. Engineers provide mobility, counter mobility, survivability, and limited general engineering support. Mobility includes the assessment and fortification of roadways and bridges and the clearing of obstacles. Counter mobility involves the creation of obstacles and barriers for the enemy. Survivability consists of the construction and fortification of new bases and positions.

Air Force Engineers. Air Force engineers support airfield operations. Engineer units rapidly deploy in support of operational tasks such as airfield pavement evaluations, crash and fire rescue, EOD, emergency management response, airfield damage repair, facility construction and maintenance, utility systems construction, maintenance, aircraft arresting system installation and maintenance, airfield lighting, and navigation aids. Organized as Prime Base Engineer Emergency Force (Prime BEEF), Rapid Engineer Deployable Heavy Operational Repair Squadron, Engineer (RED HORSE) or as detached units, engineers provide an array of general and geospatial engineering capabilities.

Other Engineering Capabilities. Alliance, coalition and contingency partner military engineers also provide valuable engineering capabilities.

Department of Defense Construction Agents. The Secretary of Defense has designated the US Army Corps of Engineers (USACE) and the Naval Facilities Engineering Command (NAVFAC) as agents for the design and construction of US military facilities worldwide. USACE and NAVFAC provide significant engineering capabilities to joint operations. Both USACE and NAVFAC support FOB planning, construction, and infrastructure development. USACE and NAVFAC provide technical engineering assistance for design and award of construction contracts to civilian contractors in support of military operations.

Reachback Capabilities. Deployed engineers from all Services can obtain reachback support from USACE, NAVFAC, and Air Force Civil Engineering Support Agency (AFCESA). Available services include technical support, assistance in planning and designing infrastructure, environmental assistance, real estate acquisition, geospatial engineering, and contract construction. Prior coordination with these organizations to establish support procedures is recommended. See Chapter 12, Field Force Engineering for additional details on engineer reachback.

References:

JP 1-02. *Department of Defense Dictionary of Military and Associated Terms,* 15 July 2011.

JP 2-01.3. *Joint Intelligence Preparation of the Operational Environment,* 16 June 2009.

JP 3-10. *Joint Security Operations in Theater,* 03 February 2010.

JP 3-34. *Joint Engineer Operations,* 30 June 2011.

FM 3-0. *Operations*, June 2001.

FM 3-37. *Protection*, September 2009.

EP 500-1-2. *Emergency Employment of Army and Other Resources- Field Force Engineering- United States Army Corps of Engineers Support to Full Spectrum Operations*, 01 August 2010.

This page intentionally blank

CHAPTER 2
THREATS

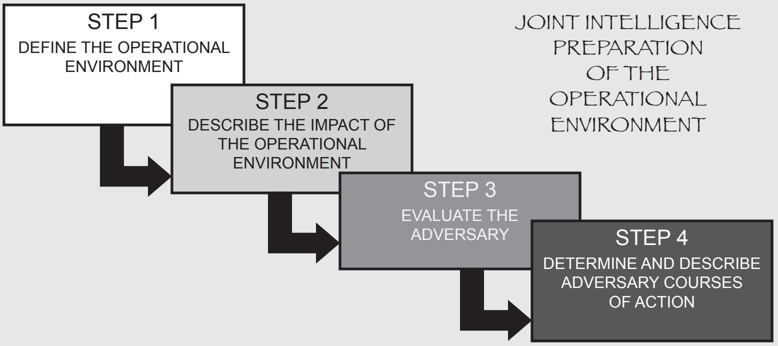
A threat is any opposing force, adversary, condition, source, or circumstance with the potential to negatively impact mission accomplishment and/or degrade mission capability. This Handbook addresses threats from unconventional enemy forces such as insurgents and terrorists. Attempts to degrade FOB mission capability can range from snipers to deliberate complex attacks against coalition or HN forces or civilians. Four major objectives describe adversary behavior:

- Inflict injury or death on military/civilian FOB personnel
- Destroy or damage FOB facilities, property, equipment, or resources
- Steal FOB equipment, materiel, or information
- Create adverse publicity

Threat Analysis

A threat analysis is a continual process of compiling and examining available information concerning potential adversaries that could target DoD components, elements, and personnel. Threat analysis researches and analyzes intelligence, counterintelligence, and open source information to identify likely adversaries to FOB operations. The threat analysis provides input into a Threat Assessment document that addresses the full range of adversary capabilities and intentions.

The joint intelligence preparation of the operational environment (JIPOE) process is a key tool for conducting threat analysis. JIPOE provides a systematic approach to analyze the adversary and other relevant aspects of the operational environment. Figure 2-1 shows the JIPOE process, which is detailed in JP 2-01.3, *Joint Intelligence Preparation of the Operational Environment* (JP 2-0).



- A systematic methodology used by intelligence personnel
- Used to analyze information about the physical environment and the adversary
- A key tool for conducting joint intelligence analysis
- Can be applied to the full range of military operations
- Identifies most probable course of action and most dangerous course of action

Figure 2-1. Joint Intelligence Preparation of the Operational Environment (JP 2-0, *Joint Intelligence*)

Threat Levels

The greatest threat to a FOB is an attack capable of producing mass casualties. Adversaries will employ a variety of weapons and tactics to achieve this aim. Potential adversaries may resort to asymmetric methods. Such methods include unconventional, surprise, innovative, or disproportionate means to exploit weaknesses. Adversaries may resort to inexpensive approaches that circumvent US strengths and test vulnerabilities. Threat activities are generally described and categorized in three levels (Figure 2-2) ranging from civil disturbances to full combat operations. Each level or any combination of levels may exist simultaneously in an AO.

Level I threats include adversary agents and terrorists whose primary missions include espionage, sabotage, and subversion. Adversary activity and individual terrorist attacks may include:

- Killing of military and civilian personnel
- Kidnapping, hijacking vehicles for use in direct attacks
- IEDs, vehicle-borne IED (VBIED), personnel borne IED (PBIED), and rocket propelled grenade (RPG) attacks
- RAM attacks
- Sniper attacks

THREAT LEVEL	EXAMPLES	CAPABILITY REQUIREMENT
LEVEL I	Agents, saboteurs, sympathizers, terrorists, civil disturbances	Base or LOC internal defense capability, may require limited military police presence
LEVEL II	Small tactical units, unconventional warfare forces, guerrillas, may include significant standoff weapon threats	Same as Level I, but will require base mobile security force or area security force with specialized base or LOC security related mission requirement
LEVEL III	Large tactical force operations, including airborne, heliborne, amphibious, infiltration, and major air operations	Same as Level II, but may require the employment of a tactical combat force

Figure 2-2. Threat Levels (JP 3-0, *Joint Security Operations in Theater)*

Civilians sympathetic to an adversary may become significant threats to US and coalition partner operations. Civilians are not normally part of an established adversary network, often making their actions random and unpredictable. Countering criminal activities, civil disturbances, and terrorist activities requires doctrinal guidelines that differ from those used to counter conventional forces. Such counter-activities require detailed coordination with HN military, security, and police forces. More significantly, based on political, cultural, or other perspectives, events that disrupt friendly operations may be perceived as legitimate by the local populace.

Countering Level I threats is part of the day-to-day protection measures implemented by all commanders. Key to countering these threats is active civilian support from those sympathetic to US or multinational goals

Level II threats include small scale (less than company-sized equivalents) irregular forces conducting unconventional warfare that threatens military and civilian personnel. Level II attacks can cause significant disruption to military operations and the orderly conduct of local government. Irregular forces are capable of conducting well coordinated but small-scale hit and run attacks, IED and VBIED attacks, and ambushes that may include standoff weapons such as RAM and SAM. Level II threats may include special operations forces that are highly trained in unconventional warfare.

Threat activities typically associated with Level II threats include the Level I threats as well as raids and ambushes. Level II threat forces establish and activate espionage networks, collect intelligence, conduct sabotage missions, develop target lists, and conduct target damage assessments. Countering Level II threats requires a dedicated, highly trained and properly equipped FOB security force.

Level III threats may be encountered when a threat force has the capability to project combat power by air, land, or sea, anywhere into the AO. Specific examples include airborne, heliborne, and amphibious operations; large combined arms ground force operations; and large numbers of individuals or small groups infiltrated into the AO, regrouped at predetermined times and location, and committed against priority targets. Air and missile threats to bases/base clusters and LOC may materialize with little warning. Level III threats necessitate a decision to commit tactical combat forces or other available forces. Level III threats are beyond the capability of FOB or base cluster defense and response forces.

Hybrid Threat. A hybrid threat is the diverse and dynamic combination of regular forces, irregular forces, and/or criminal elements unified for common benefit. The term “hybrid” captures the increased complexity of war, the multiplicity of actors involved, and the blurring between traditional categories of conflict. Hybrid threats employ changing varieties of conventional and unconventional organizations, equipment, and tactics to create multiple dilemmas. Regular forces are governed by international law, military tradition, and custom. Irregular forces are unregulated and act with no restrictions on violence or targets for violence. The ability to combine and transition between regular and irregular forces and conduct operations to capitalize on perceived vulnerabilities makes hybrid threats particularly effective.

Threat Tactics

There are many threat tactics that can be employed against a FOB. A threat assessment should identify possible threat tactics based on likely adversary objectives and history of attacks at FOBs in the AOR. Table 2-1 provides possible adversary courses of action (COA) based on historical tactics and techniques. Table 2-1 is not all-inclusive, and implies neither the presence nor absence of a particular tactic. Always refer to a threat assessment or consult a supporting intelligence office before attempting to determine adversary COA.

Tactics commonly employed against FOBs in current contingencies are summarized below:

Vehicle-borne Improvised Explosive Device (VBIED). A VBIED is a vehicle filled with explosives, driven to a target, and detonated. VBIEDs are among the most effective threat weapons and can deliver large explosive payloads directly to a target. VBIEDs typically contain an improvised explosive or incendiary mixture to provide the charge. The bomb can be carefully constructed at a safe distance from the target and explosives may be concealed in a car or truck. Once assembled, the bomb can be delivered at a time of the adversary's choosing and with reasonable precision. VBIEDs can be remotely detonated with a timer or remote control, or detonated by a suicide driver. Explosive weights range from 200 lbs to 4,000 lbs or larger.

Person-borne Improvised Explosive Device (PBIED). These devices are usually carried in vests or containers such as rucksacks or briefcases, which are chosen to blend with the target surroundings. Given the portability requirement, such bombs usually weigh 50 lbs (25 kg) or less, although an ordinary-sized briefcase can hold up to 25 lbs (12 kg) of explosive. A 50 lb (25 kg) suitcase bomb can destroy a house or cause serious structural damage to larger buildings. Adversaries often increase casualties by packing bombs with nails, nuts, bolts, and other metallic items that act as shrapnel. Such weapons are devastating in confined spaces.

Rockets, Artillery, and Mortars (RAM). RAM are indirect fire weapons that can be launched over obstacles to hit targets. RAM do not require line of sight like direct fire weapons, but RAM do require a clear line of flight. Indirect fire weapons include mortars and small rockets, which are usually improvised military rockets with small explosive or incendiary charges, and historically representative of terrorist attacks. Mortars include both military and improvised mortars. Typically, improvised mortars have carried larger explosive yields than the military versions. Employment of large artillery is limited to combat forces. Typical rockets include 107-mm and 122-mm and 240-mm. Typical mortars range from 60-mm to 120-mm.

Rocket-propelled Grenades (RPG). RPGs are a type of antitank weapon fired from a distance and may be directed against facilities, vehicles, or other assets. RPGs can be used in the same manner as any direct fire weapon. Shoulder-fired RPG launchers are most commonly encountered, including the Russian RPG-7, RPG 18, and RPG 22, and the U.S. M-72 Light Antitank Weapon (LAW).

Small-arms Fire. Small arms include pistols, rifles, shotguns, and submachine guns, and can be either military or civilian weapons. These weapons must be aimed directly at a target and line of sight must be clear. Adversaries use small arms to attack from a distance and to overpower guards and sentries.

Snipers. Traditionally, snipers are trained, experienced professionals with customized or large caliber weapons. Snipers are exceptional marksmen and masters of camouflage and deception. They operate independently and are noted for adaptability, patience, and cunning. Effective sniper ranges can easily exceed 1,000 m.

For planning purposes, the general information associated with threat levels (see Figure 2-2) and the threat-tactic matrix in Table 2-1 can be used as indicators or checklists to assist in developing a list of potential threats and tactics. In addition, Table B-1 (FOB Common Threats, Attack Tactics, and Mitigation Measures) at Appendix B, Risk Management, provides a list of current potential threats to FOBs based on historical analysis.

Table 2-1. Threat-Tactic Selection (Source: Data from UFC 4-020-01 and JP 3-10)

Threat Level ▼	Adversary ▼	Tactics														
		Surveillance			Entry		Weapons			Explosives		Attacks			Contamination	
		Visual	Acoustic	ElEm	Forced	Covert	IF	SC	MDF	IED	MHX	Assaults	Waterfront	Aerial	Airborne	Waterborne
Level I	Foreign Intel Services	●	●	●	●	●				●						
	Agents	●			●	●				●						
	Criminals				●	●		●		●						
	Vandals				●	●		●		●						
	Extremist Protestors				●	●	●	●		●						
	Sympathizers				●	●		●		●						
	Saboteurs	●			●	●	●	●		●			●		●	●
	Terrorists	●			●	●	●	●	●	●	●	●	●	●	●	●
Level II	Small Tactical Units	●			●	●	●	●	●	●	●	●	●	●	●	●
	Unconventional Warfare Units	●	●		●	●	●	●	●	●	●	●	●	●	●	●
	Guerrillas	●			●	●	●	●	●	●	●	●	●	●	●	●
	Special Operations Forces	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

ElEm - Electronic Emanations
IF - Indirect Fire Weapons (Mortars, Artillery)
SC - Small Caliber Weapons (Rifle, Pistol, Shotgun)
MDF - Military Direct Fire Weapons (Machine Gun, SAM, RPG, Cannon)
IED - Improvised Explosive Device
MHX - Military High Explosive

References:

JP 2-0. *Joint Intelligence,* 22 June 2007.

JP 2-01.3. *Joint Intelligence Preparation of the Operational Environment,* 16 June 2009.

JP 3-10. *Joint Security Operations in Theater,* 03 February 2010.

JP 3-15. *Barriers, Obstacles, and Mine Warfare for Joint Operations,* 17 June 2011.

UFC 4-020-01. *DoD security Engineering Facilities Planning Manual*, 11 September 2008.
.
FMI 4-93.2. *The Sustainment Brigade*, 04 February 2009.

TC 7-100. *Hybrid Threat,* November 2010.

CHAPTER 3
SITE SELECTION & LAYOUT

FOB site selection and design layout are controlled by competing demands and considerations, such as mission concerns, civil/military constraints, HN requirements and combatant commander and Service regulations. Protection considerations should be deliberately integrated into FOB planning, design, and construction. A design with protection measures in mind will greatly reduce the materials, time, and energy required to protect the FOB and will improve the FOB's ability to enhance its defensive posture when threat levels increase.

Site Selection Considerations

FOB site selection is determined by many factors including the tactical situation, access to transportation infrastructure, proximity to the civilian population, terrain, weather, protection considerations, and the effects of selecting an alternate location. Site selection is crucial to effective operations. A poorly located FOB may be difficult to secure and could hinder rather than enable operations.

The primary concern during FOB site selection is mission accomplishment. However, protection considerations cannot be ignored. Early identification of protection and security requirements reduces construction costs and manpower demands and helps ensure adequate protection of personnel and assets. Protection measures are easier and more cost effective to establish during the planning/site selection/design layout process than after the FOB is constructed. Early consideration of protection measures may preclude or simplify the application of more robust measures at a later time.

Planners facilitate the site selection effort by conducting a terrain analysis that considers the military aspects of a location from the viewpoint of both the defenders and the enemy. This analysis and the site selection process should be governed by METT-T[C] (Figure 3-1) and other FOB protection-specific factors (Figure 3-2).

METT-T[C] CONSIDERATIONS FOR FOB SITE SELECTION

Mission

- ☐ What is the proposed FOB's mission?
- ☐ Does the FOB's mission override other site selection considerations?
- ☐ Is the FOB's mission affected by existing infrastructure,facilities,struc tures, natural and manmade features, types and quantity of indigenous construction materials, and available real estate?
- ☐ Does the FOB's mission require access to the local transportation infrastructure? Does the proposed site provide access to local road networks?

Enemy (Threat)

- ☐ Have specific enemy threats been identified, both current and future, for the proposed FOB site?
- ☐ If so, what are the characteristics, capabilities, techniques and tactics of these threats? (Special consideration should be given to standoff weapons and mass attack capabilities such as RAM and CBRN materials.)
- ☐ What effect will the identified threat(s) have on the proposed site?
- ☐ What are the enemy's tactical, operational, and strategic objectives and intentions as they relate to FOB protection?
- ☐ What is the organization, size, and composition of enemy forces in the proposed FOB's area of operation (AO)?
- ☐ What is the enemy's intelligence capability? Can the enemy collect intelligence using local contract workers/vendors?
- ☐ What is the level of local support for the enemy?

Terrain and Weather

- ☐ Consider the military aspects of a proposed site from both friendly and enemy standpoints.
- ☐ Observation and Fields of Fire – Does the site limit the enemy's ability to observe friendly forces and FOB operations? Conversely, does the site offer friendly forces the opportunity to observe the surrounding terrain and potential enemies? Given that the highest terrain offers the best observation and fields of fire, is the site elevated? Does the site limit possible enemy fields of fire, assault positions, and ambush points? Does the site limit or block an attack by direct line-of-sight weapons from potential enemy vantage points?
- ☐ Cover and Concealment – Does the site offer cover and concealment to friendly forces? Does the site provide cover and concealment to

an attacking force? Have potential enemy vantage points and hiding places been considered? Can vegetation, topography, and natural or man-made barriers (drainage channels, ditches, culverts, or ridges) be used as protective measures, or similarly used by the enemy? Does the site provide unobstructed clear zones around the FOB?

- Obstacles – Can natural terrain features (trees, fences, land forms, and rivers) be used as barriers to obscure enemy vantage points or prevent, block, or disrupt an attack? Can terrain features be used by an attacking force to launch an attack?
- Key terrain – Is control of key terrain on or adjacent to the site critical to mission accomplishment? Has the site been selected away from terrain such as natural (hills, mountains) or man-made (tall buildings, towers) vantage points? Does the site avoid low-lying topographic areas that can aid the effects of enemy CBRN weapons?
- Avenues of Approach – Does the site limit likely enemy avenues of approach? Does the site prevent enemy ease of movement?
- Weather – Will weather and visibility conditions have an adverse effect on the proposed FOB site and/or operations? For example, will heavy rains cause flooding? Will prevailing winds aid the effectiveness of enemy CBRN weapons or releases of toxic industrial materials? Conversely, can adverse weather be used to exploit advantages over enemy vulnerabilities?

Troops and Support Available

- Does the proposed site provide adequate space for planned tenant units/organizations?
- Do planned tenant units have specific requirements or constraints that may affect site selection?
- How close are adjacent FOBs located from the proposed site? Will the proposed site be part of a base cluster (a collection of bases, geographically grouped for mutual protection and ease of command and control)?

Time Available

- How much FOB construction time will be required at the proposed site?
- Will alternate sites allow quicker construction?
- Is the proposed site located in a remote location that will cause delays in construction material support or security force (Tactical Combat Force) response?

Civil/Military

- ☐ Does the local civil/military/political situation influence FOB site selection, design, layout, or land use?
- ☐ How close is the proposed site to the local civilian population?
- ☐ Will an unpopular site selection decision encourage attacks?
- ☐ What effect will the proposed site have on the local community? Will the site cause traffic congestion? Will the site inconvenience or threaten the safety of the local populace? Will any restrictions have to be imposed on the local populace, such as limiting public access to the area?
- ☐ Will site selection affect adjacent landowners?
- ☐ How will the public perceive the FOB - as a threat, an undesirable fortress, or welcomed?
- ☐ Does site selection address the type and quantity of indigenous and other available construction materials, equipment, funding, and contractor support?

Figure 3-1. METT-T[C] Considerations for FOB Site Selection

PROTECTION CONSIDERATIONS FOR FOB SITE SELECTION

Protection Requirements

- ☐ Can combatant commander (COCOM) and Service required standoff distances be attained between potential threats and the proposed site and its inhabited structures?
- ☐ Does the proposed site maximize the distance between the FOB perimeter and surrounding developed areas? Does the site provide as much open space (clear zone) as possible around the FOB perimeter?
- ☐ Can proposed inhabited structures within the FOB achieve adequate dispersion?
- ☐ Is enough land available to increase standoff or dispersion distances as threats increase?
- ☐ Does the proposed site support or enhance defense in depth?
- ☐ Does the site require an attacker to negotiate a series of varied, and often alternating, obstacle/barrier layers (natural or man-made), interspersed with varying distances of open ground (clear zones)?
- ☐ Have protection requirements for the proposed site been established, and does the site support these requirements?
- ☐ Does the proposed site aid or impede the implementation of protection measures?

- ☐ Does the site simplify protection by increasing the difficulty of enemy attack?
- ☐ Does the proposed site support perimeter security requirements such as standoff, perimeter barriers, entry control points (ECPs), access control, guard towers, lighting, sensors, etc.?
- ☐ Is enough land available to accommodate the space needed to construct an adequate ECP and to make improvements as threats increase?
- ☐ Does the site provide a location for an external parking lot for unauthorized vehicles? Does the parking lot location provide adequate standoff to protected assets?
- ☐ Can main thoroughfares around the site be controlled to limit unauthorized vehicle access and maintain standoff distances?
- ☐ Does the site minimize the number of access roads and entrances into the FOB? Does the site allow for the design of entry roads that do not provide direct or straight-line vehicular access?

Procedural Requirements

- ☐ Do FOB procedural or operational requirements affect site selection?
- ☐ How will deliveries (mail, supplies, materials, trash service, and construction vehicles) be handled?
- ☐ Will the proposed FOB have any special access control measures (identification of personnel, weapons, vehicles, and packages) that will affect site selection?
- ☐ Will the FOB have "Restricted Areas" (weapons or ammunition storage areas, communications sites, petroleum, oil and lubricants (POL) sites) that must be considered during site selection?

Figure 3-2. Protection Considerations for FOB Site Selection

Layout and Design Considerations

Planners concerned with FOB layout and design must consider many challenges, such as FOB operational and functional issues, infrastructure requirements, protection and security measures, HN requirements, safety, and fire protection. Some layout considerations are similar to site selection considerations. In general, layout concerns and constraints will be FOB-specific. Throughout the design process, planners should recognize conflicts, establish priorities, and focus on most favorable solutions. The FOB layout and design should:

- Facilitate current and future operations
- Maintain a layered, defense in depth security approach
- Include ECPs that maintain security and control vehicle and personnel access
- Include redundant utilities, protected critical assets, and accessible protective shelters throughout the FOB
- Disperse facilities and structures to support rapid incident response
- Maximize protection of high occupancy structures using measures such as overhead and sidewall protection designs

Protection measures that reduce vulnerability and diminish potential threat to personnel and critical assets should be addressed during FOB layout. These measures include establishment of standoff distances, perimeter security, vehicle barriers, ECPs, access control, and security lighting. In addition, protective structural designs to harden walls, roofs, floors, and windows should be considered during FOB layout since these designs may require additional space to implement. FOB layout designers should consider the factors in Figure 3-3.

FOB LAYOUT AND DESIGN CONSIDERATIONS

General Considerations

- ☐ How will mission and operational requirements affect FOB layout?
- ☐ What units/organizations will occupy the FOB? Does the layout provide adequate space for tenants and address other occupancy related constraints?
- ☐ Does the layout make use of existing structures on the site?
- ☐ Does the FOB layout comply with pertinent COCOM/Service regulations?
- ☐ Does the layout address operational or procedural considerations such as deliveries, contractor/vendor access, sanitation, garbage, and load/off-load areas?
- ☐ Does the layout include a commercial delivery vehicle load/off-load or transfer point that is off-site and distant from critical assets and high occupancy structures?
- ☐ Does the layout address safety and fire concerns?
- ☐ Does the layout provide pedestrian and vehicle control?
- ☐ Are adequate weapon and ammunition storage areas included in the design layout?
- ☐ Are adequate petroleum, oil and lubricants (POL) storage areas designed in the layout? Have POL storage facilities been located at the required standoff distance from critical assets and occupied structures?
- ☐ Does the layout provide secure access to utilities and water supplies?

- ☐ Does the layout and design provide redundant utility systems, particularly electrical services?
- ☐ Are redundant utility systems provided to the Base Defense Operations Center (BDOC), security forces and medical personnel?
- ☐ Are water treatment and storage facilities adequately protected in the layout and design?
- ☐ Does the design layout include a mass notification system?
- ☐ Have interoperable, secure, reliable, flexible, survivable, and decentralized communications been designed into the FOB layout?

Protection Considerations

- ☐ Does the FOB layout provide adequate standoff distances?
- ☐ Does the layout limit or block line of sight (LOS) from potential adversary vantage points using natural screens (hedges, trees, and shrubs), man-made obscuration screens, or non-critical structures?
- ☐ Does the layout eliminate potential hiding places near or around the FOB that screen covert activity?
- ☐ Does the layout minimize the number of access roads and eliminate roads that provide direct or straight-line vehicle access? Does the layout direct unauthorized vehicles away from the FOB?
- ☐ Does the layout incorporate the concept of a layered defense in depth?
- ☐ Does the layout incorporate perimeter security measures such as barriers, lighting, sensors, access control, and guard towers?
- ☐ Does the design layout secure all perimeter penetrations (utilities, concrete trenches, drainage culverts) by use of screens, fences, grates, locks on manhole covers, and intrusion detection sensors or other visual surveillance system?
- ☐ Does the layout include an adequate ECP design? Has the number of ECPs been kept to a minimum?
- ☐ Does the layout include an external parking lot with adequate standoff for unauthorized vehicles?
- ☐ Does the layout include internal parking lots that restrict parking within standoff zones and near critical assets?
- ☐ Are FOB structures adequately dispersed to aid incident response and quick reaction by security forces and minimize collateral damage?
- ☐ Have protective shelters/bunkers and defensive positions been strategically located throughout the FOB?
- ☐ Have high occupancy structures been avoided or limited by not placing large numbers of personnel in one structure?
- ☐ If not, are critical and high occupancy structures located away from the FOB perimeter?
- ☐ Has the distance between the FOB perimeter and inhabited structures been maximized?

- ☐ Have structural/retrofit hardening techniques been included in the FOB design layout for existing and planned occupied structures?
- ☐ Does the layout consider any additional space needed for structural hardening/retrofit of existing or planned structures?
- ☐ Have windows in existing or planned occupied structures been limited or designed to reduce the risk of casualties caused by glass fragmentation?
- ☐ Do designs include the secure anchoring and the opening outward of doors to prevent separation as a result of blast and to ease egress?
- ☐ Does the layout conceal, disperse, create "defensible space" for and restrict access to critical assets? Does the layout and design minimize the use of signage that identifies critical assets?
- ☐ Are critical assets located in the interior of the FOB, away from the perimeter? Are critical assets located to protect against visual surveillance?
- ☐ Have CBRN defense concerns been incorporated into the FOB layout?
- ☐ Does the FOB layout incorporate the following base defense requirements?
  - Positions of critical internal assets, external coordination points, and no-fire areas
  - Locations of any obstacles or mines
  - Locations and direction of fire of crew-served weapons
  - Locations of target reference points and designated or preplanned fires
  - Locations of OPs
  - Final protective fires
  - Clear fire zones
  - Locations of sensors and defensive positions
  - Location of CBRN collective protection and decontamination sites
- ☐ Does the layout address HN security requirements/restrictions?
- ☐ Does the layout address coalition force security requirements/restrictions, if applicable?
- ☐ Will the FOB commander exercise tactical control (TACON) over forces assigned or attached to the base primarily for the purpose of base defense?
- ☐ Do tenant units/organizations have an inherent protection capability that can be incorporated into the FOB protection mission?
- ☐ Have funding limitations for protection been considered?

Figure 3-3. FOB Layout and Design Considerations

References:

JP 3-10. *Joint Security Operations in Theater*, 03 February 2010.

CHAPTER 4
STANDOFF

The preferred technique to reduce the effects of explosive attacks, particularly VBIEDs, is to maximize standoff distance between critical assets and potential attack locations. Standoff should be a primary consideration in FOB site selection. Generally, costs for hardening an asset for blast protection will decrease as standoff increases. However, increasing standoff also requires more land and increases the overall size of the perimeter. If adequate standoff outside the perimeter is not possible, an alternate technique is to maximize standoff from the perimeter to individual inhabited structures within the FOB Allowances for standoff distance should also provide opportunities to upgrade structures in the future to meet increased threats or accommodate additional protection. Even with adequate space, standoff must be coupled with appropriate operations security (OPSEC) procedures, such as access control, to be effective. Figure 4-1 illustrates the importance of standoff distance to personnel safety.

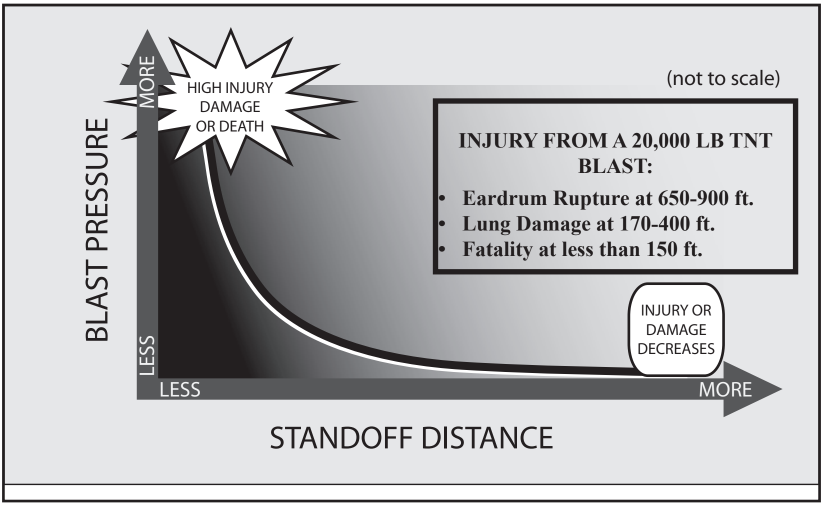


Figure 4-1. Increased standoff distance decreases personnel injuries due to explosives effects.

Physics of an Explosion

An explosion is an extremely rapid release of energy that produces a blast wave. An explosive blast wave (Figure 4-2) is formed by the following sequence of events:

1. A rapid chemical reaction characterized by a detonation wave travels at velocities of 5,000 to 30,000 ft/sec from the point of initiation through the explosive compound (Figure 4-3).

Figure 4-2. High speed camera sequence showing blast wave formation.

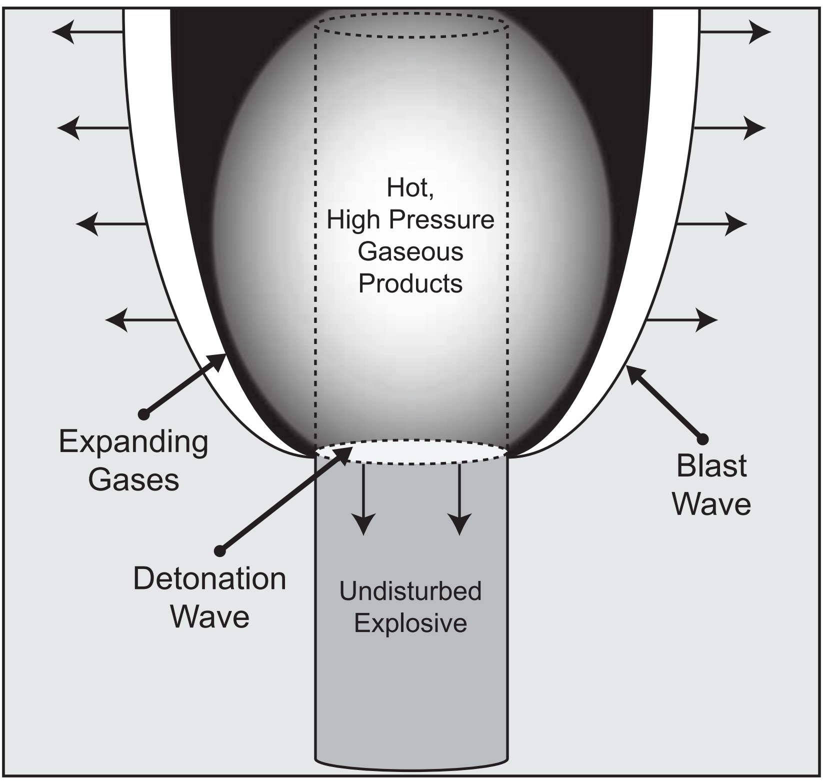


Figure 4-3. Depiction of a Detonation in a solid explosive.

2. This rapid chemical reaction converts the explosive compound into an extremely hot, high pressure gas with temperatures of 5,000-7,000 °F and pressures of 1,500,000–4,500,000 psi.
3. The hot gaseous fireball expands by rapidly displacing the air around it, and then transfers its momentum to the surrounding air as a layer of highly compressed air. This forms the shock or blast wave. This blast wave contains most of the explosively released energy. As the fireball expansion slows, its overpressure falls to zero, and due to overexpansion, becomes negative, creating a suction phase in the blast wave before returning to zero.

The blast wave travels radially outward from the source at super sonic velocities. As it expands, compressed air pressure falls rapidly with increasing distance. However, if the wave meets a surface perpendicular to its direction of travel (such as a building), the wave is reflected and amplified by a factor of up to thirteen. Figure 4-4 shows how pressures behind the wave front also decay rapidly over time (exponentially) and exist only for milliseconds. After the positive phase, the shock wave becomes negative, creating suction. A portion of the energy can also be imparted to the ground, creating a crater and generating a ground shock wave similar to a high-intensity, short-duration earthquake.

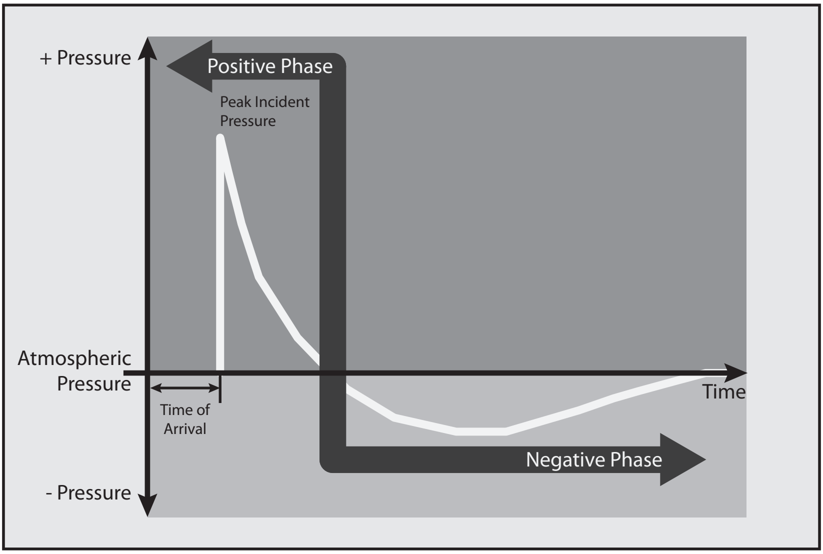


Figure 4-4. Depiction of blast pressure response with time. (FEMA 426)

Blast Effects

Standoff is the preferred method for explosive attack mitigation. Table 4-1 shows personnel injuries typically associated with blast effects. An explosive device generates the following personnel hazards:

Blast Pressures. The explosive force transmitted through the air (airblast) can cause injury to personnel in the open. Primary blast injuries are those resulting from the impact of the overpressure wave with body surfaces. Gas-filled organs such as the lungs, middle ear, and gastro-intestinal tract are most susceptible to blast injuries. Other injuries include those caused by personnel being thrown against other objects by the blast wind. Burns and toxic inhalation are also common.

Primary Fragments. Primary fragments are small, high speed fragments generated from the casing, container, or other material immediately adjacent to the explosive, such as a vehicle. These fragments can travel long distances. Primary fragments are generally the most lethal bomb projectiles. Injuries may include both penetrating and blunt force trauma wounds.

Secondary Fragments. Barriers and structures damaged by a nearby explosion can produce secondary debris. This debris will be launched at relatively low trajectories, but at high velocity. Secondary fragments are usually larger than primary fragments and can cause more serious blunt force trauma wounds. For example, concrete T-walls can provide some shielding from blast and primary fragments. However, T-walls located too close to the explosion can break into pieces and become hazardous shrapnel.

Building Damage. The blast wave is the primary cause of building damage. Due to high reflected pressures on the building side facing the explosion, damage to this side may be significantly more severe than on sides not facing the detonation. Window glass and exterior walls may fail and become hazardous to personnel in the building. Glass breakage may extend for miles in large explosions. A significant portion of all blast injuries are caused by lacerations from high-velocity glass fragments. When walls fail, large pieces of debris are generated that can cause blunt force trauma injuries. In addition, if the walls are primary load bearing elements, failure may lead to building collapse. In frame buildings, failure of a load-bearing member such as a column or girder may lead to progressive building collapse. Building collapse is a major cause of fatalities. Adequate standoff and avoidance of buildings with load bearing walls minimizes collapse potential. Figure 4-5 is an example of building blast damage.

Figure 4-5. Building damage resulting from the Khobar Towers attack.

Table 4-1. Typical Injuries Based on Distance from Blast Detonation (AFH 10-2401)

Standoff Distance	Type of Injuries
Very Near to the Detonation, Inside the Fireball	Dominant lethal injury mechanisms are primary fragment penetration and/or blast lung. Eardrum ruptures are common, but not lethal. Depending upon the blast size, burns, whole-body translations, gastrointestinal (GI) tract injuries, and inhalation injuries are likely, but are usually considered superfluous.
Near the Detonation, Outside the Fireball	Dominant lethal injury mechanisms are primary fragment penetration and/or blast lung. Eardrum ruptures are common, but not lethal. Burns are unlikely with conventional high explosives. GI tract injuries are less common. If the detonation occurs in the free-field or a vented enclosure, inhalation injuries are unlikely. If the detonation occurs in a frangible structure, blunt trauma from secondary debris and/ or crushing due to structural collapse may result in injuries ranging from minor to fatal in severity.
Mid-range from the Detonation	Eardrum ruptures are common. In an urban environment, blunt trauma from secondary (structural) debris and penetration injuries from secondary (window) debris are likely. These injuries are not likely to be lethal, but may result in operational casualties, major disruptions to operations, and heavy loads on the medical responders.
Far-range from the Detonation	Glass penetration is the most likely source of injuries. These injuries are likely to be only minor to moderately severe, but may be significant operationally, may place heavy loads on the medical responders, and may have a significant psychological impact.

Standoff Guidelines

In most cases, commanders and planners should base standoff distances on explosive weights for blast threats as identified in the FOB threat assessment. However, if there is no identified threat, as a minimum, commanders should use the standoff distances for expeditionary and temporary structures as specified in UFC 4-010-01, *DoD Minimum Antiterrorism Standards for Buildings* and UFC 4-010-02, *DoD Minimum Antiterrorism Standoff Distances for Buildings.*

Table 4-2. DoD Minimum Standoff Distances (based on UFC 4-010-01 & UFC 4-010-02)

Structure Category ▼	Location ▼	Fabric Covered/ Metal Frame Structures [1]	Other Expeditionary Structures [1,2]	Applicable Explosive Weight (TNT) [3]
		Standoff Distance or Separation Requirement ▼		
Billeting and Primary Gathering Structures	Controlled Perimeter or Parking and Roadways without a Controlled Perimeter	102 ft. (31 m)	233 ft. (71 m)	220 lb. (100 kg)
	Parking and Roadways within a Controlled Perimeter	46 ft. (14 m)	105 ft. (32 m)	55 lb. (25 kg)
	Trash Containers	46 ft. (14 m)	105 ft. (32 m)	55 lb. (25 kg)
Structure Separation [4]	Separation Between Structure Groups	59 ft. (18 m)	59 ft. (18 m)	2.2 lb. (1 kg) [5]
	Separation Between Structure Rows	30 ft. (9 m)	30 ft. (9 m)	2.2 lb. (1 kg) [5]
	Separation Between Structures in a Row	12 ft. (3.5 m)	12 ft. (3.5 m)	2.2 lb. (1 kg) [5]

NOTES: Refer to Appendix A of UFC 4-010-01 for definitions necessary for application of this table
1. See Definitions in UFC 4-010-01 or 4-010-02 for a complete description of these structure types.
2. For container structures, Appendix B in UFC 4-010-01 applies.
3. When the explosive specific weights in this column are removed from this table, is no longer considered For Official Use Only.
4. Applies to Billeting and primary Gathering Structures only. No minimum separation distances for other inhabited structures.
5. Explosive for building separation is an indirect fire (mortar) round at a standoff of half the separation distance..

See Table 4-2. Geographic combatant commanders may establish additional guidance for standoff distances for a specific deployment area.

Tables 4-3 through 4-6 provide example standoff distances for estimates of lung damage, concrete wall debris, tent damage, and glass fragment hazards. Select the appropriate table based on the scenarios below:

Personnel Location	Use Table
In open, fatalities from air blast	4-3
In open, fatalities from concrete wall debris	4-4
In tents exposed to air blast	4-5
In building with glass windows	4-6

Table 4-3. Distances for Lung Damage from Air Blast
(UFC 3-340-02, *Structures to Resist the Effects of Accidental Explosions*)

Fatality Estimates►	99% Fatalities	50% Fatalities	1% Fatalities	Almost No Fatalities
Explosive Weight † ▼	Estimated Standoff *			
220 lb. (100 kg)	16 ft. (4.9 m)	21 ft. (6.4 m)	26 ft. (7.9 m)	44 ft. (13.4 m)
500 lb. (227 kg)	24 ft. (7.3 m)	30 ft. (9.1 m)	38 ft. (11.6 m)	60 ft. (18.3 m)
1,000 lb. (454 kg)	33 ft. (10.0 m)	40 ft. (12.2 m)	49 ft. (14.9 m)	80 ft. (24.4 m)
4,000 lb. (1,814 kg)	59 ft. (17.9 m)	70 ft. (21.3 m)	85 ft. (25.9 m)	134 ft. (40.8 m)
10,000 lb. (4,536 kg)	85 ft. (25.9 m)	101 ft. (30.8 m)	119 ft. (36.3 m)	189 ft. (57.6 m)

† TNT-Equivalent Explosive Weights
* Based on a 150 lb .(68 kg) person

Table 4-4. Distances for Fatalities from Concrete Wall Debris (USAF Force Protection Battlelab, *Barrier Assessment for Safe Standoff*, 2001 and AFH 10-2401, *Vehicle Bomb mitigation Guide*, 2006)

Fatality Estimates►	Concrete Wall 10 ft. (3.0 m) From Detonation	Concrete Wall 35 ft. (10.7 m) From Detonation
Explosive Weight † ▼	Estimated Safe Standoff *	
220 lb. (100 kg)	10 ft. (3.0 m)	0 ft. (0.0 m)
500 lb. (227 kg)	80 ft. (24.4 m)	10 ft. (3.0 m)
2,000 lb. (908 kg)	1,000 ft. (304.8 m)	10 ft. (3.0 m)
10,000 lb. (4,536 kg)	3,000 ft. (914.4 m)	650 ft. (198.1 m)

† TNT-Equivalent Explosive Weights
* Estimated Low Level of Protection (moderate injuries, fatalities unlikely). Assumes a 1-ft. (0.3m) thick by 6.5 –ft. (2m) high wall with a 1.5 ft (0.5m) x 3.25 ft. (1m) base.

Table 4-5. Distances for Tent Damage from Explosive Threats (ERDC/GSL TR-06-7, *Evaluation of the Current Vulnerability of Expeditionary Shelters to Airblast*, 2006)

Damage and Injury Estimates►	Tent collapses, Canvas Drags Furniture at High Velocity; Potential Fatalities	Connection at Tent Poles Fail and Tent Partially Collapses; Possible Injury, No Fatalities	Minimal Damage; Injuries Unlikely
Explosive Weight † ▼	Estimated Standoff *		
220 lb. (100 kg)	102 ft. (31.1 m)	160 ft. (48.8 m)	220 ft. (67.1 m)
500 lb. (227 kg)	150 ft. (45.7 m)	230 ft. (70.1 m)	290 ft. (88.4 m)
1,000 lb. (454 kg)	200 ft. (60.9 m)	300 ft. (91.4 m)	380 ft. (115.8 m)
2,000 lb. (908 kg)	260 ft. (79.2 m)	400 ft. (121.9 m)	480 ft. (146.3 m)
4,000 lb. (1,814 kg)	330 ft. (100.6 m)	520 ft. (158.5 m)	620 ft. (188.9 m)
10,000 lb. (4,536 kg)	460 ft. (140.2 m)	720 ft. (219.5 m)	850 ft. (259.1 m)

1. TNT-Equivalent Explosive Weights
2 Modular General Purpose Tent System - Injuries caused by impact from tent frame and debris from furniture inside tents.

Table 4-6. Distances for Glass Fragment Hazard from Explosive Threats (*U.K. Glazing Hazard Guide* SSG/EP/4/97.1997)

Hazard and Injury Estimates►	High Hazard: Severe to Very Severe Lacerations; Potential Fatalities	Low Hazard: Large Number of Lacerations; May Require Hospitalization	Break Safe: Small Cuts and Abrasions; Medical Aid Needed without Hospitalization
Explosive Weight † ▼	Estimated Standoff *		
220 lb. (100 kg)	257 ft. (78.3 m)	363 ft. (110.6 m)	491 ft. (149.6 m)
500 lb. (227 kg)	350 ft. (106.7 m)	500 ft. (152.4 m)	670 ft. (204.2 m)
1,000 lb. (454 kg)	450 ft. (137.2 m)	660 ft. (201.2 m)	870 ft. (265.2 m)
4,000 lb. (1,814 kg)	750 ft. (228.6 m)	1,090 ft. (332.2 m)	1,430 ft. (435.9 m)
10,000 lb. (4,536 kg)	1,030 (313.9 m)	1,480 ft. (451.1 m)	1,970 ft. (600.4 m)

1 TNT-Equivalent Explosive Weights
2 Minimum standoff distance needed to reduce hazard, based on a 2 ft. x 4 ft. (0.6m x1.2m) 5/32-in. (4.0 mm) thick annealed glass window.
3 Low Level of Protecton (LOP)
4 Medium LOP
5 High LOP

Table 4-7 provides standoff distances required to prevent breach of modular concrete barrier walls from explosive threats. Barrier walls with higher strength concrete can resist breaching at smaller standoff distances than those shown. More information on concrete barriers can be found in Chapter 5.

Table 4-7. Standoff Distance to Prevent Breaching of Concrete Wall from Explosive Threats
(UFC 3-340-01, *Design and Analysis of Hardened Structures to Conventional Weapon Effects*)

Explosive Weight †►	220 lb. (100 kg)	440 lb. (200 kg)	1,000 lb. (454 kg)	2,200 lb. (1,000 kg)	4,400 lb. (2,000 kg)	22,000 lb. (10,000 kg)
Wall Thickness ▼	Standoff Needed to Prevent Breaching *					
12 in. (304.8 mm)	20 ft. (6.1 m)	25 ft. (7.7 m)	33 ft. (10.1 m)	43 ft. (13.2 m)	54 ft. (16.6 m)	93 ft. (28.5 m)
16 in. (406.4 mm)	15 ft. (4.7 m)	25 ft. (7.7 m)	33 ft. (10.1 m)	43 ft. (13.2 m)	54 ft. (16.6 m)	93 ft. (28.5 m)
20 in. (508.0 mm)	11 ft. (3.3 m)	21 ft. (6.5 m)	33 ft. (10.1 m)	43 ft. (13.2 m)	54 ft. (16.6 m)	93 ft. (28.5 m)
24 in. (609.6 mm)	8 ft. (2.4 m)	16 ft. (4.9 m)	33 ft. (10.1 m)	43 ft. (13.2 m)	54 ft. (16.6 m)	93 ft. (28.5 m)
28 in. (711.2 mm)	6 ft. (1.8 m)	13 ft. (3.9 m)	28 ft. (8.6 m)	43 ft. (13.2 m)	54 ft. (16.6 m)	93 ft. (28.5 m)

† TNT-Equivalent Explosive Weights
* For barrier concrete with 2,000 psi (13.8 MPa) compressive strength. This information is applicable to bare concrete wall barriers without soil backing or other material to mitigate breaching.

More refined calculations of structure damage and resulting human injury can be performed with blast effect software (Figure 4-6). However, a structural engineer familiar with blast effects should be involved to ensure that building structural characteristics are correctly modeled in the software.

Antiterrorism (AT) Planner

AT Planner is a digital analysis tool to evaluate building damage and injury to occupants resulting from explosive threat scenarios. AT Planner emphasizes the evaluation of structural components, windows, personnel, and other assets. Structural components are defined for columns, walls, and roofs, including common construction materials. The software is available from the U.S. Army Engineer Research and Development Center at https://atplanner.erdc.usace.army.mil (Accept the security certificate presented and login with User Name **atpuser** and Password **4u2plan**. Follow the site instructions to obtain the software and an activation key).

Blast Effects Estimation Model (BEEM)

BEEM is an assessment tool for modeling the effects of various types of explosive devices and indicates the degree of damage to personnel and nearby buildings. BEEM incorporates versions of the AT Planner Tool (see description above) and the Force Protection Tool. BEEM can be used to assess blast and fragmentation effects. BEEM is available from the U.S. Army Corps of Engineers Protective Design Center at https://pdc.usace.army.mil/software/beem/. Follow the instructions on the site to obtain the software.

Building Injury Calculator and DatabaseS (BICADS)

The BICADS software approximates the number of human injuries from the building debris generated by a blast load on the structure. The user defines the basic building construction, building occupants, and blast source. The software then calculates injury estimates based on data from terrorist bombings, accidental explosions, explosive tests, simple engineering models, and engineering judgment. BICADS is available from the U.S. Army Corps of Engineers Protective Design Center at https://pdc.usace.army.mil/software/bicads/. Follow the instructions on the site to obtain the software.

Vulnerability Assessment Protection Option (VAPO)

VAPO is designed to support force protection evaluators and planners with the ability to address modern asymmetric threats such as improvised IEDs and chemical and biological weapons. VAPO uses fast running, physics-based algorithms to predict cratering, fragmentation, blast damage and subsequent collateral effects resulting from chemical or biological agent dispersion. VAPO calculates the blast and fragmentation environment for urban scenes, to include effects of reflection and diffraction of blast pressures off and around structures. VAPO also models progressive collapse of buildings. All VAPO requests must be made on the Defense Threat Reduction Agency, Assessment of Catastrophic Events Center (ACECenter) web site at https://acecenter.cnttr.dtra.mil/acecenter/.

Figure 4-6. Blast Effect Analysis Software

References:

AFH 10-2401. *Vehicle Bomb Mitigation Guide,* 01 September 2006.

UFC 4-010-01. *DOD Minimum Antiterrorism Standards for Buildings,* 08 October 2003 (Including change 1, 22 January 2007).

UFC 4-010-02. *DoD Minimum Antiterrorism Standoff Distances for Buildings*, 08 October 2003 (Including change 1, 19 January 2007).

UFC 3-340-02. *Structures to Resist the Effects of Accidental Explosions*, 05 December 2008.

ERDC/GSL TR-06-7. *Evaluation of the Current Vulnerability of Expeditionary Shelters to Airblast,* 2006.

CHAPTER 5
BARRIERS

Barriers are vital to FOB protection. Barriers maintain standoff distances, establish boundaries, limit and control access of personnel and vehicles, channelize movement, obstruct line-of-sight observation from outside the perimeter, and protect critical assets. Barriers can be natural, man-made, or a combination of both. Natural barriers are terrain features, such as mountains, cliffs, rivers, canals, waterways, and swamps. Man-made barriers include berms and ditches, personnel and vehicle barriers, gates, and expedient barriers such as military vehicles, construction equipment, and rubble.

Barrier Classification

Barriers are categorized as either active (containing moving parts) or passive (non-moving parts). Barriers are further characterized as fixed (permanently installed) or portable (moveable: may require heavy equipment). Many barrier types exist; barriers should be selected based on their specific intended applications.

Active Barriers. Active barriers are electronically or manually operated. Examples include barricades, retractable bollards, beams, and gates. Active barriers are normally employed at FOB entry and exit points or at entrances to critical assets with controlled perimeters. From a safety standpoint, active vehicle barriers are capable of causing serious injury or death, even when properly operated. Most injuries result from equipment malfunction, inadvertent activation, or operator error. If employing active barriers, alert incoming vehicles of their presence with warning signs and lights. In addition, these barriers should include backup power, emergency cutoff switches, and adequate lighting.

Passive Barriers. Passive barriers contain no moving parts and are designed to absorb energy upon impact, and transfer that energy to the foundation. Examples include portable or permanent concrete structures, concrete bollards, soil-filled containers, posts, guardrails, ditches, and reinforced fences. Passive barriers used along the perimeter or interior fence line should be designed to allow little or no penetration, especially if available standoff distance is limited. Passive barriers are commonly found in expeditionary environments and limited duration operations.

Fixed Barriers. Fixed barriers are permanently installed and usually require heavy equipment to move or dismantle. Examples include hydraulically-operated rotation or retracting systems, pits, and concrete or steel barriers. Fixed barrier systems can be active or passive.

Portable Barriers. Portable barrier systems are relocatable, although heavy equipment may be required for relocation. Examples include hydraulically operated, sled-type barricades, jersey barriers, and filled 55-gallon drums. Portable barrier systems can be active or passive.

Barrier Selection

FOB planners should determine the number and types of barriers needed. Additional requirements to consider include employment locations, barrier pre-positioning (if applicable), barrier purpose (traffic control, perimeter security, etc.), and resources necessary for barrier relocation (anchors, cables, forklift, trailer, etc.). The following actions guide barrier selection:

- **Determine the threat**. Past history of threat tactics will influence the number, type, and size of barriers required to defend a FOB. A detailed threat assessment usually provides insight to likely threat scenarios.
- **Determine assets to be protected.** Assets with high exposure and high concentrations of personnel should be considered at higher risk.
- **Determine required standoff distances**. Standoff distances are selected based on building construction (new, existing, expeditionary, and temporary), threat levels, and the value and availability of land. If required standoff is not available or achievable, evaluate alternate means to mitigate threat (for example, harden the facility or build a blast wall); decide to accept additional risk; or restrict use at higher threat levels.
- **Select perimeter barriers**. Perimeter barriers define and maintain standoff zone boundaries. Barrier selection is different for each tactic (stationary or moving vehicle bomb, RPG, sniper, etc.) and should be based on current threat assessments.
- **Identify Entry Control Point (ECP) requirements**. Barriers should be selected to restrict vehicle and personnel access to the FOB. ECP barrier requirements should be consistent with the perimeter barrier system. Refer to Chapter 6 for additional information on ECP planning and barrier selection concepts.
- **Establish standard operating procedures (SOP)**. SOPs should explain how active barriers are employed, operated, control access, and outline specific rules of engagement (ROE). ROE should address activating barriers against high-speed, threatening vehicles. Security personnel should be alert, well trained, show good judgment, and fully understand current threat, SOP, and ROE.

Figure 5-1 shows general considerations relating to barrier selection. Additional information and specific guidance can be found in Joint Publication 3-15, Barriers, Obstacles, and Mine Warfare for Joint Operations; MIL-HDBK-1013/10, *Military Handbook Design Guidelines for Security Fencing, Gates, and Guard Facilities*; and UFC 4-022-02, *Selection and Application of Vehicle Barriers*.

BARRIER BEST PRACTICES AND SELECTION CONSIDERATIONS

- □ Can barriers be placed to maximize standoff distance?
- □ Can barriers be combined with each other, the natural terrain, or man-made obstructions? [Barrier combinations and layers are more effective than single barriers; barrier combinations must afford an equal degree of continuous protection]
- □ Can barrier placement be far enough away from other structures-- trees, telephone poles, antenna masts—to prevent them from being used to circumvent the barrier?
- □ Can barrier placement prevent vehicles from parking nearby? [Vehicle bombs adjacent to concrete barriers can break the barriers into high-velocity projectile fragments that threaten occupied structures]
- □ Can concrete barriers be backed by soil or soil-filled bins to mitigate fragmentation?
- □ Can barrier combinations and layers be separated by a minimum of 30 ft. (9.15 m) clear zones on the sides and between layers for adequate observation and maintenance?
- □ Can additional barrier toppings be added to outer and inner perimeter walls? [These include concertina wire, multiple-strand razor or barbed wire, or other devices that deter enemy efforts to vault or scale the barrier]
- □ Can barriers provide mounting locations for FOB sensors, surveillance platforms, and lighting?
- □ Can barrier placement prevent enemy use as cover and concealment? [Eliminate enemy hiding places with concertina wire, multiple-strand razor or barbed wire, or expedient devices]
- □ Will barriers be continuously monitored with intrusion detection systems (IDS) and patrolled/observed by security force personnel?
- □ Do barrier weak points exist that require continuous monitoring? [Consider IDS to detect and assess intrusion attempts]

□ Are vehicles - including destroyed and captured enemy vehicles - available for expedient barrier use? [Parked bumper-to-bumper, vehicles provide an effective personnel barrier. Large construction-type vehicles or armored vehicles are effective supplemental barriers behind gates or as a temporary serpentine in ECPs.]

□ Can barriers be frequently inspected and maintained? [Barriers can be compromised through breaching or erosion and should be inspected at least weekly and maintained as required]

□ Can overwatch and protective fires be integrated to support perimeter barriers?

□ Can barriers be placed to eliminate line of sight (LOS) surveillance and conceal FOB activities?

□ Has the FOB threat assessment identified a specific explosive threat?

□ What is the type, weight and expected speed of threat vehicles?

□ Have all impact points along the perimeter been identified and can barriers be used to mitigate these points?

□ Will the barrier considered absorb the kinetic energy developed by the threat vehicle?

□ Will the barriers be subject to severe environmental conditions?

□ Is the selected barrier designed to resist corrosion or other environmental effects?

□ Will barriers interfere with established clear zone requirements?

□ Does the active barrier have a manual override in case of power failure?

□ Have appropriate safety features being considered?

□ Has the selected barrier been crash tested?

CHAIN-LINK AND METAL MESH FENCE BEST PRACTICES

□ Are fences located to prevent circumvention by use of terrain features or structures (buildings, utility tunnels, light and telephone poles)?

□ Can chain-link and metal mesh fences be anchored with metal posts placed in concrete at intervals no greater than 10 ft. (3.0 m)?

□ Can fences be topped with razor wire, general purpose tape obstacle (GPTO), barbed concertina wire, or barbed wire outriggers (listed in order of most effective to least effective)?

□ Can fence height, including outriggers, reach 8 ft. (2.4 m)?

□ Can horizontal wire be woven through the bottom and top of the fence to keep the edges rigid?

□ Will the bottom fence edges extend no more than 4 in. (10.2 cm) above ground? [Preferred installation includes concrete footings that encase fence bottoms around the entire perimeter. This prevents lifting, delays burrowing, and diminishes erosion.]

□ Can synthetic screens be woven into fences to prevent outside observation of the FOB? [Ensure the screen does not block outward observation]

Figure 5-1. Barrier Best Practices and Selection Considerations

Perimeter Barriers

Barriers are an integral part of the perimeter security system. Barriers establish a continuous physical impediment that:

- Defines the FOB perimeter
- Establishes a physical and psychological deterrent to attackers and individuals attempting unauthorized entry
- Optimizes use of security forces
- Enhances detection and apprehension opportunities for security forces

Perimeter barriers can consist of natural barriers like terrain features and vegetation, and man-made vehicle and personnel barriers. Perimeter barriers are placed to obscure observation and control personnel and vehicle access. Barrier systems are enhanced with clear zones, multi-strand razor or concertina wire toppings, obscuration/sniper screens, security lighting, and electronic surveillance and sensor systems. Any structures originating from or extending outside the perimeter, such as utility ducts, drainage culverts, concrete trenches, and storm drains should be secured with screens, grates, or sensors.

Clear Zones. Each Service has established varying dimensions for clear zones. As a general rule, a clear zone should be created at least 30 feet (9.2m) on both sides of a boundary barrier. Clear zones must be kept free of vegetation and debris that might conceal intruders. Vegetation within any clear zone should not exceed 6 inches (152mm) in height. If clear zone requirements are not feasible then other measures should be considered; consider increasing barrier height, increasing security-patrol coverage, additional security lighting, or installing a perimeter sensor system. Objects that present no aid to circumvent the perimeter barrier or do not provide concealment to an intruder (patrol road, light poles) may be permitted to stay within the clear zone.

Obscuration Screens. Perimeter barriers can be used in conjunction with obscuration screens to block direct lines-of-sight to sensitive FOB areas from outside the perimeter (Figure 5-2). Screening reduces targeting opportunities from direct fire weapons. Obscuration screens do not provide total protection from direct fire weapons. However, some obscurations screens can function as pre-detonation screens (see Chapter 7) to help protect against direct shoulder-fired rockets. Obscuration can also be accomplished with trees, dense vegetation, chain-link fences, wooden fences, camouflage netting, and soil berms. Ideally, obscuration screens should allow FOB security personnel outward visibility.

Figure 5-2. Obscuration Screen on Perimeter Fence

Sniper Screens. The combination of obscuration screens and perimeter barriers are also an effective deterrent against snipers. Berms, tall concrete barriers, soil-filled containers and the modular protective system (see Chapter 7) can provide protection from snipers. These barriers can be positioned at building entrances and exits where personnel gather. Camouflage netting is an expedient obscuration method (Figure 5-3). Apply netting to areas where personnel might be observed. When hard stand buildings are not available, tents offer concealment for many operations (e.g., maintenance, logistics, food service, and religious services).

Figure 5-3. Netting Used for Obscuration

Drainage Culverts and Utility Openings. Culverts, storm drains, sewers, air intakes, exhaust tunnels, and utility openings require special protective measures. Openings with a cross-sectional area of at least 96 sq. in. (0.06 sq. m) or greater with the smallest dimension being greater than 6 in. (150 mm) must be secured. Measures include securely fastened grills, locked manhole covers, or equivalent means that provides security penetration resistance of approximately 2 minutes (Figures 5-4 and 5-8). MIL-HDBK-1013/10, *Military Handbook Design Guidelines for Security Fencing, Gates, and Guard Facilities,* provides detailed design options.

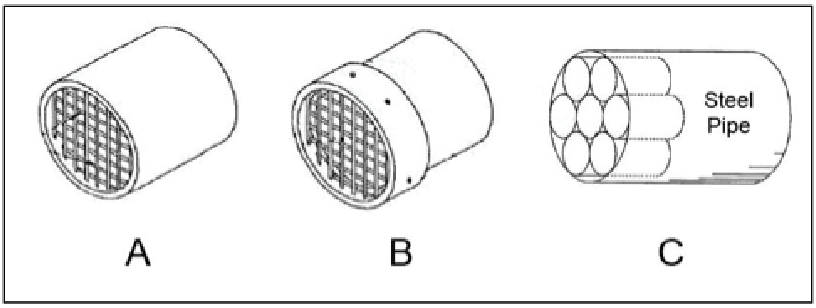


Figure 5-4. Culvert grill examples. A: Steel culvert grill; B: Concrete culvert grill; C: Large culvert with short honeycomb pipes. (MIL-HDBK-1013/10)

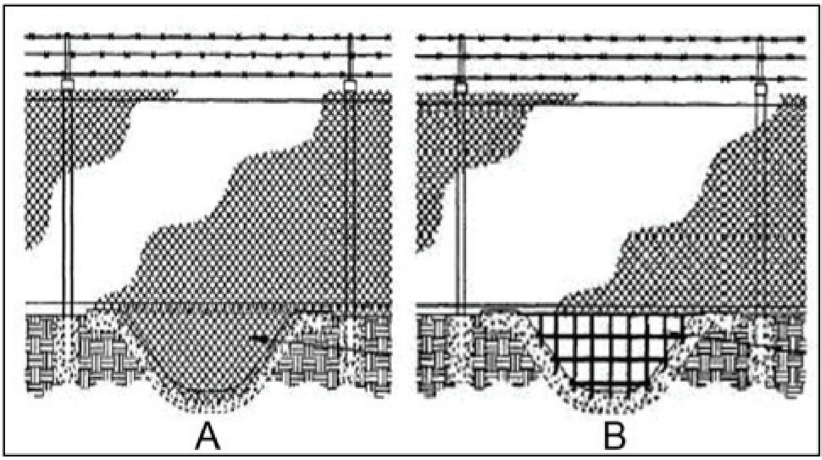


Figure 5-5. Under-fence utility openings. A: Swale crossing with ground stakes; B: Bar grill embedded in concrete. (MIL-HDBK-1013/10)

Figure 5-6. Culvert Bar Grill

Figure 5-7. Under-fence Bar Grill

Figure 5-8. Honeycomb Type Culvert Grill

Double-Wall Perimeter System. A double-wall perimeter system is effective against a two-stage VBIED attack; the system is capable of stopping a second VBIED after detonation of a first VBIED. This concept includes an outer low-wall for standoff and inner high-wall that provides obscuration and direct fire protection (Figure 5-9). This combination also allows for observation and engagement of clear zones from guard towers and fighting positions. Use soil-filled containers to minimize the debris and fragment hazard. Existing sites may require backing or replacing concrete walls with soil-filled containers. The double-wall configuration was successfully tested against two consecutive 4,000 lb. (1,818 kg) TNT-equivalent dump truck VBIEDs.

Soil-filled containers or vehicle ditches are preferred for the outer low-wall since they do not create debris hazard. Double jersey barriers with soil between them are an acceptable alternative. The soil will mitigate the velocity of concrete debris. Place the outer barriers on a good soil foundation rather than on a concrete or thick asphalt road surface to minimize debris.

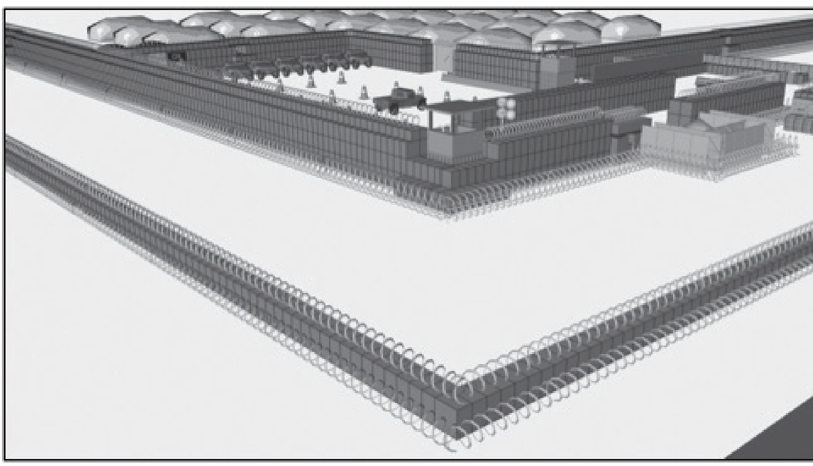


Figure 5-9. Double-wall perimeter concept.

Vehicle Barriers

Vehicle barriers are used along the FOB perimeter and at the ECPs to stop vehicles, establish adequate standoff distance, and channelize vehicles into and through ECPs. Vehicle barriers are effective personnel barriers when coupled with multi-strand razor or concertina wire toppings. High speed and straight-line avenues of approach along the perimeter should be minimized, but where unavoidable, particular attention should be given to barrier design in these areas. Vehicle barriers are generally categorized as passive or active. Depending on construction method and operational function, commercial barriers can be dual-classified when they meet the requirements of both categories (fixed-active, portable-passive, etc.).

Barrier Performance. Vehicle speed at the point of barrier impact greatly influences barrier performance. The highest attainable vehicle speed results from a long, straight path between the starting point and barrier. A threat vehicle's destructive energy depends on its weight and speed (known as kinetic energy). For example, a heavier, slow-moving vehicle can deliver the same destructive energy as a lighter, fast-moving vehicle. UFC 4-022-02, *Selection and Application of Vehicle Barriers* provides additional details.

Full-scale testing determines barrier performance capabilities. Barrier selection can also be based on engineered computer models. The US Departments of State and Defense rate barriers based on full scale crash tests conducted by independent test laboratories or government-approved facilities. See the USACE Protective Design Center website (https://pdc.usace.army.mil/library/BarrierCertification/) for current barrier certifications.

Vehicle Barrier Types. Typical FOB vehicle barriers include: berms and ditches, concrete barriers (Jersey, Texas, Alaska), soil-filled barriers, reinforced concrete walls, cabled concrete blocks, guardrails, bollards, steel cable-reinforced chain-link fence, plastic barriers, reinforced concrete knee walls, cabled steel hedgehogs, tetrahedrons and dragon teeth, hydraulic security barriers, portable hydraulic barriers, and expedient barriers.

Berms and Ditches. Berms and ditches, used in concert together, are effective vehicle deterrents that provide a simple method of rapidly securing a FOB perimeter. Well maintained berms and ditches can act as permanent perimeter barriers or as temporary barriers during FOB construction until permanent barriers are installed. Berm and ditch profiles, including approach slopes, are critical design considerations.

There are two vehicle attack methods commonly used against ditches. First, a slow, covert attack where a vehicle attempts to breach the ditch at an oblique angle, using the ditch profile to the vehicles' advantage. Second, a fast-attack vehicle approaches the ditch perpendicularly and attempts a high-speed jump to breach the near edge of the ditch. Ditches are also vulnerable to coordinated attacks where a lead vehicle modifies the ditch profile, and then a full attack is mounted before the ditch is repaired.

Numerous profiles for vehicle ditches have been proposed in previous DoD documents. These ditch profiles were based on ditch profiles used primarily to slow tank attacks and were not tested against simulated moving terrorist vehicle bombs until recently. The results of these tests along with simple trajectory simulations have led to revised ditch profile designs. The ditch profiles shown in Figures 5-10, 5-11 and 5-12 are recommended for medium-sized sport utility vehicles (SUV) traveling at up to 50 mph. The profile in Figure 5-10 provides the greatest resistance against a moving vehicle threat, but requires a stabilized slope, such as concrete riprap or sand-bag cover, since natural soil cannot maintain a 45 degree slope. The profile in Figure 5-11 provides less resistance, but sandy soil can theoretically maintain a 34 degree slope. Finally, the profile in Figure 5-12 is similar to Figure 5-11 except that it does not have the additional safety factor of a berm for stopping a moving vehicle threat.

Soil berms adjacent to the protected (near) side of the ditch provide additional vehicle resistance, but can also create hiding places for attackers on foot and as a result should be enhanced with personnel barriers. This is less significant when overwatch positions and guard towers can cover the ditch. Soil berms and spoil placement from ditch excavation should not be placed on the attack (far) side of the ditch because this can inadvertently create a ramp that allows high speed vehicles to jump the ditch.

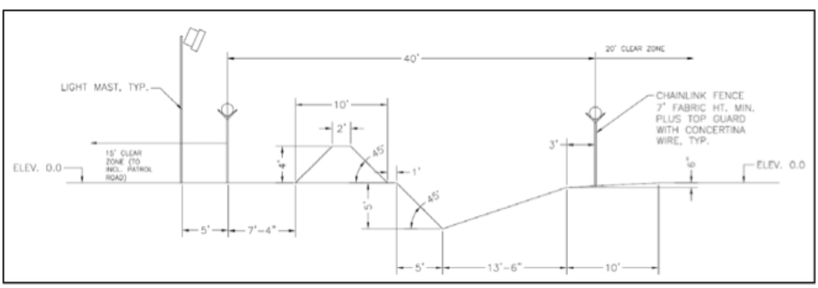


Figure 5-10. Vehicle ditch profile with stabilized slope. Protected side is to the left. (UFC 4-022-02)

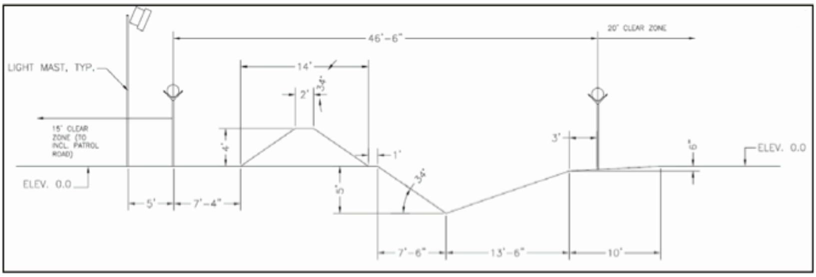


Figure 5-11. Vehicle ditch with slope not stabilized. Protected side is to the left. (UFC 4-022-02)

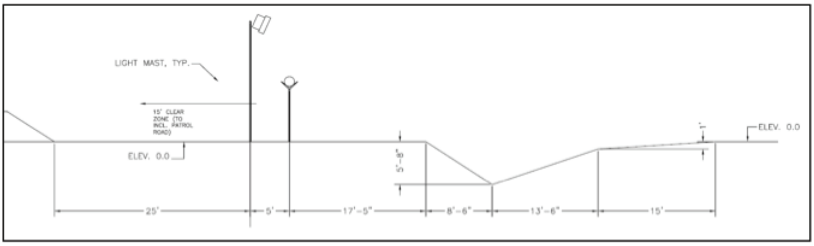
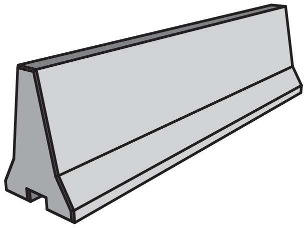


Figure 5-12. Vehicle ditch with no berm and slope not stabilized. Protected side is the left. (UFC 4-022-02)

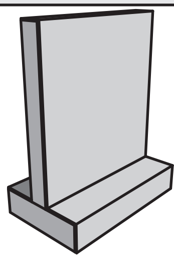
Concrete Barriers. Concrete barriers (Figure 5-13) are among the most widely employed vehicle barriers and are readily accepted by HNs because of their temporary nature. Concrete barriers are typically employed for counter-mobility, blast/fragment mitigation, and along avenues of approach. Sufficiently high concrete barriers will stop VBIED fragments. However, these barriers can disintegrate and become secondary debris fragments in the immediate vicinity of large explosions. Soil-backed concrete barriers are less likely to create secondary debris fragments (Figure 5-14).

Smaller concrete (jersey) barriers are most effective when used to control traffic flow and should only be used as a vehicle barrier when cabled together. Cabling causes a ramming vehicle to push the entire wall's weight instead of a single barrier. At least 3/4 in. (1.9 cm) steel cable is required. If the potential threat vehicle angle of impact can exceed 30 degrees, concrete barriers should be anchored to a concrete foundation in conjunction with cabling. See UFC 4-022-02.



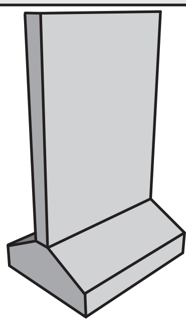
JERSEY BARRIER

Height: 3 ft.
Bottom Length: 10 ft.
Bottom Width: 2 ft.
Top Width: 10 in.
Weight: 2 Tons



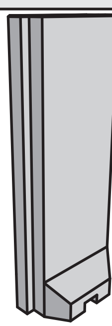
TEXAS "T" BARRIER

Height: 6 ft.-8 in.
Bottom Length: 6 ft.-8 in.
Bottom Width: 3 ft.-3 in.
Top Width: 1 ft.-9 in.
Weight: 6 Tons



ALASKA BARRIER

Height: 10 ft.
Bottom Length: 6 ft.-1 in.
Bottom Width: 4 ft.-4 in
Top Width: 1 ft.
Weight: 7 Tons



INTERLOCKING T-WALL

Height: 12 ft.
Bottom Length: 5 ft.
Bottom Width: 4 ft.
Top Width: 1 ft.-3 in.
Weight: 6 Tons

Dimensions shown are approximate and can vary by manufacturer.

Figure 5-13. Typical Concrete Barriers

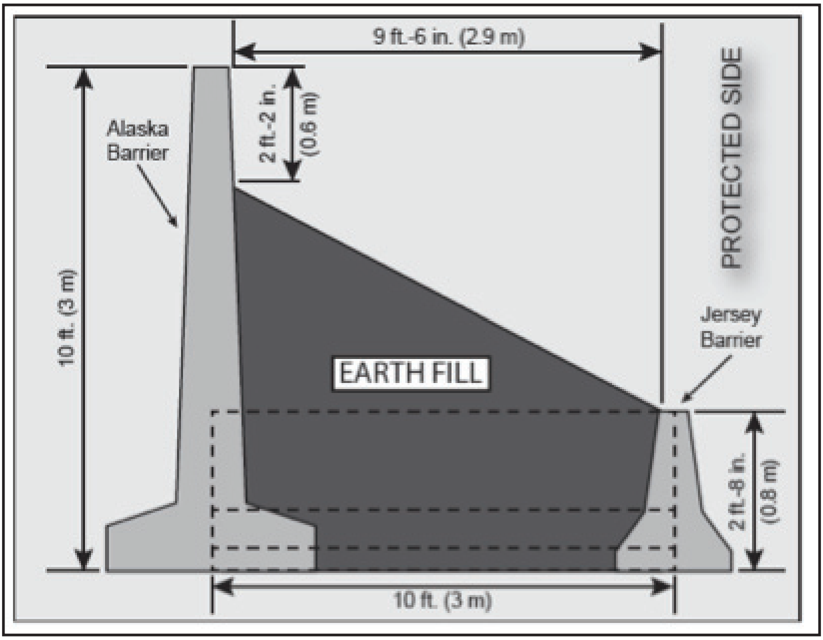


Figure 5-14. Soil-Backed Concrete Barrier Concept

Soil-Filled Barriers. Soil-filled barriers are typically employed as vehicle barriers and for both blast and fragment protection. Soil-filled barriers are also used for fighting positions and shelters. See Appendix H for additional soil-filled container applications.

- **Wire and Fabric Container**. Wire and geotextile fabric containers are effective perimeter barriers. Use of this barrier minimizes transportation weight and space while increasing protection. Geotextile barriers are normally constructed with two-row wide bases and a second level for vehicle-stopping mass (Figure 5-15). In experimental tests, this design stopped a 15,000 lb. (6,818 kg) truck traveling at 30 mph. (48.2 kph).

Figure 5-15. Wire and Fabric Container Barrier

- **Metal Container**. Metal soil-filled containers are effective vehicle barriers (Figure 5-16). Like wire and fabric containers, metal barriers can be collapsed and stacked during transport and require minimum logistical support.

Figure 5-16. Metal Container Barrier

Reinforced Concrete Walls. Reinforced concrete and reinforced concrete masonry unit (CMU) walls can be a costly, labor-intensive yet effective vehicle barrier. To optimize effectiveness, these walls should be smooth-faced, topped with outriggers or other material (razor wire, general purpose tape obstacle, barbed concertina wire), and be at least 9 ft. (2.7 m) tall. While walls provide more structural support than chain link fences to a climbing intruder, walls provide fewer handholds. Explosives can breach concrete walls. Table 5-1 provides wall thicknesses needed to prevent explosive breaching.

Cabled Concrete Blocks. Like concrete barriers, cabled non-reinforced concrete blocks (Figure 5-17) can effectively slow oncoming vehicle speeds along FOB perimeters or ECP access roads. Concrete blocks alone will not stop vehicles. Blocks can be cast in place and anchored together with 3/4 in. steel cable to prevent movement or removal. Concrete blocks are most effective when placed in a serpentine pattern.

Table 5-1. Concrete Barrier Wall Thicknesses to Prevent Breaching from Explosives (TM 5-855-1)

Standoff ft (m)	Wall Thickness to Prevent Breaching,* inch (cm)					
	220 lb (100 kg)	440 lb (200 kg)	1,000 lb (454 kg)	2,200 lb (1,000 kg)	4,400 lb (2,000 kg)	22,000 lb (10,000 kg)
0 (0)	43 (110)	55 (140)	76 (194)	No data	No data	No data
4.9 (1.5)	30 (76)	44 (111)	67 (170)	No data	No data	No data
8.2 (2.5)	23 (59)	35 (88)	55 (140)	No data	No data	No data
16.4 (5)	15 (38)	23 (59)	39 (98)	62 (157)	No data	No data
32.7 (10)	9 (23)	15 (37)	25 (63)	41 (104)	52 (133)	137 (347)

* For barrier concrete with 2,000 psi (13.8 MPa) compressive strength.
* This data applies to concrete wall barriers without material backing.

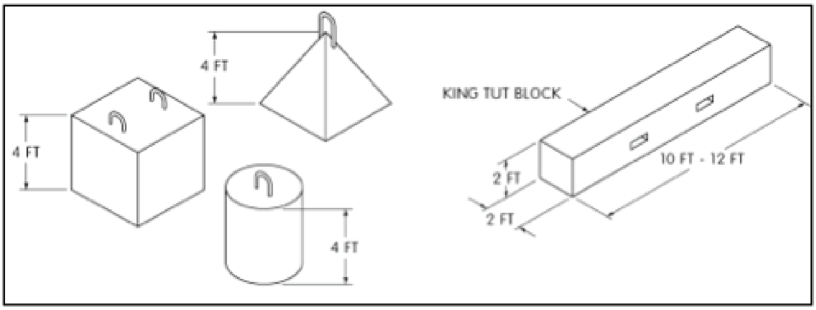


Figure 5-17. Typical Cabled Concrete Blocks (UFC 4-0222-02)

Guardrails. Standard highway guardrails (Figure 5-18) installed on a FOB perimeter can be effective vehicle barriers. Typical guardrail types and dimensions are detailed below:

- Cable guardrail (American Association of State Highway Transportation Officials (AASHTO) type G1) consists of three 3/4 in. (1.9 cm) diameter steel cables spaced 3 in. (7.6 cm) apart. The posts are S3x5.7 steel, spaced at 16 ft. (4.9 m) intervals. The height from surface to top rail is 30 in. (76.2 cm). From the end post, all three cables are turned down at 45-degree angles and anchored to buried concrete deadmen.

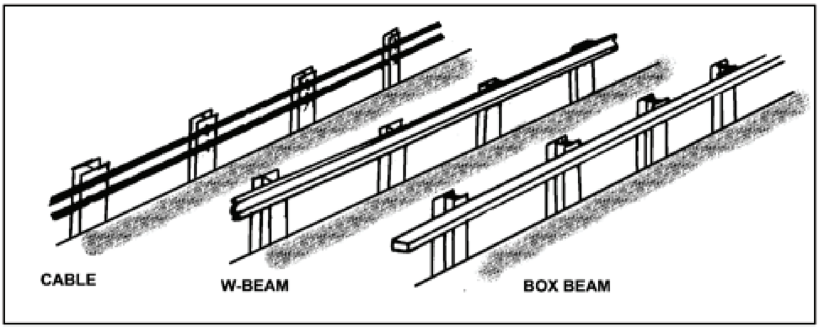


Figure 5-18. Typical Guardrail Construction (UFC 4-022-02)

- W-beam flexible guardrail (AASHTO type G2) consists of a 12 gauge "W" section bolted to S3x5.7 steel posts, spaced at 12.5-ft. (3.8 m) intervals. A Blocked-Out W beam (AASHTO type G4) guardrail system uses 12 gauge "W" sections bolted to W6x8.5 posts, spaced at 6.25-ft (1.9 m) intervals. A three-beam (AASHTO type G9) guardrail system consists of a steel three-beam bolted to W6x8.5 steel posts at 6.25-ft. (1.9 m) intervals.
- Box-beam guardrail (AASHTO type G3) consists of a 6 in. x 6 in. x 0.180 in. (15.2 cm x 15.2 cm x 0.46 cm) steel tube bolted to S3x5.7 steel posts, spaced at 6.33-ft. (1.9 m) intervals.

Bollards. Bollards are metal or concrete columns anchored into the ground. Figure 5-19 shows a bollard construction drawing. Bollards can be active or passive barriers. Active entry control bollards can be pulled from the ground by hand or hydraulically raised and lowered. Effective passive bollards are constructed of structural steel pipe filled with concrete. Steel pipes should have an 8 in. (20 cm) minimum outside diameter; pipe walls should be 1/2 in. (1.3 cm) thick and a minimum 7 ft. (2.1 m) length. Bollards should extend 3 ft. (0.9 m) above ground from a 2 ft. wide continuous footing. Place bollards 3 ft. (0.9 m) apart on center. Avoid bollard placement along unsecured sides of perimeter fences to prevent the bollard being used as a climbing aid.

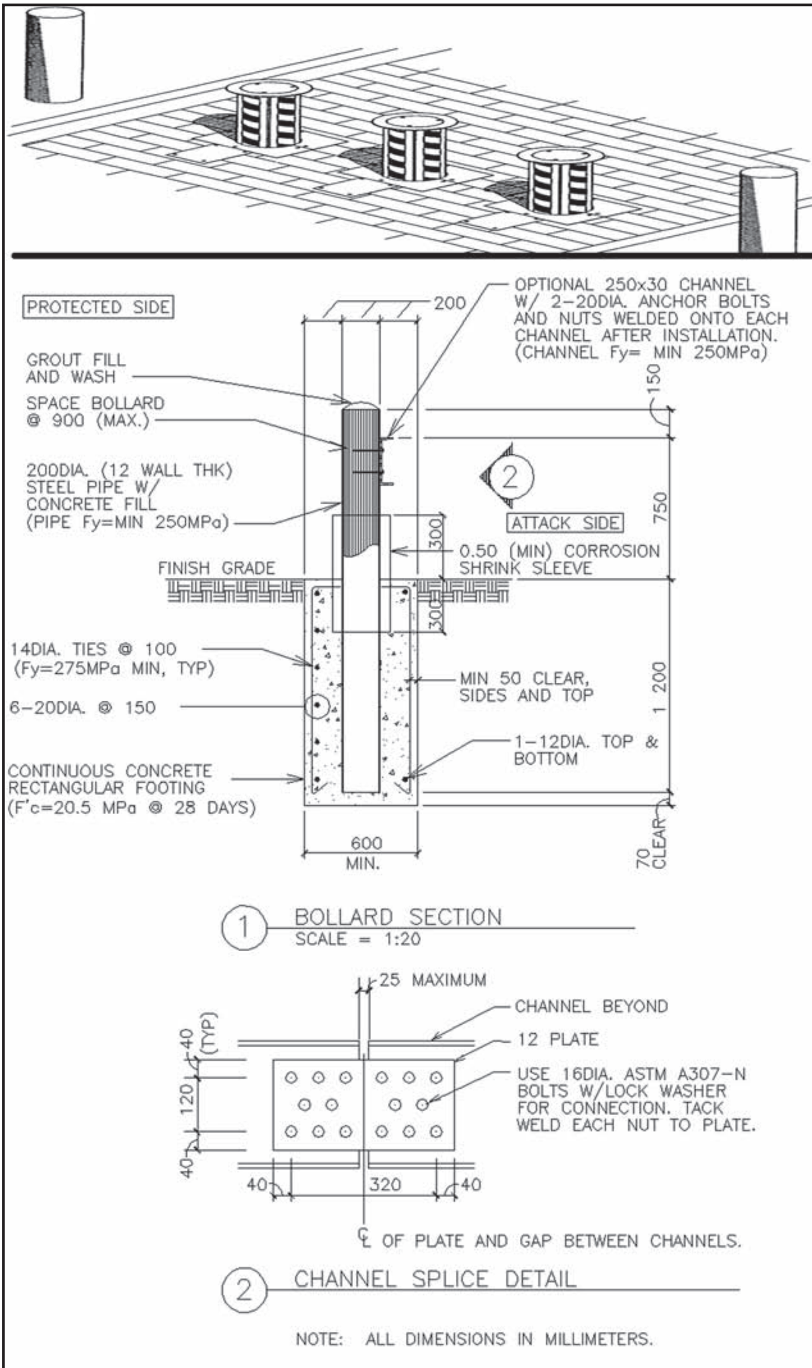


Figure 5-19. Typical Bollard Construction Detail (Above: Retractable bollards; Below: Fixed bollard construction detail) (UFC 4-022-02)

Steel Cable-Reinforced Chain-Link Fence. Chain-link fences can be utilized as vehicle barriers by reinforcing the fence line with steel cable (Figure 5-20). This is a low-cost, low-profile barrier option. Reinforce fences with two 3/4 in. (19.1 mm) steel cables tied to the fence at heights of 30 in. and 35 in. (0.76 and 0.89 m) above ground. Attach each end cable end to a concrete deadman anchor. Reinforcing posts placed at 4 ft. (1.2 m) intervals further reduce vehicle penetration. Crash tests conducted on chain-link fence reinforced with two 3/4 in. (19.1 mm) steel cables restricted penetration of a 4,000 lb. (1,814.4 kg) vehicle traveling at 52 mph (84 kph) to 13 ft. (3.9 m).

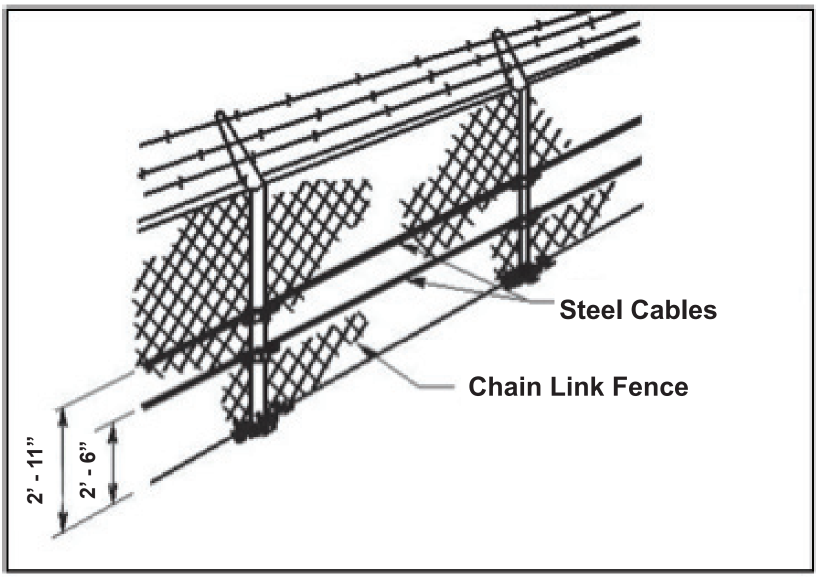


Figure 5-20. Typical Cable-Reinforced Chain-Link Fence (UFC 4-022-02)

Plastic Barriers. Plastic barriers (Figure 5-21) are molded in a configuration similar to jersey barriers. Plastic barriers weigh approximately 130 lbs. empty and 1,600 to 1,800 lbs. filled with water. The units are made from easily transported polyethylene sections. Sections must be linked for added vehicle impact resistance and reduced lateral barrier movement. Surface mounting limits barrier effectiveness to impacts below 15 mph (24 kph) and angles less than 25 degrees. Plastic barriers can be used for channelizing vehicles into or through an ECP.

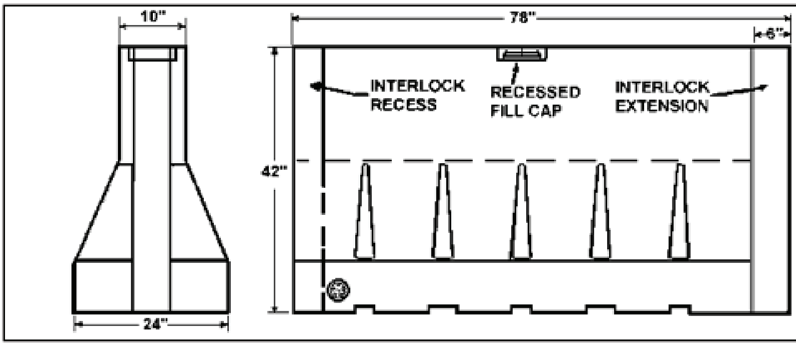


Figure 5-21. Plastic Barrier System (UFC 4-022-02)

Reinforced Concrete Knee Wall. When a perimeter wall or chain-link fence needs to serve as a vehicle barrier, this can be achieved by using a reinforced concrete knee wall structure. Concrete knee wall barriers rest on footings embedded in existing soil or a crushed stone mix. Figure 5-22 shows construction details. In experimental tests, this barrier stopped a 15,000 lb. (6,818 kg) vehicle traveling at 50 mph (80 kph) in 3.28 ft (1 m).

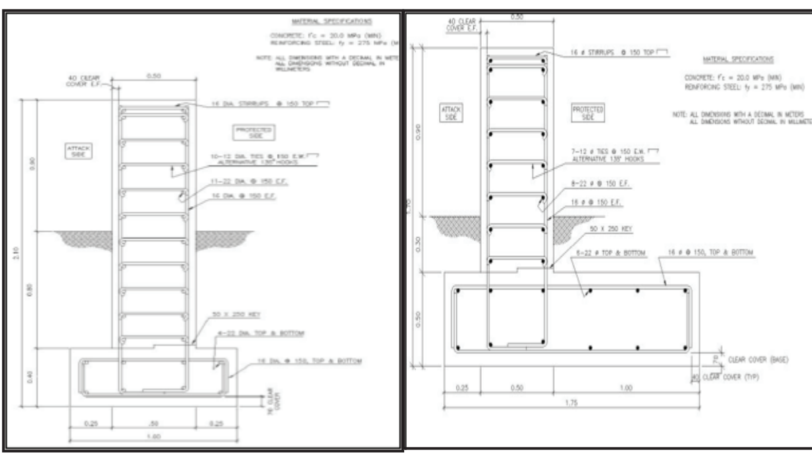


Figure 5-22. Anti-Ramming Walls. Left: Foundation wall; Right: Knee wall. (UFC 4-022-02)

Cabled Steel Hedgehogs. These barriers are designed to roll beneath a ramming vehicle and destroy its driveshaft and undercarriage. Hedgehogs must be used on paved areas. When cabled to adjacent barriers, hedgehogs will stop a vehicle. Typical hedgehog construction includes three 4 in. by 4 in. (10.1 cm by 10.1 cm) pieces of angle iron approximately 4 ft. (1.2 m) in length. The pieces are welded to a 4 in. (10.1 cm) steel plate (Figure 5-23).

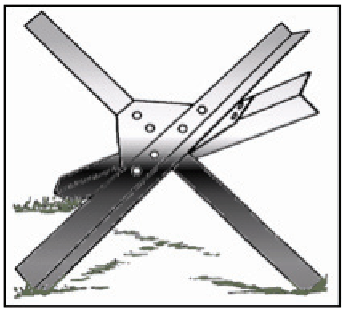


Figure 5-23. Steel Hedgehog (AFH 10-222v14)

Tetrahedrons and Dragon Teeth. Tetrahedrons are pyramids with triangular bases; dragon teeth are pyramids with square bases (Figure 5-24). Both are constructed from angle iron or concrete and employed in multiple rows at 4- to 5-ft. (1.2 to 1.5 m) intervals across an avenue of approach. Rows can be aligned or staggered. Both barriers are most effective when cabled together.

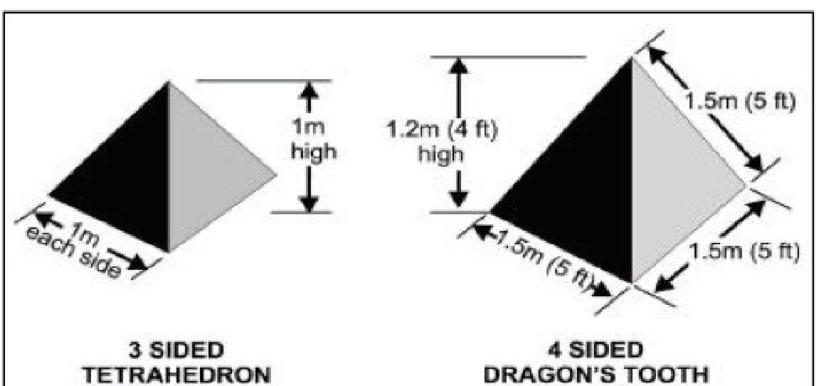


Figure 5-24. Tetrahedron and Dragon Tooth (AFH 10-222v14)

Tire Shredders. Tire shredders are normally used for traffic control purposes and are designed to slow or stop a vehicle by deflating its tires (Figure 5-25). When crossed in the wrong direction, shredder spikes penetrate the tire casing, which deflates the tires and limits vehicle mobility. Shredders are available from many commercial manufacturers, but should not be considered stand-alone vehicle barriers due to limited stopping capability. Tire shredders should be used in combination with other vehicle barriers. Tire shredders are not recommended where vehicle traffic crosses these devices at speeds exceeding 5 mph (8 kph). These systems may also not be effective against run-flat tires, heavy truck tires, or tires that can bridge two or more shredder spikes.

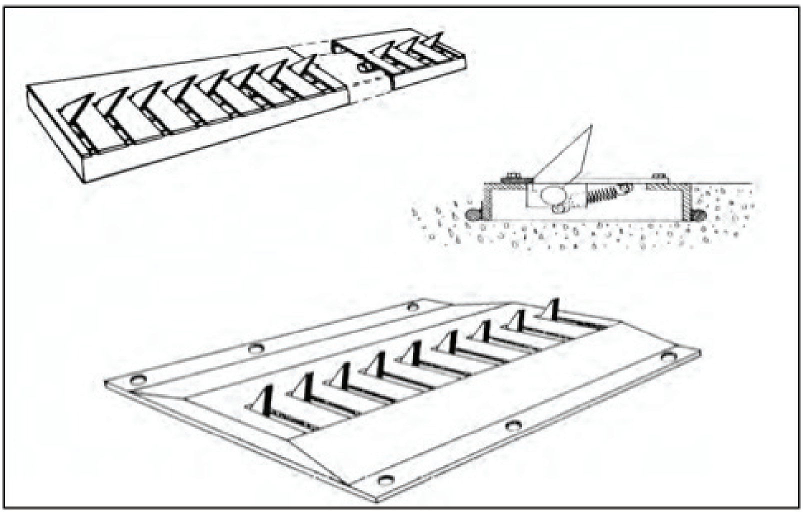


Figure 5-25. Tire Shredders (UFC 4-022-02)

Hydraulic Security Barrier. The hydraulic security vehicle barrier (Figure 5-26) is commercially available, fully electronic, and multi-functional. Multiple barriers can be controlled from a single hydraulic power system. Most models can be installed in 24 hours without roadway construction by bolting the barriers to the roadway. This barrier type can also be installed below ground and flush-mounted. Most models are similar in construction and operation, varying only in barrier height and foundation construction. Tests have shown a 14,980 lb. (6,809 kg) vehicle traveling at 50.3 mph (81 kph) failed to penetrate this barrier. This barrier is well-suited for use in ECP lanes to control or stop vehicles. Appendix G (Material and Technology Support) provides additional information.

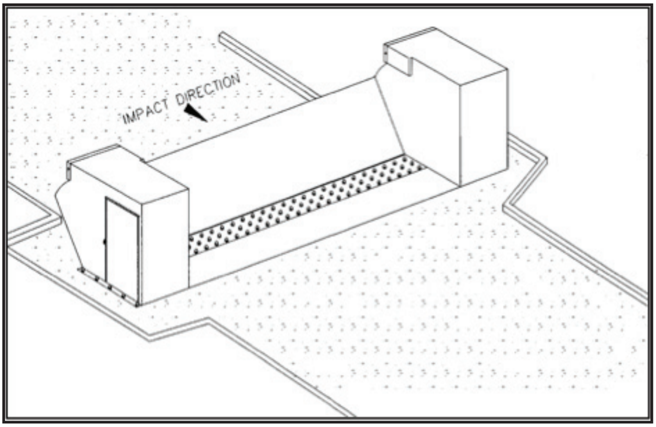


Figure 5-26. Typical Hydraulic Security Barrier (UFC 4-022-02)

Portable Hydraulic Vehicle Barriers. The portable hydraulic vehicle barrier (Figure 5-27) is commercially available, relocatable, self-contained, and controllable as a manned checkpoint. For unmanned control, options include an electronic card reader or keypad. The self-contained hydraulic system is located in the curb panels and sealed to prevent fluid leaks. This unit can be placed on any roadway or other flat surface with passive barriers installed to prevent bypass. Once power is connected, the system is operational. This barrier is best employed at FOBs, where portability is required or a high water table limits buried barrier options. Tests have shown that this barrier is capable of stopping a 15,200 lb. (6,909 kg) truck traveling at 50.5 mph (81 kph). This barrier is well-suited for use in ECP lanes to control or stop vehicles. Appendix G provides additional information.

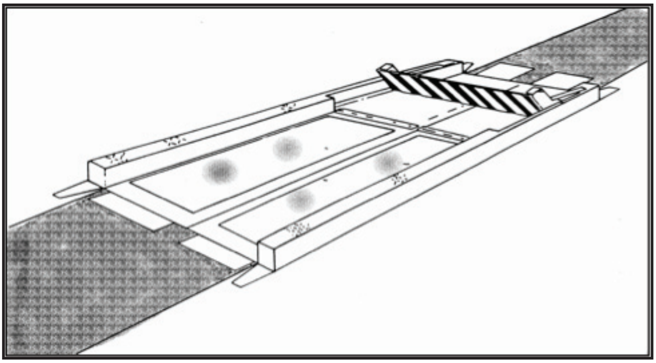


Figure 5-27. Typical Portable Vehicle Surface Barrier (UFC 4-022-02)

Expedient Barriers. Expedient barriers can be built from common construction items or available vehicles. Large-diameter concrete culverts and steel pipes can form makeshift barriers. Large, high mass construction vehicles such as dump trucks and earth moving equipment can be modified for expedient barrier use. Expedient barriers should be stabilized and anchored to reduce displacement by a ramming threat vehicle. Expedient barrier materials include:

- Three-foot (0.9 m) sections of large-diameter, corrugated metal or reinforced concrete culverts placed on end and filled with sand or earth
- Steel pipe stacked and welded together in a pyramid
- Construction or damaged military vehicles anchored together with cable or chain
- Half-buried, heavy equipment tires (Figure 5-28); employ rigid 7 to 8-ft (2.1 to 2.4 m) diameter tires

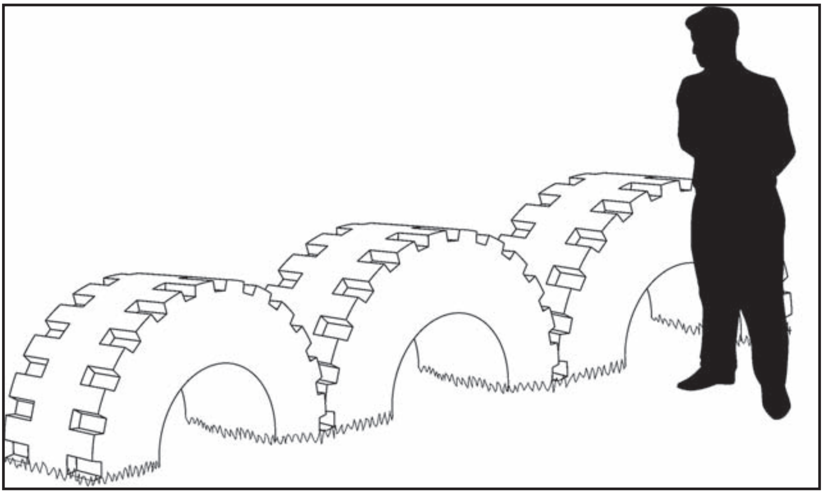


Figure 5-28. Typical Heavy Equipment Tire Barrier Construction (UFC 4-022-02)

Personnel Barriers

Personnel barriers are designed to define the perimeter, direct and control personnel traffic flow, establish clear zones, and deter unauthorized entry into the FOB. Personnel barriers are more effective when used in conjunction with berms and ditches and tall vehicle barriers such as concrete barriers, soil-filled barriers, metal barriers, and reinforced concrete walls. Typical personnel barriers include chain-link fences with barbed wire outriggers, multi-strand razor and concertina wire fences, concrete walls (see Reinforced Concrete Wall discussion), and barbed wire fences.

Most personnel barriers/fences are easily penetrated by moving vehicles and will resist impact only with reinforcement. In most instances, fences can be penetrated by climbing over or burrowing under them or using wire cutters to cut holes. Consequently, fences must remain under constant observation and clear zones established and maintained. Additional security fencing details can be found in MIL-HDBK-1013/10, *Design Guidelines for Security Fencing, Gates, Barriers, and Guard Facilities.*

- **Chain-Link Fencing**. Chain-link fencing (Figure 5-29) is cost-effective and readily available. Razor, concertina or barbed-wire toppings enhance the effectiveness of chain-link fencing. Chain-link fences should be reinforced with steel cable (see Steel Cable-Reinforced Chain-Link Fence discussion and Figure 5-20) to resist vehicle penetration and laced with wire along the bottom edge to prevent lifting. Fences must be continually inspected for signs of tampering and to identify maintenance needs.

Figure 5-29. Chain-Link Fence with Razor Wire and Barbed-wire Outriggers

- **Multi-Strand Razor and Concertina Wire Fence**. Razor and concertina wire is a common expeditionary barrier that can be used as a topping for vehicle barriers or to create a stand-alone fence. To be effective razor and concertina wire must be staked or tied down;

ensure wire is connected together and stakes are not too far apart. The most effective multi-strand razor or concertina wire fence (Figure 5-30) utilizes several rolls of stacked wire. For example, one roll is stacked on top of two rolls running parallel to each other, forming a pyramid. This barrier method delays intrusion and allows time for security force response and engagement.

Figure 5-30. Concertina Wire Fence

Gates

Gates facilitate the control and flow of authorized personnel and vehicle traffic and establish specific entrance/exit points for a defined perimeter. Gates also establish traffic patterns for restricted areas. Perimeter gates must provide at least an equivalent level of protection as the adjacent perimeter barrier system. Gates normally require additional hardening features. If used at the actual entrance into the FOB then the gate should be constructed as a final denial barrier with the capability to stop a threat vehicle. Hardening addresses the inherent vulnerabilities of hinges, latches, and associated mechanical devices. MIL-HDBK-1013/10, *Design Guidelines for Security Fencing, Gates, Barriers, and Guard Facilities contains detailed design guidelines.*

Personnel Gates. Personnel gates should be designed to permit only one person to approach security personnel at any time. Examples of personnel gates include single swing gates, double swing gates, and turnstile gates. For pedestrian use, consider single swing gates (Figure 5-31) as an alternative to turnstile gates. Also, consider operational and security requirements and security manpower availability in determining FOB personnel gate selection.

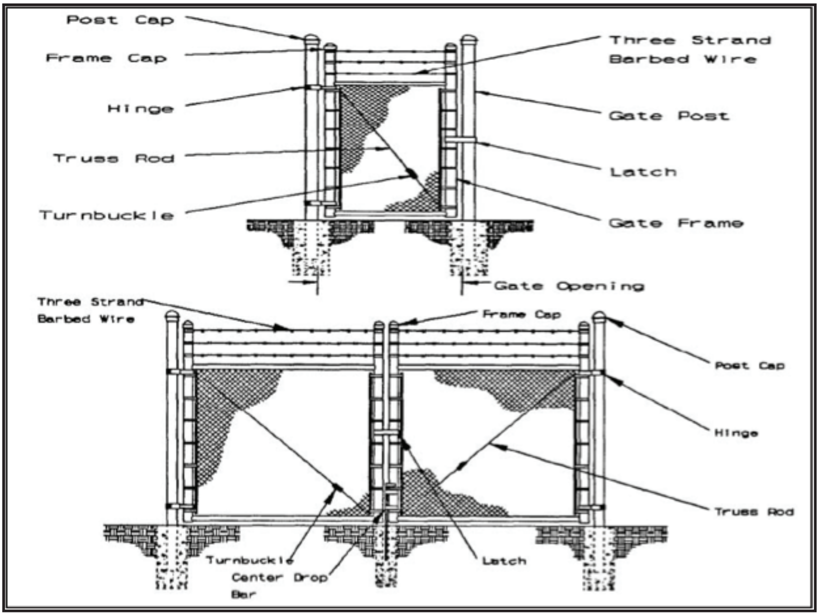


Figure 5-31. Typical Personnel Gates. Top: Single-Swing; Bottom: Double-Swing. (MIL-HDBK-1013/10)

Turnstile (Rotational) Gates. Turnstile gates (Figure 5-32) are recommended for personnel access control through ECPs or into restricted areas. Automated turnstile gates can lessen guard requirements for controlling personnel. Turnstile gates are manufactured as single or tandem units. Only consider full-height turnstile gates. Direction of travel can be clockwise, counterclockwise, or bi-directional. Automated access control systems, such as card readers, push button, and wireless remote can be incorporated into turnstile gates. Tubing should be at least 1-1/2in. (3.8 cm) diameter, 14 gauge (38 mm). Overall exterior height should be 91 in. (2.3 m) with a pedestrian walk-through height of 84 in. (2.1m).

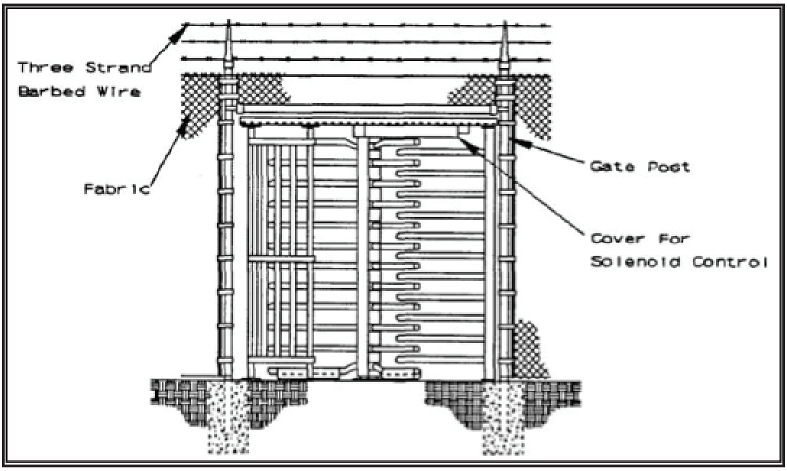


Figure 5-32. Turnstile (Rotational) Gate (MIL-HDBK-1013/10)

Cabled Crash Beam Barriers. Crash beam systems (Figure 5-33) are cable-reinforced, manually or hydraulically-operated, bollard-mounted barriers. The beam is counterbalanced and lifts at one end to allow vehicle access. This system is frequently used for low impact conditions where vehicle speeds can be limited and as interior barriers for ECP vehicle inspection areas. Tests have shown a crash beam barrier successfully stopped a 10,000 lb. (4,545 kg) vehicle at 17 mph (27 kph). Appendix G provides additional information.

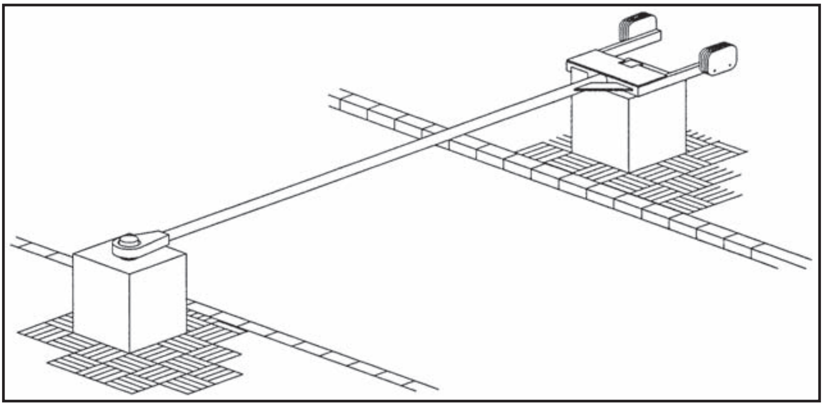


Figure 5-33. Typical Cable Reinforced Crash Beam Barrier (UFC 4-022-02)

Crash Gate. A crash gate system, (Figure 5-34) is a sliding gate that allows pedestrian access and provides heavy vehicle impact resistance. Crash gates can be operated manually or electrically. Automated versions typically have a 30 to 100 ft/min (9 to 30 m/min) sliding speed (instantly reversible). Safety infrared sensors and front edge obstacle sensors are standard features. Gate systems are normally employed where wide openings are required (up to 25 ft. (7.6 m) clear opening). Tests have shown this gate will stop a 15,000 lb (6,818 kg) vehicle at speeds of 34 and 40 mph (55 and 65 kph respectively).

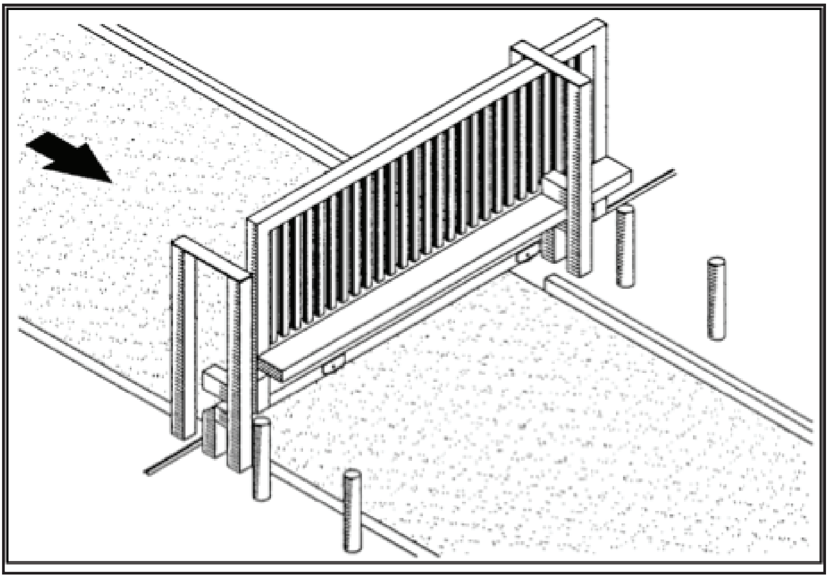


Figure 5-34. Crash Gate System (UFC 4-022-02)

Cable-Reinforced Chain-Link Fence Gates. If cable-reinforced chain link fence gates are employed, then wheel-supported or cantilever sliding gates offer the best vehicle security (Figure 5-35). Swing gates require a large arc of space for operation. That arc increases ECP vulnerability, making swing gates less desirable.

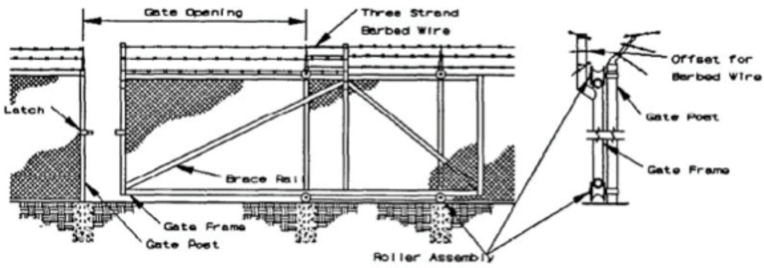


Figure 5-35. Single Cantilevered Gate (MIL-HDBK-1013/10)

Military Vehicle/Heavy Equipment/Trucks. If conventional gates are unavailable, military vehicles, trucks, bulldozers, and dump trucks will effectively block an entrance. To increase barrier effectiveness, thread cable through vehicle frames and anchor to adjacent barriers. Parked bumper-to-bumper, vehicles are also effective personnel gates. Large construction or armored vehicles can supplement vehicle gates and function as a final denial barrier.

References:

JP 3-15, Barriers. *Obstacles, and Mine Warfare for Joint Operations,* 17 June 2011.

MIL-HDBK-1013/10. *Military Handbook Design Guidelines for Security Fencing, Gates, and Guard Facilities,* 14 May 1993.

UFC 4-022-02. *Selection and Application of Vehicle Barrier*, 08 June 2009 (Including change 1, 09 August 2010).

AFH 10-222v3. *Civil Engineer Guide to Expeditionary Force Protection,* 01 May 2008.

Joint Sniper Defeat Handbook, 2007.

AFH 10-222v14. *Civil Engineer Guide to Fighting Positions, Shelters, Obstacles, and Revetments*, 01 August 2008.

AASHTO, *American Association of State Highway and Transportation Officials.*

CHAPTER 6
ENTRY CONTROL POINTS

Regardless of the threat level, entry control points (ECP) must remain a functional part of the FOB perimeter security and access control system. The ECP objective is to prevent unauthorized personnel and vehicle access while maximizing traffic flow for authorized access. ECPs should be designed and operated with a defense-in-depth concept that uses elements of distance and time to provide ECP personnel the opportunity to safely assess and react to threats.

A properly designed and operated ECP provides:

- FOB security
- Protection for ECP security forces
- A safe traffic environment for personnel and vehicles
- Traffic flow that does not negatively impact security, base operations, or off-base traffic
- A professional image of protection and security that deters potential aggressors and enhances the image of security for local nationals

This chapter describes ECP planning, design, and construction sequences. Additional guidance can be found in the *Small-Base Leader Entry Control Point Guide*. *The Joint Entry Control Point & Escalation of Force Procedures* (JEEP) *Handbook* provides recommended concepts of operations and TTPs related to escalation of force.

ECP Planning

ECP planning is a continuous process impacted by threat likelihood and tactics, site location and layout, ECP (and FOB) design and construction, FOB mission, FOB personnel, and protected assets. New ECP planning requires time, but the opportunity exists to include protective measures initially rather than retrofit later. Conversely, the assessment of an existing ECP may reveal needed improvements, some of which might not be fully attainable and require workarounds to improve security.

New ECP Planning. The steps below facilitate new ECP planning.

- **Develop a clear, concise ECP mission statement.** The primary ECP mission is to protect personnel against unauthorized FOB entry. The ECP mission will be driven by the FOB mission, which may include operations that require access by other than mission-essential personnel, such as local nationals (LNs) and vehicles.

- **Assess the threat to the ECP threat assessment**. ECP-specific threats should be part of the overall FOB Threat Assessment and should be reviewed periodically, or as needed, to address likely threats to the ECP. Threat Assessment is discussed in Chapter 2, Threats.
- **Conduct an ECP site selection survey and assess potential risks**. The site selection survey identifies potential vulnerabilities. The risk assessment identifies ECP risk levels associated with identified enemy threats and risk mitigation actions. The "Tools Section" of the *Small-Base Leader ECP Guide* provides an ECP Site Selection Checklist and ECP Risk Assessment Worksheet.
- **Develop an ECP design that reduces risk**. General and essential design concepts are discussed in this chapter. The design should allow for continual improvement and upgrades that increase protection and adapt to new enemy tactics.
- **Develop Standard Operating Procedures (SOP) during ECP construction**. A priority of effort should be established for constructing a new ECP; with the focus on providing initial protection and maintaining operational capability. Improved capabilities and protection can then be implemented as more resources become available. During construction, create SOP that reduce risk and include random operational procedures to frustrate enemy attempts to identify routines and plan attacks.

Existing ECP Planning. The primary difference between new and existing ECP planning is that the location and layout of existing ECPs are already established. The focus then becomes assessment and validation of previous planning efforts to identify existing vulnerabilities. The steps below facilitate existing ECP planning.

- **Validate the ECP mission statement**. Ensure that established security and access control measures are mission-consistent and do not adversely impact FOB operations.
- **Validate the threat assessment**. Ensure the assessment specifically identifies and prioritizes courses of action/tactics that could be used against the ECP. Also, identify worst case scenarios and the impact of threat tactics on ECP design and operations.
- **Conduct ECP vulnerability and risk assessments**. Identification of vulnerabilities is a vital step to strengthening the ECP's protection posture. Appendix B, Risk Management, includes a risk assessment worksheet that identifies and prioritizes ECP vulnerabilities. The Tools Section of the *Small-Base Leader ECP Guide* provides an ECP

Vulnerability Assessment Checklist. These checklists/worksheets should be tailored to the specific ECP to enhance their value.

ECP vulnerabilities are identified as either procedural or programmatic. Procedural vulnerabilities are defined by inadequate or non-existent operational procedures, and poorly trained personnel who disregard SOP. Programmatic vulnerabilities include inadequate ECP design or the lack of proper material, equipment, and personnel.

The ECP vulnerability and risk assessment in Appendix B will assist in:

- o Identifying ECP vulnerabilities to likely threat tactics
- o Estimating the likelihood of threat tactics
- o Estimating attack consequences
- o Determining the overall risk of threat tactics

- **Validate the ECP design and operational concept**. Ensure the ECP design and operational concepts support the FOB mission, address current threats, provide defense-in-depth, and incorporate the operational objectives of deter, deny, detect, defend and defeat. Modify the design as necessary to mitigate identified vulnerabilities and reduce risk. Allow for continual design updates that increase protection and adapt to new enemy tactics.
- **Validate the ECP SOP**. Continually review SOP and training and incorporate random operational procedures to thwart enemy attack planning; update as needed.
- **Implement ECP modifications**. Prioritize modifications to first implement those measures that provide the greatest risk reduction.

Functional Zones

The design of an ECP should be subdivided into functional zones, each encompassing specific functions and operations.

Approach Zone: The approach zone is the initial interface between public roadways and the ECP. The approach zone length will depend on the land available, distance required for traffic queuing and sorting, and, if needed, the space for additional lanes to prevent backup onto adjacent public roads. Space may also be required to employ speed management techniques that eliminate straight-line, high-speed avenues of approach. Design the approach zone to accomplish the following:

- Reduce the speed of incoming vehicles with speed management techniques

- Eliminate or reduce straight-line access from local roads
- Provide adequate stacking distance for incoming vehicles
- Provide initial verification of authorized access for personnel and vehicles
- Sort traffic by vehicle type; begin the containment, segregation, and channelization of authorized personnel and vehicles
- Provide space to redirect unauthorized vehicles that attempt ECP entry
- Provide early warning of potential threat personnel/vehicles
- Deny unauthorized entry through outbound traffic lanes
- Provide an off-site parking area for unauthorized vehicles
- Maximize protection of ECP security personnel

Access Control Zone: The access control zone is the ECP main body. This zone includes vehicle and personnel search/inspection areas, speed and traffic management devices, overwatch, and hardened positions for ECP security forces. The access control zone design should be flexible enough to support future inspection demands, access control equipment, and technologies. The design should include:

- Base defense-in-depth concept
- Maximum standoff
- Verification of personnel identification
- Vehicle turn around and rejection areas
- Capability to conduct 100 percent inspection of incoming personnel and vehicles
- Nonlinear layout, speed reduction, and traffic management techniques
- Containment, segregation, and channelizing of vehicle and pedestrian traffic
- Parking/transfer yard for authorized logistics and delivery vehicles
- Overwatch
- Maximum protection for ECP security personnel
- Exits that prevent unauthorized entry

Response Zone: This zone extends from the start of the approach zone to the final denial barrier or gate into the FOB. The response zone encompasses the entire ECP and should:

- Allow time to react to a threat, activate the final denial barrier and gate closure
- Provide a hardened perimeter gate to act as a final denial barrier
- Provide overwatch for the entire ECP
- Define the base perimeter
- Integrate with perimeter security systems and maintain defense-in-depth

The JEEP Handbook divides the response zone into Primary and Secondary Response Zones. The primary response zone is located between the approach and access control zones, serving as the ECP engagement area for force escalation. The secondary response zone is co-located with the access control zone and provides a final engagement area and overwatch of the access control zone.

Safety Zone: The safety zone extends from the final denial barrier in all directions to protect FOB personnel from an ECP attack. An acceptable standoff distance must be determined from estimated VBIED and PBIED explosive charge weights based on the Threat Assessment.

ECP Design

ECP design is normally influenced by competing demands such as:

- FOB mission
- Host nation (HN) requirements
- Political constraints
- Combatant command and Service-specific regulations and guidance
- Site selection and terrain constraints
- Logistics support and material availability

Protection measures should be integrated into the design process early to increase the FOB defensive posture and ability to protect personnel and assets. Early identification of ECP protection and security requirements ensures the design is compatible with overall FOB security efforts and is more cost effective than applying requirements after an ECP is constructed.

Adapt the design concepts and considerations below to specific FOB and ECP mission requirements.

General Design Concepts and Considerations

ECP mission and access control. The FOB commander should establish a mission for each ECP based on the type of access the ECP will control. The preferred type of access is one that limits all pedestrian and vehicle access to only mission-essential personnel and vehicles. If the FOB mission requires local national (LN) and civilian vehicle access, the ECP design will differ. The design should consider future changes to access control requirements, methods, and equipment.

The following factors should be considered when determining the type of access:

- FOB mission and operations
- Threat
- Number of ECP security personnel available for ECP access control duties
- Available materials and construction equipment
- Whether the ECP will control vehicle access, personnel access, or both
- Whether the ECP will limit access to only coalition personnel and trusted vehicles
- Whether the ECP will allow access to HN personnel and vehicles

Limited number of ECPs. Limit the number of ECPs to minimize required protective measures and manpower. FOB designs typically include a primary and alternate ECPs. Alternate ECPs should not be continuously manned, but secured and opened only for emergency access or egress.

Specific threats. Design ECPs based on current and expected threats.

Site selection/terrain constraints. Terrain characteristics can either enhance or limit ECP designs. Urban sites typically have more design limitations than rural sites. Similarly, mountainous terrains are more constraining than open flat terrain. Commanders should maximize opportunities to use natural terrain features as barriers and should avoid locations advantageous to enemy forces. Flat terrain with a slight rise in elevation is generally preferred. This elevation rise allows clear observation of approaching vehicles and assists security personnel in assessing potential threats.

HN and political constraints. Design ECPs to have minimal impacts on HN activities. Once FOB mission and protection requirements are met, minimize local traffic disruption and land appropriation from LN.

Higher HQ regulations. Review pertinent regulations and include requirements in the ECP design.

Logistics support and material availability. Logistics support impacts ECP design and influences the choice of construction materials. In austere environments with limited logistics support, technology solutions presented in this handbook might not be available. As a result, the ECP mission and access control measures may be limited.

Integration with perimeter security system. The ECP is an integral part of the perimeter and must be designed to seamlessly integrate with established perimeter security measures. ECP protection measures should mirror that of the perimeter.

Capacity. Maximize authorized vehicle and personnel traffic flow to eliminate undue delays and congestion that could affect FOB operations and present attack opportunities. The design should accommodate future ECP expansion and the potential for increased traffic volume.

Available space. ECP spatial requirements will vary depending on the required access control, traffic volume, and security measures. Foremost is the need to establish a clear zone between the ECP perimeter and surrounding areas. Planners must think three-dimensionally to include spaces above, below, and to the sides of the proposed ECP.

Available security personnel. The number of security personnel available to operate the ECP will impact the mission, type of access control and should be factored into the design.

Integration of HN security personnel. Some FOBs may integrate HN security personnel into ECP operations. The design should ensure HN personnel are afforded the same level of protection as US personnel.

Random operational measures. Design the ECP to accommodate random operational measures that reduce operational predictability. This will thwart enemy surveillance attempts. Examples include:

- Barrier and obstacle movement to vary traffic and serpentine patterns
- Random ECP personnel shift times
- Changes to ECP operating hours
- Random access control procedures
- Random vehicle and personnel search procedures
- Relocation of ECP overwatch positions
- Random patrols

Available technology. Incorporate technology solutions as a force multiplier and to enhance random operational measures. Include space and power requirements for available technology into ECP designs. Configure primary and emergency power sources to ensure continuous ECP operations. Preferred technologies include: closed-circuit television (CCTV), intrusion detection systems (IDS), redundant communication equipment linked to the FOB tactical operations center (TOC), vehicle and personnel search equipment, and fire-fighting equipment. Inoperable technology can be deceptively employed while waiting for maintenance. Appendix G, Materiel and Technology Support, and the *Small-Base Leader ECP Guide* provide listings of available ECP equipment.

Essential Design Concepts and Considerations

Maintain defense-in-depth. Incorporate a layered defense-in-depth concept into the design that conforms to established FOB perimeter security measures. Include pre-planned, mutually supporting fighting positions for ECP security personnel. To maintain defense-in-depth, require potential aggressors to negotiate a series of varied and alternating barrier layers interspersed with varying distances of open ground and clear fields of fire.

Maximize standoff. Standoff is the best risk reduction technique. Increased standoff provides ECP security personnel the space and time to assess, detect and respond to a threat. Allowances for standoff should permit upgrades to meet future threats and changes to the ECP mission.

In urban environments, the required design standoff is often difficult to achieve. In such cases, incorporate enhanced blast and ballistic construction, and retrofit techniques to include protective fighting and overwatch positions. In such cases, incorporate enhanced blast and ballistic construction, retrofit techniques, protective fighting and overwatch positions and increase ECP wall heights.

Eliminate or reduce straight-line access from local roadways. Eliminate or minimize perpendicular lines of approach and straight-line, uncontrolled vehicle access into the ECP (see Figure 6-1). Redirect vehicle and civilian pedestrian routes away from the ECP. Techniques to slow vehicles and control access roads are discussed in the Speed Management Techniques section.

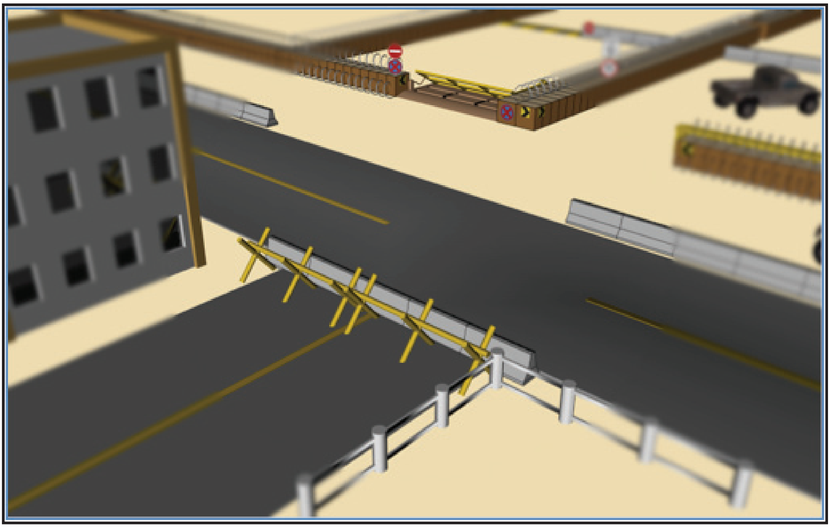


Figure 6-1. Elimination of straight-line access from a local access road

Eliminate natural or man-made enemy vantage points. ECPs should have a dedicated right-of-way that provides protection from building encroachment, tree overhang, and other natural or manmade objects that provide enemy vantage points. Design ECPs to prevent the enemy from observing ECP operations. ECPs should not be constructed adjacent higher natural terrain or tall buildings that provide observation platforms. Design ECPs and use screening to limit or block an attack by direct-line-of-sight weapons. Screening materials should not block the view of ECP overwatch positions. Crew-served weapons and counter-sniper teams in these positions should be able to observe and cover the entire ECP. Although a challenge in urban environments, design considerations include:

- Construct the ECP on high ground.
- Take advantage of natural or manmade obstructions, such as trees, walls or buildings that obscure enemy line-of-sight. Weigh the need for obstructions against the need to maintain ECP clear zones.
- Employ screening materials in and around the ECP. Also, use screening material during ECP construction to deter enemy surveillance.

Eliminate potential enemy hiding places. Design the ECP to eliminate nearby hiding places (see Figure 6-2). Create clear zones that allow an unobstructed view of the surrounding area. Eliminate vegetation, drainage channels, ditches, ridges, or culverts that might provide concealment. Restrict access to such areas by emplacing personnel barriers.

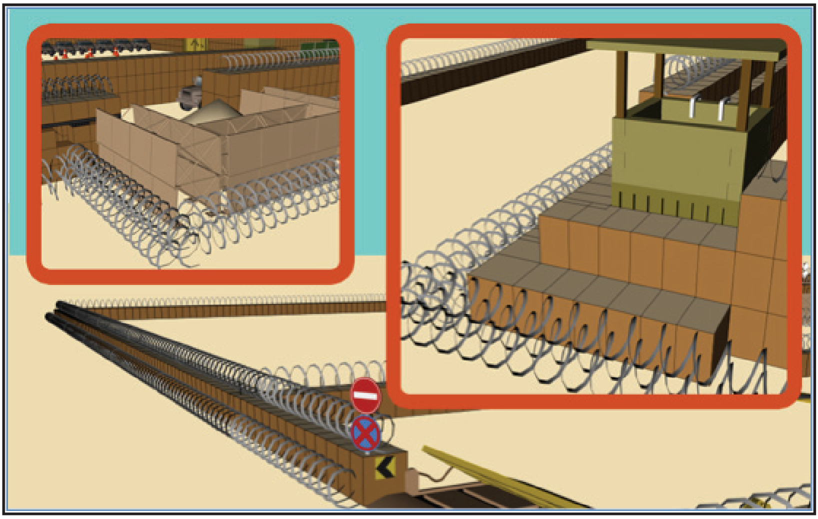


Figure 6-2. Elimination of potential enemy hiding places

Incorporate nonlinear, serpentine design with speed management techniques. Design the ECP with a nonlinear, serpentine layout and vehicle barriers to channelize, control vehicle speed and prevent unauthorized access. The nonlinear design should be extended to a length that provides ECP security personnel adequate time to observe, assess, and respond to inbound vehicle and personnel traffic.

Install movable vehicle barriers at ECP entrances. Vehicle barriers at entrances should be quickly relocatable to allow authorized vehicle access (see Figure 6-3). Removable bollards, portable vehicle barriers, cable-reinforced crash beam barriers, and crash gate systems (see Chapter 5) are all viable options. Heavy vehicles in all sizes and configurations can be employed as expedient barriers. Large, construction-related and armored vehicles (including damaged and captured enemy vehicles) are effective ECP entrance barriers or as expedient barriers for the serpentine lanes.

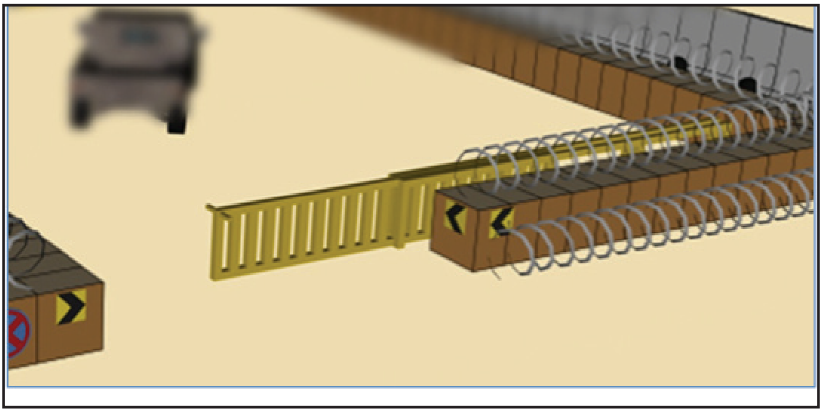


Figure 6-3. Movable ECP entrance barrier

Ensure entrance/exit points maintain access control. Design entrance/exit points to eliminate high-speed approaches as a method of forced entry and to deny unauthorized entry through exit lanes. The objective should be to ensure that attackers cannot enter the ECP by going against the flow of exiting vehicle traffic. Construct entry and exits to prevent ramming-vehicle attacks. Maintain positive control over exit lanes with an active barrier (see Figure 6-4). Additional vehicle barriers should be installed behind the gates for defense in depth against such attacks. Use both passive and active (if available) vehicle barriers and traffic control devices such as tire shredders, speed bumps/tables, and drop-arm crash barriers. See Chapter 5 for additional details.

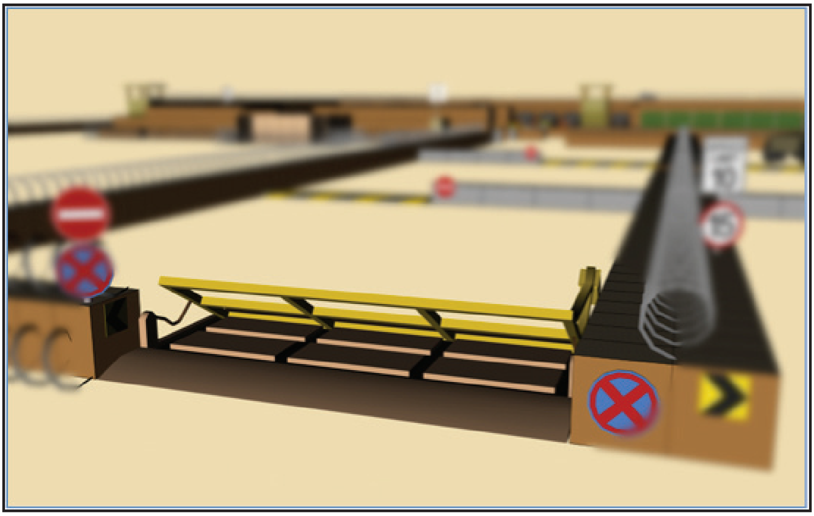


Figure 6-4. Access control at an entrance/exit point

Construct vehicles barriers throughout the ECP. Vehicle barriers should be used to form the ECP walls and nonlinear serpentine lanes. Employ soil filled containers, cabled jersey barriers, cabled concrete blocks, bollards, or heavy vehicles (see Chapter 5) throughout the ECP. Choose barriers based on their ability to stop or defeat an identified threat. Installed barriers should be continuous and anchored together for maximum blast-mitigation and counter-mobility.

Maximize protection for ECP personnel (hardened fighting positions). Protection of and risk reduction to security personnel are vital. Incorporate both primary and alternate hardened fighting positions/guardhouses with overhead cover throughout the ECP to provide protection from dedicated assaults, sniper attacks, VBIED/PBIED blasts, fragments and debris (see Figure 6-5). Design protective structures with adequate space for personnel, ECP equipment, weapons, and ammunition. Appendix H, Soil-filled Container Applications, provides examples of hardened fighting positions.

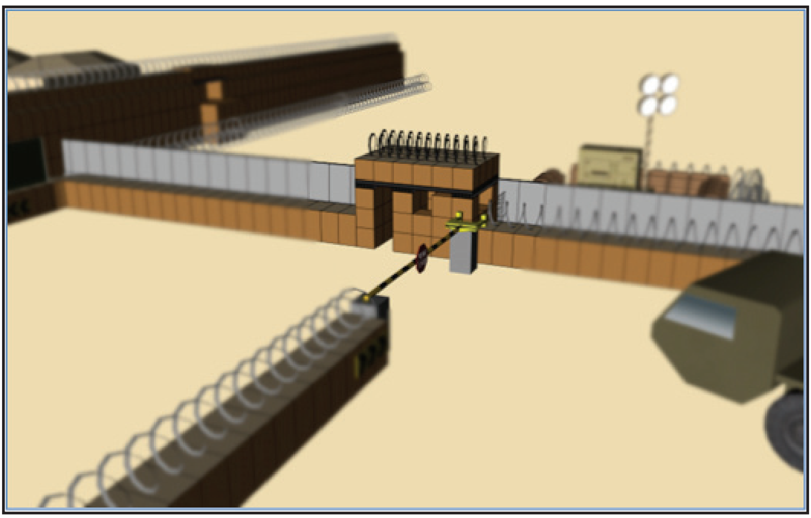


Figure 6-5. Hardened fighting position for ECP security personnel

Contain, segregate, and channelize vehicles and pedestrian traffic. Design the ECP to fully contain and control entering vehicles and pedestrians. Segregate and channelize vehicle and pedestrian traffic into separate access control lanes. Similarly, segregate commercial and passenger vehicles; if both vehicle types use the same lanes, distances between barriers must be increased and lanes must be widened to allow larger vehicles. Such modifications reduce the effectiveness of speed management techniques. Containment and segregation is accomplished with a combination of passive, active, and natural barriers.

Construct ECP lanes to accommodate oversized vehicles. If oversized vehicle traffic is anticipated (military/truck/commercial), the ECP design will require modifications to lane widths, size of inspection areas, and spacing of barriers. If wider lanes are incorporated into the design then additional speed management techniques and vehicle barriers must be used to prevent smaller passenger vehicles from gaining unauthorized access through the expanded lanes. The minimum lane width to accommodate passenger and smaller military vehicles should be 10 ft. (3.0 m). The preferred lane width is 12 ft. (3.6 m). However, the overall lane width will expand when vehicle barriers are added to create a serpentine layout. Proper lane widths are determined by calculating the widths of anticipated vehicles, barrier dimensions, and desired speeds (see Speed Management Techniques).

Maximize pedestrian access control. If pedestrians are allowed FOB access, the ECP design should direct foot traffic to a specified walkway that is separated from vehicle traffic. Separation of vehicles and pedestrians mitigates the effects of VBIED or PBIED attack. Maintain a minimum width of 4 ft (1.2 m) for pedestrian walkways. Pedestrian walkways should be designed with limited obstructions to ensure security personnel maintain continuous visual contact with approaching pedestrians. In addition, establish FOB-specific guidance detailing personnel access control measures and search procedures.

Maximize vehicle access control. If vehicles are allowed to enter and exit the FOB then access should be controlled with simple features such as clear instructions on signs, adequate turning dimensions, and FOB-specific guidance detailing vehicle access control and search procedures.

Construct vehicle turnaround and rejection areas. Design the ECP entrance with adequate space for vehicle turnaround. The Access Control Zone should include a method to reject or redirect unauthorized vehicles with minimal disruption to traffic flow. Design the approach roadway with the required turning radius to allow a single, continuous vehicle movement. The following are recommended, minimum, inside turnaround radii:

- Locations serving only passenger vehicles: 15 to 30 ft. (4.57 to 9.14 m);preferred width is 20 ft (6.1 m)
- Corners where larger vehicles turn: 35 ft. (10.67 m)
- Intersections where large trucks (WB-50), including semi-trailers (WB-67) turn: 150 ft. (5.24 m)
- Turnaround areas for large trucks: 65 ft. (19.81 m)

Construct a parking/transfer yard for authorized vehicles. If the FOB allows only mission-essential/trusted vehicle access, design an ECP parking/transfer yard. Preventing vehicles from entering the interior of the FOB allows positive vehicle control while maintaining a safe VBIED standoff distance. Provide adequate space for the expected number of vehicles. The design should allow for the entire area to be continuously monitored and kept under observation by security personnel and covered by fires from guard towers/overwatch positions. Also, provide protection for personnel exiting from vehicles and entering the FOB interior. Personnel protection measures include taller barriers for perimeter walls surrounding the vehicle parking/transfer yard and screening materials. Shield the vehicle parking/transfer yard to prevent enemy observation of security operations.

Build separate vehicle and pedestrian inspection/search areas. Design separate vehicle and pedestrian search areas (see Figure 6-6) with the capability to search all entering vehicles and pedestrians for IEDs, weapons, and contraband. Establish FOB-specific policies that detail search requirements and procedures.

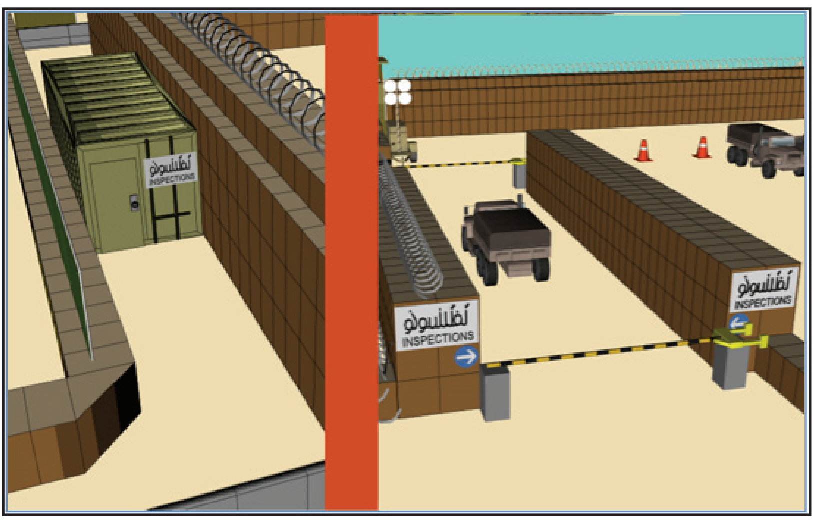


Figure 6-6. Separate vehicle and pedestrian inspection/search areas

Vehicle Search Area - Concepts include:

- **Separate search areas.** Vehicle search areas should be a separate and distinct area of the ECP that is offset from traffic lanes and at an acceptable standoff distance.
- **Segregate vehicle types**. Segregate larger vehicle (truck/commercial) traffic from passenger vehicles and construct search areas for each.
- **Adequate staging space.** Provide adequate space to stack and stage waiting vehicles (distance from Approach Zone to Access Control Zone). Prevent staged personnel from observing search procedures.
- **Blast mitigation measures.** Include blast mitigation measures (berms, soil-filled bins/walls, soil-backed concrete barriers) in vehicle search areas to protect personnel from VBIED effects.
- **Adequate size to accommodate anticipated vehicle types**. To facilitate safe inspections, design vehicle search areas that are a minimum width of 18 ft. (5.5 m) and a minimum length of 40 ft. (12.2 m). Expand this length if oversized vehicles are expected. Design search areas that can be closed to protect inspection equipment during inclement weather. Provide the following dimensions for inspection areas:
  - o For standard passenger vehicles: 15 x 25 ft. (4.5 x 7.2 m) inspection bays
  - o For commercial/oversized vehicles: 18 x 80 ft. (5.5 x 24.4 m) wide by 17 ft.-6 in. (5.4 m) high inspection bays
- **Driver/passenger holding area.** Design holding areas that prevent drivers/passengers from observing search operations. Holding areas should not protect drivers and passengers from explosive effects. Drivers and passengers should be searched and kept under constant observation by armed personnel not involved in search procedures.
- **Screen search areas from external surveillance.** Obstruct observation of the search area from outside the FOB with berms, tall barriers, camouflage netting, or other screening material.
- **Military Working Dog (MWD) rest area**. Extreme heat and sun cause fatigue and reduce MWD effectiveness. To extend effectiveness, keep animals not actively engaged in searching vehicles in an air-conditioned tents or containers. Other measures to improve dog endurance include cold collars, cooling-mist fans and dog shoes.
- **Shade.** Provide overhead shade for search areas to maximize ECP personnel and MWD effectiveness.

- **Ramps/search pit**. Consider vehicle ramps and a mechanic's (search) pit that allow searchers an effective means to visually inspect vehicle undercarriages. Absent technology, this is the only way to thoroughly search a vehicle's underside.
- **Cargo truck search.** Consider using an automated vehicle inspection system such as the Military Mobile Vehicle and Cargo Inspection System (MMVACIS) to reduce security force exposure inherent to manual searches.
- **Mirrors.** Use mirrors to detect poorly or hastily concealed explosives placed near outer vehicle edges. The mere act of searching beneath a vehicle is often a psychological deterrent to terrorists.
- **Floor.** If no search pit is available, search area floors should be flat and hard to allow searchers to crawl under vehicles with a mechanic's creeper. Suitable surfaces include asphalt, concrete, AM2 matting, and plywood. Astroturf or similar matting placed over the floor protects MWDs' feet from ground heat.
- **Illumination.** Search pits should be well illuminated to allow searchers to see all portions of the vehicle. Lighted ramps and mechanic's pits facilitate detailed underbody searches. Flashlights or extension lamps should also be available to ECP security personnel
- **Closed Circuit Television (CCTV) systems.** CCTV can record vehicles for observation and later review. Position cameras to prevent vehicle or perimeter lights from blinding the camera. Cameras placed outside should be protected from the environment.
- **Electronic explosive detection devices**. Commercially-available explosive detection devices that utilize chemical indicator, backscatter, or transmission imaging can augment manual visual search explosive detection capabilities. Appendix G, Material and Technology Support, the Technology Section of the *Small-Base Leader ECP Guide,* and the *JEEP Handbook* provide equipment that may be available for this purpose.
- **Power requirements**. Electronic equipment such as active barriers, detection devices, CCTV, lighting, and communication systems require power. Develop a design that provides power for planned and future electronic devices. Incorporate a reliable alternate power source such as a standby generator to ensure continuous ECP operations.

Pedestrian Search Area. Design considerations are similar to those of vehicle search areas. However, the following pedestrian-specific issues should be considered:

- **Separate male and female search areas.** Design separate search areas for female and male searches.
- **Adequate staging space.** Design adequate space to stack pedestrians awaiting search (distance from Approach Zone to Access Control Zone). Prevent pedestrians waiting to be searched from observing search operations. Keep pedestrians under constant observation by armed personnel not involved in search procedures. If available, employ CCTV to assess pedestrian activities as they proceed through the ECP.
- **Blast mitigation measures.** Include blast mitigation measures such as soil-filled bins/walls, modular protective system (MPS)) and shipping containers to protect pedestrians from PBIED/VBIED detonations.
- **Screen search areas from external surveillance.** Employ screening measures to prevent observation of search area from personnel outside the FOB.
- **Electronic explosive detection devices**. Consider commercially available explosive detection devices for the pedestrian search area. Appendix G, Material and Technology Support, the Technology Section of the *Small-Base Leader ECP Guide*, and the *JEEP Handbook* detail the equipment that may be available for ECP applications.

Construct hardened overwatch positions. Overwatch positions are critical to defense-in-depth. The ECP overwatch should provide observation and coverage of the entire ECP with crew-served weapons that can employ deadly force to stop vehicles and repel attackers attempting to bypass, ram, or run through an ECP. Design alternate overwatch positions as a random operational measure.

Design overwatch positions with the same considerations as those used against an ambush - fix the enemy in place so they can be neutralized.

- Establish an overwatch kill zone to engage hostile vehicles
- Install barriers to maximize a hostile vehicles time in the kill zone
- Position the overwatch to provide effective engagement of targets in the kill zone

Equip overwatch positions with weapons that can disable a vehicle or kill the driver. Preferred weapons are no smaller than a medium machine gun (M60 or M240G). Heavy guns (M2 .50-caliber machine gun or MK19 40-mm grenade launcher) are better at stopping a vehicle.

Once the kill zone is established, evaluate weapons system ranges to determine the risk to friendly guard posts, HN buildings, and personnel likely to be in the field of fire (range fan). All overwatch positions should have range cards that denote the weapon system's principal direction of fire (PDF), distances to key terrain features, and the final protective line (FPL). Range cards will enhance the gunner's ability engage a target, determine ranges, and estimate ranges to other targets. Some weapon systems have a required minimum range to activate the round. The kill zone for the overwatch position must be beyond that minimum range.

Weapon systems selected for overwatch positions should require minimal traverse and elevation (T&E) adjustments to continually fire on the kill zone. Employ large, strong firing stakes if a T&E device is not available to define fields of fire during periods of darkness or low visibility. Finally, rules of engagement (ROE) should be well defined and readily available. ROE should be considered when selecting an overwatch position location. Consider Figures 6-7 and 6-8 when selecting overwatch positions.

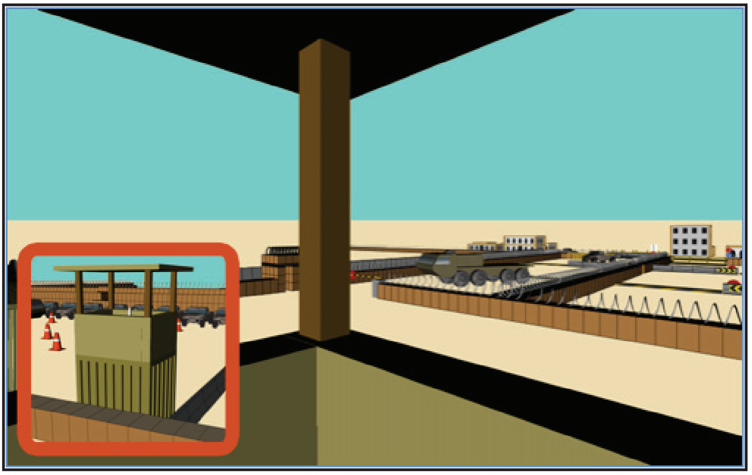


Figure 6-7. Example overwatch positions

- □ Can the overwatch clearly observe the entire ECP and its barriers?
- □ Is the overwatch able to clearly determine the circumstances under which they are authorized to employ deadly force?
- □ Does the overwatch allow adequate distance to engage target vehicles?
- □ Is the overwatch able to engage a hostile vehicle at least 100 meters away?
- □ What is the effective causality radius (ECR) of ammunition used in the overwatch weapon system?
- □ What are the maximum and minimum ranges of overwatch ammunition?
- □ Are friendly troops (to include HN troops and civilians) located within the field of fire (range fan) of the weapon system?
- □ Will ricochet rounds endanger friendly forces?
- □ Can the overwatch weapon systems engage enemy targets for 10 – 15 seconds?
- □ Can the weapons bring enfilade fire on hostile vehicles?

Figure 6-8. Overwatch Considerations

Construct a hardened final denial barrier. The final ECP design element is a hardened perimeter gate or final denial barrier that is capable of preventing a ramming vehicle or VBIED from penetrating the FOB perimeter. This can be accomplished with active or movable vehicle barriers or relocatable vehicles (see Figure 6-9). Final denial barriers require a level of security equivalent to adjacent ECP and perimeter barriers. The most common active barriers are cabled crash-beam or drop-arm barriers. Other active barriers include hydraulic pop-up barriers and metal crash gates. At a minimum, reinforce fence gates with cables that increase resistance to penetrating vehicles. Gates should be capable of denying access to both vehicles and personnel. Gates are further detailed in Chapter 5.

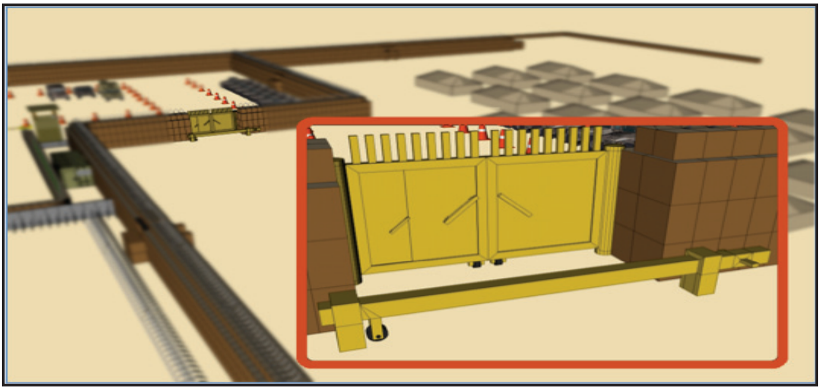


Figure 6-9. Final denial barrier

Off-site parking lot. Consider and identify off-site parking lot requirements. Off-site parking discourages unauthorized vehicles from requesting FOB access. Direct personnel not requiring FOB driving privileges to this area; this limits FOB traffic to mission-essential/trusted vehicles. Locate parking areas away from critical assets, inhabited areas, and ECP security personnel to maintain adequate standoff and minimize VBIED blast effects. Keep parking areas under constant observation by security personnel and regularly search for signs of unauthorized activity.

Consider an exterior logistics transfer point or "cool down" area for delivery vehicles. A logistics transfer point is a protected area outside the FOB perimeter designed to screen and transfer logistics supplies. The purpose is to eliminate commercial delivery vehicle traffic through the ECP. If a logistics transfer point is constructed, positive control of delivery vehicles and the operator/passenger(s) is essential. One technique is to establish a 24-hour cool down period that requires vehicles to remain parked and under observation for at least 24 hours before off-load is allowed. Appendix E provides additional details.

Install security lighting. ECP security lighting employment is threat-dependent (Figure 6-10). At night, the commander may opt for FOB light discipline to limit the profile of the base. However, if the ECP mission requires night operations then the design should include multiple, redundant lighting systems. Redundant lighting and power to support these systems prevents degraded lighting and ensures uninterrupted ECP operations.

Lighting requirements must be weighed against light discipline requirements. In operational situations, the ECP might remain darkened until friendly egress/ingress is ready to proceed. In such cases, consider on-demand lighting systems.

Adequate ECP lighting should provide enough intensity to identify vehicles, pedestrians, security personnel, signs, and hazards. Lighting should not be directed in the eyes of approaching drivers or backlight security personnel. Chapter 10, Security Systems, describes lighting equipment and techniques.

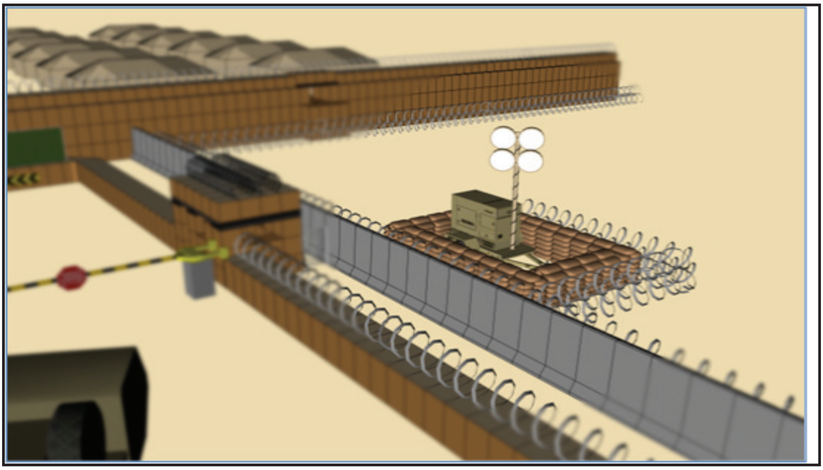


Figure 6-10. Example of security lighting

Install signage. ECP signs should be clear, concise, easily read, and displayed in the local language. Signs should stipulate access control requirements and provide specific instructions for vehicles and pedestrians, including the route to follow through the ECP and noncompliance warnings.

Example ECP Designs. The Army Facilities Component System (AFCS) Web Portal (https://www.tcms.net/afcsportal/) has example ECP designs for a small and large FOB, a commercial vehicle ECP, and a tactical vehicle ECP. Once in the AFCS portal, look under the drawing section and search for “Entry Control Point” to find the drawings. While these drawings are labeled as “Contingency Standard Designs”, they should be considered only as examples to be used in developing a good site-specific ECP design.

Speed Management Techniques

A moving vehicle must have a certain level of kinetic energy to penetrate perimeter barriers and inflict damage. Kinetic energy depends on an object’s mass and speed. Since an approaching vehicle’s mass remains essentially constant, kinetic energy increases with higher speed. In fact, a vehicle traveling at 20mph has quadruple the kinetic energy of one traveling at 10mph. A vehicle’s impact speed will depend on its mechanical performance and the distance traveled before impact. Approach angle also influences vehicle speed. Impact speed can be limited with forced cornering and off-angle approaches.

Possible attack routes and angles should be analyzed for each FOB and ECP. Prepare a site sketch of the surrounding topography, buildings, and streets (see Figure 6-11) to identify long, straight, level avenues of approach and possible attack routes. Do not limit potential attack routes to only established or improved roadways. Any surface suitable for vehicular traffic (street, parking lot, lawn, or sidewalk) can be used for an attack. Potential attack paths must be at least as wide as the attack vehicle, approximately 8 ft. (2.4 m) and wider for large trucks. Suitable attack paths must have no radius of curvature more than 22.5 ft. (6.8 m). Steep grades also affect vehicle speeds. Uphill grades reduce approach/impact speed while downhill grades increase it.

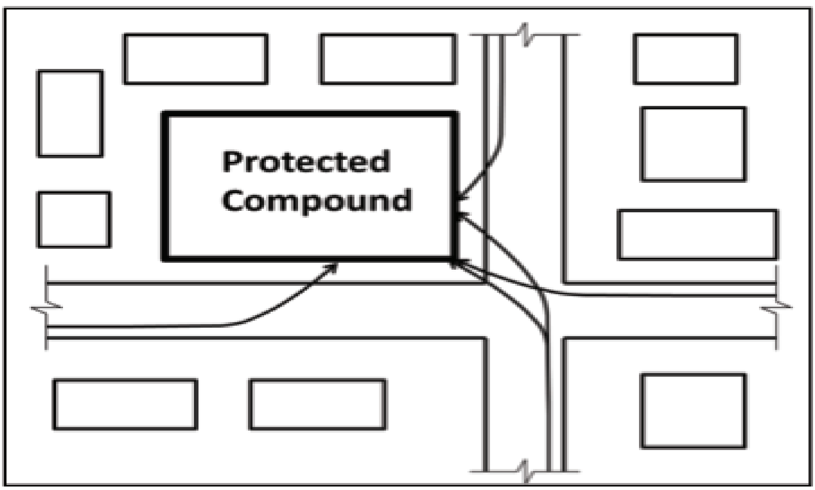


Figure 6-11. Example of Site Sketch with Possible Vehicle Attack Scenarios.

Utilize the FOB layout, surrounding roads, buildings, terrain, barriers and ECP design concepts to eliminate straight-line access routes and reduce vehicle speeds. Speed management techniques include:

- Sharp 90 degree turns into the ECP that force vehicles to slow to 10 mph or less
- Traffic circles leading into the ECP
- Vehicle barriers to block straight-line avenues of approach
- Speed bumps and speed tables
- Nonlinear, serpentine traffic lanes

The nonlinear, serpentine layout of traffic lanes is a simple, effective technique. The “S” layout constructed with vehicle barriers significantly reduces approaching vehicle speeds. Figure 6-12 provides an example of a serpentine layout using concrete vehicle barriers.

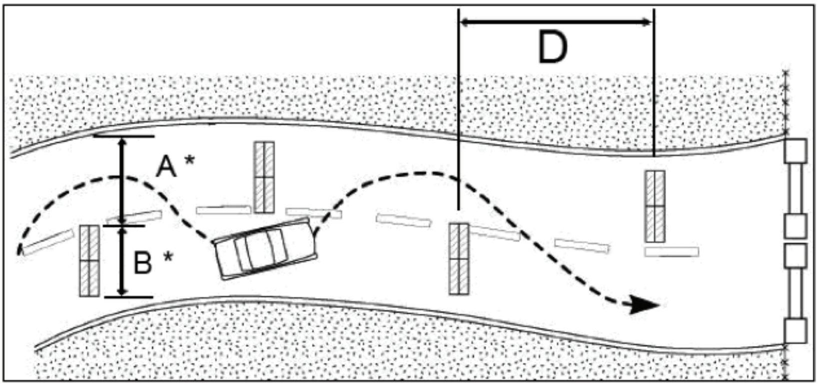


Figure 6-12. Traffic Lane with Nonlinear Serpentine Layout
*A — 12 Feet Maximum; *B — Varies Depending on Road Width (UFC 4-022-02)

Tightening serpentine curves and shortening the distance between barriers additionally reduces vehicle speeds. For example, a road with a 30 ft. (9.3m) width would require 20-ft (6.1 m) vehicle barrier spacing to reduce vehicle speeds to 10mph. Figure 6-13 provides barrier separation distances and accompanying maximum vehicle speeds. Figure 6-13 should be used in conjunction with Figure 6-12. If trucks are included in traffic lanes with passenger vehicles, the ability to slow and control passenger vehicle speeds is diminished. Optimize serpentine layouts by designing separate passenger vehicle and truck traffic lanes.

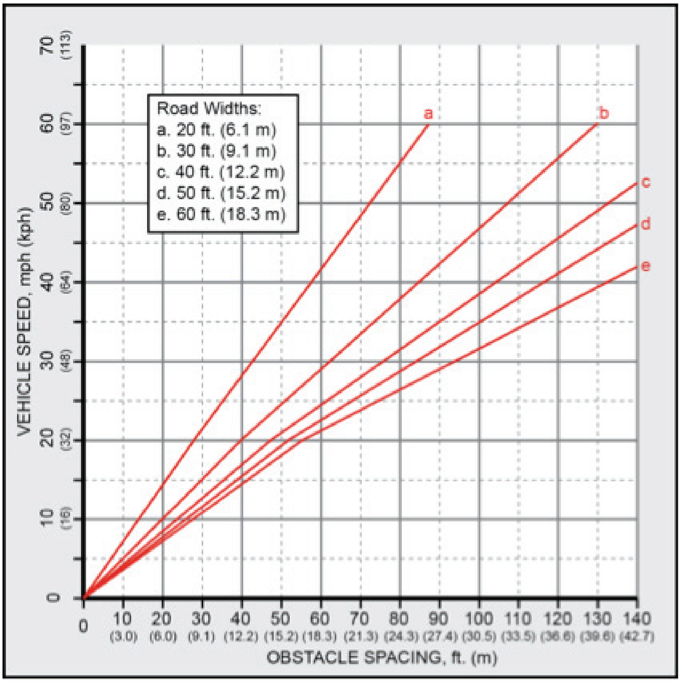


Figure 6-13. Separation Distance (D)* for Barriers to Reduce Speed of Passenger Vehicles on a Straight Path

ECP Barrier Concepts

Vehicle barriers accomplish many ECP design requirements including containment, segregation, and compartmentalization of vehicles, rejection of unauthorized vehicles, and vehicle speed management. Active and passive barriers are more effective when combined and integrated into the adjacent perimeter barrier system. Barriers alone do not address all protective requirements, but will complement other physical and procedural security measures. Chapter 5 provides additional information regarding ECP barriers.

Include the following barrier considerations in ECP designs:

- Select barriers based on their ability to stop threat vehicles
- Address the potential hazardous debris produced by concrete barrier systems exposed to a blast; soil-backed concrete barriers and soil-filled bins will better mitigate hazardous debris

- Employ movable, easily operated barriers at entrances to maintain positive traffic control
- Construct ECP perimeter walls with passive vehicle barriers
- Create nonlinear, serpentine lanes throughout the ECP with vehicle barriers for traffic control
- Select barriers with limited profiles for interior walls/lanes to minimize intruder cover and concealment positions
- Select and locate barriers to limit or block enemy surveillance attempts
- Arrange barriers in a continuous layout to contain vehicles
- Construct a final denial barrier at the FOB entrance for complete containment
- Position barriers away from trees, telephone poles, antenna masts, or adjacent structures to prevent barrier circumvention
- Place barriers in concert with each other, the natural terrain, and any man-made obstructions
- When a single barrier cannot stop a vehicle, combinations or layers of barriers are more effective; separate layers by a minimum 30 ft (9.15 m) clear zone for increased protection and control
- Maintain unobstructed clear zones on both sides and between barriers
- Install additional personal barrier toppings on ECP perimeter walls to inhibit efforts to vault or scale the wall; concertina, multi-strand razor, and barbed wire are all effective
- Install multi-strand concertina or razor wire along the top and outer base of perimeter walls to prevent their use by attackers as cover/protection. Employ movable personnel barriers in conjunction with movable vehicle barriers at ECP entrances. Staked strands of concertina or razor wire will deter unauthorized personnel entry.
- Continuously monitor, patrol, and inspect barriers
- Augment perimeter barriers with IDS, if available
- Integrate overwatch and final protective fires to support the ECP barrier system

ECP Construction Sequence

There is no standard sequence for constructing an ECP. ECP construction is site dependent and driven by previously discussed design considerations. The following generic steps should be adapted for each FOB. Several steps should be conducted simultaneously to rapidly maximize protection. As a general rule, begin ECP construction adjacent to the base perimeter and continue outward to completion. The Tools Section of the *Small-Base Leader ECP Guide* provides an ECP Construction Sequence Checklist.

- Post sentries and prepare hasty fighting positions
- Construct overwatch/towers; position crew-served weapons systems for ECP overwatch; ensure overwatch positions have interlocking fields of fire that provide cover and observation of the entire ECP
- Clear fields of fire around the ECP
- Establish interim entry/access control measures during ECP construction
- Install signs with simple, clear instructions for ECP access
- Employ vehicle barriers or other expedient methods to block high-speed avenues of approach; mitigate straight-line access from local roadways
- Use vehicle barriers to form nonlinear, serpentine lanes through the ECP and create perimeter walls that contain, segregate, and channelize vehicle and pedestrian traffic
  - Ensure lanes are wide enough to accommodate oversized vehicles
  - Ensure vehicle turn-around and rejection areas are included in the layout
  - Ensure exit lanes maintain the same security level and required access control measures
  - Seamlessly connect ECP barrier walls into the perimeter security/wall system
  - Construct a parking/transfer yard for authorized vehicles; ensure adequate space to conduct vehicle searches
  - If required, construct a vehicle search area; construct a holding area to segregate and search drivers/passengers and prevent observation of search procedures
  - If required, construct a pedestrian search area; construct a holding area to segregate pedestrians and prevent observation of search procedures
  - Install personnel barriers around and on vehicle barriers to prevent intruders from scaling the ECP walls
  - Ensure the layout eliminates potential enemy hiding places

- Install movable vehicle barriers at the ECP entrance
- Construct hardened fighting positions for ECP security personnel; construct both primary and alternate positions; include overhead cover for RAM protection
- Construct a final denial barrier/hardened perimeter gate at the FOB entrance
- Install vehicle barriers for speed management
- Install screening to prevent observation of ECP operations
- Eliminate natural or man-made enemy vantage points
- Install power sources
- Install security lighting
- Install additional technology solutions (i.e., vehicle and personnel screening equipment)
- Construct an external parking lot for unauthorized vehicles
- Add additional signs, if needed
- Update entry/access control measure
- Update entry/access control measures to reflect ECP completion
- Establish/update vehicle and pedestrian search procedures
- Train/rehearse ECP personnel on access control measures and response/escalation of force/ROE procedures
- Continually improve and structurally harden the ECP

ECP Operations

ECP effectiveness is directly related to the training and skill of security force personnel. For that reason, FOB commanders should develop ECP operational procedures that project professionalism, commitment to mission accomplishment and protection of personnel, and ensure adequate training and exercises. Whether occupying an existing ECP or establishing a new one, a team approach is the most effective method of developing or reassessing operational procedures.

The *Small-Base Leader ECP Guide* and *JEEP Handbook* provide detailed discussions of ECP operational concepts and considerations. The concepts presented are common to ECPs; however, ECP differences require that guidance be adapted and tailored to specific FOB requirements.

References:

Small-Base Leader Entry Control Point Guide (ECP Guide).

Joint Entry Control Point & Escalation of Force Procedures (Jeep Handbook).

UFC 4-022-01. *Security Engineering: Entry Control Facilities/Access Control Points*, 25 May 2005.

AASHTO WB-15M. *Policy on Geometric Design of Highways and Streets,* April 2003.

Defense Department. *Vehicle Inspection Guide*, 2007.

CHAPTER 7
SIDEWALL PROTECTION

Protection for above ground assets from IED effects and conventional weapons generally requires materials and construction that are resistant to blast and penetration effects. Ideally, this protection should be in all directions, including overhead. However, sidewall protection mitigates most direct fire weapons, near-miss indirect fire weapons, and IED effects, and should be the first protective priority. Sidewall protection provides the primary protection for lightweight structures such as tents and modular housing units and can be used to enhance protection for other structures such as existing indigenous buildings. It can also be used to protect mission-critical equipment such as weapons storage and fuel bladders. Protection from direct hits of indirect fire weapons can be addressed with overhead cover (see Chapter 9).

Sidewall protection usually consists of free-standing walls or revetments (Figure 7-1) that stop projectile and fragment penetration. One of the most efficient materials for stopping fragments is dense granular soil such as sand. Most revetments designs are just variations of techniques to hold soil in a vertical position. Simple soil berms, soil filled containers, free-standing reinforced concrete walls, and lightweight modular systems all enhance protection. Specific designs depend on threat, logistics, and operational constraints.

Figure 7-1. Sidewall protection example

Soil Berms

Soil berms have provided protection to military personnel and assets for centuries. Berms are typically employed at the perimeter of a FOB located in open, lightly populated terrain and may be the best initial sidewall protection method for critical assets. Properly sited, constructed, and maintained berms mitigate fragmentation effects from near-miss RAM detonations. Berms can act as vehicle barriers, block lines of sight, and protect against direct fire weapons. Berms can also withstand multiple blast events and be reconstructed if necessary. Their main disadvantages are their large footprint and specialized equipment needed for construction. Berms may not be a practical sidewall protection option in rocky or urban terrain or where grading equipment is not available.

Construction. Proper berm construction requires abundant soil, heavy equipment (dump truck, backhoe, bulldozer, roller compactor), and skilled operators. Berms can be employed as free standing structures or constructed against walls (Figures 7-2 thru 7-5). Berms are most effective when constructed of compacted soil at its angle of repose; typically 30 to 45 degrees. The angle of repose is the steepest grade at which the soil will remain in place without reinforcement. Steep slopes are difficult to stabilize with loose, granular soil but more attainable with soils containing clay or with soil stabilization techniques. The minimum practical crown width is 2-3 ft. Where susceptible to erosion, the use of vegetation, geotextile fabrics, and proper slope drainage may be required. However, vegetation that does not provide concealment for intruders should be selected. Consideration should also be given to the berms' possible disruption of established surface water drainage patterns that could affect the FOB interior.

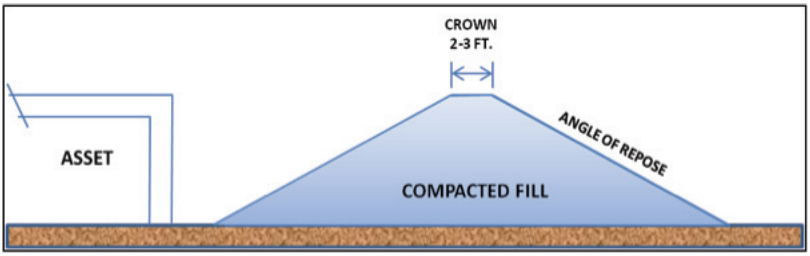


Figure 7-2. Free-standing Berm Configuration

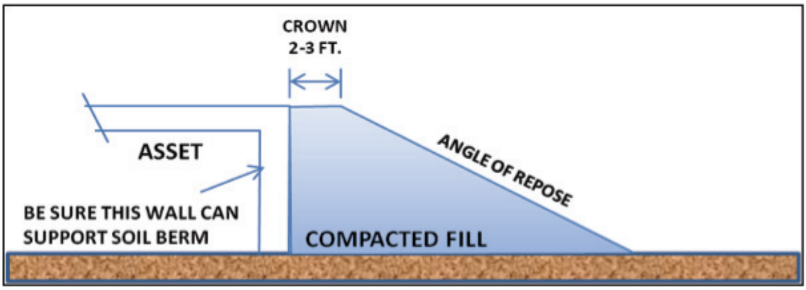


Figure 7-3. Wall-Berm Configuration Figure

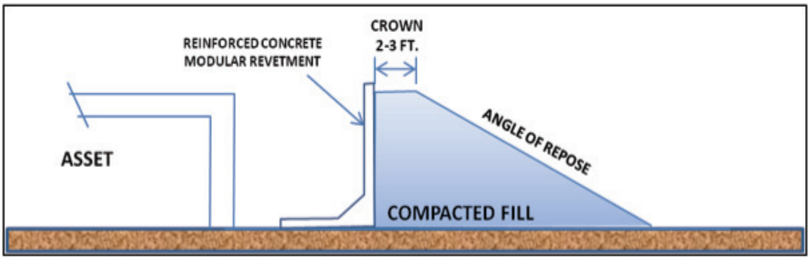


Figure 7-4. Soil Berm and Reinforced Concrete Revetment

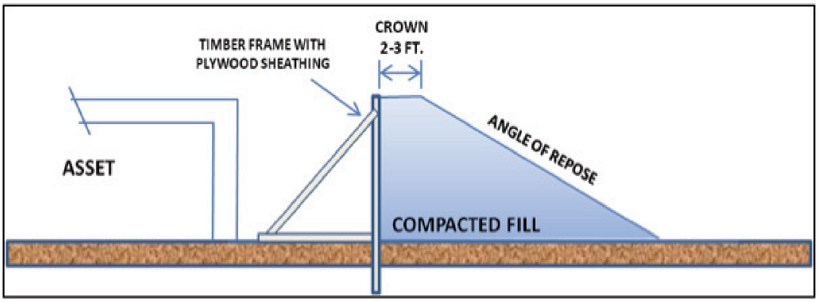


Figure 7-5. Soil Berm and Wooden Retaining Wall

Berms supported by the protected building (Figure 7-3) must be assessed by a structural engineer to ensure the wall can support the berm's load. Berms can also be supported with properly designed, L-shaped pre-cast, concrete retaining walls (Figure 7-4). In addition, expedient retaining walls can be built with plywood, corrugated metal, landing mats, or other sturdy materials with the facing material either braced or tied to deadman supports located in the berm or on its slope (Figure 7-5). Consult a structural engineer to ensure design safety.

Performance. The height and thickness of the berm will determine how much protection it provides. For example, a 10 ft. high free-standing berm will be at least 20 feet thick and will protect against small arms, RPGs and near miss RAMs.

Sandbags

Sandbags are a traditional method for providing protection from small arms and RAM fragments (Figure 7-6). Sandbag revetments may not effectively protect against blast overpressure unless properly positioned. Unless shielding can be located close to the asset, blast overpressure will remain a concern. Close revetments deflect blast waves (See Chapter 4). Sandbag walls can be constructed as either freestanding or supported on one side by the protected structure.

Figure 7-6. Sandbag Sidewall Protection (note overhead pre-detonation screens).

One sandbag requires approximately 0.3 cubic feet (0.008 cubic m) of sand. Twelve bags form a wall 1 ft. (0.3 m) high by 4 ft. (1.2 m) long. Fill sandbags with clean dry sand or any granular material. Shovels are the only required equipment. Avoid loose gravel or crushed rock as these can become secondary fragment sources in high-explosive events. Wet fill material performs poorly and is not recommended. Improved durability is obtained by mixing fill material with cement (1 part cement to 10 parts soil).

Sandbag wall construction is both labor and time intensive. Sandbag requirements often exceed the capabilities of personnel using only shovels. If bags are filled from a stockpile, sandbag fillers as shown in greatly speed and simplify the fill process . The proximity of the sand fill area to the construction site significantly affects construction speed and cost.

Depending on climate and fill material, sandbags can rapidly deteriorate. Most modern sandbags have at least a 2-year lifespan with no visible deterioration. However, some older cotton bags deteriorate much more quickly.

Construction. Sandbag revetments with unsupported vertical faces higher than 4 ft. (1.2m) are potentially unstable. Taller unsupported walls should have a slope of 1:4 and the base must stand on firm ground. Stack sandbags as shown in Figure 7-7. Stagger joints and use header layers for more stable walls. During construction, tamp the top of each sandbag with a flat object for settling and stabilization. Always place the bags' closed ends and side seams inward and away from the threat direction. Construct walls high enough to protect assets from incoming projectiles and fragment spray. For tents, freestanding walls 6 to 7 ft. (1.8 to 2.1 m) high are advised. Walls 8 to 9 ft. (2.4 to 2.7 m) tall may be required to account for structures with crawl spaces.

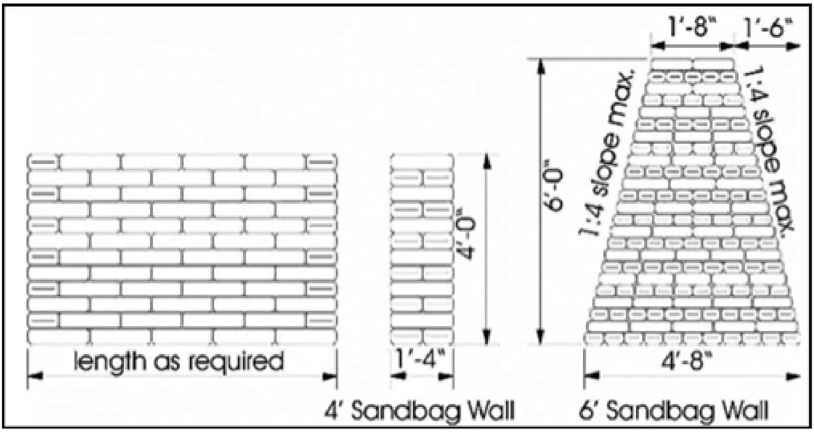


Figure 7-7. Freestanding Sandbag Revetment Details

Performance. Tests have shown that a two-layer sandbag wall, approximately 16 in. (40.6 cm) wide, provides protection from blast and fragmentation effects of 82-mm and 120-mm mortars, and near-miss (4 ft. (1.2 m)) 122-mm rocket detonations. In addition, if kept dry, the wall will stop small arms up to 7.62mm (See Table 7-1).

Sand Grids

Sand grids are prefabricated plastic forms that expand into honeycomb-shaped cells to confine sand or gravel fill material. Sand grids are more easily transported and require less construction time than sandbags. Expanded grids (Figure 7-8) can be stacked vertically and filled with sand to form a revetment.

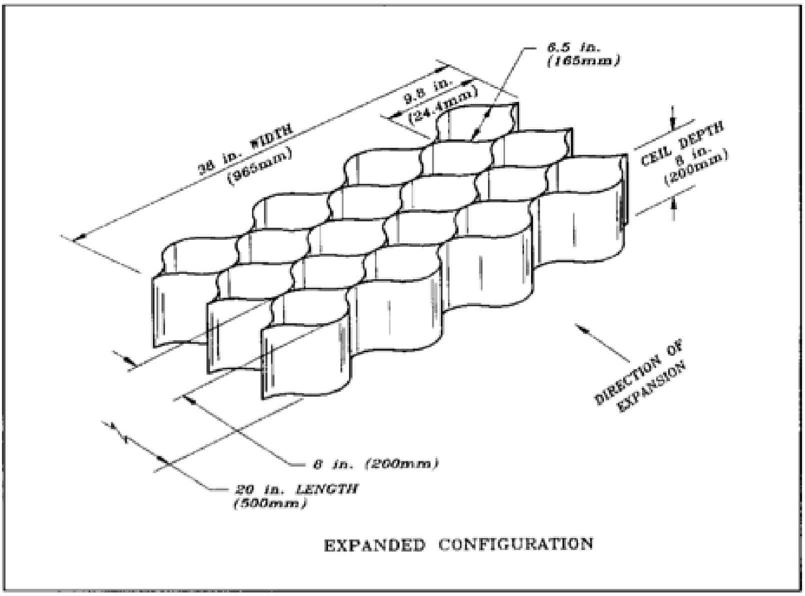


Figure 7-8. Sand Grid (MIL-HDBK-1013/1A)

Construction. Grids are expanded and laid over metal pickets at each end and stacked one layer on the next. The maximum freestanding revetment height is 8 ft (2.4 m) (approximately 12 layers) with a 38 in. (96.5 cm) wide base. Only 6 ft. heights (1.8 m) [approximately 9 layers] are recommended unless additional picket anchors are added to the standard anchors. For additional height over 8 ft., use either wider sand grids or additional grid rows side by side, tied together. . Use narrower sand grids for the upper rows. Make sure all rows have anchor pickets or additional intermediate pickets extended through adjoining layers. To prevent erosion and soil loss with sand grids that do not interlock, place geotextile fabric between each grid layer, then cover the top layer with impervious sheeting and sandbags to keep dry.

Performance. The thickness of the sand grid wall will determine how much protection it provides. Typically a 3 ft. (0.9 m) thickness is adequate to stop all fragments from 60-mm mortar through 122-mm rocket and 155-mm artillery rounds as well as all small arms fire.

Soil-Filled Wire and Fabric Containers

Soil-filled wire and fabric containers consist of large, linked, self-supporting cells (Figure 7-9). Each cell is a collapsible wire mesh lined with geotextile fabric. Individual cells are expanded from a compact storage configuration. During construction, containers can quickly be unloaded, expanded, and filled with sand or native soil. Wall sections can be connected to increase length, separated to form shorter sections, or stacked to increase height.

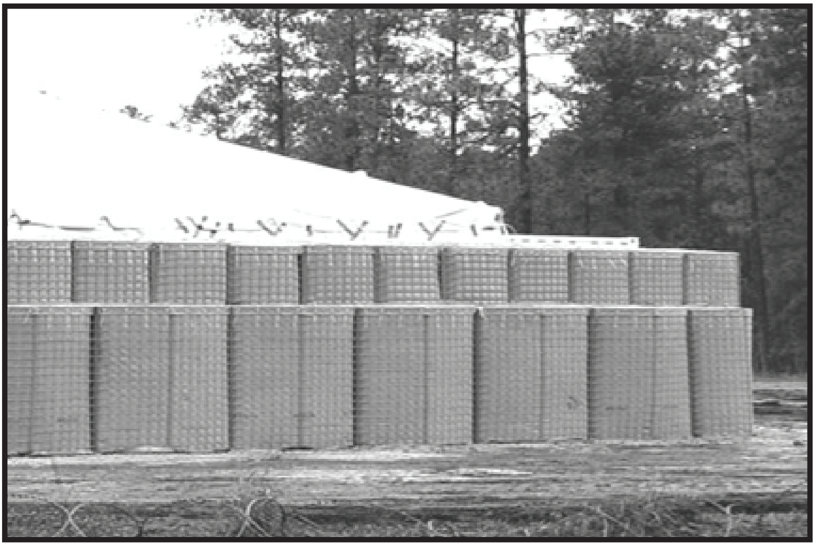


Figure 7-9. Soil-filled geotextile (wire and fabric) containers for sidewall protection

Construction. Container shipments come with detailed instructions that must be followed to ensure stability, durability, and minimum maintenance. Containers arrive flat-packed and should be located and orientated prior to expansion and fill. Construction requires heavy equipment such as bulldozers and front-end loaders, and hand tools (shovels, rakes, pliers, wire cutters).

Select or construct a level surface with a sub grade of sufficient strength and drainage to support the structure and prevent tipping. If anticipated use will exceed 6 months, improve the container foundation. Proper placement of fill material is critical to performance. The fill must be compacted or the wall will eventually sag, deform, or collapse. The fabric material liner is sensitive to UV light and may degrade over time. Appendix H, Soil-Filled Container Applications, provides additional construction details.

Performance. Soil-filled containers are simply a technique to hold fill materials in a vertical position. Research has shown a 2 ft. (0.6 m) thick container filled with dry, dense granular soil such as sand is adequate to stop all fragments from 60-mm mortar through 122-mm rocket and 155-mm artillery rounds as well as all small arms fire.

Soil-Filled Metal Containers

Soil-filled metal containers are made of roll-formed metal, typically 16- or 18-gauge steel. These revetments are based on the USAF Metal Revetment Kit, Type B-1, which has been employed in some fashion since the Vietnam War. ERDC developed a smaller kit for FOB applications that provides blast load protection and primary RAM fragment shielding. Figure 7-10 shows a metal container sidewall configuration. Like wire and fabric containers, metal container kits are shipped flat and unassembled, then filled on-site.

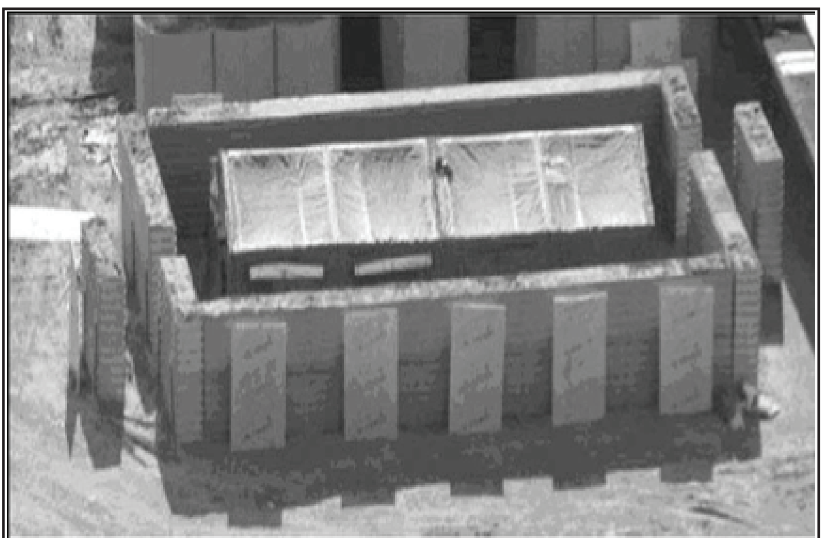


Figure 7-10. Soil-filled Metal Containers Used for Sidewall Protection

Construction. Each kit contains side, end, cross, and brace panels, connecting pins, flaring tools, and corner containment materials. The cell sections are assembled in place or can be assembled on the ground and lifted into place with a crane. A well-prepared foundation is vital to this container's performance and durability. The ground surface must be level, well-compacted, and stable enough to support the structure for its intended lifespan. If an improved surface (concrete paving, asphalt paving, stabilized soil), is unavailable, the foundation area must be improved to ensure stability.

To fill metal revetments, first line the bottom with a 1/2- to 3/4-in. (1.3 to 1.9 cm) gravel layer to allow for drainage. Add an impervious sheeting material along the sides to contain soil material and a waterproof cap to prevent fill saturation. Appendix H provides additional soil-filled container applications and construction details.

For near-miss 122-mm rocket protection, laterally brace walls shorter than 24 ft. (7.3 m) in length to prevent wall toppling. Brace with 3 in. (7.6 cm) diameter, schedule 40 (minimum) steel pipe (Figure 7-11). Other strong materials such as U-pickets and 4 in. by 4 in. (10.2 cm by 10.2 cm) timbers can also be used. To prevent toppling in either direction, brace both sides of the wall. For braced walls, particularly with loosely compacted base material, bracing should provide vertical support extending from the base to at least mid-height of the upper lift.

Figure 7-11. Bracing metal revetment wall for 122-mm rocket threat. Steel pipe bracing is shown; U-pickets and 4 x 4 timbers can also be used.

Performance. Explosive field tests showed that the 2 ft. (0.6 m) container thickness will stop all fragments from near-miss 60 mm mortars through 122 mm rockets. However, some walls overturned, posing a serious threat to personnel located within 7 ft. (2.1 m). Results from 120-mm mortar experiments indicate that for close proximity (approximately 4 ft. / 1.2 m) detonations, bracing the 2 ft. (0.6 m) thick wall prevents overturn. Four ft. (1.2 m) thick walls subject to fragment and blast loadings of close proximity have sufficient mass to prevent overturn and defeat primary fragments. ERDC tests also showed that the thin revetments can defeat an RPG-7 when supplemented by a vertical pre-detonation screen at sufficient standoff.

Modular Reinforced Concrete Walls

Prefabricated, reinforced concrete walls (Figure 7-12) can provide full-height sidewall protection around tents, trailers, and small buildings. Properly designed and constructed, these walls (sometimes referred to as T-walls) provide small arms and near-miss RAM protection. Pre-cast reinforced concrete walls are available in many sizes and configurations (see Chapter 5).

Figure 7-12. Modular reinforced concrete barriers for sidewall protection.

Construction. If concrete walls are acquired locally, ensure the material and construction meet military standards. The minimum recommended thickness is 6 in. with a minimum concrete compressive strength of 4500 psi. For lower strength concrete, thicker walls are recommended. Flat-bed trailers, forklifts, and cranes are normally required to move and place these walls. The minimum recommended height is 6 ft. (1.8 m), but taller units may be necessary for structures with crawl spaces. Provide a level, stable placement surface. An uneven foundation reduces prefabricated wall stability and effectiveness. Eliminate gaps between wall sections to prevent fragment penetration, especially at corners. This can be done using precast walls that have notched edges that overlap and have chamfered footings. If possible, construct sections so they can be connected together with cables. Consider bracing tall sections to prevent toppling.

Performance. 4,500 psi, 6-in. (15.2 cm) thick concrete walls will stop all fragments from 60-mm mortar through 122-mm rocket at standoff distances of 10 ft. (3.0 m) or greater. Detonations within 10 ft. (3.0 m) may pose a hazard for blast-induced back-face spall. For additional protection or lower strength concrete, use thicker walls. A sheet steel liner (at least 16 gauge) reduces spall and increases fragment penetration resistance. Reinforced concrete walls, however, can still be breached by large, near-miss and direct RAM impacts, and large IEDs. The resulting wall debris may be a personnel hazard. Concrete walls 6-1/2 in. thick will protect from most small arms (see Table 7-1).

Modular Protective Systems

The Modular Protective System (MPS) (Figure 7-13) consists of an expandable steel frame that accepts fragment-resistant E-glass and ultra high-strength concrete panels. The frame contains Z-bar clips that allow panel insertion. Armor panels can be either Underwriters Laboratory Level 3 ballistic E-glass, ultra high-strength concrete, or a combination of the two (Figure 7-14). These panels are designed to stop mortar fragments and provide small arms protection. The MPS requires a reasonably level site and at least two people for setup. The system is portable, easily relocated, and able to protect straight-line areas or turn corners. Contact ERDC through the USACE Reachback Operations Center (UROC) (see Chapter 12) for availability, construction and additional performance details.

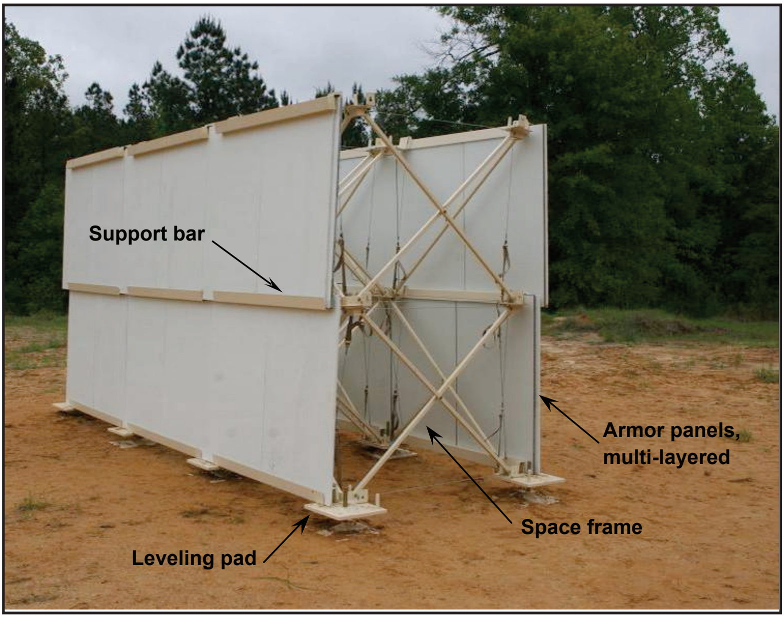


Figure 7-13. Key Components of the Modular Protective System.

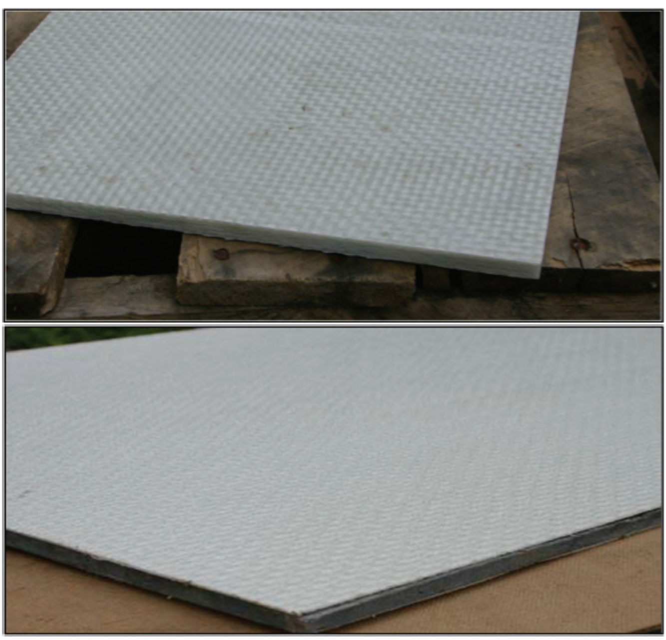


Figure 7-14. Modular Protective System Panels (top: Ballistic-grade E-glass Panel; bottom: Ultra High-Strength Concrete Panel with Fiberglass Facing)

Construction. The MPS requires no construction equipment beyond that necessary to ensure a relatively level foundation. The MPS has adjustable leveling pads that can compensate for minor grade deviations. Each 4 ft. x 4 ft. x 5 ft. (1.2 m x 1.2 m x 1.5 m) unit, including armor panels for heavy threats, weighs approximately 680 lbs. (308.4 kg). All MPS units, including armor panels, can be collapsed to a standard 463L pallet. Ten frames and associated components, enough to construct a 25 ft. (7.6 m) long x 8 ft. (2.4 m) tall wall, can be shipped on a single pallet. A four-person team can deploy a 10 ft. (3.0 m) tall MPS section in 18 minutes and recover the same section in 10 minutes (Figure 7-15).

Figure 7-15. Deployment of Modular Protective System

Performance. The recommended armor configuration consists of four panels: two inner, high strength concrete panels and two outer ballistic E-glass panels. In explosive field testing, this configuration provided 100% fragment protection from 60-mm mortar contact detonations through 120-mm mortars at a 10 ft. (3.0 m) standoff. Additionally, a similar armor combination of one E-glass and three concrete panels provided 100% protection from 122-mm rockets at a 15 ft. (4.6 m) standoff. Any four-panel combination will protect against small arms fire up to 0.30 cal armor piercing rounds.

Navy Physical Screen Protection System. The Navy developed an MPS version called Physical Screening Protection (PSP). This system meets Navy Expeditionary Combat Command and Seabee requirements. The primary differences between PSP and MPS are:

- The standard PSP kit includes its own modified Tricon II shipping container
- PSP armor panels are larger, ballistic-grade E-glass panels
- PSP frame components are galvanized for improved corrosion resistance
- The PSP is more easily assembled and its frame can be placed on uneven terrain

The four-panel (2 inner and 2 outer) PSP E-glass system provides full protection from small arms up to 0.30 cal ball ammunition. The PSP also provides full protection from near-miss (five feet) 82-mm mortar and partial protection (stops 99% of fragments) from near-miss (10 feet) 120-mm mortar.

E-Glass and U-Picket Walls

One expedient option for tent sidewall protection is the use of 3 to 6 layers of ballistic-grade E-glass panels supported by metal fence posts. This configuration can be located inside or outside the tents, but provides only 4-ft. of vertical protection for fragments. Individual panels (NSN 9340-01-533-3758; Figure 7-16) are 4 ft. x 8 ft. x 1/2 in. (1.2 m x 2.4 m x 12.7 mm) thick (nominal). Steel U-picket fence posts (NSN 5660-00-270-1587) and fastening hardware are also required. A similar concept for compartmentalizing large-facilities is discussed in Chapter 8.

Construction. Walls are constructed with panels supported approximately every 3.5 feet (1.0 m) with the 4 ft. (1.2 m) dimension positioned vertically. Steel U-picket fence posts are driven a minimum of 12 in. (30.5 cm) into the ground (Figure 7-15). The fence posts are fastened to the E-glass by self-tapping screws or preferably with complete thru bolts and back side nuts.

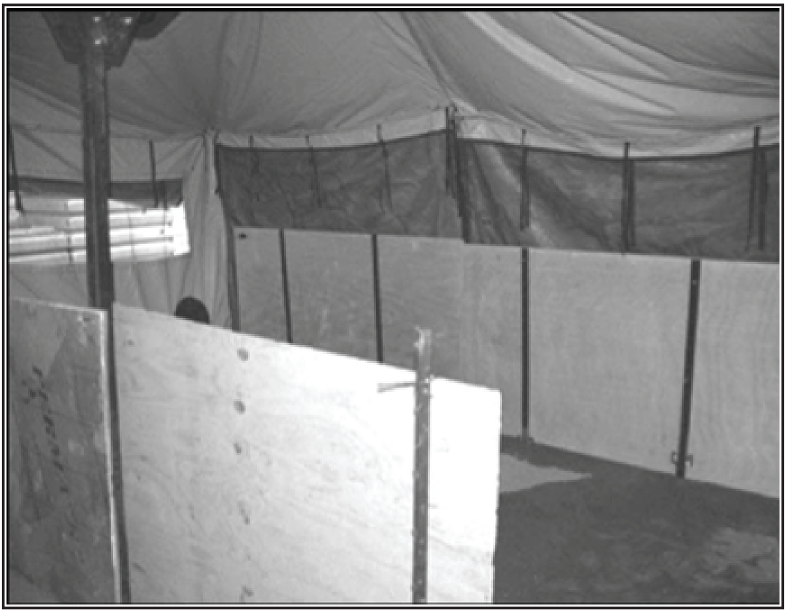


Figure 7-16. E-glass and U-picket walls for low height protection

Performance. In explosive tests, 3-layer and 6-layer E-glass panels stopped 97% and 100%, respectively, of 120-mm mortar fragments from detonations 10 to 13 ft. (3.0 to 3.9 m) away. The blast pressure caused wall movement and rotation; closer detonations could cause wall collapse. See Table 7-1 for small arms protection.

Ballistic

Small Arms. Sidewall protection from small arms may be required for assets near the FOB perimeter or exposed to line-of-sight threats from nearby tall buildings or high terrain. One prevention/deterrence method is to obscure these assets with screens. Another method that provides greater protection is to construct a shield or wall that defeats incoming fire. Table 7-1 provides material and thickness data to defeat small arms. Included are materials used in typical building walls or protective sidewalls. Also included are steel and ballistic grade E-glass that could be used alone or retrofitted to light walls to increase ballistic resistance.

Table 7-1. Small Arms Protection Characteristics of Various Materials (Compiled from Multiple Sources)

	Small Arms Projectile								
Material	9 mm M882 (NATO) Ball	5.56 mm x 45 M885 (NATO) Ball	7.62 mm x 39 M67 Ball	7.62 mm x 54R Type LPS Ball	7.62 mm x 51 M80 (NATO) Ball	7.62 mm x 51 M61 AP	.50 cal M2 & M33 Ball	.50 cal AP M2 & API-T M20	14.5 mm API
Mild Steel Plate thickness (inches)	1/4	11/16	7/16	13/16	9/16	13/16	1-1/4	ND	ND
Thickness of Armor Steel Plate (inches)	3/16	11/16	ND	ND	7/16	11/16	1	1-1/4	ND
Concrete Thickness (inches)	2	5	ND	ND	4	6-1/2	12	18	ND
Wythes of Nominal 4 in. thick brick	1	2	1	2	2	2	6	ND	ND
Layers of Nominal 1/2 in. thick E-glass, Ballistic Grade	1	3	1	ND	3	7	12	14	ND
Layers of nominal 8 in. □10 in. thick sandbags (inches)	1	2	2*	2*	2	2	3	3	3
8 in. thick Hollow CMU	Protects	Fails	Fails	Fails*	Fails	Fails*	Fails	Fails*	Fails*
8 in. thick Grout-filled CMU	Protects*	Protects	Protects	Protects	Protects	Protects	Fails*	Fails*	Fails*
4 in. Brick/2 in. Air/8 in. Hollow CMU	Protects*	Protects*	Protects	Protects	Protects	Protects	Fails*	Fails*	Fails*
Sand and Steel Plates	ND	ND	ND	10 in. of sand + 0.4 in Mild Steel	ND	10 in. of sand + 0.4 in Mild Steel	ND	10 in. of sand + 0.8 in Mild Steel	20 in. of sand + 0.4 in Mild Steel

NOTES: Table data based on single shots. Multiple shots in or near the same area may penetrate

ND = No data available

* = Inferred from other data

† = Other sand-filled containers of equal thickness can also be used. Data shown is for dry sand. For wet sand, use twice the indicated thickness.

Shoulder-Fired Rockets. Another common direct fire weapon is the shoulder-fired anti-tank rocket. These weapons fire a rocket-propelled grenade (RPG) with an explosive warhead attached to a solid fuel rocket motor. The RPG-7 system is a terrorist/insurgent weapon of choice due to low cost, ease of use, and availability.

RPGs employ several warheads, but most common is the high explosive anti-tank (HEAT) warhead. The HEAT warhead incorporates a metal-lined (often copper), conical shaped charge with high explosive packing (Figure 7-17). On detonation, the metal liner collapses to form a focused hypervelocity jet of molten metal traveling more than 20,000 feet per second and capable of penetrating a foot or more of armor steel. Also, the spent rocket motor continues along its flight path and can become a dangerous high-energy projectile. While HEAT rounds penetrate deeply, the penetration hole is small (Figure 7-18). Table 7-2 provides typical RPG HEAT warhead penetration into various materials.

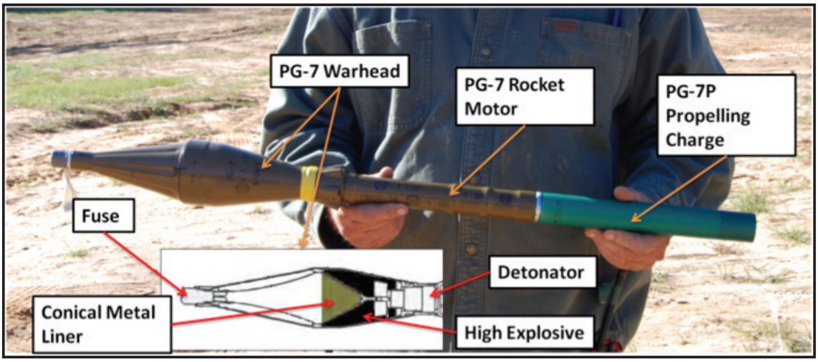


Figure 7-17. RPG-7 Components

Figure 7-18. Impact Effect of RPG-7 on CMU Wall

Table 7-2. Typical RPG Penetration Capabilities
(UFC 4-023-07, *Design to Resist Direct Fire Weapons; and UK MOD Military Engineering Volume II, Field Engineering, Pamphlet No. 2, Field Fortifications***)**

Material	Thickness
Steel	12 in. (0.3 m))
Concrete	40 in. (1.0 m)
Brick Masonry	46 in. (1.2 m)
Crushed Rock	38 in. (0.9 m)
Sand	60 in. (1.5 m)
Green Wood	66 in. (1.7 m)

Other than soil berms and soil-filled containers, sidewall protection of sufficient thickness to directly defeat an RPG is generally not practical in an expeditionary environment. However, if the RPG warhead can be pre-detonated at a distance from the target, then penetration is considerably reduced due to solidification, dispersion, and velocity reduction of the copper jet. Even relatively lightweight materials can function as pre-detonation or triggering screens.

Pre-detonation Screens

Employ pre-detonation screens (Figure 7-19) in conjunction with sidewall protection. While the screen detonates the RPG, the target must be capable of withstanding the spent rocket motor impact as well as other threats such as small arms projectiles and RAM fragments. An example combination of a pre-detonation screen and soil-filled metal container wall is shown in Figure 7-20.

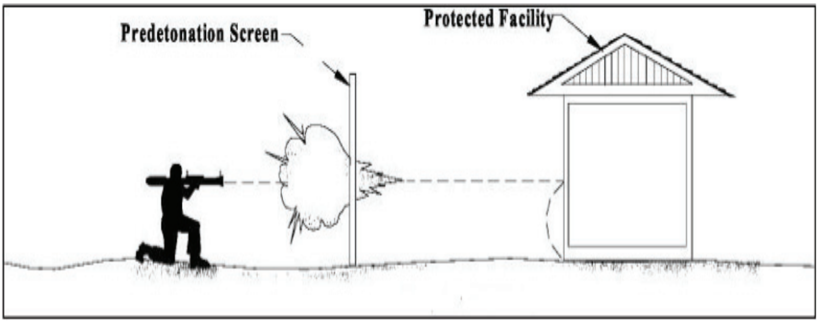


Figure 7-19. Pre-detonation Screen Concept (UFC 4-023-07)

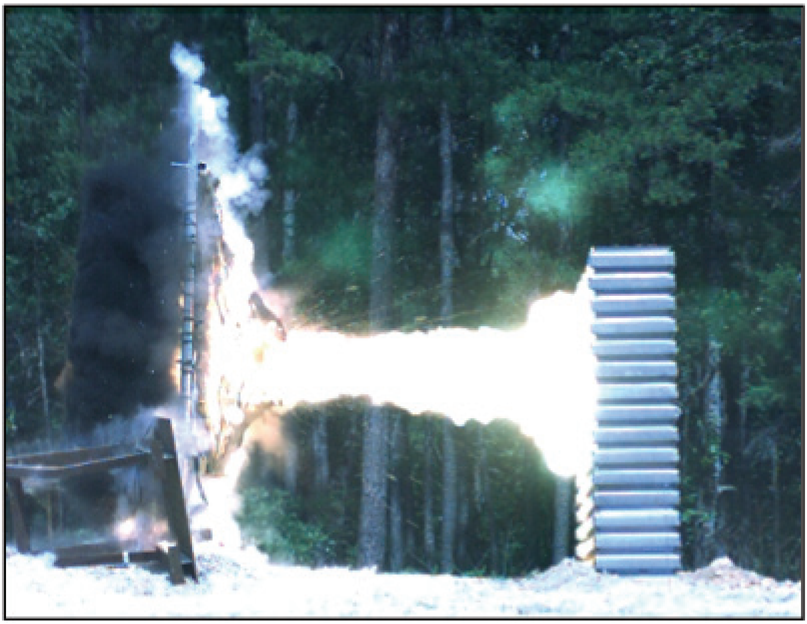


Figure 7-20. Pre-detonation screen (at left) causes RPG warhead detonation at a standoff and prevents perforation of the metal container wall (at right).

Pre-detonation screens should be as tall as the protected assets. This limits screens to intercepting rounds fired at the lower portions of tall assets. However, screens can be hung from a tall structure such as a guard tower to protect the occupants. Also, exterior building walls can act as pre-detonation screens if the protected assets are in interior rooms with walls that provide adequate protection against pre-detonated warheads.

Construction. Effective pre-detonation screens are constructed from a variety of materials including wood, metal fabric, expanded metal mesh, concrete, and masonry.

Wood screens can be made with slats or plywood panels at least 3/8 in. (9.4 mm) thick. Slats should be spaced no more than 1/4 in. `(6.4 mm) apart.

Spaces in metal fabric screens must be no more than 2 in. by 2 in. (50 mm by 50 mm) and the fabric a minimum of 9 gauge (3.8 mm). Expanded metal mesh with an areal density of at least 0.65 psf (31 Pa) and a maximum opening in the short direction of 0.75 in. (19 mm) successfully detonates the RPG.

The thickness of concrete or masonry pre-detonation screens need not exceed 1 in. (25 mm). These screens are only limited by structural stability requirements. However, concrete and masonry pre-detonation screens can disintegrate and produce flying hazardous debris.

Pre-detonation screens can constructed as free-standing vertical walls supported with posts or braces. Be sure to consider wind loads during design. Screen standoff distances away from sidewall protection measures usually range from several to tens of feet.

Performance. Standoff distances for typical wall construction to defeat common anti-tank RPG weapons are shown in Table 7-3. Additional pre-detonation screen information can be found in UFC 4-020-01, *DoD Security Engineering Facilities Planning Manual,* and UFC 4-023-07, *Design to Resist Direct Fire Weapons Effects.*

Table 7-3. Predetonation Screen Standoff Distances for Wall Materials (UFC 4-023-07, ***Design to Resist Direct Fire Weapons*****)**

Wall Material	Standoff Distance to Pre-detonation Screen
4 in. (102 mm) brick / 2 in. (51 mm) air gap / 8 in. (203 mm) hollow CMU	49 ft. (14.9 m)
8 in. (203 mm) grout-filled CMU or 8 in. (203 mm) brick	36 ft. (10.9 m)
6 in. (152 mm) reinforced concrete	25 ft. (7.6 m)
8 in. (203 mm) reinforced concrete	11 ft. (3.4 m)
12 in. (305 mm) reinforced concrete	7 ft. (2.1 m)

References:

UFC 4-023-07. *Design to Resist Direct Fire Weapons Effects*, 07 July 2008.

AFH 10-222v14. *Civil Engineer Guide to Fighting Positions, Shelters, Obstacles, and Revetments*, 01 August 2008.

AFH 10-222v1. *Guide to Bare Base Development*, 01 February 2006.
FM 5-103. *Survivability*, 10 June 1985.

ERDC/EL TR-08-29. *Technical Guidelines for Environmental Dredging of Contaminated Sediments*, September 2008.

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

ERDC/GSL Fact Sheet: *Field Expedient Fighting Positions.*

ERDC/GSL *Executive Summary: Investigation & Field Verification of Metal Revetments Systems Subjected to 80mm Mortar, 120mm Mortar, & 122mm Rocket,* November 2004.

ERDC/GSL Quick Look Report: *Protection from the Rocket Propelled Grenade.*

ERDC/GSL Quick Look Report: *ERDC Compartmentalization Techniques,* December 2004.

ERDC/GSL TR-10-10 *Development of the Modular Protective System: Validation of Protection from Direct Fire, Indirect Fire, and Bare Charge Threats,* 2010.

ERDC/GSL TR-10-33 *Physical Screening Protection Rapid Technology Transition Project: Direct and Indirect Fire Performance Evaluation,* September 2010.

ERDC/GSL TR-10-28 *Investigation into the Material Requirements for Mitigation of Indirect Fire Fragmentation from 82-mm and 120-mm Mortars*, 2010.

ERDC TR SL-90-5 *Penetration Tests of Masonry Walls with Small-Arms Ammunition,* April, 1990.

FM 3-06.11. *Combined Arms Operations in Urban Terrain,* 28 February 2002.

AFH 10-222v3. *Civil Engineer Guide to Expeditionary Force Protection*, 01 May 2008.

This page intentionally blank

CHAPTER 8
EXISTING STRUCTURES PROTECTION

FOB development often incorporates indigenous buildings for housing, office space, base exchanges, and recreation facilities. These buildings, however, may not provide acceptable threat protection. Also, expeditionary construction, which can be lightweight in nature, may not provide sufficient protection. Improved small arms and near-miss RAM protection can be achieved with the sidewall measures presented in Chapter 7. Similarly, the overhead cover techniques in Chapter 9 provide direct-hit RAM overhead protection.

If large blast loads such as large VBIEDs cannot be mitigated with standoff or with sidewall protection concepts, methods to improve the blast resistance of existing walls should be considered. These retrofit methods can be time and labor intensive, and often require structural engineering support. Still, the protective benefits provided may justify the effort. In addition, where overhead cover is not possible, facility protection can be improved with compartmentalization techniques.

Improved blast resistance is usually best achieved with interior or exterior retrofits alone or a combination. Structural assessments and retrofit planning and construction should address the following:

Inadequate blast standoff. If an existing structure must be occupied and is determined to have inadequate standoff, avoid exterior rooms on the building side(s) most vulnerable to VBIED attack. A structural engineer familiar with blast design and software tools such as AT Planner or BEEM (see Chapter 4) can estimate safe standoffs.

Glass fragmentation. Glass windows shatter at low blast loads and send hazardous fragments inward. Remove windows and cover or fill the openings with material that is as strong as the surrounding wall. Fasten the cover material to adjacent walls. If window removal is not an option, locate occupants away from line-of-sight glass fragment exposure.

Structural upgrades. Structural upgrades and blast resistant designs should be reviewed by a structural engineer. Improvised strengthening measures may cause more harm than good.

Load-Bearing Walls. Where a blast threat exists, avoid occupying buildings with load-bearing exterior walls. Failure of these walls can lead to roof and building collapse. These walls are also typically difficult to retrofit. Many buildings in contingency operations are likely to have load-bearing walls.

Connections. Structural connections are critical to many blast resistant retrofit concepts. Retrofits that are otherwise satisfactory may still fail due to weak or poorly installed fasteners. Fasteners tend to fail instantaneously during blast events. Connections should therefore receive special attention during retrofit construction.

Anticipated debris fields. Injuries to building occupants from explosive effects are usually not the result of blast overpressures; rather, debris from failed building components (such as walls and windows) and internal, non-structural items (bookcases, light fixtures, etc) cause most of occupant injuries. Debris near head height is typically most lethal. Design upgrades and retrofits to prevent component failure or “catch” the debris. Place loose items near the ground. Also, lighter, more crushable items are less dangerous than heavy, rigid items. Remove hazardous, non-structural components, both interior and exterior, from exterior walls and rooms. If necessary, secure larger items to the building’s primary structure.

Exterior Retrofits

Soil-Filled Container. In addition to providing sidewall ballistic and fragment protection, when properly designed and constructed soil-filled containers can be an effective blast retrofit method for existing structures. Chapter 7 describes soil berms placed directly against exterior walls. Soil-filled containers can be similarly employed. Figure 8-1 shows an exterior, soil filled container retrofit for blast protection.

- Construction. See Appendix G for materials and Appendix H for details on constructing soil-filled containers. As shown in Figure 8-2, these containers should be free standing and located near the wall. A small gap is needed between the wall and the containers to prevent any container settlement or movement from exerting pressure on the wall. Any gaps at the top and sides should be closed with plywood to prevent blast pressures from entering. Designs should be reviewed by a structural engineer.
- Performance. Soil-filled containers were placed in front of an 8-in. thick brick wall typical of those used as infill walls in Middle-Eastern concrete frame construction. The configuration was subjected to two

blasts from 4,000 lbs (TNT equivalent) at distances of 145 ft. (44.1 m) and 121 ft. (36.8 m). The soil-filled container and the brick wall were undamaged (Figure 8-2). This retrofit is most practical for ground floors and will protect occupants from small arms fire, shoulder-fired rockets, near-miss RAM detonations, and VBIED blast effects.

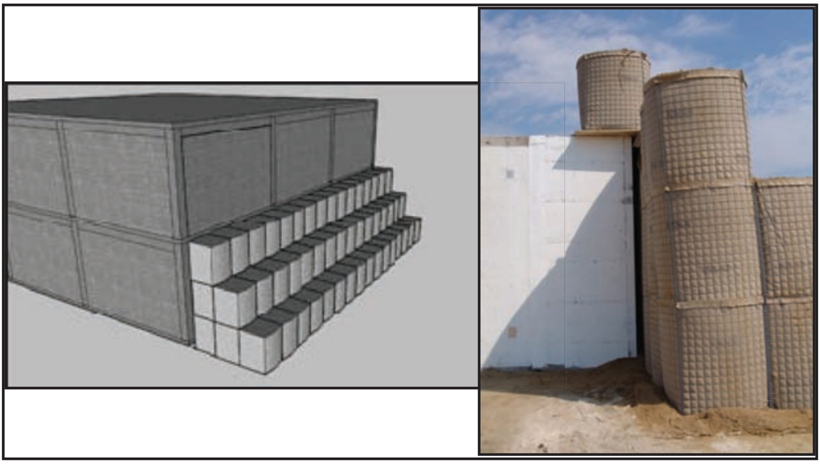


Figure 8-1. Soil-filled container exterior wall retrofit concept and test wall with gap.

Figure 8-2. Soil-filled container and interior of brick wall after blast test

Modular Concrete Wall. This exterior retrofit concept can be applied to reinforced, concrete-frame structures with concrete floors or roof slabs. Pre-cast, modular concrete walls are supported by bottom footings and a top leg that bears against the building floor or roof slab. Figure 8-3 shows a conceptual retrofit design. Note that the end opening would have to be closed to prevent blast penetration through the gap.

- Construction. A structural engineer with blast experience must design these walls. The specific design and construction will be based on

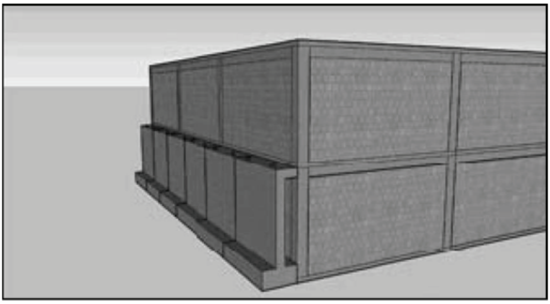


Figure 8-3. Modular concrete wall, exterior retrofit concept.

anticipated threat scenarios, structural details of the building, and available construction material properties.

- Performance. This retrofit is effective against large blast loads, small arms fire, and near-miss RAM. Depending on the employed design and existing structure walls, this retrofit may provide RPG protection.

Interior Retrofits

The interior side of exterior walls can also be retrofitted to provide blast protection. Table 8-1 provides summary information on several blast–resistant wall retrofit concepts. These retrofits apply only to the walls of non-load-bearing wall structures. Windows and doors may still fail and create hazards; these should be removed and openings sealed or personnel relocated away from these openings. Before proceeding with any building upgrade consult a structural engineer familiar with blast resistant design.

Geotextile Fabric Catcher. Existing masonry walls can be retrofitted with geotextile fabric curtains secured over the inside face. The fabric does not strengthen the wall, but traps the debris from the wall. Geotextile fabric is lightweight, easily installed, and inexpensive relative to full structural hardening.

- Construction. These fabrics cannot be applied to walls that require window or door openings since the fabric must stretch uninterrupted from ceiling to floor. Figure 8-4 shows a notional retrofit design.
- Performance. Qualitative test results and analytical studies indicate that geotextile fabric will significantly reduce debris volume, decrease explosive standoff distance, and reduce occupant casualties/injuries.

Table 8-1. Summary of Interior Wall Upgrade Concepts for Blast Protection				
Reftrofit System	**Brief Description**	**Applicable Wall Type(s)**	**Difficulty to Install**	**Load Bearing Walls?**
GeotextileFabric Catcher	A curtain of geotextile fabric anchored behind existing wall	Unreinforced Masonry	Low	No
Elastomeric Polymer (for Masonry) Spray-on polymer coating applied to interior wall surface	Spray-on polymer coating applied to interior wall surface	Unreinforced Masonry	Low to Medium	No
Elastomeric Polymer (for Wood Construction)	Spray-on polymer coating applied to interior wall surface	Wood Stud	Low	No
Reinforced Elastomeric Film	Peel and stick rolls similar to wallpaper anchored behind wall	Unreinforced Masonry	Very Low	No
Polyvinyl Chloride (PVC) Flexible Sheeting	PVC sheeting (commonly known as shower pan liner) anchored behind wall	Unreinforced Masonry	Very Low	No
Additional Wood Reinforcing	Plywood attached to interior stud walls, floor; dimension lumber to reinforce frame, trusses	Expeditionary Wood Structures (SEA Huts)	Low	N/A

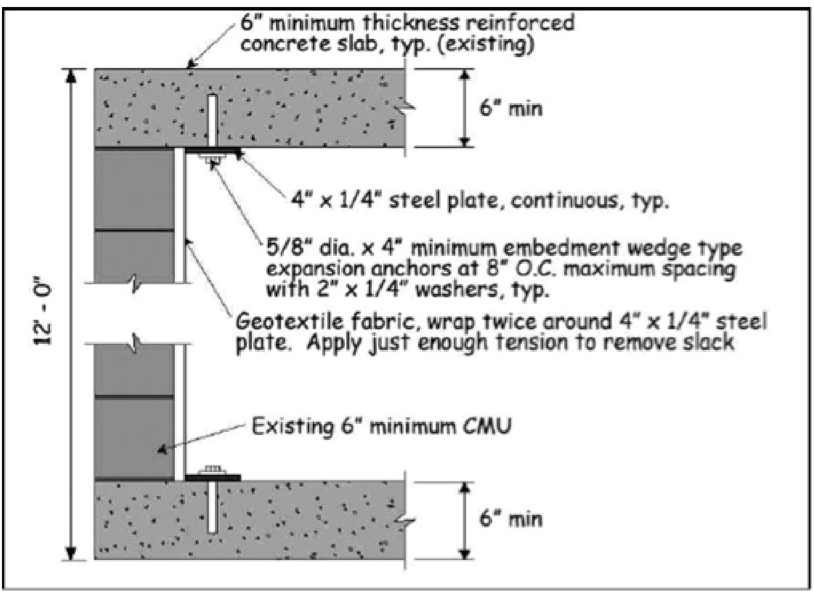


Figure 8-4. Geotextile fabric catcher system (side view)

Elastomeric Polymer. Unreinforced masonry walls and lightweight modular structures can be retrofitted with an elastomeric coating that improves blast resistance. This material is similar to those used in industrial coatings and spray-on, truck bed liners. Treated walls might still disintegrate from blast overpressure, but the polymer material remains intact and contains debris (Figure 8-5). This retrofit method employs lightweight materials and is inexpensive relative to full hardening techniques.

- Construction. The polyurethane coating is applied in three ways: the first requires special equipment and trained personnel (Figure 8-6) while the second is a straightforward trowel application (Figure 8-7). The third method uses an elastomeric sheet. The polymer coating typically cannot be applied over windows and doors. With modular office and housing units, interior steel frames must be installed in the structure, both the walls and the ceiling must be sprayed, and the entire structure must be ground-anchored.
- Performance. Tests have shown that debris is significantly reduced even though large wall deformation occurs. Polymer retrofits do not strengthen load-bearing walls against explosive events that would collapse the building.

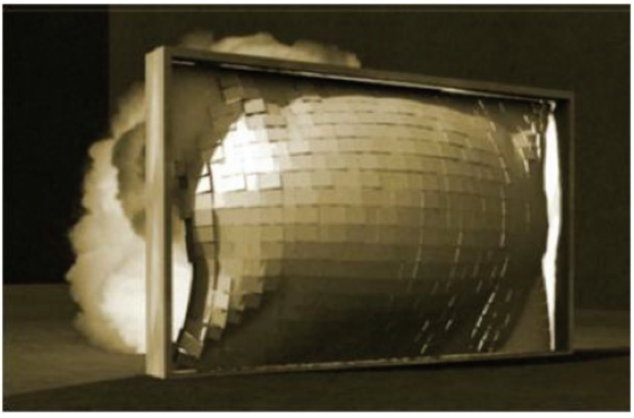


Figure 8-5. Wall blast debris trapped with elastomeric retrofit material

Figure 8-6. Spray on elastomeric polymer

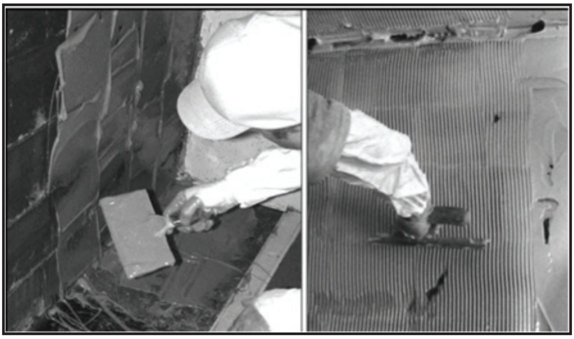


Figure 8-7. Trowel on elastomeric polymer

Reinforced Elastomeric Film. Reinforced elastomeric film consists of an open-weave aramid fiber reinforcement encapsulated in a polyurethane film backed with a pressure sensitive adhesive (PSA). The reinforced film is packaged in 48-in. (122 cm) wide rolls with a PSA applied to one face. The film requires only a simple peel-and-stick application to the wall similar to a wallpaper application and is then anchored to floor and ceiling slabs with steel channel and concrete expansion anchors (Figure 8-8). This retrofit technique should be designed by a blast engineer..

- Construction. Installation of the retrofit system consists of four steps:
  - Prime the wall with a paint roller to apply an aqueous polymer primer.
  - Apply the film by peeing off the backing paper while working the film up the wall. Overlap the floor and roof slab by 12 in. (30.5 cm) and vertical strips by 8 in. (20.3 cm).
  - Apply pressure with a roller to ensure good adhesion.

- Anchor film to the concrete floor and roof slabs with a steel stud and expansion bolts.

- Performance. The elastomeric film was applied to the interior of an 8-in. (20.3 cm) thick brick infill wall typical of Middle-Eastern concrete frame construction. After two 4,000 lbs (TNT equivalent) blasts at distances of 145 ft. (44.1 m) and 121 ft. (36.8 m), the walls experienced only moderate damage (Figure 8-9).

Figure 8-8. Reinforced Elastomeric Film retrofit application to brick wall at left; anchoring to floor slab at right.

Polyvinyl Chloride (PVC) Flexible Sheeting. This system is easily installed and consists of PVC flexible sheeting that meets ASTM D4551 standards. The sheeting is 40 mils thick, distributed in 4 – 6 ft. (1.2 – 1.8 m) wide rolls, typically used as a shower pan liner, and available at building supply stores. Cost is approximately $2.25 per square ft. The sheet is anchored at the top and bottom with 5-in. (12.7 cm) wide 11 gauge aluminum plate, an additional layer of sheeting, and a powder actuated nail gun (Figure 8-10). This retrofit should be designed by a structural engineer familiar with blast resistant design.

- Construction. Installation of the retrofit system consists of three steps:
  - Unroll sheeting and cut sections to match width and height of wall. Allow four inches of overlap between vertical strips and 12 in. (30.5 cm) overlap with the concrete slab at top and bottom. Also, cut additional strips approximately 12 in. (30.5 cm) wide to place beneath the anchor plates.

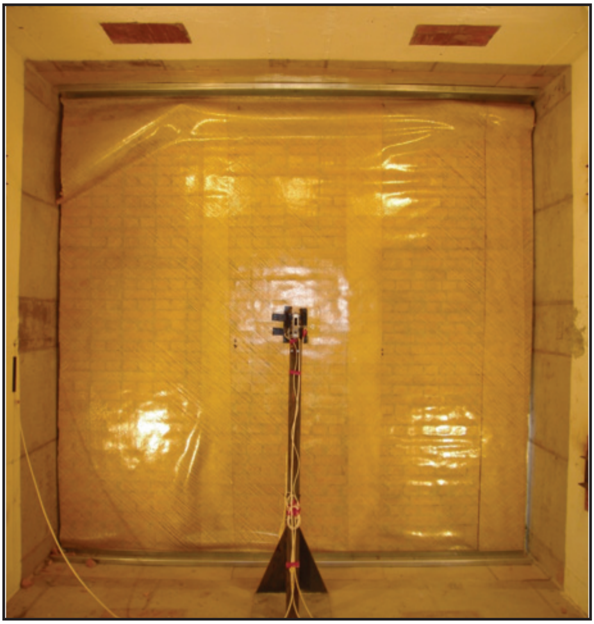


Figure 8-9. Damage to wall with reinforced film after two blast tests

  - Overlap strips 4 in. (10.2 cm) and bond together with PVC sheet adhesive. The sheet manufacturer will indicate the proper adhesive product.
  - Anchor the sheet to the concrete floor and roof slabs with additional strips of sheeting placed under the aluminum clamp plates. Nail to the slab with a powder actuated nail gun (proper nail loads will depend on slab condition.)

- Performance. The PVC flexible sheeting was applied to the interior of an 8-in. (20.3 cm) hollow CMU wall in an infill application like the above mentioned elastomeric wall. It was exposed to a 1,000 lb. ANFO blast at 75 feet (22.9 m). The wall failed, but the sheeting contained all the wall debris (Figure 8-11).

Figure 8-10. PVC Flexible sheeting application to CMU wall at left; anchoring to floor slab at right.

Figure 8-11. Damage to CMU test wall with PVC sheeting after blast test: exterior at left, interior at right.

Additional Wood Reinforcing. A field-constructed upgrade for expeditionary wood structures, such as Southeast Asia (SEA) Huts, is to add plywood and dimensional lumber for increased blast resistance. The wood reinforcement consists of 5/8-in. (1.6 cm) plywood sheets nailed to the floor, and 2 x 8 studs nailed along the top and bottom of the walls and the bottom chords of the roof trusses. This reinforces connections between all the building components and enhances roof strength. Doors should be installed to open outward. Figures 8-12 and 8-13 show this retrofit applied to a SEA Hut. This retrofit is further detailed in Air Force Handbook 10-2401, *Vehicle Bomb Mitigation Guide.*

- Construction – Installation of the retrofit system consists of the following:
  1. Cover windows with 3/4-in. (1.9 cm) plywood and reverse the doors to open outward.
  2. Add a second layer of 3/4-in. (1.9 cm) plywood to the existing floor. Attach this layer with nails 6-in. (15.2 cm) on center. Stagger the new layer of flooring panels opposite to the existing floor so that no seams overlap.
  3. Add 3/4-in. (1.9 cm) plywood to the interior walls. Nail the sheets at 6 in. (15.2 cm) on center.
  4. Attach a 2 x 6 floor plate around the interior periphery. Ensure that the narrow edge of the plate is butted firmly against the lower wall edge paneling. Nail through the floor into the floor joists at 6 in. (15.2 cm) on center.
  5. Attach 2 x 8 upper wall plates to all four walls. Butt the upper edges of the plates firmly against the lower edges of the existing lower truss members. Nail through the wall panels into the wall studs at 6 in. (15.2 cm) on center.
  6. Attach 2 x 8 rafter doublers to every other rafter with nails at 6 in. (15.2 cm) on center. Position the doublers such that half the width is suspended below the bottom of the existing lower truss members. Ensure the length of each rafter doubler fits tightly between the upper wall plates on either of its ends.
- Performance. This retrofit method was applied to a standard SEA Hut and exposed to a 12,200 lbs ANFO blast at 600 feet (183 m). The structure survived with minor damage (Figure 8-13).

Figure 8-12. Additional wood members added to SEA Hut. Plywood on floor and walls at left. Wall plates and rafter doublers at right.

Figure 8-13. Damage to strengthened SEA hut following blast test

Compartmentalization

Compartmentalization is a retrofit technique to reduce casualties from detonations that occur in high occupancy areas. Compartmentalization employs walls capable of ballistic protection to divide these areas into smaller sections containing fewer personnel (Figure 8-14). If a detonation occurs inside a compartment, the fragments and casualties are confined to that single compartment and perhaps the immediately adjacent compartment(s). Research also indicates that most blast hazards will not extend beyond a correctly designed compartment in which detonation occurs. Also, when augmented with sidewall protection, compartmentalization provides substantial personnel protection from near-miss blasts. Compartmentalization can also be used to protect exposed exterior critical assets such as generators and fuel tanks (See Figure 8-15).

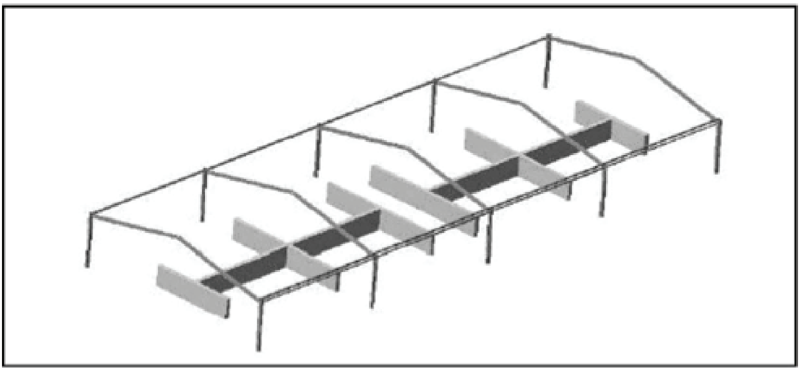


Figure 8-14. Interior compartmentalization design concept

Figure 8-15. Exterior compartmentalization for a critical asset (fuel tanks)

Detonations can result from PBIED or direct RAM hits. Mitigation of RAM through compartmentalization assumes that the incoming round passes through the roof and detonates within the compartment rather than as an airburst. This assumption may not always be valid. Live-fire tests have shown that some rounds with super-quick fuses will detonate on tent fabric. A better technique for direct-hit RAM protection is overhead cover (See Chapter 9) in conjunction with compartmentalization, assuming time and resources are available.

The minimum recommended height for compartmented interior walls is 5 ft. (1.5 m). Barriers tested for interior applications are discussed below. Table 8-2 prioritizes selection guidelines. These compartmentalization techniques all provide similar protection from fragmentation effects of 60-mm through 120-mm mortar and122-mm rockets.

Table 8-2. Compartmentalization Wall Selection Guidelines

Wall	Figure	Availability	Ease of Construction	Relative Cost	Aesthetics	Maintenance	Space
Soil-Filled Container Wall	8-16	1	1	1	4	4	4
Wooden Partition Wall	8-17	2	4	2	3	3	2
Soil-Plastic Bin Wall	8-19	3	3	3	1	2	3
E-Glass Wall	8-20	4	2	4	2	1	1
1-Most Preferred to 4-Least Preferred. Rankings are relative and not absolute.							

Soil-Filled Container Walls. Interior, soil-filled containers walls are an effective compartmentalization technique. However, practical restraints limit their utility in situations where hygiene is a concern. Figure 8-16 shows a small dining facility design with 2-ft. (0.6 m) wide fabric-lined containers. Metal containers of similar size can also be used for this application.

- Construction. Installation instructions are identical to those outlined for sidewall earth-filled barriers. Refer to Appendix H for construction details. These walls need not be anchored for stability. Wire and fabric containers 2 ft. by 2 ft. by 4 ft. (0.6 m by 0.6 m by 1.2 m) can be triple-stacked to a height of 6 ft. (1.8 m). These walls, however, require roughly three times the fill material and occupy four times the space of wooden or plastic bin walls. Also, soil-filled containers are very heavy and therefore impractical for raised floors. Hygiene must also be considered in a food service environment due to the presence of dust and loose container soil.
- Performance. A 2 ft. (0.6 m) wall thickness will stop all fragments from 60-mm through 120-mm mortars and 122-mm rockets.

Figure 8-16. Container wall compartmentalization design (bins pictured above are not yet filled with soil)

Wooden Partition Walls. Interior wooden partition walls are a simple, effective compartmentalization technique. Performance, however, is highly dependent on the employed fill material. Well-compacted dry sand is recommended. Figure 8-17 shows a wooden partition wall layout.

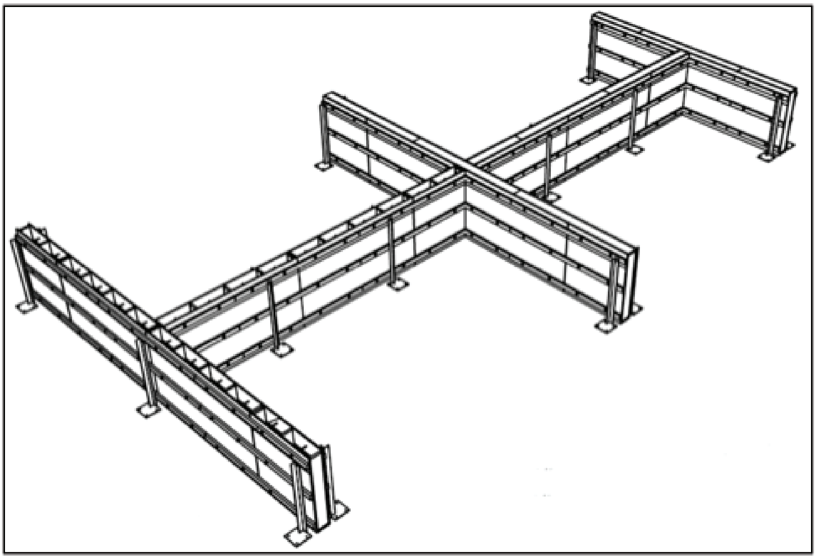


Figure 8-17. Wooden partition wall design.

- Construction. Prior to construction, evaluate the floor to ensure it can support a sand-filled wall that will weigh approximately 325 - 400 lb. per linear ft. Install intersecting walls every 20 ft. (6.0 m) for stability. Also, anchor the wall to the floor at its ends and midpoints. Wall motion must be minimized to reduce personnel hazards in adjacent compartments. The example wooden partition wall shown in Figure 8-18 is constructed from 3/4-in. (0.9 cm) plywood laid over 2 x 8 by 57 in. (1.4 m)-long studs, and 2 x 4 whaling along the outside. The 7.5 in. (19 cm) cavity formed is filled with soil and capped with 2 x 8 lumber. The fill material provides fragment mitigation. The walls and floor are connected to provide stability and prevent overturning from blast effects. Compacted dry sand is the best fill material. A mini loader is useful for placing fill in the small opening at the top of the wall. During the fill process, tap the wall sides with hammers to promote compaction and accelerate settling. Begin tapping immediately to ensure that lower fill material is properly compacted.
- Performance. The 7.5 in. (19 cm) soil-filled, wooden partition wall stopped all fragments (excluding wooden stud perforations) from 60-mm through 120-mm mortar and122-mm rocket detonations at a 7 ft. (2.1 m) distance from the bin. During live-fire tests, two 120-mm mortar fragments penetrated the 2 x 8 spacers separating the plywood panels. During 122-mm rocket tests, several fragments passed through the wooden cap at the top of the wall due to the wood’s reduced ballistic performance.

Figure 8-18. Wooden Partition Wall (Inset: corner joist detail)

Plastic Bin Wall. Interior, soil-filled, plastic bin walls provide rapid, effective compartmentalization. A simple layout is shown in Figure 8-19, similar to the wooden partition layout shown in Figure 8-16. Plastic bin walls (GSA# GS-07F-9503S) are approximately 7 ft. (2.1 m) long by 5 ft. (1.5 m) tall by 10 in. (25.4 cm) wide and filled with sand or other ballistic resistant material. Walls are keyed at each end to allow interlocking construction. Threaded caps at the bottom provide for quick fill removal.

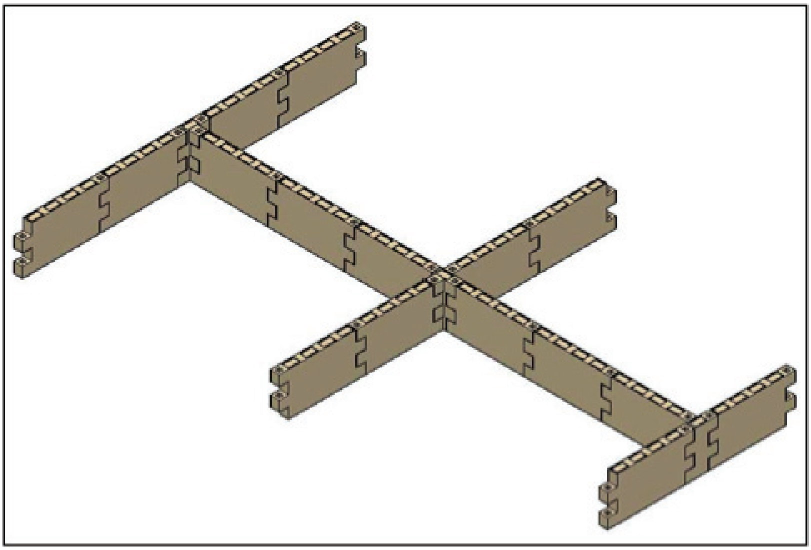


Figure 8-19. Soil-filled plastic bin wall configuration.

- Construction. Prior to construction of interior protective walls, evaluate the floor material (concrete slab, plywood, soil, etc.) for construction support characteristics. While soil-filled walls will weigh approximately 425 to 500 lb. per linear ft., unfilled bins can be carried by two people. Install intersecting walls approximately every 21 ft. (6.4 m) for stability. Place steel angle or other supports at the wall's free ends to reduce blast-induced motion; this reduces personnel casualties in adjacent compartments. Fill material affects the wall's fragment-defeating capability; compacted dry sand is most effective. Tap wall sides with hammers during fill to promote compaction and accelerate settling. Begin tapping immediately to ensure that lower fill material is properly compacted.
- Performance. A 5 ft. (1.5 m) tall plastic barrier with 10 in. (25.4 cm) of sand experienced no fragment penetration from 60-mm through 120-mm mortar and 122-mm rocket detonations at a 10 ft. (3.0 m) distance

from the bin. Research shows that fragments impacting the wall's main body are stopped when the sand fill is properly placed and void spaces are eliminated. The wall panel attachments, however, are susceptible to fragment penetrations at the 4 x 4 connections and void portions of the attachment joints.

E-Glass Walls. Interior E-glass walls with multiple layers (3-6) provide ballistic and fragmentation protection similar to soil-filled containers. E-glass panels, however, can be relocated. Figure 8-20 shows an E-glass compartmentalization design. E-glass walls are constructed from ballistic grade E-glass panels (NSN 9340-01-533-3758) supported by custom-manufactured steel stands. This configuration is similar to the interior sidewall protection concept discussed in Chapter 7.

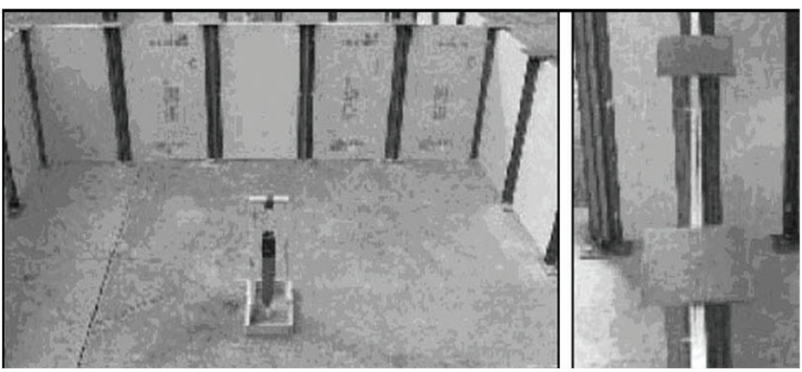


Figure 8-20. E-glass compartmentalization

- Construction. Walls are constructed of 4 ft. wide by 5 ft. tall E-glass panels that are supported at each edge by slotted steel stands. The steel stands consist of 4 pieces of angle iron welded to steel plates to form a vertical slotted frame into which the E-glass panels are inserted and attached to the angle iron with bolts 24" on center. The bottom plate of the frame is bolted to the structure's foundation.
- Performance. In 120-mm mortar tests, 3-layers and 6-layers of E-glass stopped 97% and 100%, respectively, of fragments from detonations 10-13 ft. (3 – 4 m) away. In 122-mm rocket tests, 3-layer and 5-layer E-glass panels stopped 95% and 99%, respectively, of rocket fragments from a detonation 10 ft. (3 m) away. However, against larger weapons such as the 122-mm rocket, E-glass walls anchored to wooden floors often topple due to a narrow base support.

References:

ERDC/GSL TR-02-18. *Fabric Retrofits of Concrete Masonry Exterior Walls – Blast Response Evaluation : (U.S.Israeli 1998 series, "Divine camel," Test 3)*, 2002.

ERDC/GSL *Executive Summary of Phase IV – Pre-Detonation and Fragment Shielding Experiments.*

ERDC/GSL *Compartmentalization Techniques,* December 2004.

ERDC/GSL *Installation Guidance for Plastic Bin, Soil Revetment Walls.*

ERDC/GSL *Experimental Validation of Compartmentalization Measures.*

AFH 10-2401. *Vehicle Bomb Mitigation Guide.*

This page intentionally blank

CHAPTER 9
OVERHEAD COVER

Overhead cover provides protection from direct hits of indirect fire RAM and is usually installed over inhabited structures or where personnel gather. In expeditionary environments, overhead cover is intended to protect temporary facilities with lightweight, cost-effective solutions that provide significant blast and fragment mitigation. The overhead cover concepts presented will not prevent penetration of delay-fused weapons, rocket motors that continue to travel post-detonation, and dud rounds. Protective layers that address such threats require more permanent hardening techniques that exceed the scope of this handbook.

Overhead Cover Protection Concept

Overhead cover research conducted by ERDC led to the development of specific RAM protection configurations for a variety of high population facilities such as dining facilities and billeting areas. This research produced overhead pre-detonation and shielding layer designs that have been applied to many FOB assets. The basic overhead cover concept shown in Figure 9-1 is to provide pre-detonation and shielding layers over the protected area. The pre-detonation layer causes incoming mortar or rocket fuses to detonate before penetrating the facility. This pre-detonation layer concept assumes a fast-fuse setting. The shielding layer, located at least 5 ft. (1.5 m) below the pre-detonation layer, mitigates blast and fragmentation effects (Figure 9-2). Figure 9-3 shows the aftermath of an actual attack on a dining facility. The overhead cover structure detonated the incoming mortar round and prevented damage to the building underneath.

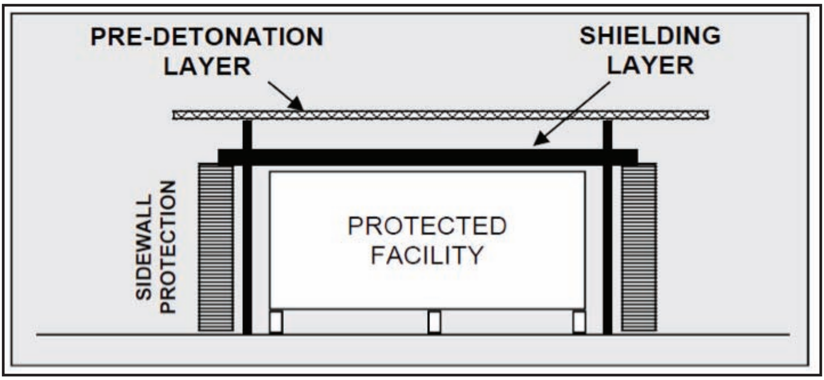


Figure 9-1. Overhead Cover Protection Concept

Overhead protection should always be used in conjunction with adequate sidewall protection to mitigate both direct hit and near-miss RAM detonations. Figure 9-4 shows a facility without overhead cover and how it is vulnerable to direct hits from RAM on the roof and near-miss RAM detonating on the ground inside the concrete barriers. The vulnerability zone (gray shaded arc) extends 180 degrees around the structure. Figure 9-5 shows how the overhead cover concept significantly reduces this vulnerability. The vulnerability zone is reduced directly above the structure. However, with barriers located away from the facility, a large area still exists to the sides where mortars and rockets can detonate and cause damage. Therefore, overhead cover construction should be supplemented with barrier walls of sufficient height placed tightly against the vulnerable sides of buildings. Figure 9-6 shows how using sidewall barriers greatly reduce the vulnerability zone (shaded area) around the structure. Be sure to consider all viable threats posed to each facility and determine whether existing barriers can be relocated, or whether new barriers must be acquired. When considering barrier locations, maintain viable entry/exit and accessibility for normal traffic and emergencies.

Figure 9-2. Overhead cover test: pre-detonation layer (top) and shielding layer (bottom)

Figure 9-3. Aftermath of an attack on a dining facility.

Overhead Cover Applications

Relative to sidewall protection (Chapter 7) and compartmentalization (Chapter 8), overhead protection measures are complex and require more time and resources to design and construct. They should be considered for all high population facilities and other critical assets such as the BDOC and main power plant switch gear (See Figure 9-7). Such measures significantly enhance protection and have been used extensively in current contingencies. Structural engineers should review or design overhead protective measures. Additional information and assistance with overhead cover protection is available via the UROC (See Chapter 12)

Custom Designs. Large overhead cover designs for existing structures are facility-specific. A generalized process, however, is described below. Examples of large overhead cover designs are shown in Figures 9-8 through 9-10.

1. Choose a fragment shielding layer. The choice of fragment shielding layer will depend on identified threats. Shielding layer materials shown in Table 9-1 are based on live-fire tests. Not shown is the 122 mm rocket. Even after detonation the large spent rocket motor of this round continues along the original flight path. Recent tests show that 12” of 5000 psi concrete is needed to stop the motor after predetonation.

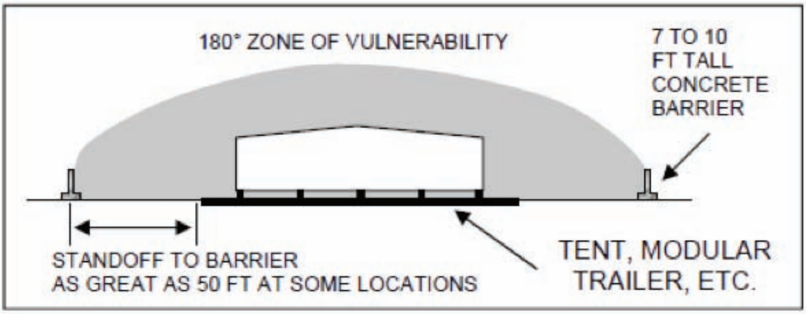


Figure 9-4. Existing facility with no overhead cover.

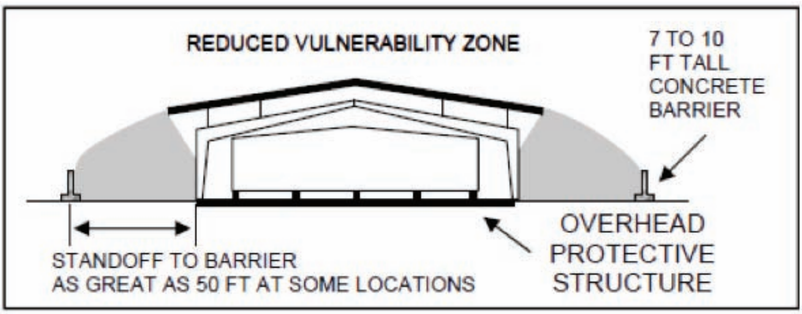


Figure 9-5. Overhead cover protection without tight sidewall protection.

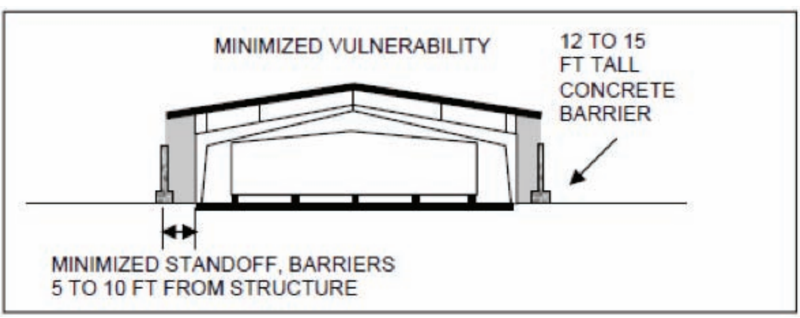


Figure 9-6. Overhead cover protection with tight sidewall protection.

2. Choose Shielding Structure Type. This supports the shielding layer and can be constructed from welded pipe, welded tube, bolted I-beam, steel frame, soil-filled containers, or other structural systems.

3. Identify Pre-detonation Structure Type. A pre-detonation deck is usually fastened to horizontal support beams (purlins) to prevent uplift displacement. Purlins must be able to support loads for given span, and should maximize width to provide adequate room for deck fastening.

4. Choose Pre-detonation Layer. Like the fragment shielding layer, pre-detonation layer selection should be threat-based. Pre-detonation layer materials are shown in Table 9-2 and are based on live fire tests. Not shown are test results for lightweight materials such as netting, welded wire mesh, expanded metal mesh, and chain-link fence. These materials do not consistently pre-detonate test rounds and should be avoided. Tent fabric was also tested and will sometimes cause pre-detonation, but is not recommended. The recommended materials have been tested to near normal impact conditions. Impacts at high obliquity have not been tested and may or may not result in fuze function.

Table 9-1. Material Options for Shielding Layers
(*ERDC C-RAM Overhead Protection Quick Look Report*)

Shielding Layer Material	60-mm Mortar	82-mm Mortar	120-mm Mortar	107-mm Rocket [3]
3-1/2 in. Sand	Y	Y	Y [1]	Y
1/4 in. Steel Plate	Y	Y	N	N
5/8 in. Steel Plate	Y	Y	Y	Y
2 Layers of Ballistic E-Glass	Y	Y	N	N
3 Layers of Ballistic E-Glass [2]	Y	Y	Y	Y

(“Y” indicates fragments were stopped, “N” indicates fragments penetrated)

1. Experiments show that 3 ½ in. sand will stop approximately 90 percent of fragments and 7 in. will stop nearly 100 percent of fragments.
2. Assumes a 5 ft. minimum space between pre-detonation and shielding layers. For spacing between 3.5 ft and 5 ft., use four Layers. For spacing between 2.5 ft. and 3.5 ft. use five layers.
3. Based on 120-mm mortar results.

Table 9-2. Recommended Material Options for Pre-detonation Layers (*ERDC Executive Summary of Phase IV, Draft AFRL Report on Fuze Initiation, TSWG Desert Cobra Final Test Report*)

Pre-Detonation Layer Material	60-mm Mortar	82-mm Mortar	120-mm Mortar	107-mm Rocket	120-mm Rocket
1 Layer of Ballistic E-Glass		Y			
22 ga. Corrugated Steel	Y	Y	N		Y
19 -- 20 ga. Steel Deck		Y		Y	
1/2” Cement Board	Y	Y	N		Y [6]
1/2” OSB	Y [5]	Y	N		Y
1/2” Plywood	Y	Y	Y		Y [4]
3/4” Plywood [1]	Y	Y	Y	Y	
4” Sandwich Panel (Sheet steel/Foam/Sheet steel) [2]	Y	Y	Y [7]	---	
1/4” Steel Plate [3]	---	Y	Y	---	

Based on live-fire tests. “Y” indicates round detonated,” N” indicate poor on no detonation, a blank indicates no test was conducted.

1. The recommendation for the 60mm mortar is based on tests against 1/2” plywood.
2. A 2 in. thick panel was also tested but was not as consistent as the 4” panel in detonating mortar rounds. The recommendation for the 82mm mortar is based on results of the 2 in. panel.
3. Potentially hazardous secondary debris may be generated when the 120 mm mortar pre-detonates on steel plate.
4. Based on the performance of ½” OSB.
5. Based on the performance of ½” plywood.
6. Based on performance of 3/8” cement board.
7. Based on tests where 2 of 3 rounds detonated.

Figure 9-7. Critical Asset (Switchgear) that may require Overhead Cover and Sidewall Protection.

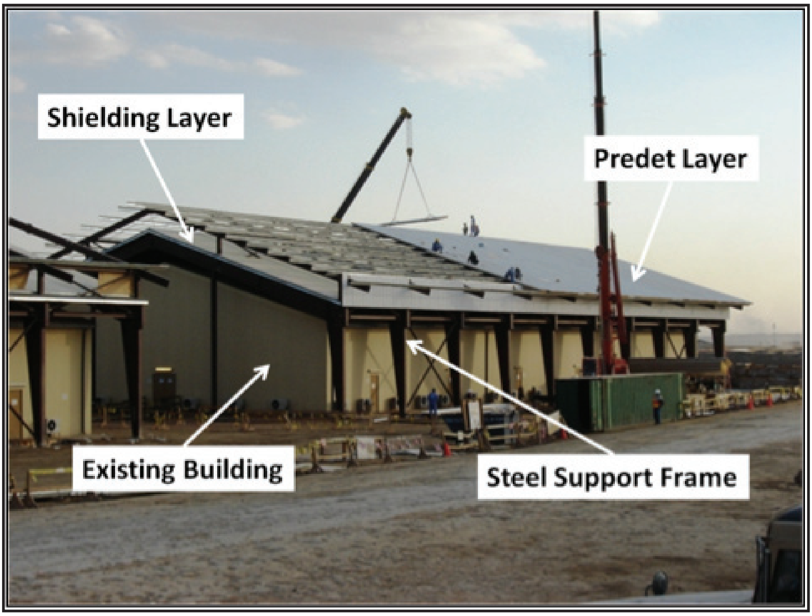


Figure 9-8. Overhead Cover Construction.

Figure 9-9. Overhead Cover with Sidewall Protection.

Figure 9-10. Container units protected with a large overhead cover structure

SEAhut Overhead Cover Retrofit. Overhead cover can be applied to the standard Theater Construction Management System (TCMS) South East Asia hut (SEAhut) as shown in Figure 9-11. This retrofit uses the existing 1/2 in. (12.7 mm) plywood roof as the pre-detonation layer. A shielding layer of ballistic-grade E-glass is then added beneath the roof joists. The shielding layer is supported on steel beams that rest on full height sidewall protection constructed from soil filled containers.

- **Construction**. Construct 10 ft. (3.0 m) tall, 4 ft. (1.2 m) thick load-bearing soil-filled revetment walls around the SEAhut. Insert steel (W6x9) beams through holes cut in the sidewalls of the SEAhut every 4 ft. (1.2 m) and rest them on the revetments. Fasten three layers of E-glass to the steel beams every 12 in. (304.8 mm) with self tapping screws before the roof joists are installed. Finally, install the remaining SEAhut roofing material as usual.
- **Performance**. This retrofit provides nearly 100 percent near-miss RAM protection. The destructive potential of direct-hit mortars is also reduced. In live fire tests with 120-mm mortars, only one fragment penetrated the 3-layer E-glass shielding. This retrofit should protect from a 122-mm rocket near-miss, but not a direct hit due to the penetration capability of the spent rocket motor.

Figure 9-11. SEAhut Overhead Cover Retrofit (Left: placement of shielding layer; Right: completed retrofit)

Modular Protective System (MPS) Overhead Cover Concept. The MPS (Chapter 7) also has overhead cover applications (Figure 9-12). The MPS with overhead cover is based on using MPS walls to support two open-web steel joist decks. The upper pre-detonation deck consists of sandwich foam panels while the lower shielding deck is E-glass panels. MPS overhead cover research is ongoing. Tests show that the MPS with overhead cover will provide protection from direct hits of up to 120mm mortars and 107 mm rocket warheads. Contact ERDC though the USACE Reachback Operations Center (UROC) (see Chapter 12) for current availability, construction and additional performance details.

Figure 9-12. Modular Protective System Overhead Cover Application.

Other Applications. Overhead cover using standard shipping containers for the pre-det and shielding layer have been used for guard towers (see Chapter 11). Most protective bunker and fighting position designs provide overhead protection from direct hits using a single protective layer of soil to detonate the incoming round and mitigate blast and fragment effects (see Chapter 11 and Appendix H).

References:

ERDC *C-RAM Overhead Protection Quick Look Report.*

AFH 10-222v14. *Civil Engineer Guide to Fighting Positions, Shelters, Obstacles, and Revetments*, 1 August 2008.

ERDC/GSL *Field Expedient Protective Positions,* June 2003.

Draft AFRL Report on Fuze Initiation, 2010.

TSWG Desert Cobra Final Test Report, 2010.

CHAPTER 10
SECURITY SYSTEMS

Electronic security systems, security lighting, and mass notification warning systems are basic components of FOB physical security systems. This chapter presents concepts, system types, and guidance on system selection. Specific equipment data is provided in Appendix G.

Selection of security systems should follow a well-planned, systematic process that produces an integrated protective system. Security systems should be designed with mutually supporting elements that prevent gaps or overlaps in responsibilities and performance.

Electronic Security Systems

The function of an Electronic Security Systems (ESS) is to detect and assess a threat and initiate a response by security personnel. ESS provides an integrated and layered approach to FOB protection that includes sensors, access control, closed-circuit television, data transmission, and annunciation. ESS are centrally controlled and operated by security personnel and used to accomplish the following:

- Permit more economical and efficient use of FOB security personnel
- Enhance the security force capability to detect and defeat intruders
- Provide the earliest practical warning to security forces of an attempted penetration
- Provide additional access controls for critical assets

ESS Selection. ESS requirements should be determined during FOB site selection and layout (Chapter 3). System integration and compatibility are major ESS design considerations. ESS selection is particularly dependent on site environmental conditions such as soil, terrain, and weather. These factors can adversely affect ESS performance or increase false alarm rates. To ensure an effective system is selected and designed, FOB planners should consider the following performance parameters:

- Coverage area
- False and nuisance alarm rates
- Probability of detection
- Alarm zone
- Delay time
- Maintenance requirements and technician availability

ESS Components. Typical ESS components are described below:

- **Access Control System (ACS).** The ACS ensures that only authorized personnel are permitted FOB ingress and egress. The ACS logs all normal access activities and alerts security forces to unauthorized entry attempts. ACS can interface with CCTV to assist in intrusion assessments.
- **Closed-Circuit Television (CCTV)**. CCTV is normally integrated into the overall ESS and centrally monitored. CCTV provides surveillance, assessment, deterrence, archival imagery, facial recognition, and intrusion detection.
- **Sensors/Intrusion Detection System (IDS)**. IDS elements include interior and exterior sensors and a CPU or local controllers. IDS also communicate and interface with ACS, CCTV, and the Security Operations Center.
- **Security Operations Center (SOC)**. The SOC houses a central monitoring, annunciation and assessment station for ACS, CCTV, and IDS. Operators assess alarm conditions and determine appropriate responses, to include security force disposition. The SOC is typically staffed 24/7 by trained personnel and may be co-located with other FOB functions.
- **Data Transmission Medium (DTM)**. DTM transmits information from sensors, access control devices, and video components to display and assessment equipment. A DTM is the data transmission link between sensor components and the SOC. DTM links should be secure, redundant, and rapidly repairable.

Sensors

Sensors are employed on FOB perimeters (including the ECP) and selected critical assets for early intrusion prevention, detection, and response. Most are integrated into ESS while others such as explosive detectors are stand-alone devices. Regardless, sensors provide security personnel with real time data that classify, pinpoint, and record intruder threats. See Appendix G, Materiel and Technology Support, for sensor information.

Sensor Types. Commonly available FOB sensors include:

- **Infrared.** Infrared sensors, also known as thermal infrared, are typically passive sensors that generate alarms when thermal radiance changes within the detection zone or imaged scene.
- **Microwave Radar.** These sensors generate an alarm when the receiver

detects a change in the microwave field. There are two types of microwave radar sensors: bi-static systems have separate transmitter and receiver units; mono-static systems combine transmit and receivefunctions in one unit. Radar sensors collect and display data as representations of fixed targets and moving target indicators.

- **Seismic.** Seismic sensors detect ground motion and are most effective in remote areas where human or vehicle-generated ground motion is rare. Seismic sensors also have tunnel detection applications.
- **Acoustic**. Acoustic sensors detect vehicle-generated noise. Acoustic sensors are not used to detect personnel. Acoustic sensors such as microphones are typically employed in conjunction with ground motion or seismic sensors.
- **Ground Motion.** Buried ground motion sensors such as seismic and fiber optic cable detect ground vibrations produced by foot traffic or moving vehicles in the immediate sensor vicinity.
- **Electrostatic Field/Capacitance.** These sensors consist of a vertical arrangement of horizontal wires that are free-standing or mounted to a chain link fence. An electrostatic field is generated between the wires and ground. The sensor detects intruders passing through this field. Intruders do not have to contact the wires.
- **Closed Circuit Television (CCTV)**. CCTV is the system of cameras, recorders, switches, keyboards, and monitors that allow viewing and recording of security events. CCTV is often used to augment security forces when manpower is limited. CCTV is most effective when linked to motion detectors and a dedicated monitoring system. Some CCTV cameras have pan, tilt, and zoom (PTZ) capabilities. PTZ cameras can be manually operated or set to automatically scan and zoom through a set path. CCTVs are usually not PTZ and only monitor a specific area. When mounted inside mirrored globes, CCTV can track personnel without their knowledge. Mirrored globes can also be employed as decoy CCTV systems.

Security Lighting

FOB commanders will determine the type of security lighting utilized based on the need for light discipline. Commanders may decide to enforce strict light discipline; if so, the type of lighting used for protection may be limited.

Lighting should be used to enhance threat detection, assessment, and interdiction, deter covert activities by illuminating potential concealment areas, and enable security force personnel to discretely observe FOB activities. Lighting should supplement other security means and measures such as fixed guard posts, patrols, fences, and alarms. Lighting is particularly important to increasing the effectiveness of ESS.

Lighting Selection. Requirements for protective lighting should be determined during FOB site selection and layout process. Factors to consider include: terrain, environmental/weather conditions, and security requirements. If lighting is impractical then additional compensating measures should be implemented. Figure 10-1 provides lighting concepts and best practices that can be used for lighting selection.

Types of Security Lighting. Four lighting types support FOB security systems: continuous, standby, movable (portable), and emergency. Light systems should also support IDS that rely on visibility, particularly CCTV.

- **Continuous Lighting.** The most common security lighting system is a series of fixed lights arranged to continuously illuminate a given area. Two primary methods of continuous lighting are glare projection and controlled lighting.

  Glare lighting is typically installed along a security perimeter and directed outward. Security personnel remain in comparative darkness behind the light. Glare lighting is considered a deterrent to intruders because it makes it difficult to see inside the protected area. Figure 10-2 shows glare projection lighting.

  With controlled lighting, the width of the lighted strip is limited and adjusted to fit a particular need, such as illumination of a wide strip inside a fence and a narrow strip outside, or floodlighting a wall or roof. Figure 10-3 shows the light directed downward, but the controlled beam aperture allows the guard to remain in darkness. Controlled lighting facilitates light discipline and reduces light pollution on adjacent roadways.

- **Standby Lighting**. Standby lights are either automatically or manually activated in response to suspicious activity or IDS alarms. Standby lights do not offer the constant deterrent of continuous lighting, but require far less energy. Motion-activated lighting can be very effective in deterring intruders as it is turned on by the intruder’s movement into a protected area.

SECURITY LIGHTING CONCEPTS AND BEST PRACTICES

- □ Security lighting is most effective when it adequately provides glaring light in the eyes of the intruder but does not illuminate security forces
- □ High-brightness contrast between intruder and background should be a primary consideration
- □ The volume and intensity of lighting should vary according to the surfaces to be illuminated
- □ Dark, dirty surfaces, or surfaces painted with camouflage paint require more illumination than surfaces with clean concrete, light brick, or glass
- □ Rough, uneven terrain with dense underbrush requires more illumination to achieve a constant level of brightness than do desert landscapes
- □ In cases where light discipline is strictly enforced, an alternative to bright illumination is the use of night vision devices and infrared detection systems
- □ In many cases illumination requirements for closed circuit television (CCTV) will drive lighting requirements
- □ Direct lighting toward likely avenues of approach and provide relative darkness for patrol roads, paths and posts and minimize exposure of security force personnel at ECPs
- □ Illuminate shadowed areas caused by structures within or adjacent to critical assets and restricted areas
- □ Avoid drawing unwanted attention to critical assets/restricted areas
- □ Provide overlapping light distribution
- □ Select lighting that resists the effects of environmental conditions; all components should be located to provide maximum protection against intentional damage
- □ Design lighting to be expandable so that future ESS requirements (i.e., CCTV) and recognition factors can be installed

Figure 10-1. Security Lighting Concepts and Best Practices

- **Movable Lighting.** Movable lighting (stationary or portable) consists of manually operated light systems. This type of lighting normally supplements continuous or standby lighting.
- **Emergency Lighting.** Emergency lighting may duplicate the above systems. Emergency systems are normally employed during power failures or other events that render normal systems inoperative. Emergency lighting is powered by dedicated generators or batteries.

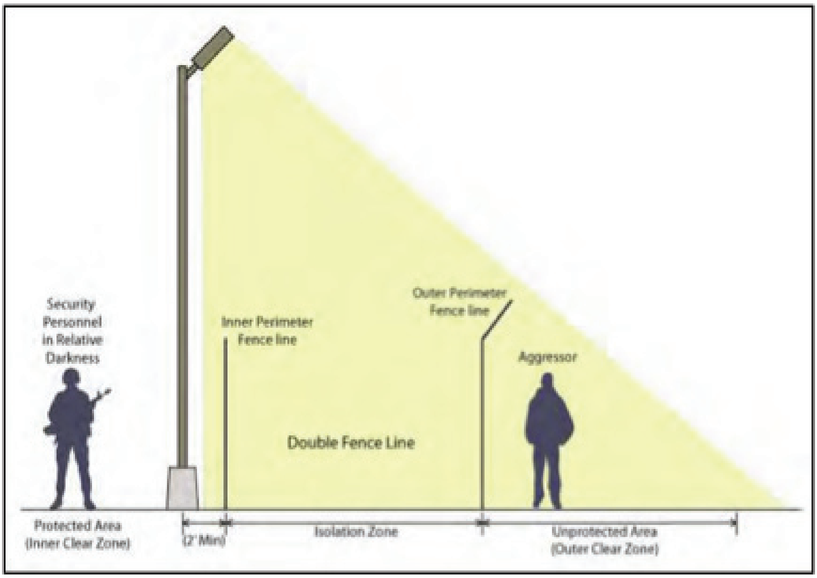


Figure 10-2. Example of glare projection lighting for a double fence line (UFC 3-530-01)

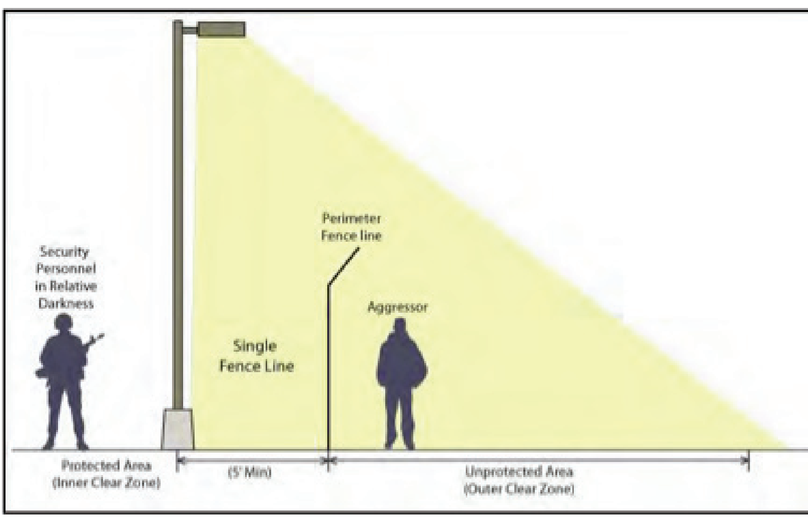


Figure 10-3. Example of controlled lighting for a single fence line (UFC 3-530-01)

Security Lighting Applications. Specific application considerations are detailed below.

- **Perimeter Lighting**. Perimeter lighting can be continuous or standby, with controlled glare projection as defined by SOP. Perimeter lighting includes exterior and interior clear zones adjacent to the fence or, in some applications, the area between dual fence lines. Light poles, power circuits, and controls should be sited within the protected area. Pole locations should not interfere with clear zone patrols.
- **Critical Assets/Restricted Areas.** Lighting installed and focused to illuminate critical assets and restricted areas assist security force surveillance and deter intruders. These areas or structures may include parking areas, storage areas, power, and water distribution systems
- **Guard Posts and Overwatch Positions.** Guard posts and overwatch positions should have interior lighting to perform security duties. Interior light levels, however, should remain low relative to exterior levels to minimize adversary surveillance and targeting of security personnel. This prevents potential mirroring or reflection effects that could limit outward visibility while increasing guard exposure. Limited individual workstation lighting can remain at normal levels, but shielding of interior lights might be necessary to minimize reflections on the window glass. Light intensities should be adjustable and colored lights should be avoided.
- **CCTV**. Cameras respond to light differently than the human eye. Glare and high contrast limit a camera's effective range. Uniform illumination is vital to limit camera saturation and improve CCTV system performance. Light sources are best located above the camera.

ECP Lighting Considerations. Within the ECP, the lighting requirements vary, depending on the type of zone and light discipline restrictions. Unified Facilities Criteria (UFC) 4-022-01, Security Engineering: Entry Control Facilities/Access Control Points, provides specific details and requirements concerning security lighting at ECPs and recommends foot-candle capabilities.

- **Approach Zone Lighting.** The approach zone requires typical roadway lighting with enough intensity that pedestrians, security personnel, roadway islands, barriers, signage, and other hazards are visible. Lighting should not be directed in the driver's eyes and should not backlight important signage or security personnel. Transitional lighting is necessary on approaches to the ECP so that drivers are not blinded during arrival and departure. Additional lighting should illuminate pedestrian lanes and allow security personnel to observe approaching pedestrians.

- **Access Control Zone Lighting.** Area lighting provided in the vicinity of the search facilities should be at a higher level to facilitate identification and inspection procedures. The lighting should illuminate the exterior and interior of a vehicle. In addition to good vertical illumination, additional task lighting may be necessary for adequate identification of vehicle occupants and contents. Such lighting should be directed across the roadway; then illuminate the roadway in front of the guardhouse, the driver, and the security personnel. Lighting may also be mounted at or below pavement level to facilitate under-vehicle inspection. Lighting should originate behind the guard and illuminate incoming vehicles. Different luminance and brightness levels could lead to eye strain and reduced security personnel performance.
- **Restrike or Restart Capability.** An important consideration with ECP lighting is the restart, or restrike, time for the selected lamps. Restart occurs when a lamp experiences a loss of power and there is a delay before backup power restores power to the lamp and triggers the subsequent restrike or restart of the lamp. As an example, high intensity discharge (HID) lamps are more energy conserving than incandescent lamps; however, they require several minutes to warm up and restart after power is interrupted. This warm-up period could be 15 to 20 minutes, an unsatisfactory delay for high-threat security operations. The selection of light sources, especially in the access control zone, should include an evaluation of restart or restrike time. It may be necessary to provide lamps and auxiliary equipment with rapid startup and restrike time to ensure minimal adequate lighting in the event of a power interruption. Consider LED and fluorescent lamp systems in lieu of light sources that require re-lighting periods.
- **General Requirements.** The ECP should be provided with multiple, redundant lighting to ensure that the loss of a single luminary does not seriously degrade the total lighting available for security personnel. The lighting at the ECP should be designed as controlled lighting to increase traffic safety. Glare projection, or glare lighting, should be avoided where a safety hazard would be created.

Electrical Requirements. Backup power is required for critical, pre-determined lighting systems, particularly emergency lighting. Backup systems vary in power output and cost. Generators are common and among the simplest, least expensive power sources. However, short periods of darkness after an outage can be expected before the generator activates.

An uninterrupted power supply (UPS) is an independent battery source that provides instantaneous backup power. UPS systems are expensive and are best employed in support of critical lighting systems where uninterrupted visibility is required.

Mass Notification Systems

To reduce the risk of mass casualties, FOBs must have the capability to notify personnel of threats. Mass notification provides real-time information and instructions to FOB personnel with intelligible voice communications, possibly supplemented with visible signals, text, and graphics, and other communication methods. While mass notification systems can be used for general purpose announcements, the most important function is to indicate life-threatening emergencies and instruct personnel of appropriate response actions. Voice communications are superior to coded tone systems.

Mass notification systems and FOB communications infrastructure must be compatible and integrated. Implementation plans should conform to criteria in UFC 4-021-01, *Design and O&M: Mass Notification Systems*.

Wide Area Mass Notification System. Wide area mass notification systems are installed to provide real-time information to FOB personnel. These systems include subsystems such as central control stations, high power speaker arrays, communication links, and ancillary equipment. Installation requirements are FOB-specific.

Outdoor mass notifications are normally issued by high-power speaker arrays. Redundant controller and communications links are encouraged. Wide area systems can also interact with telephone dialers, tone alert systems, computer network alerting systems, pagers, facsimile machines, and vehicle traffic signs. Text messaging and computer notifications are effective for large groups and off-site personnel. Desktop notifications allow more complex information to be conveyed.

Giant Voice System. Giant Voice systems provide siren signals, and pre-recorded and live voice messages. These systems are most useful for outdoor mass notification to expeditionary structures and temporary buildings. These systems, however, may not provide intelligible voice signals throughout the FOB and are not recommended inside buildings.

Existing giant voice systems do not broadcast well between multi-story buildings in high population areas. Consider newer speaker technologies for these areas. Closer spaced and less powerful speaker arrays are often required to enhance intelligibility.

Individual Building Mass Notification System. Individual building mass notification systems provide real-time information to building occupants and can be connected to wide area systems.

Telephone Alerting System. Telephone alerting systems can supplement mass notification in small facilities such as housing. Telephone alerting systems should not be outsourced to HN personnel or contractors.

References:

UFC 3-530-01. *Design: Interior and Exterior Lighting and Controls*, 22 August 2006.

UFC 4-021-01. *Design and O&M: Mass Notification Systems*, 09 April 2008.

FM 3-19.30. *Physical Security*, 08 January 2001.

CHAPTER 11
BUNKERS, TOWERS, AND FIGHTING POSITONS

FOB bunkers, towers, and fighting positions should be designed to protect personnel from the typical threat weapons found in operational environments. These structures are typically designed based on commander requirements to meet the desired level of protection. Expedient field designs are also common, but should be reviewed by a structural engineer prior to employment to ensure they are safe to occupy.

Bunkers

Bunkers offer protection from direct and indirect fire weapons effects. Both above- and below-ground bunkers are typically constructed of reinforced concrete, soil-filled revetment material, or timber. A bunker design must be functional while enhancing occupant protection. Certain prefabricated or modular bunker assemblies allow rapid construction, placement flexibility, and have proven effective. Normally bunkers are used to temporarily protect personnel during an attack or if an attack is imminent. For planning purposes, recommended occupancy criteria is 5 square feet of floor area per person for two hour occupancy and 20 square feet/person for 24 hour occupancy.

Concrete Bunkers. An improvised, reinforced-concrete bunker design, commonly known as a SCUD bunker, has proliferated in current theatres of operation. The bunker is typically constructed of reinforced concrete "C" sections with Jersey barriers placed across the ends. Sandbags are placed around the bunker body and in front of the barriers as shown in Figure 11-1. Sandbags increase fragment protection from near-miss detonations.

Figure 11-1. Improvised concrete culvert bunker.

The above design fails to fully shield the bunker entrances. Occupants are exposed to line-of-sight fragmentation from rounds detonated between the Jersey barrier and bunker entrances. This exposure can be mitigated with reinforced concrete shields as shown in Figure 11-2. Entrance shielding can also be accomplished with buried bunker designs.

Figure 11-2. Shielded bunker design prior to placing sandbags or soil on sides and roof.

The shielded entrance design was tested against 82-mm and 120-mm mortar, and 122-mm rockets. Performance data are linked to soil cover employment guidelines below. The modular concrete bunker can also be constructed in multiple configurations and located on the ground surface or partially or fully buried. The water table depth, rainfall drainage, and how water will drain from the bunker should be considered before burying the bunker.

Soil cover employment guidelines include:

- Place 2 to 3 sandbag layers on the roof to defeat quick-fused 82-mm and 120-mm mortars. Without sandbags, an 82-mm mortar causes only minor spall hazards, whereas a 120-mm mortar causes significant spall hazards and potential breach.
- Cover or bury bunkers with approximately 48 in. (1.2 m) of sandbags or soil to defeat quick-fused 122-mm rockets.
- Place at least 2 sandbag layers along bunker walls for full blast and fragmentation protection from near-miss (4 ft./1.2 m) detonations of 82-mm and 120-mm mortars, and 122-mm rockets.
- Figures 11-3 and 11-4 provides dimension and reinforcing details for the bunker sections. Concrete compressive strength of 4,000 psi (6.9 kPa) is recommended. Sections are connected with steel straps (Figure 11-2). For additional design and performance details contact ERDC via the UROC (Ch.12) or see ERDC/GSL TR 08-29.

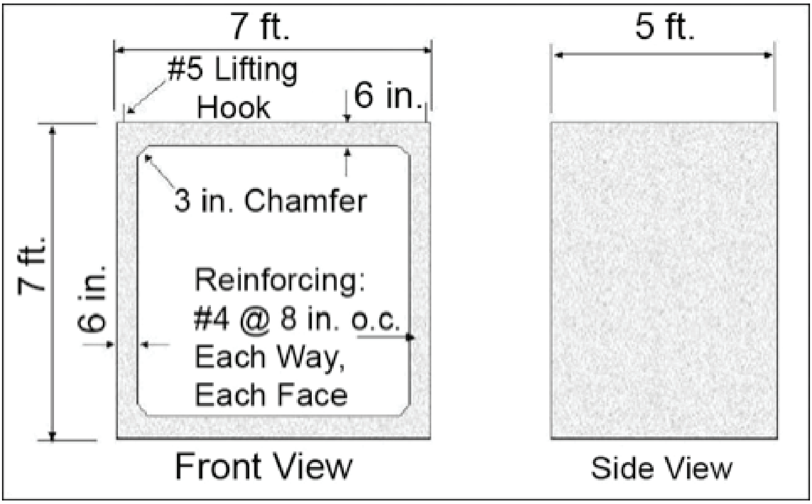


Figure 11-3. Primary concrete bunker module

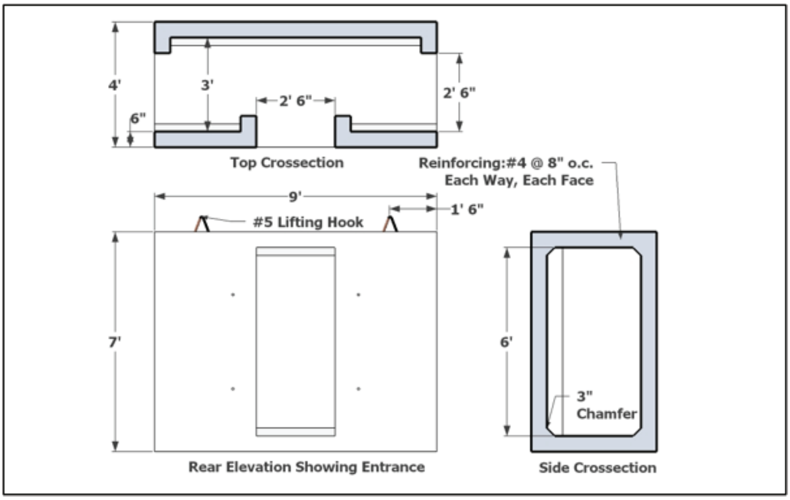


Figure 11-4. Entrance unit for modular concrete bunker

Belowground ISO/MILVAN Container Personnel Bunker. An ISO container can be employed as a below-ground personnel bunker (Figure 11-5). However, the container must be reinforced with steel frames as shown in Figure 11-6. Unreinforced containers may collapse under static loads or direct weapon impacts, exposing personnel to potentially lethal hazards. For additional construction details refer to the *Construction Guide for Reinforced Below-ground 40' Milvan Bunker* (USACE ERDC).

Figure 11-5. Below-ground ISO container bunker

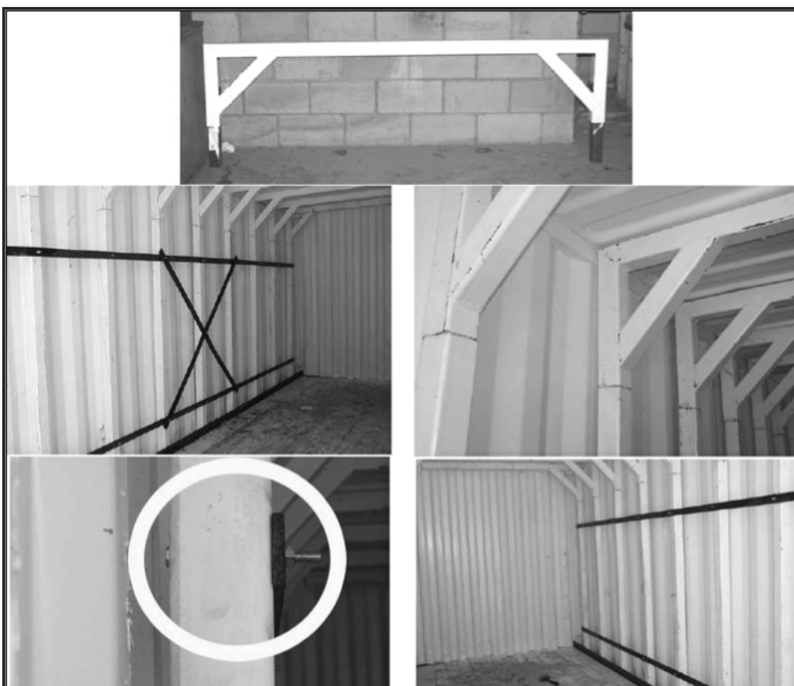


Figure 11-6. Underground bunker steel frame reinforcement assembly. Steel frame assembly and installation (clockwise from top: Upper portion of frame; frames installed at 2' o.c.; flat bar strips attached to frames; flat bar connected to frame with bolt-- note bolt head is on outside of frame; diagonal bracing in place)

Soil-Filled Container Bunkers. Soil-filled containers have many applications, including bunker construction. These bunkers will defeat 82-mm mortar direct hits and provide sidewall fragment protection from near-miss 120-mm mortar, 122-mm rocket, and 155-mm artillery munitions. Figure 11-7 shows a soil-filled container personnel bunker. Soil-filled container walls are also discussed in Chapter 7, Sidewall Protection. Appendix H, Soil-filled Container Applications, provides additional bunker design and construction details.

Figure 11-7. Aboveground 20 foot ISO/MILVAN Personnel Bunker.

Timber Bunkers. Timber bunkers can be constructed above-ground and partially covered, or below-ground. Numerous designs are presented in FM 5-103, *Survivability*. All designs employ soil cover for fragment and blast protection.

Properly constructed timber bunkers provide contact burst protection from 82-mm and 120-mm mortar, 122-mm rocket, and 152-mm artillery rounds. Figure 11-8 shows a partially covered timber bunker configuration. This design is exclusively for construction in soil or rock material that is capable of maintaining the original vertical excavation in all weather conditions. Figure 11-9 shows a typical, timber earth-covered roof design and its structural components. Table 11-1 provides data on stringer size and soil cover thickness necessary to defeat the listed munitions.

Timber bunker designs are adaptable to expedient, guard tower designs. The “Towers” section below details a common timber-and-plywood perimeter application.

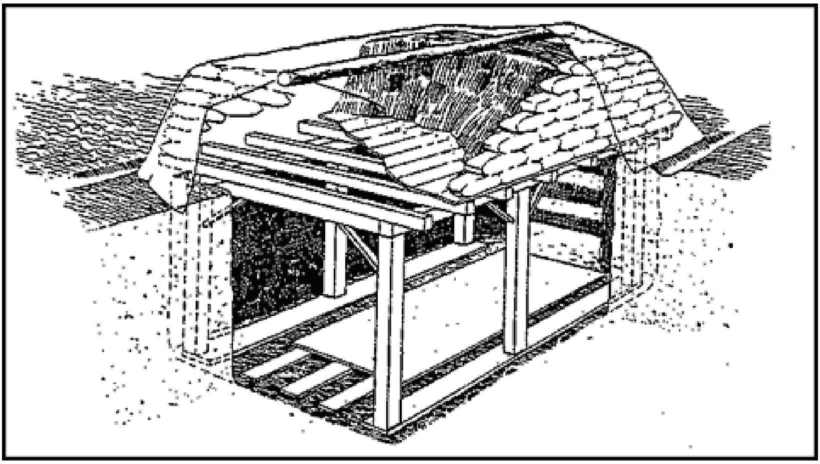


Figure 11-8. Partially covered timber bunker
(FM 5-103, *Survivability*)

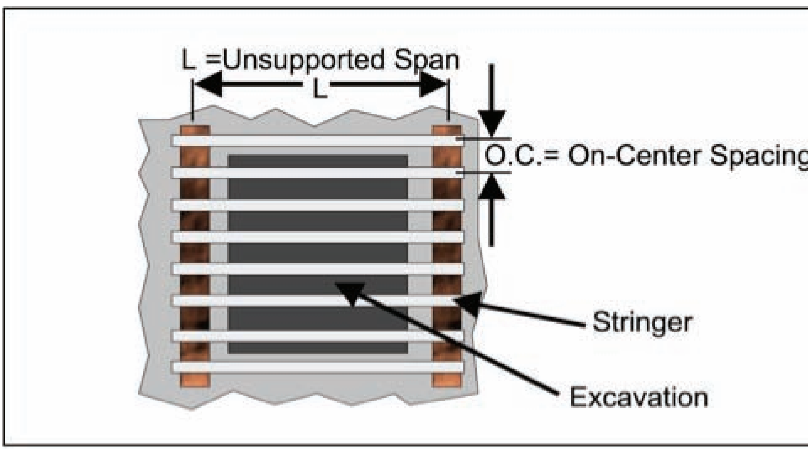


Figure 11-9. Timber bunker roofing design.

Table 11-1. Center-to-center Spacing for Wood-Supporting Soil Cover to Defeat Various Quick-Fuse Mortar Bursts (FM 5-34, *Engineer Field Data*)

	Nominal Stringer Size (in.) ▼	Depth of Soil, ft. (m) ▼	Span Length, ft. (m) ► 2 (0.6)	4 (1.2)	6 (1.8)	8 (2.4)	10 (3.0)
			Center-to-Center Stringer Spacing, in. (cm) ▼				
82-mm Contact Burst	2 x 4	2.0 (0.6) 3.0 (0.9) 4.0 (1.2)	3 (7.6) 18 (46) 18 (46)	4 (10) 12 (30) 14 (36)	4 (10) 8 (20) 7 (18)	4 (10) 5 (13) 4 (10)	3 (8) 3 (8) 3 (8)
	2 x 6	2.0 (0.6) 3.0 (0.9) 4.0 (1.2)	4 (10) 18 (46) 18 (46)	7 (18) 18 (46) 18 (46)	8 (20) 16 (41) 18 (46)	8 (20) 12 (30) 11 (28)	6 (15) 8 (20) 7 (18)
	4 x 4	2.0 (0.6) 3.0 (0.9) 4.0 (1.2)	7 (18) 18 (46) 18 (46)	10 (25) 18 (46) 18 (46)	10 (25) 18 (46) 18 (46)	9 (22) 12 (30) 10 (25)	7 (18) 8 (20) 7 (18)
	4 x 8	1.5 (0.5) 2.0 (0.6) 3.0 (0.9)	4 (10) 14 (36) 18 (46)	5 (13) 18 (46) 18 (46)	7 (18) 18 (46) 18 (46)	8 (20) 18 (46) 18 (46)	8 (20) 18 (46) 18 (46)
120-mm and 122-mm Contact Burst	4 x 8	4.0 (1.2) 5.0 (1.5) 6.0 (1.8)	3.5 (9) 12 (30) 18 (46)	4 (10) 12 (30) 18 (46)	5 (13) 12 (30) 18 (46)	5 (13) 11 (28) 16 (41)	6 (15) 10 (25) 12 (30)
	6 x 6	4.0 (1.2) 5.0 (1.5) 6.0 (1.8)	--- 14 (36) 18 (46)	--- 14 (36) 18 (46)	5.5 (14) 13 (33) 18 (46)	6 (15) 12 (30) 16 (41)	6 (15) 10 (25) 12 (30)
	6 x 8	4.0 (1.2) 5.0 (1.5)	5.5 (14) 18 (46)	6 (15) 18 (46)	8 (20) 18 (46)	9 (23) 18 (46)	10 (25) 18 (46)
	8 x 8	4.0 (1.2) 5.0 (1.5)	7.5 (19) 18 (46)	9 (23) 18 (46)	11 (28) 18 (46)	12 (30) 18 (46)	13 (33) 18 (46)
152-mm Contact Burst	4 x 8	4.0 (1.2) 5.0 (1.5) 6.0 (1.8) 7.0 (2.1)	--- 6 (15) 17 (43) 18 (46)	--- 6 (15) 16 (41) 18 (46)	--- 7 (18) 14 (36) 18 (46)	--- 7 (18) 12 (30) 15 (38)	3.5 (9) 7 (18) 10 (25) 11 (28)
	6 x 6	5.0 (1.5) 6.0 (1.8) 7.0 (2.1)	7 (18) 18 (46) 18 (46)	8 (20) 18 (46) 18 (46)	8 (20) 15 (38) 18 (46)	8 (20) 12 (30) 15 (38)	7 (18) 10 (25) 11 (28)
	6 x 8	4.0 (1.2) 5.0 (1.5) 6.0 (1.8)	--- 10 (25) 18 (46)	--- 11 (28) 18 (46)	--- 12 (30) 18 (46)	--- 12 (30) 18 (46)	6 (15) 12 (30) 17 (43)
	8 x 8	4.0 (1.2) 5.0 (1.5) 6.0 (1.8)	--- 14 (36) 18 (46)	--- 14 (36) 18 (46)	--- 16 (41) 18 (46)	--- 17 (43) 18 (46)	8 (20) 16 (41) 18 (46)

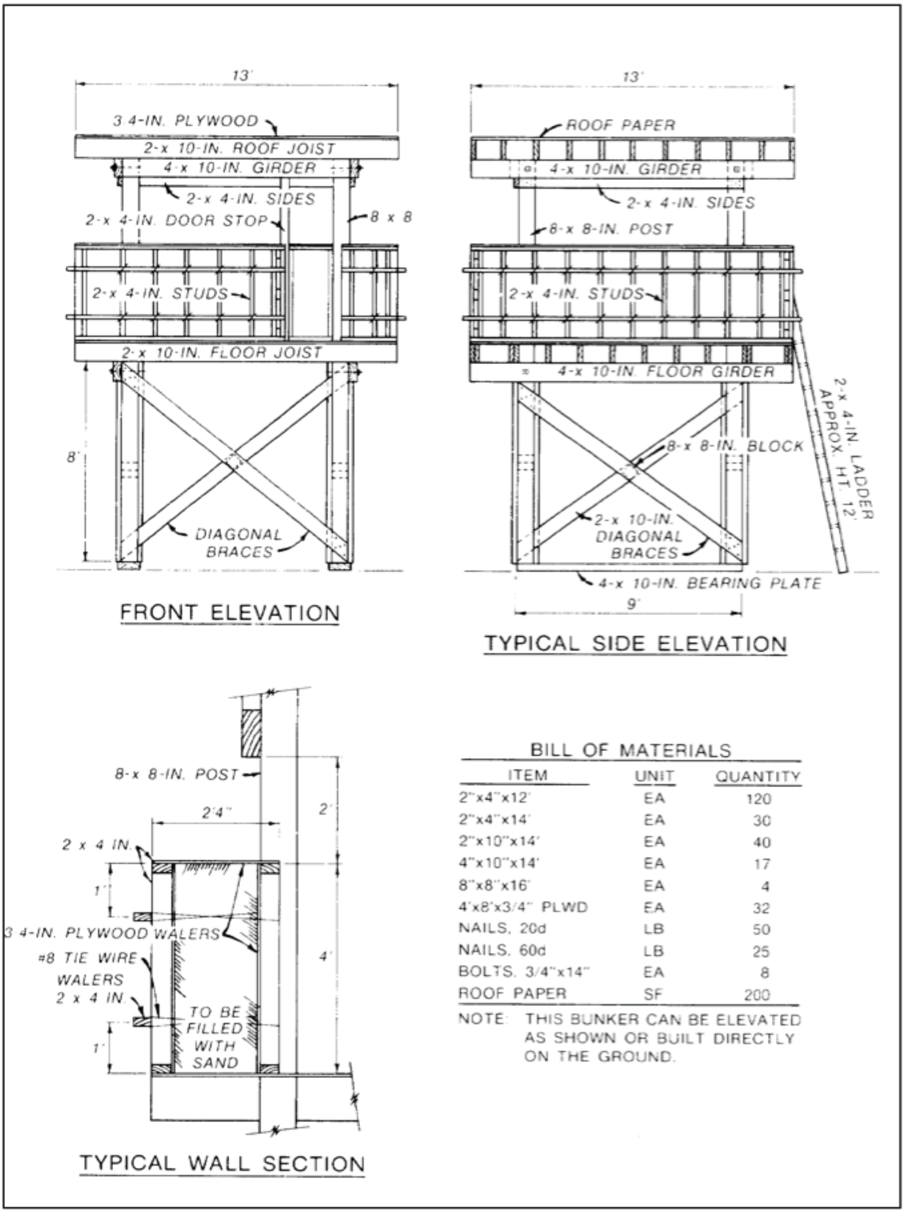
Note: The maximum beam spacing listed in Table 11-1 is 18 in. (457 mm). This precludes further design for roof material placed over the stringer. Use a maximum of 1 in. (25.4 mm) wood or plywood over stringers to support the earth cover for 82-mm burst; use 2 in. (50.8 mm) for 120-mm, 122-mm and 152-mm burst. Table information is based on *both* Dead Load and Blast Load Effects. Consult a structural engineer for further clarification.

Towers

Tower designs must be based on a physical site assessment, security requirements, and practical combat considerations that include:

- Maximum required occupancy to meet security requirements
- Required number of towers/observation posts
- Heating, ventilation, air conditioning (HVAC), and plumbing requirements
- Threat-based small arms protection for security force personnel
- Secure, reliable, redundant communications equipment and techniques that ensure uninterrupted contact with security personnel, particularly during combat operations
- Remotely or manually operated searchlight(s)
- Weapons compatible gun ports that cover the entire perimeter and clear zone
- Tower locations inside the FOB perimeter with a 30 ft (9.1m) minimum, inner clear zone.

Timber and Plywood Perimeter Bunker/Tower. This is an aboveground bunker design adapted for guard tower employment. Variants of this design have proliferated in current theaters of operation. Figure 11-10 shows a simple timber and plywood tower design. Figure 11-11 shows an operational tower of similar design with soil-filled containers around its base and overhead sandbags. The soil-filled containers provide a protected occupancy compartment on the ground and blast protection for the main support beams.



BILL OF MATERIALS

ITEM	UNIT	QUANTITY
2"x4"x12'	EA	120
2"x4"x14'	EA	30
2"x10"x14'	EA	40
4"x10"x14'	EA	17
8"x8"x16'	EA	4
4'x8'x3/4" PLWD	EA	32
NAILS, 20d	LB	50
NAILS, 60d	LB	25
BOLTS, 3/4"x14"	EA	8
ROOF PAPER	SF	200

NOTE: THIS BUNKER CAN BE ELEVATED AS SHOWN OR BUILT DIRECTLY ON THE GROUND.

Figure 11-10. Timber and Plywood Tower Design
(FM 5-103, *Survivability*)

Figure 11-11. Plywood guard tower (top) and with soil-filled containers and overhead sandbags (bottom).

CONEX Box Guard Tower. CONEX boxes can be employed individually or stacked to provide elevated guard platforms. The tower shown in Figure 11-12 is a variation of the timber/plywood tower. This design requires interior sandbags or other fragment resistant material to mitigate small arms and indirect fire threats. The Portable Guard Tower detailed in Appendix G is also a variant of this design.

Figure 11-12. CONEX Box Guard Tower

Freight Container Guard Tower. This US Navy design (Figure 11-13) consists of up to five stacked steel containers. These containers are approximately 8 ft. x 8.5 ft. x 20 ft. (2.4 m x 2.6 m x 6.1 m) and 5,000 lb (2,268 kg) empty weight. The bottom container is attached to large, cast-in-place concrete footings with anchor bolts. Additional containers are bolted to the container below to address conventional design loads. The top container is empty and acts as a pre-detonation screen against direct-hit RAM. A shielding layer on the top container floor resists downward fragment penetration. E-glass or similar fragment resistant materials are placed along the inside faces of the container walls to protect inhabitants against direct and indirect fire threats. Ballistic resistant glazing can also be employed over windows. Contact Naval Facilities Engineer Command for details (See Ch. 12).

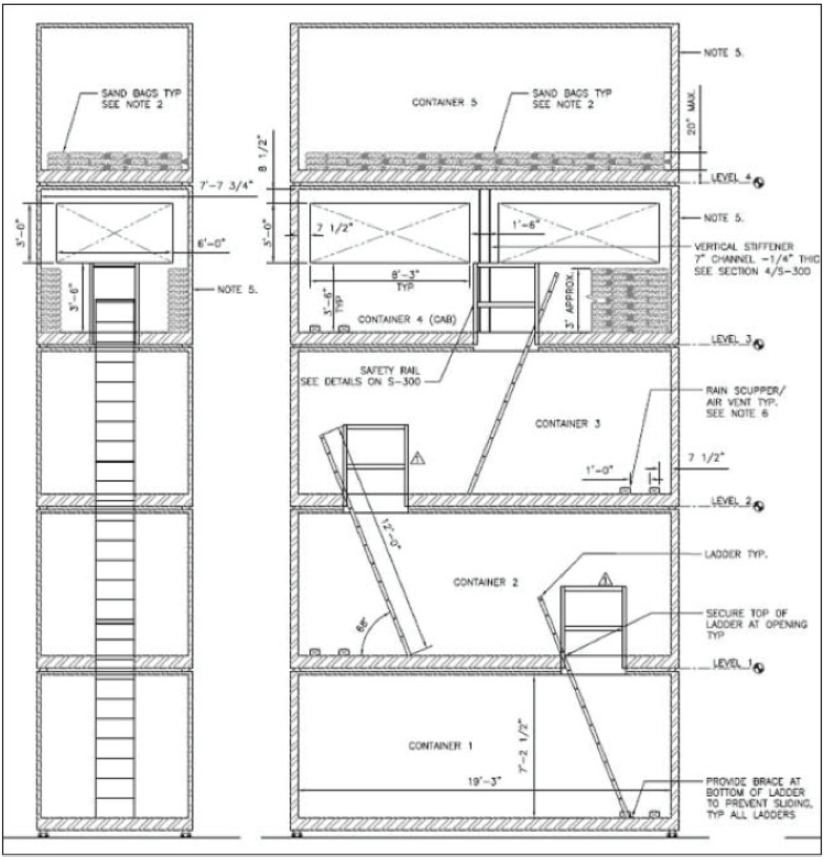


Figure 11-13. Freight Container Guard Tower Design

Pre-cast Concrete Guard Tower. The tower in Figure 11-14 consists of pre-cast modular concrete sections with Welded plates embedded in each segment connecting the sections. The tower incorporates an energy diverting cylindrical shape and includes an interior stairwell. The tower can be disassembled and re-deployed for other operations. Due to its weight, the tower requires a crane or similar equipment capable of lifting the concrete sections. The tower depicted in Appendix G is a variation of this design.

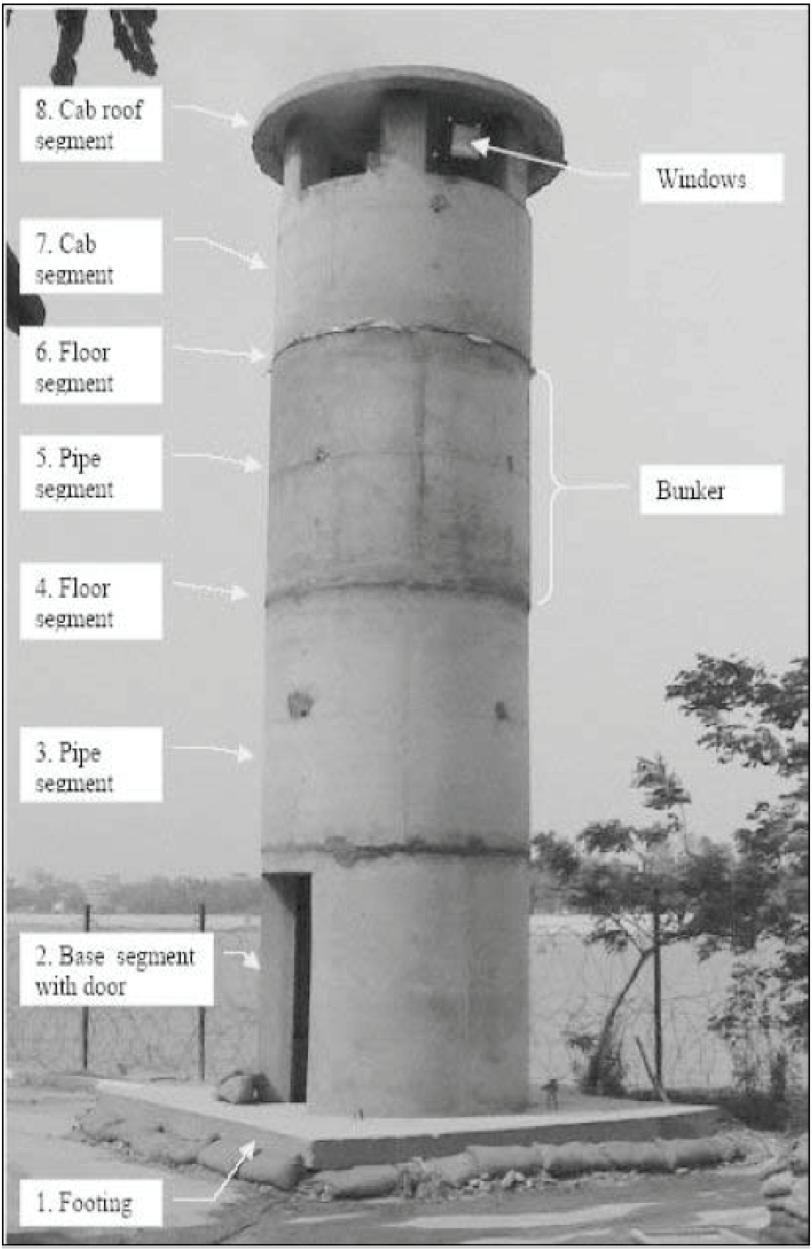


Figure 11-14. Pre-cast Concrete Guard Tower

Fighting Positions

Fighting positions and observation posts facilitate both offensive and defensive operations. Above-ground posts provide an observation vantage, require less construction labor, and are easier to enter and exit than below-ground shelters. Conversely, these positions are harder to conceal and require large amounts of cover and revetment material. While fighting positions should provide maximum protection to personnel and equipment, effective weapon employment is also a consideration. In offensive operations, weapons are often sited wherever natural or existing positions exist, and minimal digging is required (Figure 11-15).

Figure 11-15. A rooftop fighting position

Fighting positions and observation posts are often constructed from soil-filled containers (Figure 11-16). These positions provide small arms, VBIED, and RAM protection while allowing enemy engagement. Experimental test results indicate the overhead soil cover will defeat direct-hit 82-mm mortar. The sidewalls will defeat fragmentation from near-miss detonations up to 120-mm mortar, 122-mm rocket and 155-mm artillery rounds. Appendix H, Soil-Filled Container Applications, and FM 5-103, *Survivability*, contain additional fighting position designs and details.

Figure 11-16. Soil filled Container Two-Man Fighting Position

References:

ERDC/USACE *Construction Guide for Reinforced Below-ground 40' Mil-van Bunker, May 2003.*

FM 5-103. *Survivability,* 10 June 1985.

FM 5-34. *Engineer Field Data,* 19 July 2005.

ERDC TR-08-29. *Technical Guidelines for Environmental Dredging of Contaminated Sediments*, September 2008.

AFH 10-222v14. *Civil Engineer Guide to Fighting Positions, Shelters, Obstacles, and Revetments*, 1 August 2008.

ERDC *Field Expedient Protective Positions.*

This page intentionally blank

CHAPTER 12
FIELD FORCE ENGINEERING

Field Force Engineering (FFE) supports DoD operational capabilities through forward presence and reachback to deployed DoD components. FFE supports the planning, preparation, execution, and assessment of joint operations with subject-matter-expert (SME) teams. FFE draws on a broad range of resident capabilities within the US Army Corps of Engineers (USACE), US Army Engineer School (USAES), Theater Engineer Commands (TEC), USACE Districts and Divisions worldwide, other government agencies, academia, and private industry. FFE forward presence and reachback capabilities are also available to support agencies such as the Department of State (DOS), Department of Homeland Security (DHS), and foreign government organizations.

FFE Teams

FFE support is provided through deployed and non-deployed military and civilian teams. Military personnel are typically combat engineers while civilians are technical specialists in specific engineering disciplines. One FFE team, the USACE Reachback Operations Center (UROC), maintains a dedicated organizational and communications structure necessary to enable deployed-force reachback. An expanded description of the UROC capabilities and process is provided in this chapter. Table 12-1 summarizes FFE missions and capabilities. The following organizations are the FFE teams available for support:

Forward Engineer Support Team–Main (FEST-M). FEST-M are deployable teams that provide command and control and sustainment for USACE teams in support of deployed forces. These teams generally support joint task forces (JTFs) or land components. The FEST-M provides liaison officers (LNO) and USACE engineering planning modules to deployed units. The FEST-M is self-sustaining and supports the following mission areas: infrastructure engineering planning and design, technical engineering expertise, contract construction, real estate acquisition and disposal, environmental engineering, and geospatial engineering support. FEST-M teams can communicate through TeleEngineering Communications Equipment (TCE) or standard communications channels.

Forward Engineer Support Team–Advance (FEST-A). FEST-A are deployable teams that provide additional planning capability to combatant and component command engineer staffs. FEST-A teams can also deploy in support of JTFs that have limited execution capability. Capabilities include engineer planning and design, real estate acquisition and disposal, and contracting. FEST-A teams can also communicate with TCE.

Contingency Real Estate Support Team (CREST). CRESTs are deployable teams that acquire, manage, and dispose of real estate property on behalf of US interests. These teams can support all echelons but are tailored toward Army component HQs requiring real estate management.

Environmental Support Team (EnvST). EnvST are deployable teams that conduct environmental assessments, baseline and other surveys, and studies. These teams can support all echelons, but are most often tailored to Army component HQs requiring base camp development support. EnvST augment either the deployed force engineer staff or supporting engineer HQ.

Logistics Support Team (LST). LST are deployable teams that sustain deployed FFE or emergency management teams beyond the operational force logistics system. These teams support FEST-M C2 activities.

All support requests from the above teams should be directed to USACE UROC. Figure 12-2 provides UROC contact information.

USACE Reachback Operations Center (UROC). The UROC is a non-deployed organization that provides reachback engineering capabilities to deployed US personnel worldwide. Deployed personnel can be linked to subject matter experts (SME) within USACE, DoD, other government agencies, private industry, and academia.

Base Camp Development Team (BDT). BDT are non-deployed teams that rapidly provide base development engineering, master planning, and facilities design in response to requests for information (RFI). BDTs are managed and trained by UROC. BDT focus areas include base location, design, construction, and eventual closure or transfer.

Reachback Concept

The reachback objective is to assist FFE operations through specialized technical and communications assistance not normally found in deployed units. Deployed personnel are linked to SME within USACE, the US Army Engineer School (USAES) and Service equivalents, Theater Engineer Commands (TEC), USACE Districts and Divisions worldwide, FFE teams, other government agencies, academia, and private industry. The Navy and Air Force also maintain reachback capabilities (Figure 12-1).

FFE reachback teams provide rapid engineering guidance across the full spectrum of operational and natural disaster response. The most frequently requested FFE functions include engineering analyses, VTC communications, base camp planning, Geographic Information Systems (GIS), intelligence support, training, and equipment supply.

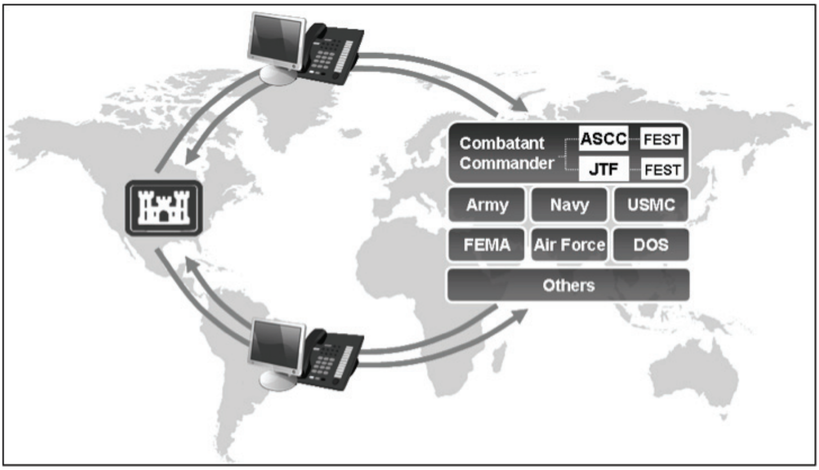


Figure 12-1. Reachback Concept (FM 3-34, *Engineer Operations*)

Reachback Operations

UROC is the primary hub for reachback technical assistance. UROC responds to RFI from the military services, DOS, Federal Emergency Management Agency (FEMA), and other agencies. As shown in Figure 12-2, UROC assistance is available via internet, the Secret Internet Protocol Router Network (SIPRNet), email, and telephone. RFI should identify the requesting unit and include a request description, necessary supporting data, unit contact information, and suspense dates. Other required RFI processing information is shown in Figure 12-3.

Table 12-1. FFE Team Capabilities Summary (Source: Data from EP 500-1-2, *Field Force Engineering*)

Team	Mission	Capabilities	Supports	Dependencies
Forward Engineer Support Team – Main (FEST-M)	Provide construction management, real estate, environmental, geospatial, and other engineering support (typically at the theater echelon level) and can provide command and control for deployed FFE teams	• Technical engineering support including construction design and management; area engineering support; support to engineer operations; and support to facilitate reachback operations • Disaster response including consequence management or civil support operations • Stability operations support including humanitarian assistance, essential services restoration, and economic and infrastructure development support	• Force-tailored to support a joint task force land component headquarters • Typically task-organized to the joint task force (corps) or joint force land component (theater Army or corps) headquarters • May be task-organized to the supporting engineer headquarters or operate as a discrete headquarters • May provide the base on which a contingency district is established	Gaining or supported organizations must provide basic life support and security
Forward Engineer Support Team – Advance (FEST-A)	Provide infrastructure assessment, engineer planning and design, environmental, geospatial, and other engineering support from theater to brigade echelon and augments the staff at those echelons	• Technical engineering support including construction design and management; area engineering support; support to engineer operations; and support to facilitate reachback operations • Disaster response including consequence management or civil support operations • Stability operations support including humanitarian assistance; essential services restoration; and economic and infrastructure development support	• Typically force-tailored to support a joint task force (in smaller-scale contingencies) or a corps, division, or brigade as a tactical headquarters • Typically task-organized to support force headquarters or to augment the engineer staff • May be task-organized to support an engineer headquarters • May operate as a subordinate to a FEST-M configured as a discrete headquarters	Gaining or supported organizations must provide basic life support and security
Contingency Real Estate Support Team (CREST)	Acquire, manage, and dispose of real property on behalf of the U.S. government (typically task-organized as part of a FEST)	• Technical engineering support including area engineering (real estate and base camp development planning) and reachback operations	• Typically force-tailored to support an Army component headquarters with real estate requirements • Typically task-organized to support force headquarters and augment engineer staff • May be task-organized to support an engineer unit headquarters or FEST	Gaining or supported organizations must provide basic life support and security

Environmental Support Team (EnvST)	Conduct environmental assessments, surveys, and studies (typically task-organized as part of a FEST)	• Technical engineering support including area engineering (environmental), engineer operations (environmental reconnaissance), and reachback operations	• Typically force-tailored to support an Army component headquarters with base camp development planning and other environmental requirements • Typically task-organized to support force headquarters and augment engineer staff • May be task-organized to support an engineer unit headquarters or FEST	Gaining or supported organizations must provide basic life support and security
Logistics Support Team (LST)	Coordinate sustainment support for deployed FFE or emergency management elements when support requirements are exceeded or are not provided by the operational force logistics system	• Disaster response including consequence management or civil support operations Stability operations support, including humanitarian assistance and restoration of essential services	• Typically tailored to support a FEST-M when the unit is operating as a discrete headquarters • Routinely tailored for emergency response operations as a planning and response team under ESF #3 * • May be task-organized to support an engineer unit headquarters or FEST team	Gaining or supported organizations must provide basic life support and security
USACE Reachback Operations Center (UROC)	Provide rapid, relevant, and reliable solutions across the full operational and natural disaster spectrum	• Comprehensive training and support to deployed units • Data repository for collected engineering data used for infrastructure analysis • Reachback capability and respond to information requests	Headquarters USACE provides FFE support to UROC	None
Base Camp Development Team (BDT)	Provide base development engineering, master planning, and facilitate design in support of FFE and other reachback requests for information	• Technical engineer support to include area engineering support (protection and base camp development planning) and reachback support • Disaster response in civil support operations • Stability operations support of humanitarian assistance	Reachback support is coordinated through UROC	Designated USACE districts train and sustain teams based on a rotational readiness model

* - Emergency Support Function (ESF) #3 – Public Works and Engineering – assists the Department of Homeland Security (DHS) by coordinating and organizing the capabilities and resources of the Federal Government to facilitate the delivery of services, technical assistance, engineering expertise, construction management, and other support to prepare for, respond to, and/or recover from a disaster or an incident requiring a coordinated Federal response. Under the National Response Framework, the U.S. Army Corps of Engineers (USACE) is assigned as the coordinator for ESF#3 and during disasters the USACE is the Primary Agency for response activities, such as ice, water and temporary power. FEMA is the Primary Agency for ESF#3 recovery activities and can assign USACE missions to assist in the execution of recovery missions, to include debris management. There are also a number of Support Agencies that ESF#3 can draw upon for assistance. Refer to the *National Response Framework* for additional details.

USACE Reachback Operations Center (UROC)

RFI Support:
1-877-ARMY-ENG
601-634-2439 or DSN (312) 446-2439

RFI Email:
UNCL : uroc@usace.army.mil
SIPR : uroc@usace.army.smil.mil

Websites:
UNCL: https://uroc.usace.army.mil
SIPR: http://uroc.usace.army.smil.mil

VTC Support:
601-634-3485 or DSN 312-446-3485

VTC Email :
UNCL: uroc-vtc@usace.army.mil

Figure 12-2. UROC Contact Information

UROC maintains archives of previous RFI and can quickly determine if similar issues have been previously addressed. Deployed personnel and FFE teams can also search the archives for information. For new RFI, the UROC will locate SME(s) and coordinate a response. UROC manages the RFI until project completion. The response is then added to the RFI archives.

Date Requested
Classification
Command
Country
Suspense Date and Comments
Time Zone (local)
RFI Subject
RFI Details and Justification
Event (optional)
POC (E-mail and contact information)
Unit (requesting)
Location
Deliverables (data format)

Figure 12-3. UROC Website RFI Elements

TeleEngineering Systems and Equipment

TeleEngineering is the UROC communications architecture that facilitates reachback when the existing communications infrastructure cannot support the mission. The UROC operates multiple video teleconference (VTC) hubs for both classified and unclassified events. VTC hubs are available through telephone dial-up, internet access, or a combination of both. Multiple personnel can simultaneously be linked into a single hub, and hubs operate independently to allow simultaneous VTC events. VTC hub access is available virtually worldwide. The TeleEngineering infrastructure includes specialized systems and software applications necessary for FFE support. These systems are described below.

TeleEngineering Communications Equipment – Deployable (TCE-D) and **Fixed (TCE-F)**. The TCE-D is a satellite-based communications system that allows data exchange and VTC (Figure 12-4). TCE-D also provides phone, internet, and e-mail access. The TCE-D is ruggedized for field use and consists of a laptop computer, encryption device, external handheld camera, and miscellaneous components. The system is capable of both Integrated Services Digital Network (ISDN) and internet protocol (IP) based video conferencing. The TCE-D connects through a satellite terminal and uses auto-switching power supplies to operate on both 110- and 220-volt AC power. The system can also be operated solely with vehicle battery power. The TeleEngineering Communications Equipment – Fixed (TCE-F) is the office or conference room variant.

Figure 12-4. TeleEngineering Communications Equipment-Deployable

UROC is the telecommunications hub for both TCE-D and TCE-F, and maintains certification with the Defense Information Systems Agency (DISA), Defense Information System Network (DISN) Video Services-Global (DVS-G). DVS-G allows the UROC to accommodate connections from its participants to larger audiences operating at different data rates or through dissimilar networks.

Broadband Global Area Network (BGAN) Terminal. BGAN is a portable, robust satellite terminal that simultaneously transmits voice and broadband data (see Figure 12-5). For satellite communications, the TCE-D and BGAN are typically combined.

Figure 12-5. Broadband Global Area Network Terminal

IKE/GATER. The "it knows everything" (IKE) is a handheld data collection device with a customized Geospatial Assessment Tool for Engineering Reachback (GATER) interface (see Figure 12-6). GATER is an applications suite that supports: field data collection (the IKE); a desktop conduit application that synchronizes field data to the desktop and data repository; and an online GIS mapping capability. Once field data are collected and uploaded at the desktop level, users can extract shape files and generate reports. Data uploaded to the UROC geodatabase populates the USACE Global Situation Map via ESRI's ArcGIS Explorer, as well as the corresponding online GATER application. Through the synchronization process, the UROC passes data collection updates and software upgrades (both GATER and IKE) to end users.

The UROC provides site-specific commercial satellite imagery and standardized data collection modules on the IKE. These data support infrastructure assessments (SWEAT-MSO), EOD, real estate lease (CREST), access/entry control points, environmental site and closure surveys (EnvST), real property (DoD RIPR), construction tracking, bridge reconnaissance, Special Operations Weather Teams, and civil affairs.

The UROC maintains a data repository and can support SECRET operations. The UROC supports both the commercial IKE 305 and military IKE 504 with SAASM GPS. All IKE data is encrypted SECRET. The UROC conducts daily data migration from the NIPR to the SIPR to allow further analysis and interoperability among various national databases

Figure 12-6. IKE/GATER Device

Automated Route Reconnaissance Kit (ARRK). The ARRK is a ruggedized laptop computer with custom software coupled to various sensors that continuously collect and display route reconnaissance information (see Figure 12-7). Coupled with the TeleEngineering Toolkit (TETK) software, the ARRK collects images, voice recordings, GPS location, accelerometer, and 3-D position data. The ARRK provides a chronological picture replay of the route and a geo-referenced display of major features that affect route classification and vehicle-mounted applications. The system also provides automated slope determination and radius of curvature. ARRK operators convert collected reconnaissance data to pre-formatted reconnaissance reports that conform to FM 3-34.170, *Engineer Reconnaissance* requirements. In its airborne configuration (see Figure 12-8), the ARRK provides aerial reconnaissance imagery that can be annotated to highlight specific route features. Figure 12-9 is a screen capture showing a preferred map route and a selected location from the video.

Figure 12-7. Automated Route Reconnaissance Kit, Standard Configuration

Figure 12-8. Automated Route Reconnaissance Kit, Airborne Configuration

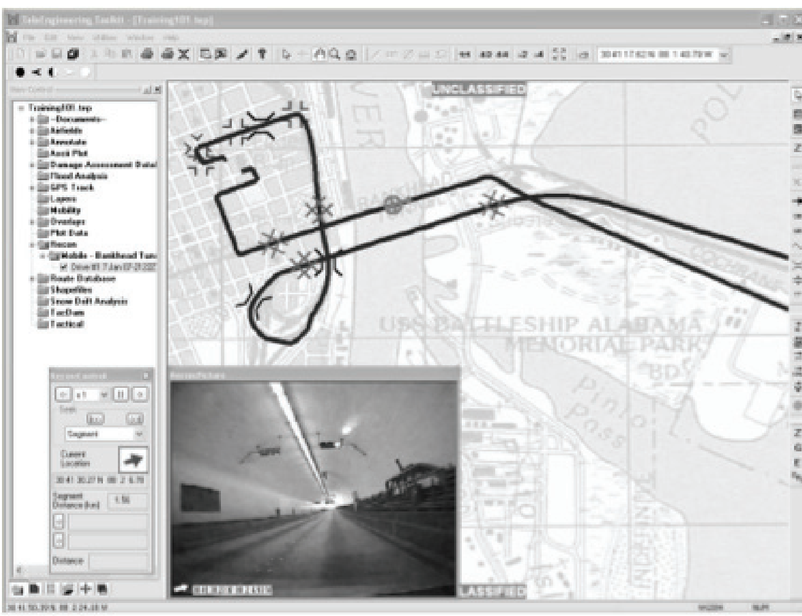


Figure 12-9. Sample ARRK product display

Theater Construction Management System (TCMS). The TCMS is a PC-based construction planning, design, management, and reporting system for military engineers assigned to OCONUS construction activities. TCMS combines commercial, off-the-shelf hardware and software with Army Facilities Components System (AFCS) designs and databases. TCMS is developed and maintained by the US Army Engineering and Support Center, Huntsville, AL. Additional information is available at http://www.tcms.net.

UROC Equipment Training Program. The UROC provides training and support for the ARRK, IKE/GATER, and TCE systems. Table 12-2 shows various training levels, up to and including train-the-trainer. Pre-deployment training must be conducted regularly to practice set-up, operation, and data processing, as these are perishable skills. Certified trainers are encouraged to educate other USACE and non-USACE personnel on FFE equipment, but UROC must approve requests for a certified trainer to train non-UROC personnel.

Navy and Air Force Reachback

Naval Facilities Engineering Command (NAVFAC). NAVFAC Contingency Engineering provides a reachback capability through NAVFAC Atlantic and NAVFAC Pacific. NAVFAC forwards RFI to the appropriate supporting organization or SME. The NAVFAC reachback contact information is:

Portal/contact: info:https://portal.navfac.navy.mil/portal/page/portal/navfac/navfac_ww_pp/navfac_navfacpac_pp/our_services/contingencyeng_final.pdf

Email: nfecl_ce_reachback@navy.mil

NAVFAC Atlantic Phone: (757) 322-8302/Cell: (757) 339-6111\
DSN: (312) 262-8302

NAVFAC Pacific Phone: (808) 472-1162

Table 12-2. UROC Training Program
(Source: Data from EP 500-1-2, *Field Force Engineering*)

System	Training	Objective
Automated Route Reconnaissance Kit	ARRK Operator (Level I.A Training)	• provide basic knowledge to install and operate the ARRK system • use the TETK software to collect route reconnaissance data and to verify that the data are properly recorded and saved
	ARRK Data Processor (Level I.B Training)	• using the TETK software for processing data collected by the ARRK, including editing recon data, generating standard reconnaissance forms, etc.
	ARRK Train-the-Trainer (Level II Training)	• review of ARRK and TETK skills • overview of the instructional materials and logistics for conducting an ARRK training class • experience instructing classes • UROC certification as a trainer to conduct Level I.A and Level I.B ARRK training upon successful completion of this Level II training **PREREQUISITES:** • successful completion of ARRK Level I training • some hands-on experience with the system highly recommended
IKE w GATER	Basic IKE w GATER Operation (Level I Training)	• basic operation of the IKE with GATER system for data collection • data management process • covers all three tiers of the GATER operating environments: online, desktop and mobile
	IKE w GATER Train-the-Trainer (Level II Training)	• detailed instruction on all three tiers of the GATER operating environments • program administration, system business rules and policies, troubleshooting and technical support • UROC certification as a trainer to conduct Level I IKEwGATER training upon successful completion of this Level II training **PREREQUISITES:** • successful completion of IKEwGATER Level I training • hands-on experience with the system highly recommended
TeleEngineering Communications Equipment (TCE) and Broadband Global Area Network (BGAN)	TCE and BGAN Operator (Level I Training)	• basic knowledge to assemble and operate the equipment • conduct video teleconferencing, data transfer, telephone, internet access (secure and/or non-secure) via satellite-based systems
	TCE and BGAN Train-the-Trainer (Level II Training)	• detailed instruction on TCE-D / TCE-SL and BGAN communications equipment • UROC certification as a trainer to conduct Level I TCE and BGAN training upon successful completion of this Level II training **PREREQUISITES:** • successful completion of TCE and BGAN Level I training • hands-on experience with the system highly recommended

Headquarters Air Force Civil Engineer Support Agency (HQ AFCESA) Reach Back Center (RBC). The Readiness Support Division of AFCESA operates the RBC, which provides rapid response to questions from civil engineers in the field, worldwide. The RBC responds to RFI through internally maintained databases. If a solution is unavailable, the RFI is forwarded to appropriate SME. AFCESA reachback contact information is:

Email: afcesar@tyndall.af.mil

Website: http://www.afcesa.af.mil
https://afcesa@aetc.af.smil.mil

Address: HQ AFCESA
139 Barnes Dr
Tyndall AFB FL 32403

Phone: (850) 283-6995/(888) 232-3721/DSN 523-6995

References:

EP 500-2-1. *Emergency Employment of Army and Other Resources- Field Force Engineering- United States Army Corps of Engineers Support to Full Spectrum Operations,* 01 August 2010.

FM 3-34.400. *General Engineering,* 09 December 2008.

FM 3-34. E*ngineer Operations*, 02 April 2009.

APPENDIX A
FOB PROTECTION MANAGEMENT

Whether establishing a new FOB or falling in on an existing one, commanders should focus initially on establishing or reassessing protection measures at the perimeter of the base. Once these measures are adequate, attention can be directed to internal security procedures. FOB protection priorities are detailed in Figure A-1:

FOB Proteciton Priorities

- Prepare a base security plan
- Establish appropriate perimeter standoff based on threat and HN situation
- Establish vehicle and personnel entry points and search areas
- Establish access control processes, badges, and HN labor and visitor control procedures
- Construct personnel survivability shelters near work centers, living areas, and recreation facilities
- Establish attack warning systems, including alarms, codes, actions, and HN education
- Integration of HN or coalition forces as required
- Establish mass casualty procedures
- Develop Joint coordinated fire plan
- Conduct rehearsals
- Establish/coordinate active patrols and tactical counterintelligence operations within the base boundary to deny enemy freedom of action
- For airbases: establish surface-to-air missile (SAM) suppression patrols and quick reaction forces (QRF) to deny launch terrain near active runways and common flight paths. This must be accomplished in coordination with the area commander.

Figure A-1. FOB Protection Priorities
(JP 3-10, Joint Security Operations in Theater)

FOB Commander Responsibilities. FOB commanders are responsible for base protection and security operations and should use all available assets to establish required security levels. FOB commander protection responsibilities are shown in Figure A-2.

FOB Commander Protection Responsibilities

- Manage Security Operations
- Conduct Command Post Operations
- Manage Information Operations
- Establish a Base Defense Operations Center
- Integrate Information Superiority Contributors
- Synchronize and Integrate FOB Requirements and Capabilities
- Integrate FOB Support Teams
- Evaluate FOB Activities and Recommend Any Necessary Improvements
- Manage FOB Operations
- Manage FOB Resources

Figure A-2. FOB Commander Protection Responsibilities

Tenant Unit Commander Responsibilities. Tenant unit commanders should actively participate in base security and defense planning. Tenant units normally provide for their own security, plus contribute personnel to the FOB protection mission. These assigned or attached forces fall under the FOB commander's TACON, however, tenant unit commanders must ensure that provided personnel are properly equipped and trained.

Critical to the success of the FOB protection mission is the need for coordination and cooperation among assigned or attached units. These units must build operational relationships based on mutual support. For example, tenant unit communications equipment may not be compatible with host unit equipment. In this case, tenant unit commanders should coordinate with the FOB commander to ensure compatibility. Key tenant unit concerns include training, rehearsals, coordination, and competing requirements between security and operational tasks. Tenant unit commander responsibilities are shown in Figure A-3.

FOB Tenant Unit Commander Protection Responsibilities

- Participate in the preparation of base defense plans
- Staff and operate base defense facilities in accordance with base defense plans
- Conduct individual and unit training to ensure readiness for assigned defense tasks
- Provide an appropriate share of facilities, equipment, and personnel for the Base Defense Operations Center (BDOC)
- Advise the FOB commander on operational concerns special to their units
- Provide for unit internal security
- Sustain and administer unit forces
- Provide unit requirements for common-user communications systems to the FOB commander's communications element

Figure A-3. FOB Tenant Unit Commander Protection Responsibilities

FOB Protection Team. A team approach should be used to develop protection measures and manage the overall FOB protection mission. To interact efficiently, team members should understand the concepts, roles, and capabilities of other members. A team approach facilitates protection plan development, intelligence sharing, and coordination between tenant units. The team should include representatives shown in Figure A-4.

Recommended FOB Protection Team Composition

- Tenant Units
- Intelligence/Counterintelligence
- Medical
- Fire/Emergency Response
- Engineers
- Security/Law Enforcement
- Chemical, Biological, Radiological, Nuclear, and High Yield Explosives (CBRNE) Defense
- Logistics
- Explosive Ordinance Disposal (EOD)
- Communications and Information Systems
- Public Affairs
- Resource Management (Comptroller)
- Legal
- Emergency Response Forces (External Security Forces, Tactical Combat Force, etc.)
- Host Nation (HN) (as appropriate)

Figure A-4. Recommended FOB Protection Team Composition

Incident Management. Incident management is a comprehensive approach to prevention, preparation, response, and recovery from enemy attacks, natural disasters, and other emergencies. Incident management includes both crisis and consequence management. Crisis management identifies, acquires, and plans resources for incident management. Consequence management involves actions taken to maintain or restore essential services, and manage and mitigate enemy attacks and natural disasters.

Response is a rapid reaction to life-threatening or damaging incidents. Response begins with immediate local emergency damage limitation and survivability actions; these should be explicitly detailed in FOB policy, training guidance, standard operating procedures (SOP), and contingency plans. A FOB response team should be task-organized for all incidents, regardless of threat, tactic, or event. This requires an on-scene commander who coordinates activities through an incident command system (a systemic procedure whereby FOB staffs are organized to provide incident response).

Incident Management Planning. FOB commanders, with tenant command representation and the FOB protection team, form a crisis management organization staffed by BDOC personnel during crisis management. A successful organization must be pre-designated, train together, and prepare for individual and collective crisis management missions as directed by the FOB commander. Tenant commanders may also serve or have staff representation in this organization. The most common components of a crisis management organization are:

- **Medical Team**. This team must be capable of conducting triage, patient decontamination, and back-up responder decontamination.
- **Fire Fighters.** The senior fire-fighter normally becomes the on-scene commander. The fire fighter team establishes staging areas and calls for HAZMAT support if necessary.
- **Law Enforcement**. This team secures the incident scene, providing responder security while controlling ingress/egress at the incident site.
- **Search and Rescue Teams.** These teams work in pairs and are respon sible for casualty extraction. If available, an attached structural engineer can conduct safety and damage assessment.
- **Explosive Ordnance Disposal (EOD)**. The EOD Team detects, identi fies, and renders safe any suspected munitions and/or secondary devices.

A FOB incident management plan should prepare for the actions shown in Figure A-5.

Recommended FOB Incident Management Actions

- Establish command and control at the incident site and secure the area
- Perform a tactical appraisal of the situation
- Prepare a damage and casualty assessment
- Take immediate actions to save lives, prevent suffering, reduce, or mitigate property damage
- Prioritize response effort and subsequent order for follow-on response forces, equipment, and supplies
- Establish staging locations for response personnel
- Establish mass casualty care and evacuation areas

Figure A-5. Recommended FOB Incident Management Actions

Operations Centers. FOB commanders establish operations centers to assist in managing FOB protection operations. Component and staff representation will vary according to mission, forces available, and security requirements.

- **Base Defense Operations Center (BDOC).** BDOCs are command and control facilities established by FOB commanders as focal points for force protection, security, and defense within base boundaries. Through the BDOC, FOB commanders plan, direct, coordinate, and control base and area security operations. BDOCs communicate with base cluster operations centers, if established. BDOC missions depend on the combination of forces involved and may include other Service components, and coalition or HN personnel. The BDOC consists of three primary sections command, intelligence, and operations. Additional sections might include logistics, area damage control (ADC), planning, and control of base emergency response/ADC resources. BDOCs are manned full time and augmented with subject matter experts as necessary.

- **Base Cluster Operations Center (BCOC)**. BCOCs are command and control facilities established by base cluster commanders as security focal points for cluster bases. BCOCs plan, directs, coordinates, and controls all cluster security efforts. BCOC personnel assess cluster security postures and notify commanders of necessary resources for security requirements. BCOCs coordinate all BDOC efforts, and integrate Joint security operations with higher-level staff designated by the JFC. BCOC staff depend on the combination of tenant forces within the cluster and may include other US Services, multinational, HN, or civilian personnel. Intelligence, maneuver, and fire support also contribute personnel to BCOC staff. Base cluster commanders provide staff representatives to augment FOB commanders as necessary. BCOCs are similar in many respects to land force tactical operations centers and, in some cases, may be the same.

- **Area Operations Centers (AOC)** and Tactical Operations Centers (TOC). Army and Marine Corps area and subarea commanders may have AOC and TOC for area security and defense missions. These facilities serve as the commander's planning, coordination, monitoring, and directing agencies for Joint security operations.

References:

JP 3-10. *Joint Security Operations in Theater,* 03 February 2010.

JP 3-28. *Civil Support*, 14 September 2007.

APPENDIX B
RISK MANAGEMENT

Risk management is the process of systematically identifying, assessing, and controlling operational risks, then balancing risk reduction costs with mission benefits. Risk management is a command responsibility that conserves operational capabilities and resources. Commanders must decide how best to employ protection measures that deter and mitigate attacks while maintaining operational viability.

The Services' policy is to utilize reasonable risk reduction measures for personnel, infrastructure, and information. This generates a protection approach that focuses on traditional, irregular, disruptive, and catastrophic threats. If prevention and protection efforts fail, quick recovery (consequence management) is an important risk management element.

All Services have similar risk management doctrine and employ structured decision-making processes. The risk management tool presented in this appendix relies on the Operational Risk Management (ORM) Process described in JP 3-0, *Joint Operations* (Figure B-1).

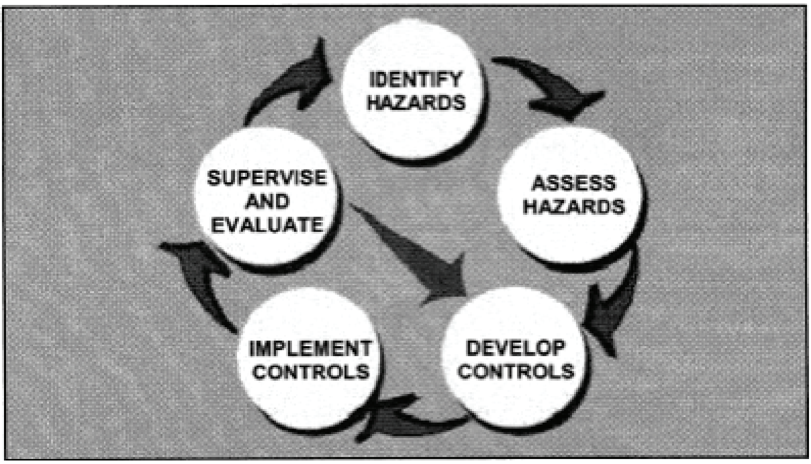


Figure B-1. Operational Risk Management Process (JP 3-0, *Joint Operations*)

Two aspects of the ORM process are emphasized: *risk assessment* to determine and prioritize risks and *risk mitigation* to determine reasonable risk reduction. Other ORM topics such as resource management, implementation, training, and results analysis exceed the scope of this Handbook.

Risk Assessment. Risk assessment systematically identifies and determines risk levels using quantitative or qualitative risk values related to realistic scenarios. Risk levels for each scenario are then prioritized by calculating or assessing both likelihood of occurrence and projected consequences. Likelihood is based on a projected threat and exploitable vulnerabilities. These values are combined to produce the equation Risk = Likelihood x Consequences, which is a measure of potential impact.

Risk Mitigation. Risk mitigation is the process of developing and implementing risk reduction strategies. Risk mitigation reduces projected risk likelihoods and risk consequences. Important risk mitigation concepts include:

- Risk mitigation actions are normally a combination of programmatic (requires funding, as for additional equipment) and procedural (does not require funding, as for conducting exercises) actions.

- If risk mitigation actions result in unacceptably high residual risks, alternate measures must be examined.

- Individual mitigation measures often reduce multiple risks. For example, sufficiently high blast walls will not only deter hostile FOB surveillance, but also mitigate direct-fire weapons.

- Mitigation measures that deter attacks also reduce risks. For instance, improved vehicle or pedestrian access controls and random operational measures confuse surveillance and make the FOB appear too hard to attack.

- Protective measures that reduce consequences also reduce risk. Side wall and overhead protection preserve mission capabilities and reduce indirect-fire attack casualties.

- Equipment demands, personnel requirements, schedules, operational constraints, external conditions, and available funding all influence potential mitigation actions.

- Risk consequences do not always justify mitigation costs. The commander must accept some risks, implement temporary measures, and plan for permanent measures.

The JFOB Handbook provides advice on how to avoid risks through the use of TTPs and best practices for FOBs and similar combat facilities. Risk management and mitigation must consider base construction, operations, and active defenses. The full spectrum of risk management is beyond the scope of this handbook. Risk avoidance and mitigation are considered for most common threat scenarios, but topics such as exercises and security force operations are not.

Risk Management Tool. The risk management tool presented in this appendix applies to both deliberate and time-critical risk management. Time-critical applications are emphasized. Deliberate FOB risk management procedures require significantly more time and planning resources than are typically available. Time-critical processes are faster approximations of deliberate processes. The FOB size and number of assets to be examined will impact the scope of required risk management efforts, but not tool applicability. The risk management tool focuses on typical combat zone threats such as VBIED, but has application to non-combat hazards and zones.

Instructions for Tool Use

1. Gather required materials.

a. A copy of these instructions for quick reference.
b. *Table B-1. FOB Common Threats and Tactics, and Common Mitigation Measures*; and *Table B-2. Potential FOB Vulnerabilities*. These tables are not comprehensive, but contain useful data examples. More thorough discussions of these topics can be found in the related chapters of the JFOB Handbook.
c. Additional copies of tool worksheets.
d. FOB site map, overhead imagery, and materials for asset sketching.
e. Camera.
f. Tape measure, detailed scaled map, or other devices to measure distances between assets, distances between assets and the perimeter, etc.
g. Copies of Worksheet 3 (*Risk Mitigation Actions*) to record possible mitigation actions.

2. Develop a prioritized asset list. Critical assets might include personnel, infrastructure facilities, defensive positions, large population dwellings and gathering places, and communications nodes.

3.Analyze collected information. Locate critical assets on the site map prior to visual inspection. Table B-1 lists common risk assessment threat tactics to consider. Table B-2 details common FOB vulnerabilities.

4.Develop threat-asset pairs. A threat-asset pair is a specific threat directed against a specific asset. Threat-asset pairs should be developed based on realistic, potential threat tactics. A single threat event may impact a single asset or asset group. Assets may face multiple threats (mortars, snipers, VBIED, etc.) singly or in combination. Some assets may not have identified threats and should be excluded from risk management procedures.

5.Prepare separate worksheets for each identified threat-asset pair.

6.Examine worksheet results. Examine the Worksheet 3 mitigation action list and the mitigation effects on Worksheet 2 as the basis of selecting mitigation actions for command review.

7.Select and implement mitigation actions. See relevant JFOB Handbook chapters for details.

Instructions for Worksheet 1 - Current Condition Risk

a. *Security Classification.* Completed worksheets should be classified. Mark and protect accordingly.
b. *Asset Information.* Enter asset information (name, type, location, important features, etc.) and approximate maximum personnel that could be present at time of attack.
c. *Threat Information.* Identify threats based on available intelligence, prior FOB activities, and AO threat conditions. Table B-1 provides important threat considerations.
d. *Vulnerability Information.* Consider Table B-2. For each worksheet, list how the asset is vulnerable. Factors to consider include threat tactics, in-place protection provided by physical security, and construction.
e. *Event Likelihood Rating.* Select the most appropriate event likelihood based on asset, threat, and vulnerability entries. Intelligence assessments and prior attack methods in the AO will indicate if the threat likelihood is high.
f. *Projected Consequence Ratings*. Enter projected casualties, property replacement cost, and mission degradation consequence values on the Estimate Losses line. Assume the attack is timed for optimum damage and casualties. Enter the 1 - 9 rating for each consequence on the Likelihood Ratings line.
g. *Sum of Consequences Ratings*. Add the 5 numbers on the Likelihood Ratings line. The Total Score should be 5 - 45.
h. *Risk Score*. Risk = (Likelihood Rating) x (Sum of Consequences Ratings). The result should be in the range 5 – 405. A higher number equates to higher risk.
i. *Risk.* Convert the risk score using this scale:

5-45	Negligible
46-90	Negligible-Low
91-135	Low
136-180	Low-Medium
181-225	Medium
226-270	Medium-High
271-315	High
316-360	High-Extreme
361-405	Extreme

j. *Risk Priority.* Prioritize completed worksheets based on mitigation need. Assign priorities beginning with “1” as the highest.

Instructions for Worksheet 2, Projected Post-Mitigation Risk and Worksheet 3, Risk Mitigation Actions.

a.Review estimated risks and vulnerabilities for each completed Worksheet. Examine Table B-1 for common mitigation actions. Enter selected actions on Worksheet 3 (Risk Mitigation Actions). Describe possible action impacts that might include cost, implementation time, and mission effects. Do not duplicatepreviously recorded mitigation actions on Worksheet 3. Do, however, note the asset and risk priority to which it applies. Some actions normally will affect multiple threat-asset pairs. In the Comments column, describe immediate actions that could temporarily provide protection until more permanent actions can be implemented. Dismiss temporary or long-term actions deemed too costly or operationally unacceptable.

b.Post-mitigation vulnerability. Assume all mitigation actions on Worksheet 3 are implemented simultaneously. Reassess asset vulnerabilities on each Worksheet 2 (Projected Post-Mitigation Risk).

c.Mitigation Effects. Complete this section of Worksheet 2 to evaluate the benefits of mitigation actions.

Table B-1. FOB Common Threats, Attack Tactics, and Mitigation Measures

Common Threats and Tactics	Common Mitigation Measures
Vehicle-Borne Improvised Explosive Device (VBIED). Most frequent mass casualty attack tactic. Could be single attack event or a distraction to enable follow-on VBIED attacks or ECP penetration. VBIED attack methods include: • Detonation in public access area • Detonation in FOB area that is accessible due to insufficient access control • Single vehicle attack on ECP or perimeter • Suicide vehicle attack on ECP • Multiple vehicle attack; first VBIED breaches the perimeter allowing deeper penetration for followon VBIEDs • During deliveries to or pickups from the FOB • In maintenance, garbage, and service vehicles	• Maximize standoff to keep attacks away from the FOB perimeter • Maximize standoff around individual inhabited structures within the FOB • Maximize standoff between perimeter and inhabited structures in the FOB • Ensure perimeter barriers and walls can stop vehicles and absorb detonation effects • Replace or fortify concrete barrier, unconsolidated stone, or masonry walls that fragment and become debris • Fill in windows to reduce glass hazard casualties • Construct guard towers and fighting positions that assist in identifying, engaging, and defeating VBIED • Establish SOPs for response to imminent threats • Conduct protection procedures training, including incident response and consequence management • Initiate access control procedures that deter, detect, deny, and protect against VBIED • Limit FOB access • Conduct vehicle inspections • Construct personnel bunkers for blast protection (requires attack warning) • Retrofit occupied structures (particularly existing conventional buildings) to increase blast protection. This would include retrofitting building walls that may fail and create hazardous debris. • Retrofit structures such as masonry walls and windows that can become fragmentation hazards to personnel.
Sniper and Other Direct Small-Arms Fire. Military or civilian pistols, rifles, shotguns, machine guns. Small arms attack methods include: • Shooters in moving or parked vehicles • Shooters in overwatch position inside or outside a structure.	• Use netting or other screens to obscure targets and personnel • Obtain counter surveillance equipment to detect adversary optics observing the FOB • Establish SOP for response to small arms fire • Utilize sniper detection equipment • Conduct protective training and exercises
Person-Borne Improvised Explosive Device (PBIED). Consequences will be highest where personnel are gathered such as pedestrian traffic around the ECP and high-occupancy facilities like dining facility. PBIED is unlikely to be over 50 lbs, but that is adequate to destroy houses and structurally damage buildings.	• Install personnel barriers that prevent access without inspection • Initiate access control and personnel inspection procedures to prevent PBIED • Limit FOB access • Construct access control facilities/barriers that reduce the likelihood of civilian casualties • Construct guard towers and fighting positions to assist in identifying, engaging, and defeating PBIEDs • Compartmentalize high occupancy facilities to limit blast effects • Install lighting and sensors to detect and assess PBIEDs • Conduct training and exercises of protection procedures

Table B-1. FOB Common Threats, Attack Tactics, and Mitigation Measures (Continued)

Common Threats and Tactics	Common Mitigation Measures
Improvised Explosive Device (IED). Hand-carried (includes pack animal/motor bike transit) used to cause casualties inside the FOB or outside among Coalition forces and gathered civilians. Used to damage a facility and its contents, left inside a facility to cause casualties, or left close to critical infrastructure power, fuel, or other assets. The IED could also be a decoy, or part of a multiple IED weapon attack. IED attack methods include: • In package delivered to FOB • Carried into the FOB by worker • Inside toy • In mail package or envelope	• Install personnel barriers • Initiate access control procedures that prevent IED placement from beyond the perimeter • Conduct vehicle and personnel inspection • Limit FOB access • Construct access control facilities/barriers that reduce the likelihood of civilian casualties • Compartmentalize high occupancy facilities to limit blast effects • Install lighting and sensors to assist in detecting and assessing IED • Institute random operational measures • Conduct protection procedures training, including incident response and consequence management
Rockets, Artillery, and Mortars (RAM). Indirect fire weapons usually launched from non-line-of-sight locations but can be fired from overwatch positions. and **Rocket-propelled grenades (RPG)**. Direct-fire weapons requiring line-of-sight. Russian RPG-7, RPG-18, and RPG-22; US M-72 Light Antitank Weapon (LAW).	• Construct personnel bunkers for blast protection • Provide full height sidewall protection for soft structures • Compartmentalize high occupancy facilities to limit fragmentation effects • Provide overhead protection to pre-detonate and absorb fragmentation from incoming indirect fire • Retrofit existing structures for protection from near miss and direct RAM hits • Use netting or other screens to obscure targets and operations • Employ standoff pre-detonation screens, barriers, and walls around targets to reduce RAM penetration • Construct guard towers and fighting positions to engage and defeat direct fire (RPG) • Conduct protection procedures training, including incident response and consequence management
Surveillance. Intelligence gathering by threat to locate targets and identify operations patterns, including response to alarms/attack in planning future attacks. Surveillance can be associated with: • Real or hoax attacks • On-base work crews • Vehicle delivery/receiving crews • Overlook positions, parked vehicles, and pedestrians	• Limit FOB access • Conduct random operational measures and SOP • Formulate a counter surveillance plan • Obtain counter surveillance equipment to detect adversary optics observing the FOB

Table B-2. Potential FOB Vulnerabilities

FOB Main Components	Vulnerability Considerations
--- PERIMETER SECURITY ---	
Standoff	• Do natural or installed barriers prevent vehicles from getting approaching the perimeter? • Can vehicles drive through the perimeter? • Is standoff from the perimeter to occupied facilities maximized?
Physical Barriers	• Are man-made or natural barriers available to deter vehicles and personnel? • Do barriers define the perimeter? • Do barriers conceal FOB activities? • Do barriers project physical and psychological deterrents to attackers? • Are barriers combined in layers and separated by a min. of 30ft? • Are areas on both sides of barriers unobstructed and maintained clear? • Do security forces keep barriers under observation?
Access Control (General)	• Is FOB access limited? To what type vehicles and personnel? • Are the movements of admitted personnel controlled?
Entry Control Points (ECP)	• Do ECPs provide primary and emergency entrances/exits? • Are recording and transmission devices such as cell phones, cameras, and pen/paper confiscated or registered at the ECP? • Is the defense layered? • Are ECPs designed to prevent high-speed vehicle approaches? • Are ECP personnel protected? • Is traffic (personnel and vehicle) segregated and channeled? • Do vehicle turn around/rejection areas exist? • Is vehicle speed management/reduction employed through serpentine traffic lanes and vehicle barriers? • Do segregated search areas provide line-of-sight denial from possible external surveillance? • Are overwatch positions hardened? • Is the perimeter gate (final denial barrier) hardened? • Do ECPs have functional zones that are well known to the security force (Approach, Access Control, Response, Safety Zones) and written into SOPs? • Approach Zone – Do the following apply to this zone: ○ Eliminate or reduce straight-line access from local entry/access roads? ○ Speed reduction of incoming vehicles through speed management techniques? ○ Sort traffic by vehicle type; begin the containment, segregation, and channelization of authorized vehicles and pedestrians? ○ Allow for verification of personnel and vehicles authorized access?

Table B-2. Potential FOB Vulnerabilities (Continued)

FOB Main Components	Vulnerability Considerations
	○ Provide adequate stacking distance for vehicles waiting entry? ○ Allow for initial verification of authorized access of personnel and vehicles? ○ Provide space to allow unauthorized vehicles that attempt to enter the ECP to be redirected? ○ Provide the first opportunity for early warning to identify potential threat personnel/vehicles, including those attempting entry through outbound traffic lanes? ○ Provide an off-site parking area for unauthorized vehicles? ○ Maximize protection of ECP security personnel operating in this zone? • Access Control Zone – Do the following apply to this zone: ○ Is personnel identification verified? ○ 100 percent inspection of personnel and vehicles? ○ Visitor control (visitor/vehicle passes)? ○ Overwatch for the ECP? ○ Vehicle speed management/reduction techniques? ○ Vehicle turn around and rejection area? ○ Contain, segregate, and channelize vehicle and pedestrian traffic? ○ Parking/transfer yard for authorized vehicles? ○ Maximum protection of ECP security personnel operating in this zone? ○ Exit points prevent unauthorized access? • Response Zone – Do the following apply to this zone: ○ Adequate reaction time to threats, operation of final denial barriers, and gate closure? ○ ECP monitored by overwatch? ○ Define the FOB perimeter? ○ Provide a hardened perimeter gate (final denial barrier)? ○ Integrate with perimeter security system and maintain small-base defense-in-depth concept? • Safety Zone – Does this zone extend from the passive and active barriers in all directions to protect site personnel from an ECP explosion?
Security Lighting	• Are all lights and hardware functional? • Does the system function well under adverse conditions such as rain and dust? • Does the system provide sufficient lighting? • Do unlit areas exist where personnel can approach the FOB without visible detection? • Is the lighted area (and areas that should be lighted) under security force observation? • Does the lighting system serve as a deterrent to intruders? • Does lighting affect the range of any electronic security systems during darkness?

Table B-2. Potential FOB Vulnerabilities (Continued)

FOB Main Components	Vulnerability Considerations
	• Are lights adjusted to glare in the direction of intruders and not toward security personnel? • Is backup power available?
Hardened Positions, Towers, Overwatch	• Do adjacent positions cover the entire perimeter with interlocking patterns of fire? • Do positions provide 360 degree observation? • Do positions cover critical areas within the FOB? • Are tower and overwatch positions hardened?
--- INTERNAL SECURITY ---	
Command	• Does the commander conduct a comprehensive protection program review? • Do FOB tenant organizations understand their security roles and responsibilities, and are they included in training and exercises? • Are tenants aware the FOB commander may exercise temporary operational or tactical control of tenant units? • Are areas of responsibility clearly defined, both inside and outside the FOB, for tenant units? • Are random operational measures employed and understood by security personnel?
Security Forces	• Do guards patrol in random patterns and locations? • Are restricted areas adequately protected and monitored? • Are all security forces, including response personnel, adequately trained? • Are ROE clearly defined and understood by security/ response personnel at the time of FOB occupation? • If non-lethal weapons are required, do security forces have proper training and understand any unique ROE?
Response Forces	• Do security forces project a high profile presence likely to deter potential attackers? • Are response forces capable of on-the-spot alarm and incident assessments? • Do response forces have the necessary personnel, equipment, and training for initial incident control and containment? • Can response forces adapt to specialized functions during incident emergencies? • Is the Quick Reaction Force prepared for: ○ Detainee operations? ○ Personnel and vehicles searches? ○ Casualty and evacuation operations? ○ Actions on Contact? ○ IED response? ○ Counter-sniper operations? ○ Civil Disturbance Control Operations? ○ Rapid checkpoint and/or roadblock operations? ○ ECP reinforcement? ○ Rapid observation activities?

Table B-2. Potential FOB Vulnerabilities (Continued)

FOB Main Components	Vulnerability Considerations
Random Operational Measures	• Do random operational measures include pattern changes such as guard shift changes and ECP SOP? • Do these measures include counter-surveillance to alter the external security appearance and force protection patterns? • Do random operational measures involve the command staff?
Mass Notification	• Does a mass notification capability exist? • Are personnel familiar with mass notification procedures?
Protective Construction	• Does a list of presumed critical assets exist? • Are assets prioritized by required level of protection? • Would damage to infrastructure and support facilities (billeting, electric, water, fuel, food, latrines, etc) cripple mission capability? • Is sidewall protection provided for high occupancy and critical assets such as the dining facility and Base Defense Operations Center (BDOC)? • Are high occupancy facilities compartmentalized? • Do critical assets have overhead cover that includes pre-detonation screens and shielding layers for RAM attacks? • Are bunkers and revetments available for protection of critical equipment? • Are occupied facilities spaced adequately to limit collateral damage? • Do occupied facilities have adequate standoff from the perimeter?
Incident Response and Consequence Management	• Are Incident Response and Consequence Management Plans current? • Are the plans exercised against at least high likelihood or significant consequence type attacks?
Communications	• Is the communications system secure? • Are system controls and auxiliary hardware adequately protected? • Are rapid system repair procedures and qualified technicians available? • Is backup power adequate? • Are systems components such as land lines installed to withstand blast effects? • Do redundant communications capabilities exist in case of system failure or destruction? • Are communications centers protected against electromagnetic eavesdropping?

Worksheet 1. Current Condition Risk

Asset: What is the asset name, location, description?

Threat: What are the presumed threat, tactics, and scenario?

Vulnerability: Why is the asset vulnerable in this threat scenario?

Event Likelihood Rating

9 Extreme	8 Extreme-High	7 High	6 High-Medium	5 Medium	4 Medium-Low	3 Low	2 Low-Negligible	1 Negligible
Event Likelihood: What is the likelihood of the event occurring? Consider asset threat, and vulnerability findings. Enter a rating from the scale above.							**Event Likelihood Rating**	

Projected Consequence Ratings

	Fatalities	Serious Injuries	Property Damage	Equipment Damage	Mission Degradation		
Estimate Losses ▶							
Likelihood Ratings ▶						**Sum of Consequences Ratings**	

Risk Score = (Event Likelihood Rating) X (Sum of Consequence Ratings). The higher the number, the greater the risk!	**Risk Score**	
Risk Scale: 5 - 45 Negligible; 46 - 90 Negligible-Low; 91 - 135 Low; 36 - 180 Low-Medium;181 - 225 Medium; 226 - 270 Medium-High; 271 - 315 High; 316 - 360 High-Extreme; 361 - 405 Extreme	**Risk**	
Subjective value established by the user. Values are typically sequential, beginning with "1" as the highest risk/asset priority.	**Risk Priority**	

Worksheet 2. Projected Post-Mitigation Risk

Vulnerability: Is the asset still vulnerable after risk mitigation actions? Why?

Event Likelihood Rating								
9 Extreme	8 Extreme-High	7 High	6 High-Medium	5 Medium	4 Medium-Low	3 Low	2 Low-Negligible	1 Negligible
Event Likelihood: What is the likelihood of the event occurring? Consider asset threat, and vulnerability findings. Enter a rating from the scale above.							**Event Likelihood Rating**	

Projected Consequence Ratings							
	Fatalities	Serious Injuries	Property Damage	Equipment Damage	Mission Degradation		
Estimate Losses ▶							
Likelihood Ratings ▶						**Sum of Consequences Ratings**	

Risk Score = (Event Likelihood Rating) X (Sum of Consequence Ratings). The higher the number, the greater the risk!	**Risk Score**	
Risk Scale: 5 - 45 Negligible; 46 - 90 Negligible-Low; 91 - 135 Low; 136 - 180 Low-Medium;181 - 225 Medium; 226 - 270 Medium-High; 271 - 315 High; 316 - 360 High-Extreme; 361 - 405 Extreme	**Risk**	
Subjective value established by the user. Values are typically sequential, beginning with "1" as the highest risk/asset priority.	**Risk Priority**	

Mitigation Effects				
Which mitigation actions most impact this threat-asset pair risk?				
How much does the risk change when mitigation actions are implemented?	Becomes Negligible	Reduced	Same	Increases
Is the risk reduction acceptable?	Y	N		
Is the remaining (residual) risk acceptable?	Y	N		

(Classification)

Worksheet 3. Risk Mitigation Actions

	Affected Assets & Their Priority	Action	Impacts (Positive and Negative)	Comments
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				

(Classification)

(Classification)

Worksheet 3. Risk Mitigation Actions

	Affected Assets & Their Priority	Action	Impacts (Positive and Negative)	Comments
1.				
2.				
3.				
4.				
5.				

(Classification)

APPENDIX C
BASE DEFENSE PLANNING TEMPLATE

Base defense planning is a methodical process that combines operational protection and mitigation strategies, site selection considerations, identified security requirements, and mission objectives. Early identification of protection requirements is essential to FOB base defense planning. Requirements established prior to construction reduce construction and manpower costs. Security measures established in the planning process are more easily applied than after FOB construction.

Joint Operation Planning Process (JOPP). JOPP is a logic-based process that examines mission objectives, suggests courses of action (COA), provides a means for best COA selection, and produces an operational plan or order (Figure C-1). JOPP supports interactive planning between the commander, staff, and subordinate commands. JOPP further defines the commander's mission intent, organizes staff objectives development, and ensures streamlined, effective mission planning.

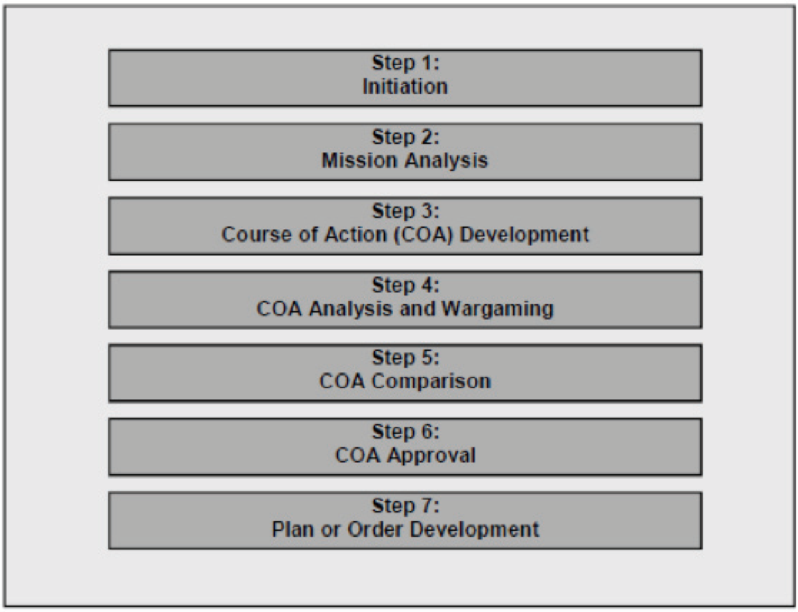


Figure C-1. The Joint Operation Planning Process (JOPP) (JP 5-0, *Joint Operations Planning*)

JOPP illustrates the planning process and types of information required for a FOB protection plan. Each service has also developed processes to guide their planning activities. The Army, for example, uses the Military Decision Making Process outlined in Field Manual 5-0, *The Operations Process.* This handbook does not advocate a single process since the key elements of plan development — mission analysis, COA development, COA selection, and publish orders — are common to all planning processes. Instead, JOPP is a joint service product and is presented here as a framework for FOB protection planning.

Step 1: Plan Initiation. JOPP begins when a possible military response is authorized to a real or potential crisis. Whether planning actually begins or not, the commander may act within approved rules of engagement (ROE) to an immediate crisis.

Step 2: Mission Analysis. This process reviews and analyzes orders, guidance, intelligence, and relevant ancillary information. The commander, planning team, and staff are provided with an understanding of the situation. This step can result in a revised mission statement pending commander approval.

Step 3: Course of Action (COA) Development. The commander's mission statement guides COA development. Planners examine each prospective COA for adequacy, feasibility, acceptability, and completeness with respect to the mission and commander's intent.

Step 4: COA Analysis and Wargaming. A detailed assessment of each COA with respect to the adversary and operational environment is conducted. Friendly COAs are wargamed against anticipated enemy COAs. This step reveals strengths, weaknesses, risks, and possible friendly COAs shortfalls. Wargaming also identifies branches and sequels that might require additional planning. Wargaming provides the most reliable COA assessment short of implementation. This step also allows the staff to reiterate initial design estimates.

Step 5: COA Comparison. COA comparisons objectively grade COAs against established command staff criteria. This identifies relative COA strengths and weaknesses, allowing those with the highest likelihood of success to be selected.

Step 6: COA Approval. Selected COAs are evaluated against established criteria and against each other, leading to a staff recommendation and the commander's decision.

Step 7: Plan or Order Development. The staff develops plans and operational orders based on COA selection and the commander's mission statement.

Transition is the orderly handover of a plan or order to those tasked with its execution. Transition provides staffs with SA and the rationale necessary for coherent planning-to-execution. The transition process, however, is ongoing. Staffs maintain running estimates and examine branches and sequels that necessitate order refinement.

Base Defense Plan. The base defense plan is necessary for development and implementation of a comprehensive FOB protection program. The FOB defense plan should:

- Convey the FOB commander's intent
- Provide a clear, concise mission statement
- Provide tasks and activities, constraints, and coordinating instructions
- Permit subordinate commanders to prepare supporting plans
- Focus on subordinate activities
- Promote initiative
- Include annexes containing subordinate information not included in the main defense plan

The FOB defense plan should focus efforts and resources toward a cohesive defense mission. A sample plan template is shown in Figure C-2.

(In Joint Operation Order [OPORD] Format)
SECURITY CLASSIFICATION
Copy No. ______
Issuing Headquarters
Place of Issue
Message Reference Number

Type and Serial Number of Operation Order.

References:

a. Maps or Charts

b. Time Zone. (Insert the time zone used throughout the order)
Task Organization. List here, in paragraph 3, or an annex. The defense organization specifies units providing forces for each defense element. Include attached or transient units and commanders' names. Also identify the defense requirements of US, HN, and civilians organizations. Determine and integrate capabilities valuable to base defense.

1. Situation. For each category below, describe the base defense environment.

a. Enemy Forces. Describe the threat, to include the composition, disposition, location, movements, and estimated strength of hostile forces and terrorists.

b. Friendly Forces. List friendly forces not covered by this operation order, to include the mission of the next higher HQ and adjacent bases, plus units not under base command whose actions affect base defense. These units may include MP or Air Force SF, fire support, naval coastal warfare forces, special operations forces, engineers, NBC decontamination, smoke, EOD, HN military, and civilian.

c. Attachments or Detachments. List elements attached to or detached from base units and the effective times.

2. Mission. Concisely state the commander's defense mission.

3. Concept of the Operation.

a. Commander's Intent. Describe the commander's mission so that subordinates have sufficient guidance to act independently.

b. Concept of Operation. Describe the commander's operational concept. Define critical facilities and establish protection priorities.

(1) Phasing. Define the commander's intended operational phases.

(2) Maneuver. Describe ground defense force organization, counters to penetrating attacks, supplementary defensive positions, and reaction force responsibilities. Describe and prioritize counterattacks.

(3) Fires. Describe supporting fire plans such as mortars, smoke, and aviation support.

c. Tasks for Subordinate Elements. Describe specific tasks for each subordinate defense element listed in the Task Organization.

d. Reserve. Provide instructions to the base's mobile reserve.

e. Coordinating Instructions. Provide instructions applicable to two or more elements, or the entire command.

(1) Control Measures. Define access and movement restrictions in critical areas to include personnel, materiel, and vehicles. Security measures may also be outlined here.

(a) Base Boundary. Define the base boundary and include a description of planned counter-standoff attacks.

(b) Personnel Access. Establish control pertinent to each area or structure.

1. Authority. Provide access authority.

2. Criteria. Provide access criteria for unit contractor personnel, local police, and armed forces.

3. Identification and Control

a. Describe the ID and control system for each area. Disseminate identity requirements to all base personnel, including visitors.

b. Describe how the system applies to unit personnel, visitors, vendors, contractor personnel, maintenance, and support personnel.

(c) Materiel Control Procedures

1. Incoming

a. List requirements for admission of materiel and supplies.

b. List special controls on delivery of supplies to restricted areas.

2. Outgoing

a. List required documentation.

b. List special controls on delivery of supplies from restricted areas.

c. List classified shipments.

(d) Vehicle Control

1. State policy on vehicle registrations.

2. State policy on vehicle searches.

3. State policy on parking.

4. State policy on abandoned vehicles.

5. List controls for restricted area access.

(e) Train Control

1. State policy on railcar searches.

2. State policy on securing railcars.

3. State policy on train ingress/egress.

(2) Security Aids. Indicate how the items below will be implemented.

(a) Protective Barriers

1. Definition.

2. Clear zones.

a. Criteria.

b. Maintenance.

3. Signs.

a. Types.

b. Posting.

4. Gates.

a. Hours of operation.

b. Security requirements.

c. Lock security.

d. Protective lighting system. Operation, control, inspection, direction, actions during power failures, emergency lighting.

(b) Intrusion Detection Systems

1. Types and locations.

2. Security classifications.

3. Maintenance.

4. Operation.

5. Probability of Detection

a. Limitations.

b. Compensating measures.

c. Redundant capabilities.

(c) Communications

1. Types.

a. Primary.

b. Alternate.

2. Operation.

3. Maintenance.

4. Authentication.

(3) Interior Guard Procedures. Describe instructions for interior guard personnel, both fixed and mobile. Attach detailed instructions such as special orders and SOP. Ensure that procedures include randomness.

(a) Composition and organization. Interior security and support guards may be civilian contractors.

(b) Tour of duty.

(c) Essential posts and routes.

(d) Weapons and equipment.

(e) Training.

(f) Military working dogs.

(g) Method of challenge.

(h) Alert force.

1. Composition.

2. Mission.

3. Weapons and equipment.

4. Location.

5. Deployment concept.

(4) Rules of Engagement. Define the circumstances and limitations under which US forces will initiate combat engagement with encountered adversary forces.

(5) Contingency Plans. Define emergency response procedures. Attach detailed plans such as anti- terrorism, bomb threats, natural disasters, and firefighting.

(a) Individual actions.

(b) Alert force actions.

(6) Security Alert Status.

(7) Air Surveillance.

(8) Noncombatant Evacuation Operation Plans.

(9) Coordination with HN or Adjacent Base Plans.

(10) Measures for Coordination with Response Force and Tactical Combat Forces.

(11) Procedures for Update of This OPORD. If the OPORD is not effective upon receipt, indicate its effective date.

4. Administration and Logistics. Detail base defense logistics support. State the administrative and logistic arrangements applicable to the operation. If the arrangements are lengthy, include as an annex.

a. Concept of Combat Service Support. Summarize base defense from the combat service support perspective.

b. Materiel and Services. List supply, maintenance, transportation, construction, and labor allocation.

c. Medical Services. List treatment, hospitalization, and evacuation plans for military and civilian personnel.

d. Damage Control. List firefighting, debris clearance, and emergency construction plans.

e. Personnel. List reporting, replacements, casualty reporting, and other procedures pertinent to base defense.

f. Civil Affairs. Describe control of civil populations, refugees, and related matters.

5. Command and Control

a. Communications. Provide pertinent communications nets, operating frequencies, codes, recognition and identification procedures, and electronic emission constraints. Refer to annexes or signal operating instructions as needed.

b. Command

(1) Joint and multinational relationships. Define command relationships, to include command succession. Shifts in relationships must be specified. Detail these relationships in chart form or as an annex.

(2) Command posts and alternate command posts. List locations of the BDOC, BCOC, and alternate sites, along with activation and deactivation times.

6. Acknowledgment Instructions

Annexes:

A. Task Organization

B. Intelligence

C. Operations

D. Logistics

E. Personnel

F. Public Affairs

G. Civil Affairs

H. Engineer Support

J. Command Relationships

K. Communications

L. Force Protection

M. Host-Nation Support

N. CBRNE

Distribution:

Authentication:

Figure C-2. Sample Base Defense Plan
(JP 3-10, *Joint Security Operations in Theater*)

References:

JP 3-10. *Joint Security Operations in Theater*, 03 February 2010.

JP 5-0. *Joint Operations Planning,* 11 August 2011.

APPENDIX D
FOB SECURITY

Security is a condition that results from the establishment and maintenance of protective measures to defend against or deter acts of aggression. In current operational environments, US forces are vulnerable to enemy surveillance, weapons and tactics. Therefore, deployed military units, forward-based activities, and FOBs must protect against threats to interrupt or impair operations with established security measures.

Effective base security requires planning, execution, and assessment to mitigate hostile actions. Coordination among FOB-assigned units is critical to this effort. FOB commanders should employ a team approach to develop security procedures and manage the protection mission. This facilitates intelligence distribution, coordinated protection operations, and incident response management.

Commanders tasked to a new or existing FOB should first establish or reassess base perimeter security measures. Once these measures are established, attention can be directed inward to personnel and FOB-interior asset security measures.

Perimeter Security. Perimeter security is the first line of FOB defense and should safeguard the FOB's property, personnel, and mission. This is accomplished through the prevention, detection, and response to enemy threats including dedicated ground attack, rocket, artillery, and mortar (RAM) attack, vehicle-borne improvised explosive devices (VBIED), personnel-borne improvised explosive devices (PBIED), sabotage, theft, trespass, espionage, and surveillance. The perimeter security mission is not limited to the actual FOB perimeter, but extends outward to surrounding uncontrolled areas that provide enemy surveillance and staging locations. Perimeter security systems should provide an integrated, layered, defense-in-depth that focuses on the capabilities shown in Figure D-1.

Recommended Perimeter Security System Capabilities

- Measures to delay or disrupt an attack
- Control of personnel and vehicles entering the FOB
- Early warning that an attack is imminent or under way
- Detection of attempted enemy surveillance
- Adequate VBIED blast standoff for occupied buildings
- Line-of-sight protection from direct-fire, standoff, and ballistic weapons
- Exterior clear zones to increase threat entry/exit times

Figure D-1. Recommended Perimeter Security System Capabilities

Rules of Engagement (ROE). Simply stated, ROE should address when, where, how, and against whom force should be used. ROE should specify actions security personnel may take without consulting higher authority and those actions taken only if explicitly ordered by higher authority. ROE provide the rules and procedures for the use of deadly force by security personnel. ROE is defined as directives issued by competent military authority which delineate the circumstances and limitations under which US forces will initiate and/or continue combat engagement with other forces encountered. Security related ROE must conform to the law of war; therefore, the ROE formulation process should account for operational, political, and diplomatic factors such as host nation laws concerning defense of others, self defense, and protection of military facilities. As a result, ROE may restrict or prohibit some uses of force that the law of war would allow.

Prior to drafting ROE for FOB security, commanders should review immediate higher-level command directives. Although ROE must be consistent with published orders, ROE should also be tailored to individual unit missions. If too restrictive, ROE could reduce combat effectiveness, inhibit initiative and put the force at greater risk. Likewise, overly lenient ROE can lead to collateral damage and fratricide. ROE are generally less restrictive with increasing ability to discriminate among friendly, enemy, and neutral personnel or situations. Essentially, ROE should strike a balance between protection requirements and FOB mission objectives.

The first rule of ROE must always include the inherent right to use of force in self-defense. ROE should specify only the minimum essential force necessary to neutralize the threat; use of force should be proportional to that threat. Effective ROE should not assign specific tasks or tactical solutions, but may extend to specific weapon systems employment criteria. ROE should evolve as protection missions change and be designed with flexibility to support the mission through various operational phases and changes in threat. ROE must be clear, enforceable, tactically sound, consistent, and legal. Commanders should continually review ROE to ensure effectiveness and mission consistency. Security force personnel should receive ROE application training prior to performing any aspect of FOB security. Basic ROE considerations for commanders are summarized in Figure D-2.

Rules of Engagement (ROE) Considerations

- □ Do ROE conform to the law of war (ROE may be more restrictive than the law of war requires)?
- □ Are ROE consistent with existing guidance (DoD, Joint Staff, COCOM, higher command)?
- □ Are nation-specific ROE applicable to multinational operations?
- □ Have any inconsistencies between service component and multinational ROE been reconciled?
- □ Are service members trained and familiar with ROE?
- □ Are ROE flexible, detailed, and understandable?
- □ Do ROE preclude the indiscriminate use of deadly force?
- □ Do ROE allow mission accomplishment and self-defense?
- □ Are ROE consistent throughout the force (an increased challenge in multinational operations)?
- □ Do physical factors affecting the ROE preclude certain weapons and munitions?
- □ Do ROE anticipate changes in the operational environment?

Figure D-2. Rules of Engagement Considerations

Security Forces. Along with physical security measures, FOB security forces are the first line of defense against attack. Security forces are specifically organized, trained, and equipped for FOB security functions. FOB commanders must interact with tenant unit commanders to ensure that personnel assigned to security forces are properly trained. Regardless of its makeup, the security force should be capable of these functions:

- Detect, deter, and defeat insurgent and terrorist attacks
- Prevent and deter theft, fire, accident, trespass, sabotage, and espionage
- Protect life, property, and individual rights
- Enforce ROE, regulations, and statutes

Figure D-3 provides general security force considerations.

Security Force Considerations

□ What commander has overall responsibility for FOB security forces?
□ What is the commander's intent for security forces?
□ What security force strength and composition are required to meet the commander's intent?
□Are the strength and composition of security forces appropriate for the required protection?
□ What is on the security force mission-essential task list?
□ What critical assets or unique systems are located at the FOB?
□ Is sufficient security equipment available and are personnel trained in its use?
□ What specialized equipment is required by security forces?
□ What reinforcements are required for the primary security force?
□ Who interfaces with auxiliary security elements?
□ Are auxiliary security elements trained on security SOP?
□ Do auxiliary security elements have required equipment and training?
□ What is the alert notification procedure for these elements?
□ What are security force ROE?
□ Who authorizes direct action by security force personnel?
□ Is the security force included in FOB protection plan development?
□ Are periodic weapons and ammunition inspections conducted?
□ Does the security force require specialized training?
□ Are no-notice exercises and rehearsals conducted?
□ Is specialized training for securing critical assets or unique systems provided?
□ Has coordination been established for patrols outside the FOB?
□ Have security force SOP been developed?
□ Does the FOB maintain a Quick Reaction Force (QRF)?
□ Does the QRF receive adequate training? Are sufficient personnel available to staff the QRF?
□ Are intrusion detection systems (IDS) employed to reduce manpower requirements?
□ Do visitor escort procedures exist to preclude the use of security force personnel as escorts?
□ Are guard assignments, times, and patrol routes varied to avoid establishing routines?

Figure D-3. Security Force Considerations

Security Post Requirements. Specific post requirements and operating procedures should be established in coordination with FOB security force personnel. Security forces are normally deployed throughout the FOB in various operating configurations that include:

- **Entry Control Points (ECP)/Gates.** ECPs and gates should be limited in number and hours of operation due to high manpower requirements. Include security force augmentation requirements during peak traffic hours in post-manning calculations. However, drawing personnel from mobile posts to man fixed posts reduces emergency response capabilities.

- **Perimeter Observation Posts (OPs)**. The number of perimeter posts required is in direct proportion to threat and security objectives. Effective perimeter security requires a combination of physical security measures to include physical barriers, fencing, protective lighting, and IDS. The number and location of perimeter OPs should be based on the requirement that all physical security measures remain under continuous observation and assessment by security force personnel.

- **Restricted Area Posts**. Restricted areas are normally established to limit critical asset access. Assign security responsibilities in restricted areas to an interior guard force. The interior guard force strength should be appropriate for protected asset importance and threat.

- **Mobile/Roving Patrols.** Mobile patrols can be vehicular or foot patrols assigned to a specific FOB area. For example, a roving patrol may be dispatched to conduct a preliminary alarm assessment, followed by a QRF if necessary. Roving patrols discourage FOB infiltration. However, intruders can determine established patterns if patrols are predictable. Roving patrols can mitigate this weakness with random patrol routes and times, or by occasionally stopping to observe random areas for extended periods. Roving patrols usually employ night vision devices (NVD) and blackout lights, and are most effective when integrated with fixed OPs on the FOB perimeter. Roving patrols can also rapidly respond to suspicious activities identified by fixed OPs and inspect dead zones not visible from the OP. Roving patrols outside the fence line must coordinate with the HN.

- **Visitor Escorts.** Avoid visitor escorts duties by security force personnel. Instead, assign visitor escort to the unit or facility sponsoring the visitor. Those receiving visitors should escort them to and from the FOB as regulated by standing access procedures.

Security Force Orders/Checklists. FOB commanders should publish, sign, and maintain security force orders and checklists that detail responsibilities and authorize security force personnel to enforce regulations. Checklists should be specifically written for each post and detail guard duties. Checklists should help security personnel identify threats and take actions not specifically spelled out in the ROE. Checklists should generally contain the following:

- Post-specific ROE scenarios and instructions for the application of deadly force
- Daily intelligence briefs
- Range cards
- Post-specific duties, hours of operation, required uniform and equipment, and guidance for the safe handling of weapons
- Training requirements for security personnel and designated posts
- Security force chain of command

Orders and checklists should be concise and periodically reviewed. Copies should be maintained at each post. Checklists should also assist guards to identify threats and take actions not defined by the ROE. For example, checklists should explain FOB-wide alert procedures.

Security Force Training. All assigned security forces should be trained in the following areas:

- The use of force, ROE, and firearms safety
- Weapons training and qualification
- Legal aspects of jurisdiction and apprehension
- Mechanics of apprehension, search, and seizure
- General and special orders and all aspects of the security force order
- Use of security force equipment
- Threat awareness

Secondary security force topics of awareness include:

- Current FPCON and threat level
- Recent local surveillance trends
- HN customs, courtesies, and sensitivities
- Basic counter surveillance techniques
- Individual protective measures
- CBRNE personal protective measures
- How to inspect vehicles, packages, work, and living spaces for IEDs
- Use of a phrase card in the HN language
- Use of emergency phone numbers and points of contact

Security force personnel, QRF, medical response, and EOD personnel all require contingency operations refresher training and exercises. The FOB population and command structure should also participate in regular drills and exercises tailored to various threats. Examples of exercises include:

- Missile attack
- Mortar attack
- Countersurveillance operations
- Sniper attack
- IED detection at ECP/gate
- Dedicated attack by an assault force

Security Force Equipment. Types and quantities of security force equipment are based on available resources and the mission. Situational requirements such as HN agreements, asset protection, and threat conditions also affect the issuance of security equipment.

The basic security force personnel weapons assignment should be a service pistol, service rifle, or shotgun for routine duties. Additional weaponry, such as crew-served weapons, can be issued depending on security force level of training and FOB commander directives.

Provide security force vehicles for guards, patrols, and QRF. Provide vehicles equipped with radios and configured for the safe transportation of passengers and prisoners. Reliable communications equipment optimizes security force performance and should also be available at all security posts.

Quick Reaction Force (QRF). QRFs are an identified, trained, and equipped force that is an integral part of the FOB security mission and provide rapid response to unusual or hostile situations. QRF are typically equipped to defeat Level I and Level II threats (See Chapter 2). Specific organization and planning requirements are driven by mission, enemy, terrain, weather, and available personnel. QRF may be attached or assigned, but are normally TACON to the FOB commander. QRF capabilities must be continually assessed and upgraded based on the threat and operational environment. QRF perform three interrelated functions:

- Deterrence. QRF are a visible reminder of FOB counterattack capabilities.
- Assessment. QRF are an essential element of IDS and typically responsible for on-the-spot assessments of alarms or incidents.
- Containment. QRF often provide initial incident control and containment.

QRF size may vary from a small team to a large squad or platoon. QRF response times vary and depend on the FOB size and layout. If manning requirements exceed security force levels, augmentation forces may be required to fill empty slots. These forces must be fully trained prior to deployment.

QRF develop and implement drills. The two events most often encountered are indirect fire and direct assault. QRF also respond to suspicious vehicles or personnel and protect mission essential and vulnerable areas. QRF should be specifically trained for the tasks shown in Figure D-4.

Recommended FOB QRF Training Tasks

- Friendly and enemy recognition
- Actions on contact
- Find and secure impact sites
- Call for fire and employment of fixed and rotary wing support
- Communication techniques to include hand and arm signals, challenge and password, running passwords, the use of pyrotechnics, and other recognition signals
- React to unexploded ordnance
- Enemy prisoner of war (EPW) procedures
- Evacuation and cordon activities
- React to hostage situation

Figure D-4. Recommended FOB QRF Training Tasks

QRF must fully understand the base defense plan through periodic rehearsals. QRF should be familiar with base barriers, sector sketches, fire support, and local medical evacuation (MEDEVAC) procedures. QRF must also exercise base SOP and ROE.

FOB commanders normally have authority to employ QRF. Prior to employment, QRF commanders should be briefed on mission specifics. If QRF are committed, BDOCs should notify medical facilities in the operational sector and direct Air Liaison Officers (ALO) to alert air support operations centers (ASOC). BDOCs should also alert either the supporting fire cells or fire support coordination centers (FSCC) to establish no-fire areas around deployed QRF. QRF operations outside the FOB perimeter should be coordinated with AOR command HQ. QRF commanders update BDOCs on force location and disposition.

Random Operational Measures. Random operational measures are intended to change a FOB's apparent security posture. Random measures alter the FOB's external appearance and frustrate adversary surveillance efforts.

The impact of random operational measures is difficult to quantify since success results in fewer or no attacks. As with any changes to routine and tempo, random measures could lead to a temporary increase in accidents and equipment demands. However, assets and routines can be obscured to outside observation. Also, variations in security routines heighten the awareness of FOB personnel to security issues.

References:

JP 3-10. *Joint Security Operations in Theater,* 03 February 2010.

JP 1-04. *Legal Support to Military Operations*, 01 March 2007.

This page intenionally blank

APPENDIX E
ACCESS CONTROL MEASURES

Access control measures screen personnel, vehicles, and materials to ensure safe, authorized FOB entry. These measures also detect contraband, reduce theft, prevent trespassing, and discourage terrorism, sabotage, and espionage. Access control should not be confused with entry control, which in this handbook refers to physical structures that allow or prevent access and are described in Chapter 6.

FOB commanders must develop, establish, and maintain access control policies that include the following:

- Defense-in-depth from the FOB perimeter inward to critical assets
- Intended degree of control over personnel, material, vehicles, and equipment entering or leaving the FOB
- Search procedures for personnel and vehicles entering, within, or leaving the FOB
- Procedures for forced removal from or denying access to the FOB
- Random measures that visibly enhance FOB security and reduce the utility of hostile FOB surveillance

Access control procedures should significantly increase the time required to forcibly breach an ECP or gate. Control procedures should also delay attackers in reaching critical assets and inhibit escape from the FOB.

Personnel Access Control. Tailor personnel access control measures to each FOB and its critical assets. Control policy should clearly define the granting authority and establish access criteria. Apply controls uniformly to visitors, vendors, contractors, host nationals, police, and military forces. Controls should also establish badge identification procedures and define personnel search procedures.

- **Access Control Lists.** Access control lists contain the names of personnel with authorized FOB access. Strictly control such lists and updated often. Never display lists to the general public. All entering personnel must be positively identified on the access control list prior to FOB admittance.

- **Pass-and-Badge System**. Pass-and-badge systems are typically employed for high volume access control. Badges should contain a picture and relevant individual information. However, badges should not contain personal information of any kind, nor identify badge holders as US soldiers or civilians. Color-coded badges are most useful in zoned or sectored FOBs. The color indicates the specific zone(s) to which personnel are restricted. Include the following in a pass-and-badge system:

- o Photo
- o Name
- o Duty
- o Title
- o Badge Number
- o Expiration Date
- o A unique mark for counterfeit badge detection

- **Exchange-Pass System.** An exchange-pass system provides more rigor ous FOB access control. Entering personnel must exchange an ID card or pass for a separate identifier badge. This is an effective identification system for large groups and requires personal interaction, allowing closer visitor scrutiny by security personnel.

- **Escort System.** Escorting is an effective means of personnel access con trol, particularly for contracted workers/vendors. However, escorts must remain with visitors at all times. Assign military personnel attached to the FOB as escorts. Escorts must ensure that all visitor materials are searched for contraband, weapons, or explosives prior to entry. Also, escorts must secure visited areas prior to departure and ensure no packages or other materials are left behind.

Contractor and Vendor Access Control. Contractors and vendors might be employed for FOB kitchen and custodial services, utility maintenance, and other support functions. Establish background screening procedures prior to allowing contractor access. However, potential threats can also be mitigated by limiting the number of outside contractors. Also, minimize fraternization between contractors and FOB personnel.

- **Background Investigation.** All potential contractors and vendors should receive preliminary employment screening. This will help identify radical or anti-American workers attempting to enter the FOB. Important background issues include:

- o Do contractors have valid identification papers?
- o Do contractors have any history of terrorist activity?
- o Do contractors have mental or physical issues that could endanger other personnel?

- **Control.** A pass-and-badge system coupled with escort is the most effective means of contractor control. Color-coded pass badges identify the areas of permitted access and level of escort required. When contractors work outside assigned zones, escort is required. Collect and reconcile badges daily to ensure all contractors have exited the FOB.

- **Access Lists.** Access lists are used in conjunction with the pass-and-badge system. If photo IDs are not available, security personnel shouldhave photographic records of authorized contractors.

- **Contractor/Vendor Uniforms.** If resources allow, provide distinctive uniforms that enhance contractor visibility. Uniforms must be controlled similarly to badges. Detain contractors without a proper uniform, badge, identification, or authorized FOB access, and contact HN security forces.

- **Control Officer.** Designate a contractor liaison or control officer for contractor issues. This officer should ensure that all contractors and vendors attend indoctrination courses to learn access control and security policies. Similarly, instruct FOB personnel and tenant units on escort procedures and actions to take in the event of suspicious activity or attack.

- **Parking**. Off-site parking must be located outside the effective FOB and ECP standoff zones. Transport contractors to the FOB with trained personnel unless off-site parking is provided. Contractors should enter the FOB only at a designated ECP.

- **Packages.** Closely restrict contractors' personal affects, carry bags, and packages allowed onto the FOB. Search all such items and packages thoroughly. Detain contractors exiting or entering the FOB with unauthorized items. Conduct custodial and food service personnel checks of all enclosed, obscured, or unidentified packages on entry and exit.

OPSEC/COMSEC/INFOSEC. Operations security (OPSEC), communications security (COMSEC), and information security (INFOSEC) procedures must be protected from contractors and vendors. Assume that contractor personnel are either deliberately or subconsciously collecting information at all times. Such information will be sought by enemy forces, insurgents, or terrorists. Therefore, conversations around contractors should be guarded; do not openly discuss details of FOB access control, security, and ECP procedures.

Work products and procedural information must be secured in the presence of contractors. Do not post sensitive information on visible bulletin boards or leave working desks unattended. Shred or destroy mail, faxes, envelopes, and correspondence (including envelopes). Never assume HN personnel do not understand English.

Vehicle Access Control. ECPs are often the most vulnerable sectors of a FOB perimeter and frequently targeted for adversary attack. ECP vehicle access control procedures must include:

- Vehicle and occupant search methods (random, 100 percent, incoming and outgoing)
- Security force requirements
- Equipment requirements
- Facilities requirements

Establish specific vehicle search procedures based on FOB mission, operational constraints, manpower, equipment, and special detection equipment. Vehicle search techniques are described below.

- **Visual Searches.** Visual searches locate hastily placed IED, or physical indicators such as extraneous wires and altered engine components. Security mirrors are limited in that personnel cannot see the entire vehicle's underside. This problem can be mitigated with inspection devices such as the Under Vehicle Surveillance System (UVSS). Entering vehicles pass over this camera system at the ECP allowing security personnel to remotely view visual color imagery of the vehicle's undercarriage. Figure E-1 shows a commercially available UVSS.

Figure E-1. Under Vehicle Surveillance System (WM Robots LLC)

- **Mechanical Searches.** Mechanical searches are deliberate efforts to locate suspected IED. Occupants must dismount the vehicle and leave doors, compartments, the hood, and trunk open. Security personnel tap expected hollow areas such as doors, side panels, and exhaust systems. The vehicle's air filter, engine reservoir fluids, glove compartment, spare tire, gas tank, and electrical system (lights, ignition wiring, etc.) are examined for anomalies. A long pole or gauge is used to probe fluid tanks for submerged objects.

  Mechanical searches can be enhanced with devices such as the Vehicle and Cargo Inspection System (VACIS). This commercial system employs gamma ray imaging technology to inspect cargo and vehicle contents. VACIS are typically mobile and project a small footprint at access control areas. Figure E-2 shows a mobile VACIS employed for port inspections.

Figure E-2. Vehicle and Cargo Inspection System
(Science Applications International Corporation)

- **Military Working Dog (MWD)** Searches. MWD detect the scent of certain explosives. However, heat and long hours will significantly degrade MWD effectiveness. Periods of MWD rest should be planned to coincide with ECP closure. The techniques below derive from USAF Handbook 10-2401, *Vehicle Bomb Mitigation Guide*. Although specific search procedures will vary, these steps are typical:

  1. The driver dismounts the vehicle, opens doors and compartments, is escorted to a holding area, and is separately searched.
  2. MWD teams approach the vehicle's downwind side.
  3. The team searches in a counterclockwise manner along the fenders, wheel wells, hubcaps, spare tire, and bumpers (see Figure E-3).
  4. Opened compartments, vehicle seats, and floorboard are searched.
  5. Packages in the vehicle are searched.

  If vehicle searches reveal suspicious packages or activities, security personnel must follow FOB-specific procedures regarding area evacuation, EOD notification, and chain-of-command notification.

Figure E-3. Explosive Detector Dog search

- **Package Searches.** Examine all packages, baggage, and personal carry items for weapons and explosives. Use MWD if available. Require drivers to open all personal items, packages, and baggage.

- **Individual Searches.** Inspect all incoming personnel for weapons, explosives, and triggering devices prior to FOB entry. Handheld metal detectors and physical searches (frisking) are the best means of individual search.

- **Vehicle Search Guidance.** Establish FOB-specific vehicle search guide lines. A vehicle is deemed suspicious if the driver is hesitant, nervous, or ignores/disobeys security personnel commands

Search vehicles from a terrorist or insurgent's perspective. Consider novel hiding places for weapons or explosives. Search tractor trailers with MWD, if available. Methodically inspect all cargo. If necessary, methodically unload the cargo for inspection. More detailed vehicle search guidance is provided in the procedures below:

Vehicle Search Procedures

- On instruction from security personnel, the driver enters the vehiclesearch area, dismounts, and opens all compartments, doors, and bags.

- Driver and passengers are escorted to a holding area that isolates occupants from their vehicle. Occupants are searched with portable metal detectors. With cause, a personal, physical search is conducted. Occupants remain under constant observation by armed personnel.

- An MWD team (if available) searches vehicle engine compartment, trunk, gas tank, interior compartments, walls, doors, upholstery, cargo areas, and packages.

- Security personnel tap vehicle doors and walls to ensure hollowness. Doors are tested for excessive weight.

- The engine compartment is searched for extraneous wires, improper reservoir fluids, new engine components, or other anomalies.

- An MWD team sweeps all cargo vehicles. Cargo containers are ran domly opened. Storage and gas tanks are probed. Commercial vehicles are inspected with the Mobile Vehicle and Cargo Inspection System (MVACIS), if available.

- The cleared driver or security personnel move the vehicle to a ramp or search pit.

- The vehicle undercarriage is inspected for extraneous wires, new components, suspicious wheel wells, and modified exhaust systems.

Exterior Vehicle Search

- Systematically search vehicle from bottom to top.
- Search by feel in non-visible areas. Inspect vehicle for recent body repairs, fresh paint, or external surface tampering.
- Inspect the vehicle undercarriage with a flashlight and creeper, if available.
- Inspect the suspension, drive train, wheel wells, bumpers, beneath the engine, and above the gas tank.
- Searchfor devices taped, tied, or otherwise attached to the undercarriage.
- Inspect for an unusually clean undercarriage, the presence of weld marks, or other indications of recent modifications.
- Inspect vehicle system connections such as gas lines and exhaust. Inspect the exhaust pipe for hidden objects.

Engine Compartment Search

- Begin at the front most corner edge on the battery side and inspect inward.
- Check for extraneous battery wires.
- Inspect clean or new components, devices, and wiring.
- Check beneath larger components such as the air filter and fan blade housing for hidden devices.
- Inspect all fuel and liquid containers.
- Check for extraneous hood light and headlight wires. Inspect empty sockets.

Vehicle Trunk Search

- Begin at the outer trunk edge and inspect inward.
- Inspect packages and electronic devices. Inspect tool boxes and tire tools.
- Inspect loose or extraneous electrical tape or wires.
- Search for hidden compartments beneath the tire well and tire tool storage area.
- Inspect brake and turn lights for extraneous wires.
- Inspect behind the rear seat.

Vehicle Passenger Compartment Search

- Begin at the floor and work up.
- Search for extraneous or unexplained electrical tape, wires, or electronic devices.
- Check beneath floor mats for wires or switches.
- Inspect beneath vehicle seats with a flashlight.
- Inspect ashtrays.
- Examine door panels for signs of tampering.
- Inspect the glove box.
- Check beneath the dash for extraneous wiring. Examine dash modifica tions such as extra switches or gauges.
- Inspect the roof liner for bulges, rips, or repairs

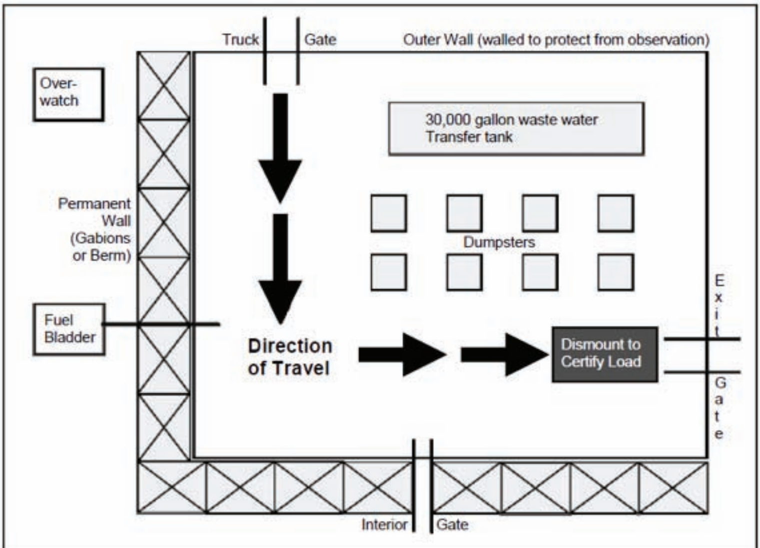
Materiel Delivery Control. Large bulk-material delivery vehicles such as water, fuel, and cement trucks cannot be screened with traditional MWD procedures. Concealed IEDs on these vehicles remain among the most serious FOB threats. However, simple but effective techniques can increase protection with minimal support demands. Successful, in-theater examples are detailed below.

- **Maintain positive control of trucks at all times**. Logistics convoys, such as food and water transports, are positively controlled. Service trucks remain in the FOB when not in use and drivers are transported to the site. Trucks exiting the FOB are escorted to waste disposal sites and remain under surveillance by military personnel.

- **Maintain constant positive control of trucks**. Assign convoy escortsfrom cargo loading at the point of supply to material yard delivery. Trucks load simultaneously and then convoy to the delivery point. Trucks are inspected prior to load and are under control of military personnel during the service period.

- **Develop a material load transfer (trans-load) yard where trucks are directed to unload** (Figure E-4). The material yard is best placed in a corner of the FOB and can be used for the transfer of gravel, waste, and fuel. This technique prevents unsearched trucks from entering the FOB through other truck or soldier gates and reduces ECP vehicle back-ups

Include a reinforced perimeter and overwatch positions at the trans-load yard. Signs should direct trucks through the download area. Trucks are moved forward with beds up to a check point at the far side of the download area. A majority of the under carriage can be seen with the bed up. Conduct overwatch of the trans-load area from a secure position.



Load Transfer Yard Operation Notes:

- Delivery on certain days only
- Material moved inside FOB by cleared trucks
- Driver stops at entry, sets tailgate chains; no contact and observed by over-watch
- Pull through yard and dump load (or transfer solid waste, liquid waste, or fuels)
- Stop, exit vehicle, and have ticket certified

Figure E-4. Typical Load Transfer Yard

Trans-load yards should be developed by the Director of Public Works (DPW) or equivalent and may support multiple FOBs. An MCAP Bulldozer (Figure E-5) may be required to support cargo spreading, inspection, and stockpiling

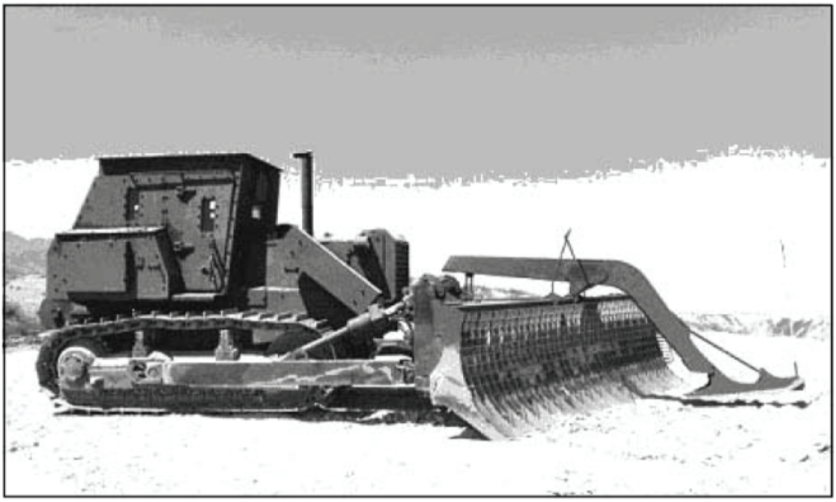


Figure E-5. Mine-Clearing/Armor Protection (MCAP) Bulldozer

A final technique, though least preferred, is to dismount drivers in a holding area and move the trucks to a separate waiting area. Vehicles are then searched privately. MVACIS, MWD, or probes may be available to supplement mirrors and physical checks. This technique is only employed when a trans-load area is unavailable and will generally increase material delivery cycle time.

References:

Department of Defense. *Vehicle Inspection Guide,* 2007.

This page intenionally blank

APPENDIX F
INFRASTRUCTURE PROTECTION

Infrastructure such as water supply, roads and bridges, and electric power support the basic services required within a FOB and enable a FOB's mission. The infrastructure support for a FOB includes infrastructure both on and off the FOB. There is additional infrastructure, outside the scope of this appendix, that supports the Host Nation inhabitants, economy, and local government, and is of concern to those FOBs with reconstruction missions (FOBs with Provincial Reconstruction Teams) but which is not directly required for FOB support. Destroying, controlling, or adversely impacting vital infrastructure can impact a FOB's mission.

Infrastructure protection is driven by a systematic analytical risk management process (see Appendix B, Risk Management). Infrastructure protection is security-related, time-sensitive, and resource-constrained. Such protection can only be effective if applied by commanders and periodically upgraded in accordance with changes in the operational environment. Critical tasks include:

- Identify critical infrastructure or assets essential to mission success (fire suppression, HAZMAT, sewer treatment, water supply, electrical systems, and computer systems)
- Determine the threat(s) to FOB infrastructure
- Analyze infrastructure vulnerabilities
- Assess the consequences of critical infrastructure degradation or loss on mission
- Assess the risk to critical infrastructure (possibility of loss or degrada tion times consequences to the FOB mission)
- Apply countermeasures where risk is unacceptable

Infrastructure reconnaissance gathers technical information on what infrastructure is available, its importance to the mission, redundancy, and how the systems function or operate. Many important infrastructure areas that must be addressed are described by the acronym SWEAT-MSO (Sewer, Water, Electricity, Academics, Trash, Medical, Safety, and Other Considerations.) See Figure F-1.

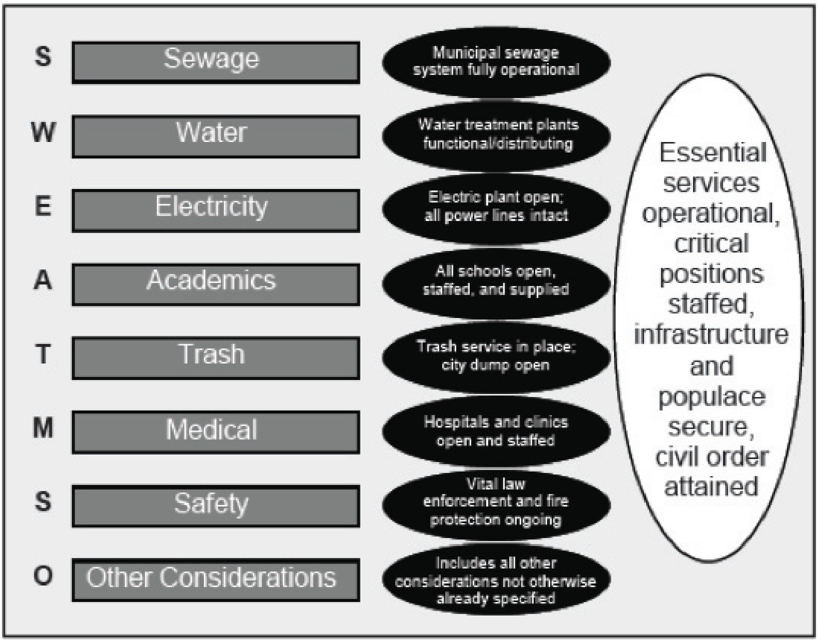


Figure F-1. Infrastructure and Assessment Survey Model
(JP 3-34, *Joint Engineer Operations)*

Infrastructure reconnaissance occurs in two stages—the infrastructure assessment and the infrastructure survey. The assessment and survey are not clearly distinguishable but rather, as shown in Figure F-2, these stages overlap and vary according to METT-T[C].

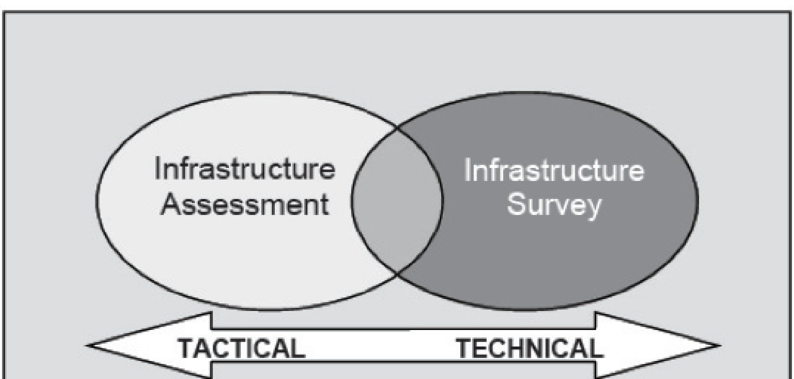


Figure F-2. Infrastructure Assessment and Survey Overlap
(FM 3-34.170, *Engineer Reconnaissance)*

Infrastructure reconnaissance is a multidisciplinary task conducted by a base team. Engineers will likely be responsible for coordinating infrastructure reconnaissance, but should rely on other specialists as needed. If possible, the reconnaissance team should include personnel from engineering, civil affairs, preventive medicine, and law enforcement/military security.

Infrastructure Assessment. The infrastructure assessment provides immediate feedback on the status of basic services necessary to sustain the local population. The assessment template (Figure F-3) can be adapted to tactical stability or civil support operations. In either type of operation, the infrastructure assessment enhances course of action development to delineate tasks, missions, and effects that support civil-military-related objectives. This example is not exhaustive, but rather an assessment aid.

Infrastructure Assessment			
Location:		Assessor:	
Local Points of Contact (Name, Location, Phone Number, etc.)			
Mayor: City Council: City Engineer: Religious Leaders: Community Leaders:		Police Chief: Fire Chief: School Administrators: NGOs:	
Male Population:	Female Population:	Religious Breakdown:	Ethnic Breakdown
S — Sewage System Assessment			
Status of municipal sewage system/distribution system: Status of sewage systems in commercial/residential properties: Immediate needs:			
W — Water Assessment			
Status of water treatment plants/distribution system: Status of potable water in commercial/residential properties: Storage capacity: Wells (location and capacity): Immediate needs:			
E — Electricity Assessment			
Status of electric plant/distribution system: Status of electric power in commercial/residential properties: Alternate power sources: Immediate needs:			
A — Academics Assessment			
Status of school building(s): Status of teachers and supplies: Immediate needs:			
T — Trash Assessment			
Status of trash collection system: Status of disposal site: Immediate needs:			

Figure F-3. Sample Infrastructure Assessment Template
(FM 3-34.170, *Engineer Reconnaissance)*

M — Medical Assessment
Status of hospital/clinic buildings: Status of physicians and supplies: Immediate needs:
S — Safety Assessment
Status of police/fire departments: Status of safety personnel and supplies: Immediate needs:
O — Other Considerations
Transportation System Assessment: Status of road system (attach sketch if necessary): Impact on critical transportation needs: Immediate needs:
Fuel distribution Assessment: Status of fuel distribution system: Storage capacity: Immediate needs:
Housing Assessment: Status of structures: Status of utilities: Immediate needs:
Explosive Hazard Assessment: Explosive ordnance locations/type (send 9-line UXO report as required by the mission): Explosive ordnance marked (if yes, marking description): Immediate needs:
Environmental Hazard Assessment: Do known hazards exist (if yes, describe): Are chemicals visible on the ground (if yes, describe): Abandoned manufacturing buildings (if yes, are waste products/streams contained): Immediate needs:
Other Critical Considerations:
Recommended Priorities:
Remarks:

Figure F-3. Sample Infrastructure Assessment Template (continued)

The basic services or categories evaluated depend on the situation, mission, and commander's intent. These surveys should be performed by engineers or designated substitutes. Commanders or designated substitutes should consult military and non government organizations to gauge any extenuating circumstances that might influence the assessment. Typically, planners then use this information to define immediate needs and determine work priorities. Assessment considerations are shown in Figure F-4.

Infrastructure Assessment Considerations

Sewage

□ What is the local sewage system status?
□ What health and environmental risks exist?

Water

□ Is adequate potable water available?
□ Has water been tested?

Electricity

□ What is the status of electrical generation?
□ Are portable generators available?
□ What is the transmission infrastructure status?
□ What critical facilities (hospitals, government buildings, schools, etc.) are not receiving adequate electricity?
□ Are transportation, heating, and cooking fuel available?
□ Is electrical distribution adequate?

Academics

□ Do schools need repair?

Trash

□ Is a waste removal and disposal system in place?
□ Is hazardous waste being generated that may have detrimental impacts on health and the environment?

Medical

□ Are medical services available and operational?
□ Does an emergency service exist?

Safety

□ Do police and fire services exist?
□ Are unexploded ordnance (UXO) or other explosive hazards present?

Other Considerations - Transportation Networks

□ Are roads, bridges, and railroads trafficable?
□ Is an operational airport available?
□ Do adequate helicopter landing sites exist?
□ Can transportation networks sustain local, humanitarian assistance traffic?

Figure F-4. Infrastructure Assessment Considerations

Other Considerations - Fuel Distribution

□ Does a fuel distribution system exist for commercial and residential customers?

Other Considerations - Housing

□ Are homes structurally sound and habitable?

□ Do homes include basic utilities?

Other Considerations - Explosive Hazards

□ Are ordnance hazards observed?

Other Considerations - Environmental Hazards

□ Are environmental hazards observed?

Other Considerations - Communications

□ Is the telephone network operational?

□ Are local media outlets (TV, radio, and newspaper) functional?

Other Considerations - Places of Worship

□ Do adequate religious facilities exist for all denominations?

Other Considerations - Attitude

□ Is the local populace supportive?

□ Do ethnic tensions exist?

Figure F-4. Infrastructure Assessment Considerations (continued)

Infrastructure Survey. As a follow-on to the assessment, the infrastructure survey details the condition of major services. The assessment and survey differ in terms of the technical expertise required.

A survey is normally conducted by US Army Corps of Engineer (USACE) personnel assigned or attached to a FEST-M (Forward Engineer Support Team-Main) team and will integrate other technical specialties (medical, civil affairs, and others) to enhance the survey quality. A large urban area might require more than one team to meet survey requirements. A survey may also require that an area be secure while an assessment may be performed in an unsecured area. Both are best performed when other branch specialties are available to support the base engineer element. Appendix C of FM 3-34.170/MCWP 3-17.4, Engineer Reconnaissance, contains a series of smartcards to assist with the conduct of the more detailed infrastructure survey.

Infrastructure Protection. Infrastructure protection is commonly addressed in the survey stage. Protection may also be necessary after the infrastructure elements are in full operation. Infrastructure protection in the survey phase requires identification of threats to infrastructure elements, vulnerabilities associated with those threats, and mitigating courses of action (COA). Selected COA might include hardening of infrastructure elements or an increased commitment of protective forces to those elements.

Figure F-5 shows a sample infrastructure protection plan.

[Issuing HQ]
[Date]
APPENDIX 16 TO ANNEX C TO [Issuing HQ OPLAN number]
CRITICAL INFRASTRUCTURE PROTECTION (CIP)
References: List documents essential to this appendix.

1. Situation

a. Enemy. List those forces that are unique threat from a CIP perspective.
b. Friendly. List those forces assigned a role in protecting critical infrastructure. Highlight military, nonmilitary, and HN agencies.
c. Assumptions. List any assumptions made about friendly, enemy, or third party capabilities and limitations.

2. Mission

3. Execution

a. Concept of Operations. Summarize the FOB commander's assurance of critical capabilities that support the mission. Summarize the concept for monitoring infrastructure readiness and availability.
b. Criticality. Identify those mission critical capabilities, requirements, infrastructures, systems, and assets that if destroyed, denied, or disrupted will jeopardize the mission.
c. Priorities. List the FOB commander's protection priorities for mission critical capabilities, infrastructure, requirements, systems, and assets. Identify application of CIP tasks and identify those not under combatant commander control.
d. Tasks. Actions to support and protect infrastructure under the commander's influence. If CIP actions are covered in other sections of the OPLAN, refer to the annex, appendix, or tab that highlights CIP measures.

4. Administration and Logistics. Address any CIP-related administrative or logistics requirements. Identify requirements for specialized personnel qualification and augmentation. Personnel requirements may include security, reaction/management, or support.

5. Command and Control. List any CIP-related C2 instructions. Identify any CIP communication or reporting requirements.

Figure F-5. Critical Infrastructure Protection Annex Template
(CJCSM 3122.03C, *Joint Operation Planning and Execution System Volume II)*

Infrastructure Rating. As the FOB commander addresses infrastructure issues, information becomes a priority. Infrastructure questions of interest include:

- Has the infrastructure been maintained?
- Who built the infrastructure component?
- Are repair parts and equipment available?
- Will the infrastructure be targeted by adversaries?
- Will host nation employees return to the site after hostilities?
- Is the infrastructure protected?

A systematic prioritization method is required to support the FOB commander's infrastructure priorities. Table F-1 provides an example of how the engineer staff can communicate the results of an infrastructure assessment or survey to the FOB commander.

Reachback is available to obtain much of the specialized support required for infrastructure assessment and survey. One source is the USACE Reachback Operations Center (UROC). Reachback and TeleEngineering provide deployed forces with expertise and computer-aided solutions not available in-theater. This support is provided real-time through secure voice and video information technology. Chapter 12 provides additional reachback and TeleEngineering details.

Table F-1. Infrastructure Category Status
(FM 3-34.400, *General Engineering*)

Area	*Green*	*Amber*	*Red*	*Black*
Sewage	Sewage system works consistently	Sewage system works, but treatment status is undetermined	No treatment observed, but treatment plant exists	No sewage treatment system; destroyed
	No sewage observed and no odor	No sewage observed, but odor is present and/or system is damaged	Sewage observed, and odor present	Presence of raw sewage is a public health issue
	Operational in 100 percent of public facilities	Operational in 50 percent or more of public facilities	Operational in less than 50 percent of public facilities	No operational sewage in public facilities
Water	Water distribution works at 100 percent capacity	Water distribution works at 50 percent or more of capacity with some leaks	Water distribution does not work	No water distribution system; destroyed
	Tested as clean and/or local populace is consuming	Appears clean, no smell, and local populace states that it is clean	Does not appear clean, and local populace states that it is not clean	Tested, nonpotable and/or appears contaminated and has bad odor
	Running water in 100 percent of public facilities	Running water in 50 percent or more of public facilities	Running water in less than 50 percent of public facilities	No running water in public facilities
Electricity	Power distribution system works; blackouts are planned	Power distribution system works; blackouts unplanned	Power distribution system is unreliable; frequent blackouts	No power distribution system; destroyed
	Electric lines are 100 percent; no damage and no power loss	Electric lines are 50 percent; some minor damage and undetermined power loss	Electric lines are less than 50 percent; major damage and noticeable power loss	Electric lines are all down; hot wires exposed; significant power loss
	Power grid station intact; secure	Power grid station operational; unsecure	Power grid station nonoperational; unable to secure	Power grid station stripped; destroyed
Academics	Building serviceable; all utilities operational; secure	Building is adequate; utilities operate over 50 percent; not secure	Building is usable; utilities operate less than 50 percent; not secure	Building is not usable; utilities are nonfunctional
	Academic resources available to all students	Academic resources available to 50 percent or more	Academic resources available to less than 50 percent	Extremely limited academic resources

Table F-1. Infrastructure Category Status (FM 3-34.400, *General Engineering*) (continued)

Area	Green	Amber	Red	Black
Trash	Formal trash collection system is operational	Formal trash collection system exists, but is limited	No formal trash collection system	No trash collection
	Trash collection is in a central area that does not present a health hazard	Unknown central trash collection area	Central trash collection area presents a possible health hazard	Trash is consolidated in an area that presents a health hazard
	No trash buildup in public facilities	Limited trash in public facilities; relatively clean	Public facilities have no means to remove trash	Public facilities have excess trash
Medical	Medical facilities are functional; backup power; minimal equipment issues; secure	Medical facilities are usable; no backup power; some equipment shortages; not secure	Medical facilities are unsanitary; significant equipment and supply shortages	Medical facilities are not usable due to damage and unsanitary conditions; looted
	Emergency services including multiple ambulatory services available	Emergency services exist; ground transport only	No emergency services; ground transport without medically trained personnel	No emergency services
	Veterinary services available; animal holding area	Limited veterinary services available; inadequate holding area	On-call veterinary services; no holding area	No veterinary services
Safety	Police department functional; secure building; equipment available and operational	Police department functional a minimum of 50 percent; building securable; equipment available and operational less than 50 percent	Police department functional less than 50 percent; unable to secure building; limited equipment available	Police department is nonfunctional; building is not usable; no equipment
	Fire department functional; secure building; equipment available and operational	Fire department functional a minimum of 50 percent; building securable; equipment available and operational more than 50 percent	Fire department functional less than 50 percent; unable to secure building; limited equipment available	Fire department is nonfunctional; building is not usable; no equipment
Other Considerations: Roads and Railroads	Minimum of a Class C road; can be upgraded; no visible damage	Minimum of a Class D road; damage and upgrade requirements will impact traffic flow	Minimum of a Class E road; upgrade requirements are significant; materials not readily available	Road is not trafficable
	Operational railroad system	Railroad is damaged, but resources to repair are available; jacks available	Railroad damage is extensive; resources to repair are not readily available	Railroad system did exist, but now has extensive damage to both track and trains
Other Considerations: Bridges and Waterways	Bridges are trafficable; no visible damage	Bridges are trafficable; damage to spans; supports intact	Bridges are not trafficable for military; risky for civilians; damage to spans and supports	Bridge is not trafficable and is impassable
	MLC verified through ERDC or other structural engineer	MLC calculated, but not verified due to damage	MLC is ineffective due to damage	Construction repair required before MLC can be determined
	Inspection and evaluation shows original strength assessment valid	Inspection and evaluation determines strength support issues	Inspection and evaluation determines minimal supportable strength	Inspection and evaluation determines that bridge cannot support weight

Table F-1. Infrastructure Category Status (FM 3-34.400, *General Engineering*) (continued)

Area	*Green*	*Amber*	*Red*	*Black*
Other Considerations: Airports	Airport capable of supporting military and civilian traffic concurrently; no visible damage	Airport can support limited military traffic; no visible damage	Airport damaged; utilities and structures are not reliable or safe	No working airport
	Runway, taxiway, and parking aprons are serviceable; working and parking MOG greater than or equal to 2 (military)	Runway serviceable, but taxiway and parking limited; C130 and C17 only	Runway is not serviceable; can repair with available resources	Runway is not serviceable; dimensions will not support military aircraft; major repair and upgrades required
Other Considerations: Housing	Residences are structurally sound and offer protection from the environment	Residences are damaged and need structural evaluation; offer limited protection from the environment	Residences are damaged and structurally unsafe; no protection from the environment	Residences are destroyed
	Utilities are working and reliable	Utilities are working over 50 percent; not reliable	Utilities work less than 50 percent; require significant repairs	Utilities are nonoperational
Other Considerations: Communications	Telephone system operational and reliable in public facilities	Telephone hookups available; some equipment available; somewhat reliable	Limited telephone hookups and equipment available; not reliable	No telephone hook-ups or equipment
	Postal system is operational and reliable	Postal system is slow; over 50 percent of mail delivered	Postal system exists; extremely slow; less than 50 percent of mail delivered	No postal system
	Media—television, internet, radio, newspaper—operational, available, and reliable	One form of media exists and is operational, available, and reliable	One form of media exists but has limited availability and reliability	No form of media
Other Considerations: HAZMAT	HAZMAT/hazardous waste properly segregated, stored, and labeled	Some HAZMAT and hazardous waste not properly segregated, stored, or labeled	HAZMAT and hazardous waste not properly segregated, stored, or labeled	HAZMAT and hazardous waste not segregated, stored, or labeled
	Containers adequate for the material	Containers not generally adequate, but limited corrosion or damage	Containers inadequate, corroded, and leaking	Containers inadequate, corroded, and leaking
	Safety measures and secondary containment in-place	Inadequate safety measures and secondary containment	No safety measures or secondary containment	No safety measures or secondary containment
	Hazards communications system in place	Limited hazards communications system	No hazards communications system	No hazards communications system
	No leaks or spills	Potential for leaks and spills	Some leaks and spills already present; contaminants may enter air, soil, groundwater, or water courses	Gross contamination present; contaminants have entered air, soil, groundwater, and water courses
	Spill prevention and cleanup measures in place/available	Limited spill prevention and cleanup measures available	No ability to prevent or clean up spills	No ability to prevent or clean up spills

Table F-1. Infrastructure Category Status (FM 3-34.400, *General Engineering*) (continued)

Area	Green	Amber	Red	Black
Other Considerations: Attitude	Community leaders not hostile; religious centers are intact; supportive of GE effort	Community leaders are neutral; religious centers are damaged but securable	Community leaders are negative; religious centers are damaged and not securable; skeptic of GE support	Community leaders hostile; religious centers destroyed; do not want GE assistance
	No ethnic tension	Distinct ethnic groups within AO; supportive of GE effort if equal among groups	Distinct ethnic groups within AO; one group dominant; GE tasks cannot be accomplished for all groups	Ethnic violence occurs; one group extremely dominant; GE effort would increase ethnic tension
	Unemployment is less than 50 percent	Unemployment is greater than 50 percent; Willing and able to work to support GE effort	Unemployment is greater than 50 percent; Unable to support GE work effort	Unemployment is a serious issue; unwilling to support GE work effort
	No formal paramilitary threat	Paramilitary threat briefed at the BCT/RCT level	Paramilitary threat a concern at BCT and RCT level	Paramilitary threat a concern at echelons above BCT and RCT level
Note. Food supply and cultural, historical, and religious are still under development.				

References:

JP 3-34. *Joint Engineer Operations,* 30 June 2011.

JP 3-34.170. *Engineer Reconnaissance*, March 2008.

CJCSM 3122 03C. *Joint Operation Planning and Execution System Volume II*, 17 August 2007.

APPENDIX G
MATERIAL AND TECHNOLOGY SUPPORT

This appendix contains construction and equipment materiel acquisition data to assist in planning FOB construction and security. TTPs for the materiel presented are detailed elsewhere in this handbook. Most items have National Stock Numbers (NSNs); those without NSNs include contact information. Expedient items such as vehicle barriers built locally at FOBs are not included. This appendix is not exhaustive and related items to those listed may be available through supply channels. Stock numbers, cost data, and availability are valid as of October 2010. These data are subject to change. Contact the Defense Logistics Agency (www.dla.mil) for additional information.

Section 1. Soil-Filled Containers

Table G-1. Wire and Fabric Container Kits

NSN	Height (ft.)	Width (ft.)	Length (ft.)	Cost/Linear Foot[1]	Cost/Kit
5680-99-835-7866 (beige) 5680-99-001-9396 (green)	4.5	3.5	32.0	$24.51	$784.17
5680-99-968-1764 (beige) 5680-99-001-9397 (green)	2.0	2.0	4.0	$14.46	$57.84
5680-99-001-9392 (beige) 5680-99-001-9398 (green)	3.25	3.25	32.0	$18.63	$596.16
5680-99-001-9393 (beige) 5680-99-001-9399 (green)	3.25	5.0	32.0	$27.82	$890.22
5680-99-001-9394 (beige) 5680-99-001-9400 (green)	2.0	2.0	10.0	$11.89	$118.89
5680-99-169-0183 (beige) 5680-99-126-3716 (green)	7.25	7.0	90.0	$47.04	$4,234.13
5680-99-335-4902 (beige) 5680-99-517-3281 (green)	4.5	4.0	32.0	$24.86	$795.41
5680-99-563-5949 (beige) 5680-99-052-0506 (green)	3.25	2.5	30.0	$17.94	$538.30
5680-99-391-0852 (beige) 5680-99-770-0326 (green)	7.0	5.0	95.0	$46.62	$4,428.55
1-Approximate cost for each linear foot, based on kit cost and length					

Table G-2. Metal Container Kits

NSN	Height (ft.)	Width (ft.)	Length (ft.)	Cost/Linear Foot[1]	Cost/Kit*
5450-01-554-1249	6	3	104	$68.16	$7,088.92
5450-01-554-1238	6	4	96	$103.86	$9,970.91
5450-01-554-1240	6	5	88	$87.63	$7,711.68
5450-01-554-1253	8	5	64	$116.85	$7,478.18
5450-01-554-1256	10	5	48	$147.30	$7,070.47
5450-01-554-1267	6	6	80	$97.37	$7,789.56
5450-01-554-1303	8	6	64	$129.83	$8,309.09
5450-01-554-1309	10	6	48	$162.28	$7,789.56
5450-01-554-1315	12	6	48	$194.74	$9,347.72
5450-01-554-1331	6	7	72	$107.11	$7,712.03
5450-01-554-1336	8	7	48	$142.81	$6,855.00
5450-01-554-1341	10	7	32	$237.65	$7,604.93
5450-01-554-1351	12	7	32	$214.21	$6,854.86
5450-01-554-1358	16	7	24	$285.62	$6,854.79
5450-01-554-1377	6	8	72	$116.85	$8,412.95
5450-01-554-1382	8	8	48	$155.80	$7,478.18
5450-01-554-1392	10	8	40	$194.74	$7,789.77
5450-01-554-1398	12	8	32	$233.69	$7,478.00
5450-01-554-1401	16	8	24	$311.58	$7,477.97
5450-01-537-7061	10	4	48	$179.56	$8,619.00
5450-01-535-7952	8	4	64	$138.48	$8,863.00
5450-01-535-7955	6	2	104	$77.38	$8,047.13
*-Approximate cost for each linear foot, based on kit cost and length					

Section 2. Fencing

Table G-3. Common Fencing Materials

NSN	Description	Cost
5660-00-270-1588	Post, Fence, Metal Steel 24 in. (size 5)	$2.95
5660-00-270-1589	Post, Fence, Metal Steel 32 in. (size 4)	$3.31
5660-00-270-1587	Post, Fence, Metal Steel 60 in. (size 3)	$6.41
5660-00-270-1510	Post, Fence, Metal Steel 72 in. (size 2)	$7.15
5660-00-262-9914	Post, Fence, Metal Steel 96 in. (size 1)	$9.81
5660-00-921-5516	Barbed Tape, Concertina 50 ft. Roll	$31.69
5660-01-248-2466	Fence Post Driver Hammer	$66.17
8415-00-926-1674	Barbed Wire Gloves	$17.71

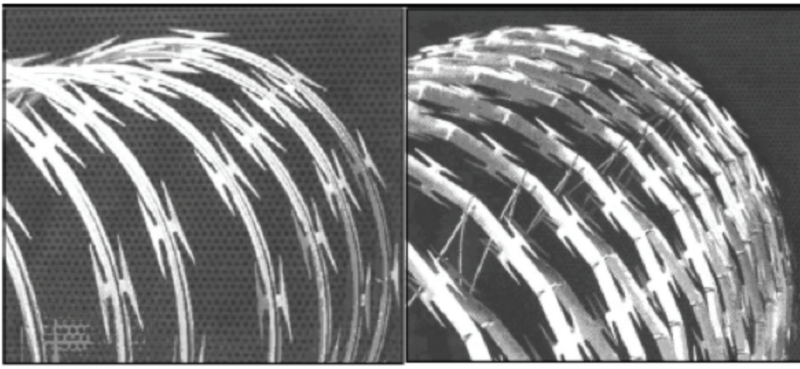


Figure G-1. Barbed Tape (Left: Reinforced; Right: Non-reinforced)

Table G-4. Barbed Tape (Figure G-1)

NSN	Diameter	Strip Material	Core Wire	Yield	Pkg	Cost
5660-01-457-9757	18 in.	SS	GA	50 ft.	5/box	$24.29
5660-01-495-6123	18 in.	GA	GA	50 ft.	5/box	$21.71
5660-01-457-9828	18 in.	SS	SS	50 ft.	5/box	$45.64
5660-01-457-9842	24 in.	SS	GA	50 ft.	5/box	$69.67
5660-01-495-6277	24 in.	GA	GA	50 ft.	5/box	$27.45
5660-01-457-9843	24 in.	SS	SS	50 ft.	5/box	$80.92
SS = Stainless Steel; GA = Galvanized Aluminum						

Table G-5. Concertina Single Coil Barbed Tape

NSN	Dia	Coil Loops	Strip Mail	Core Wire	Clips	Coil Spacing	Yield	Pkg	Cost
5660-01-457-9847	18□	31	SS	GA	3	32□	15□	4/Box	$34.40
5660-01-495-6178	18□	31	GA	GA	3	12□	15□	4/Box	$23.93
5660-01-457-9849	18□	31	SS	SS	3	12□	15□	4/Box	$71.28
5660-01-457-9850	24□	31	GA	GA	3	16□	20□	5/Box	$69.82
5660-01-495-6284	24□	31	GA	GA	3	16□	20□	5/Box	$36.23
5660-01-457-9852	24□	31	SS	SS	3	16□	20□	5/Box	$102.49
5660-01-495-9534	30□	51	SS	SS	5	12□	52□	4/Box	$111.04
5660-01-495-9566	30□	51	SS	GA	5	12□	25□	4/Box	$80.29
SS = Stainless Steel; GA= Galvanized Aluminum									

Table G-6. Non-Reinforced Concertina Single Coil Barbed Tape

NSN	Dia	Coil Loops	Strip Mail	Coil Spacing	Yield	Pkg	ATSM F1910 Item #	Cost
5660-01-495-6363	30□	101	SS	12□	50□	7/Box	#25	$427.59
SS = Stainless Steel								

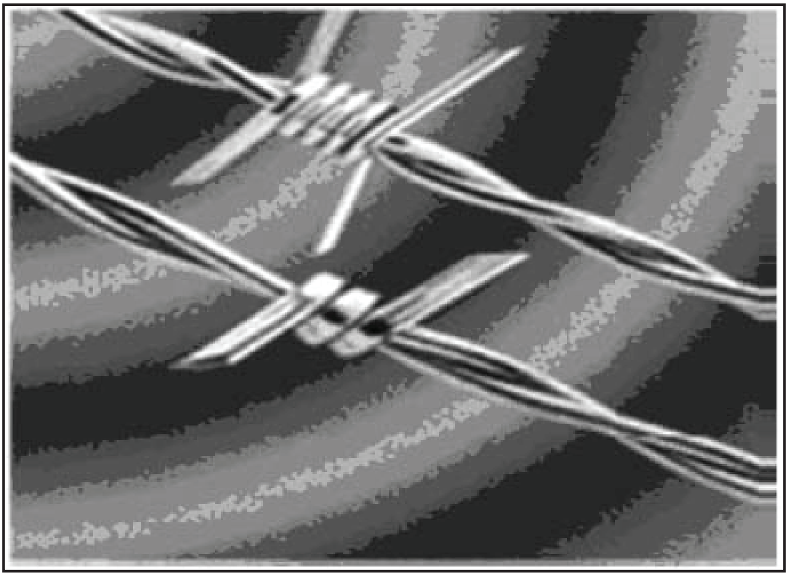


Figure G-2. Barbed Wire

Table G-7. Barbed Wire

NSN	Description	Steel	Size	Roll Length	Roll Weight	Cost
5660-00-224-8663	4 Barbed Heavyweight	Low Carbon	12.5 Gauge	1,320 ft. (402.3 m)	90 lbs. (40.8 kg)	$48.39
5660-01-390-4223	4 Barbed Lightweight	High Tensile	15.5 Gauge	1,320 ft. (402.3 m)	42 lbs. (19.0 kg)	$62.21

Figure G-3. Chain Link Fence

Table G-8. Chain Link Fence Materials (Figure G-3)

NSN	Description	Cost
5660-00-720-4527	Chain Link Fabric Fencing Wire - 8 ft high by 50 foot roll - 2 inch mesh - 9 gauge - 1.2 oz zinc coating	$333.05
5660-01-247-5681	Post --- 2.375 inch OD----10 feet long----3.65# per foot----thickness 0.154---galvanized steel pipe	$43.60
5660-00-969-5285	Top Rail pipe --- 21 feet long---1.66 inch OD-- galvanized steel pipe---0.111 wall thickness	$38.88
5660-00-408-8821	Tension Bar----94 inches long --- .188 inch thick ---0.75 inches wide ----galvanized steel bar	$6.27
5660-00-467-3276	Tension Band--- Galvanized steel straps---0.75 inches wide x 12 gauge thick---used with tension bar	$1.10
5660-00-408-8743	Arm Extension----single arm at 45 degrees---fits on top of 2.375 post---accepts 3 strands of barbed wire	$2.73
5660-01-038-1458	Rail End --- steel or cast iron with Galvanized finish---attaches to 1.666 top rail	$1.41
5660-01-063-4873	Tie Wire -- 9 gauge --- 6.5 inches long --attaches fence fabric to posts	$4.71
5660-01-021-6356	Brace band-- galvanized 0.75 inch, 12 gauge used to secure top rail end to post	$0.47

Section 3. Ground Stabilization

Table G-9. Ground Stabilization

NSN	Description	UI	Cost
5680-01-176-9076	AM2 Landing Mat	Ea.	$13,072.72
5680-01-198-7955	Sand Confinement Grid (Closed Cell)	Ea.	$256.10
5680-01-501-1032	Sand Confinement Grid (Perforated Cell)	Ea.	$281.21
5675-01-471-2683	Dura-Base Mat (Full Panel)	Ea.	$2,753.95
5675-01-476-7335	Dura-Base Mat (Half Panel)	Ea.	$1,625.95
	5675-01-476-7336 Locking Pin	Ea.	$31.25
	5675-01-476-7338 Cover Pin	Ea.	$0.80
	5675-01-476-7339 Spike	Ea.	$4.65
	5675-01-476-7345 Tool Kit	Ea.	$636.55
5675-01-471-2674	Geotextile Mat Liner	Roll	$428.88
5680-01-368-9032	Mat Set, Landing	Ea.	$26,551.20
5675-01-476-8989	Polyethylene Mat	Ea.	$649.45

Section 4. Lighting

Table G-10. Lighting Products

NSN	Item Description	Cost
Portable Lighting		
6260-01-074-4229	Light, Chemiluminescent, Green	$14.67
6260-01-178-5559	Light, Chemiluminescent, Red	$14.67
6260-01-178-5560	Light, Chemiluminescent, Blue	$12.31
6260-01-195-9752	Light, Chemiluminescent, Infrared	$22.53
6260-01-196-0136	Light, Chemiluminescent, Yellow	$14.67
6260-01-218-5146	Light, Chemiluminescent, White	$12.50
6260-01-247-0362	Light, Chemiluminescent, Green	$39.90
Vehicle Light Fixtures		
6220-00-756-5764	Spotlight	$75.96
6220-01-193-1970	Headlight	$58.26
6220-01-306-8203	Floodlight, Electric	$37.51
Electrical Portable, Hand Lighting Equipment		
6230-00-264-8261	Flashlight, Olive Drab	$8.38
6230-00-500-0523	Electric Lantern, 6VDC	$7.80
Electrical Lighting		
6220-01-217-8316	Tow Light Assembly	$1,073.37
6230-01-158-8019	Floodlight Assembly	$702.06
6240-00-019-3093	Lamp Incandescent	$0.24
6240-00-966-3831	Lamp Incandescent, Waterproof	$15.97
6260-00-270-4060	Mantle Illuminating	$1.78

Section 5. Construction

Table G-11. Construction Materials

NSN	Item Description	UI	Cost
Lumber/Plywood			
5510-01-433-1145	1x4x16, Common	Board Feet (BF)	$0.83
5510-01-433-1183	1x8x16, Common	BF	$1.47
5510-01-433-1371	2x6x16, #2 Softwood Lumber	□	$0.66
5510-01-433-3930	2x12x16, #2 Softwood Lumber	□	$0.86
5510-01-433-1199	1x10x16, #2 Common	□	$0.93
5510-01-433-1244	2x4x16, #2 Common	□	$0.75
5530-00-129-7833	¾ in. AC Plywood	Sheet (SH)	$38.92
5530-00-618-8073	¾ in. CDX Plywood	SH	$35.88
5530-00-618-6958	½ in. CDX Plywood	□	$23.78
5530-00-129-7777	½ in. AC Plywood	□	$36.75
5530-00-128-5147	5/8 in. CC Plywood	□	$28.42
5530-00-129-7889	1 in. AC Plywood	□	$53.15
5530-00-128-5134	¾ in. BB CF Plywood	□	$45.74
E-Glass			
9340-01-533-3758	E-Glass, Ballistic Grade 4 ft. x 8 ft.	Ea.	$603.26
Drums and Cans			
8110-00-292-9783	Drum, shipping & storage, 55 gallon, steel closed head	Ea.	$50.70
8110-00-030-7780	Drum, shipping & storage, 55 gallon, steel open head	Ea.	$55.22
8110-01-101-4055	Drum, steel, ship & storage, 85 gallon, steel	Ea.	$95.14
Advanced Composite Building Panel System - suitable for major load-bearing structural applications. The modular construction system consists of a small number of interlocking fiber-reinforced polymer structural components. Main building panels are 3 in. thick and 24 in. wide. Panels can be connected with toggles.			
5675-01-500-2812	6 ft. panel length	Ea.	$129.86
5675-01-500-2729	8 ft. panel length	Ea.	$440.10
5675-01-500-2761	10 ft. panel length	Ea.	$216.06
5675-01-500-2803	12 ft. panel length	Ea.	$259.70
5675-01-500-2808	14 ft. panel length	Ea.	$302.28
5675-01-496-4896	20 ft. panel length	Ea.	$450.33
Rubberized Roof			
5660-01-504-5373	Rubberized roof □non-reinforced EPDM membrane for earth-filled barrier and observation post roofs. 20 ft. x 100 ft. sections; 0.045 in. thick	Ea. (Roll)	$1,864.78

Table G-12. Sandbag Materials

NSN	Description	Cost
Sandbags		
8105-00-142-9345	Sandbag □Green, Poly	$47.04
8105-00-935-7101	Sandbag □Green, Acrylic	$120.80
8105-00-782-2709	Sandbag □Sand, Cloth	$53.12
8105-01-336-6163	Sandbag □Sand, Poly	$45.44
8105-01-331-3704	Sandbag □Sand, Acrylic	$137.70
Sandbag Filling Machines		
Manual, gravity fed machines:		
3895-01-460-3910	Two Hopper	$4,516.64 / $6,022.54
3895-01-470-5748	Three Hopper	$1,559.30
3895-01-470-5751	Five Hopper	$16,881.26
Automatic, gas powered machines:		
3895-01-460-4545	Model MB-3	$27,396.21
3895-01-470-5752	Model ASB-3	$22,107.30
3895-01-460-4548	Trailer, Model C-2T	$4,927.08

Section 6. Supporting Technologies

Table G-13. Passive Vehicle Access Control

Item	Description	NSN/GSA/POC
PreCast Concrete Barrier	• Alaska Barrier • Jersey Barrier (Figure G-4) • T-Wall (Figure G-5) • Colorado Barrier • Scud Bunker • California Barrier • Texas-T Barrier	
Caltrops	Spike designed to penetrate and flatten tires.	4240-01-539-1517
Modular Protective System	Portable, rapidly deployable protection.	5410-01-566-6439
Physical Screening Protective System (PSP)	Portable, rapidly deployable protection.	5410-01-587-0829

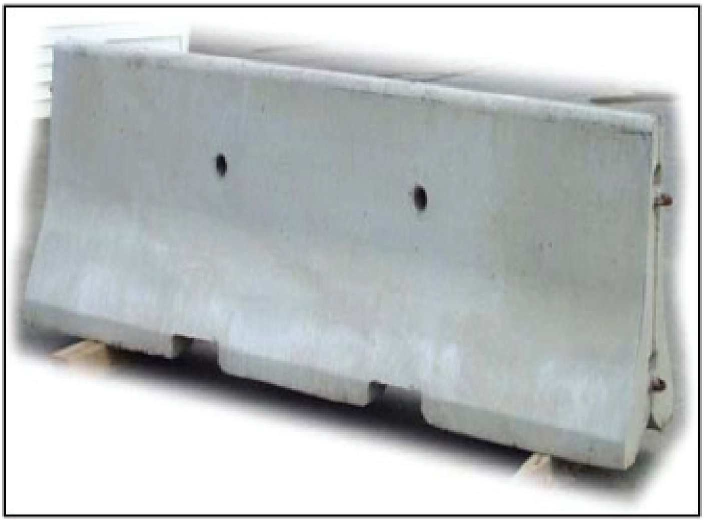


Figure G-4. Jersey Barrier

Figure G-5. T-Wall Barrier

Table G-14. Active Vehicle Access Control

Item	Description	NSN/GSA/POC
Expedient Steel Gate (Figure G-6)	Manually operated barrier.	Constructed on site
Expedient Single Piece Box Beam Gate (Figure G-7)	Back-up barrier to steel gate.	Constructed on site
Expedient Leaf Gate (Figure G-8)	Manually operated barrier.	Constructed on site
"Salerno" Style Gate (Figure G-9)	Expedient pop-up barrier.	Constructed on site
MP5000 & XV Mobile	Mobile pop-up barrier.	**www.deltascientific.com**
DSC7000	Drop-arm barrier.	**www.deltascientific.com**
DSC7500	Swing beam barricade.	**www.deltascientific.com**
Nasatka Barrier	Reloadable, mobile vehicle barrier.	GS-07F-9776H/ **www.nbistop.com**
KIT Based Vehicle Barrier System	Drop-arm barrier system.	**www.barrier1.us**
Pre-Emplaced Electric Vehicle Stopper (PEVS) (Figure G-10)	Provides an electric pulse through deployed contacts to shutdown the vehicle's power train.	**www.jnlwp.usmc.mil**

Figure G-6. Expedient Steel Gate

Figure G-7. Expedient Box Beam Gate

Figure G-8. Expedient Leaf Gate

Figure G-9. Salerno Style Gate

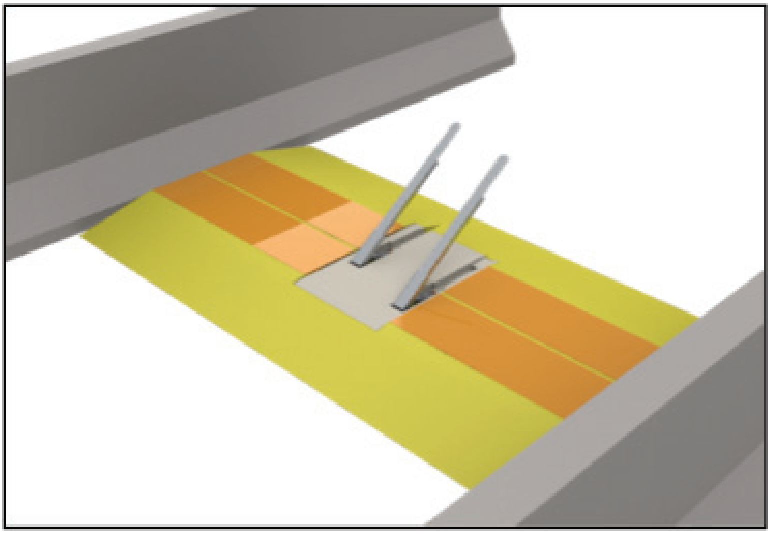


Figure G-10. Pre-emplaced Electric Vehicle Stopper

Table G-15. Vehicle Search

Item	Description	NSN/GSA/POC
Snake Eye Camera Kit	Search device for undercarriage of vehicles.	www.snakeeye.com
V1000 Inspection Wand	Tool used to search engine compartment and hard to reach areas.	www.sea-sea.com/industrial/
Explosive Trace Detector Spray Kit	Detects explosive residue or gunpowder.	6665-01-554-8014
Entry Point Vehicle Kit (EPVK) (Figure G-11)	Equipment used at vehicle entry points to search vehicles; includes: • Snake Eye Camera Kit • Security Illumination Mat System • Security Assessment Mirrors • Inspection Wand • TR-3 Flashlight • Detection Spray Kit	6350-01-532-2051
GE Mobile Trace (Sherlock)	Explosive trace detection system used to detect narcotics and explosives.	GE Security, Inc. 1-978-909-1287 www.gesecurity.com
FIDO	Explosive detection system; conducts searches by sampling the air for explosive material.	www.icxt.com/products/detection/explosives/fido/
Search Mirrors	Searches undercarriage of vehicles.	5120-01-520-8743

Figure G-11. Entry Point Vehicle Kit

Table G-16. Personnel Access Control

CONEX (Expedient Use)	Personnel search area using CONEX shipping container.	Constructed on site
Voxtec Phraselator P2mX-2 Translation Device, Model 2000 with FP Module (Figure G-12)	Hand held translation device; used to communicate with individuals in native language.	**www.voxtec.com/phraselator/**
Perey Turnstile Type B Roto-Gate (Figure G-13)	Used to control pedestrian traffic by reducing traffic to single lane.	**www.turnstile.com**

Figure G-12. Voxtec Phraselator

Figure G-13. Perey Turnstile Type B Roto-Gate

Table G-17. Personnel Identification

Biometrics Automated Toolset (BAT) (Figure G-14)	Intelligence gathering and exploitation tool. • Digital Camera • Fingerprint Reader • Iris Scanner • CF-73/74 Toughbook	www.crossmatch.com/
Handheld Interagency Identity Detection Equipment (HIIDE)	Army: field capable biometric collection tool. Marine Corps: tactical and corpse enrollment operations.	www.l1id.com/

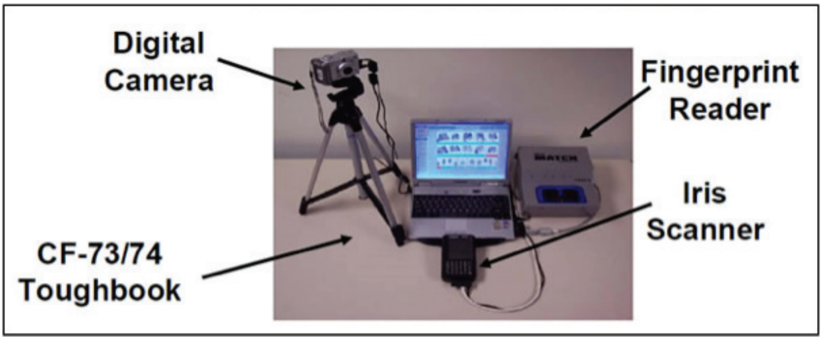


Figure G-14. BAT Enrollment Station

Table G-18. Personnel Warning and Signal

Item	Description	NSN/GSA/POC
Magnetic Audio Device (MAD) Acoustic Hailing Device (Figure G-15)	Provides directional high quality verbal challenges; automatic translation device.	**www.getmad.com**
MK 79 Signal Kit (Pen Flares)	Hand held flare system.	1370-01-230-3974 L118 **www.securitysignalsinc.com**
Laser (Figure G-16)	Tool used to signal vehicles and pedestrians.	**www.jnlwp.usmc.mil**
Green Laser (Figure G-17)	Tool used to signal pedestrians and vehicles.	**www.jnlwp.usmc.mil**

Figure G-15. Magnetic Audio Device

Figure G-16. Laser

Figure G-17. Green Laser

Table G-19. Personnel Search

Item	Description	NSN/GSA/POC
Garrett Super Scanner (Figure G-18)	Hand held metal detector.	6350-01-520-5942
Garrett Portal Metal Detector (Figure G-19)	Used to search personnel to detect concealed metal objects.	**www.garrett.com**
RapiScan Secure 1000	Non-intrusive personnel screening system; detects metallic and non-metallic objects.	5895-01-531-4671
RapiScan Metor 200WP	Walk-through metal detector for harsh climates; winter conditions and tropical climates.	**www.rapiscansystems.com**
Coral SD PBIED Detection System	Intended to search personnel for PBIED material.	585-01-536-3532

Figure G-18. Garrett SuperScanner

Figure G-19. Garrett Portal Metal Detector

Table G-20. Personnel Alerting

Item	Description	NSN/GSA/POC
SOUNDCOMMANDER 3500 System	Multi-Speaker PA System; Provides audio for 360□range of coverage.	5830-01-542-3267
Giant Voice	Mass notification system for alerting personnel to emergencies.	UFC 4-021-01
Bullhorn	Hand-held portable loud speaker.	8465-01-135-8495

Table G-21. Fighting Positions

Item	Description	NSN/GSA/POC
Blast and AP Resistant Guardhouse (Figure G-20)	10'x10'x8'-10.5' with a 3' 7□door and two gun ports; comes already assembled.	**www.nationwidestructures.com**
DefenShield	Mobile defensive fighting position.	**www.defenshield.com/** 1149-01-S01-L268
McCurdy□s Armor (Figure G-21)	Hardened guard shack; portable structure used for force protection or personnel.	**www.ddmat.com**

Figure G-20. Blast/AP Resistant Guardhouse

Figure G-21. McCurdy's Armor

Table G-22. Overwatch

Item	Description	NSN/GSA/POC
Expedient Container Tower (Figure G-22)		Constructed on site
German Tower (Figure G-23)		Constructed on site
Dutch Tower (Figure G-24)		Constructed on site
British Tower (Figure G-25)		Constructed on site
DynaTower	Precast and redeployable blast and ballistic guard tower; 7 Meter Tower and 10 Meter Tower.	5445-99-799-1297; 7 meter 5445-99-165-4133; 10 meter
Portable Guard Tower	Complete Kit contains: • One occupant compartment • One Conex • One Pallet of Helix Coils	GS-07F-9503S

Figure G-22. Expedient Tower

Figure G-23. German Tower

Figure G-24. Dutch Tower

Figure G-25. British Tower

Table G-23. Non-Lethal Munitions

Item	Description	NSN/GSA/POC
40MM Blunt Impact	Non lethal round that uses “batons”, foam tips or rubber pellets.	1310-01-452-1190
40MM Spin Stabilized Flash Bang Projectile	Used in M203; Non lethal loud report and bright flash; rubber tip provides for low fragment velocity.	1310-01-534-8941
12GA. Blunt Impact	Used in Mossberg 500 or Remington 870; uses variety or rounds that contain bean bags, rubber bullets or rubber pellets.	1305-01-454-0191
12 GA. Flash Bang	Used in Mossberg 500 or Remington 870; 100m or 200m variants that provide 50,000 candle light power and 160db of sound.	1370-01-530-6486; 100M 1370-01-530-6571; 200M
Fn-303 Weapon Attachment	Attachment that fires 0.68 caliber non-lethal projectiles which include blunt impact, dye marker, and OC liquid.	1095-01-526-7860

Table G-24. Sniper Control

Item	Description	NSN/GSA/POC
Gun Shot Detection System (GSD)	Acoustic sensor system used to determine origin of hostile fire.	W91CRB-09-T-0021
Boomerang	Uses a series of microphones to detect the direction of small arms fire.	**www.bbn.com** / **http://boomerang.bbn.com**

Table G-25. Sensors

Item	Descripton:	NSN/GSA/POC
Mobile Security Kit (Figure G-26)	Lightweight, portable, multi-camera security system.	**www.tserecon.com**
Rapid Aerostat Initial Deployment Tower (RAID) (Figure G-27)	Sensor tower used to detect personnel.	**www.raytheon.com**
Cerberus (Figure G-28)	Sensor platform optimized for targeting, surveillance and force protection.	**Jason.er.ruck.civ@mail.mil** 703-704-6072
Electro Magnetic Motion Detection and Ranging (EMMDAR)	Hand- held device that can detect personnel on the opposite side of the wall.	**www.cyterra.com**
Man-Portable Surveillance and Target Acquisition Radar (MSTAR) (Figure G-29)	Self contained Ground Surveillance Radar that provides surveillance for a range to 26 miles.	
Battlefield Anti-Intrusion System (BAIS) (Figure G-30)	Radar-based IDS; detects the movement direction of intruding personnel and vehicles.	**www.L-3.com**
Long Range Thermal Imager (LRTI)	24 hour long range surveillance; can detect personnel at 2.5 miles.	**www.iecinfrared.com**
IR Illuminator	Provides up to 720 feet of detectable IR illumination.	
Pan Tilt Zoom (PTZ) and fixed Closed Circuit Television cameras (CCTV)	PTZ: 360□continuous pan rotation camera with 24x optical zoom, and 10x digital zoom. CCTV: 2.8x - 6.7x zoom range and day/night lenses for enhanced IR image quality.	
Mid Range Thermal Imager (MRTI) (Figure G-31)	Accessory imager that provides thermal capability to the RDISS.	**www.iecinfrared.com**
Command Station, Video Archive and Distribution System (VADS) and Network Camera Controller (NCC)	FOB protection system; compiles sensor detection information and alerts station operators.	

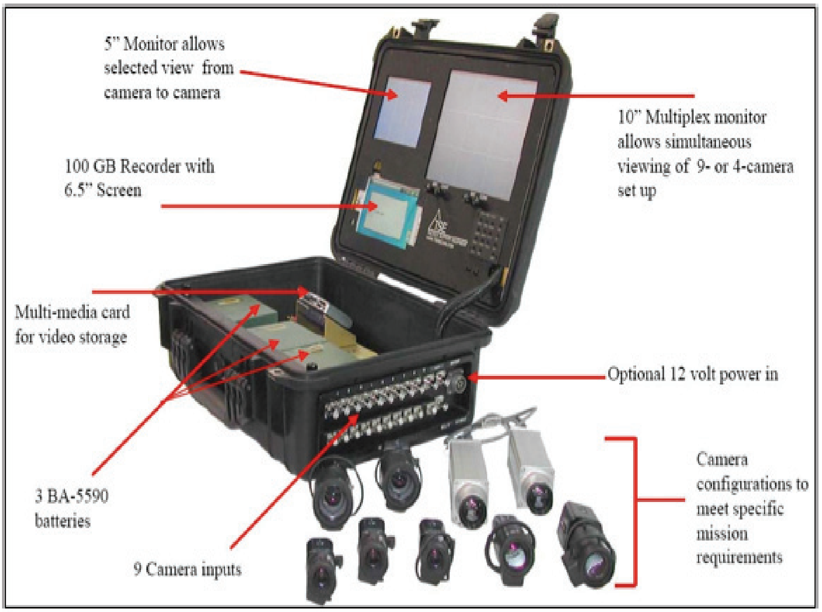


Figure G-26. Mobile Security Kit

Figure G-27. RAID Tower

Figure G-28. Cerberus

Figure G-29. MSTAR

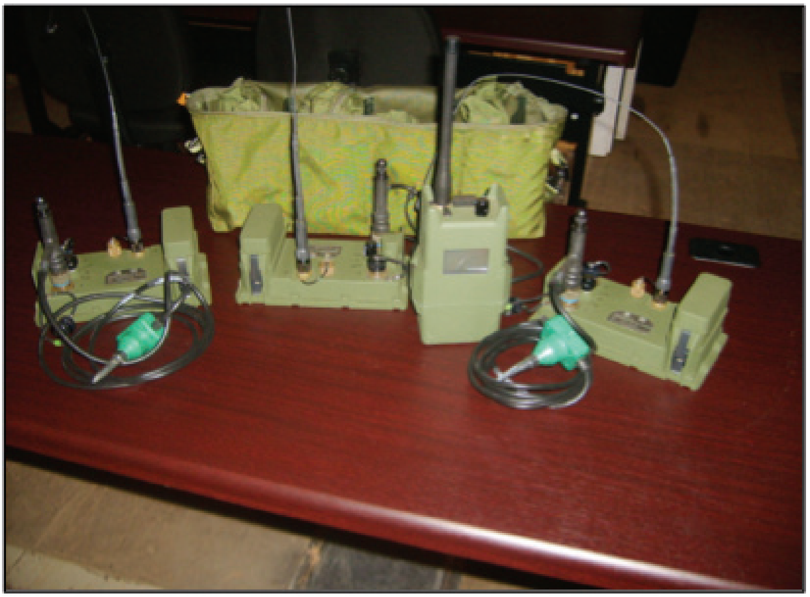


Figure G-30. BAIS

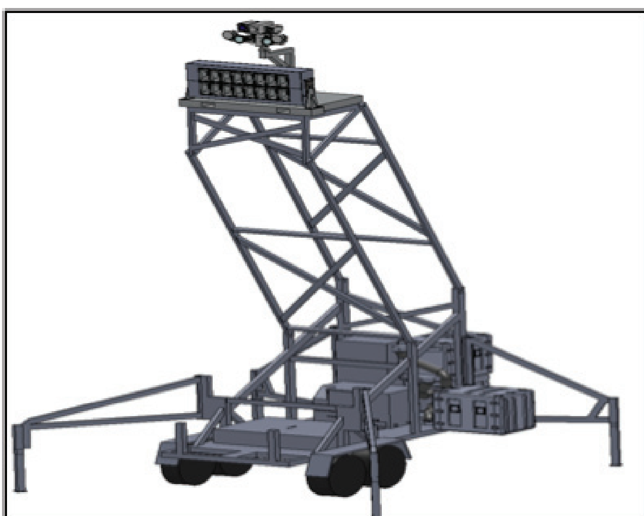
Figure G-31. MRTI

Table G-26. Power and Lighting

Item	Description	NSN/GSA/POC
Remote Area Lighting System (RALS) (Figure G-32)	Lighting system used for limited visibility operations.	6230-01-583-8453
Flood Light (Figure G-33)	Lighting system used for limited visibility operations.	6230-01-466-5315
Dewey MEP-531A	Power generator	6115-01-435-1565
Distributed Light and Sound Array (DSLA) (Figure G-34)	Delivers voice commands to distant listeners, also equipped with a laser disruptor four high intensity white lights	**www.jnlwp.usmc.mil**
Remote Area Lighting System (RALS) Air Force	Modular, transportable lighting assembly with 13 freestanding lighting fixtures.	GSA: GS-07F-0543W Part #: PDSYS-RALS-09

Figure G-32. Remote Area Lighting System

Figure G-33. Flood Light



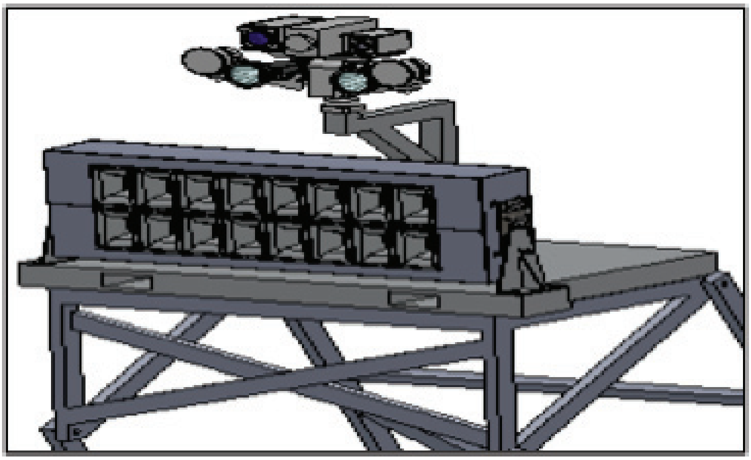


Figure G-34. Distributed Light and Sound Array

Table G-27. Surveillance and Counter-Surveillance

Item	Description	NSN/GSA/POC
MilCAM Recon III Lite (Figure G-35)	Medium range, lightweight thermal binocular.	www.gs.flir.com
Mirage 1200	Designed to aid in identifying and ranging suspect devices.	www.brandes-assoc.com
M24 Binoculars	Military issued optics that can be used for surveillance and counter surveillance.	1240-01-412-3128
Rapid Deployment Integrated Surveillance System (RDISS) (Figure G-36)	Deployed surveillance system which provides surveillance for ECP.	6710-01-C05-1215
Pole Cam	Illuminated pole camera for tactical and search operations.	6720-01-DTQ-0137
MK-880 Scope	Long range night vision scope.	5855-01-DTQ-2833
Base Expeditionary Targeting and Surveillance Sensors-Combined (BETSS-C)	Includes: • ISR • Battle Command • RAID Towers • CERBERUS Towers • Force Protection Suite • RDISS	betssclogistics.com/
FLIR Recon III Binoculars	Mid to long range thermal binoculars.	www.gs.flir.com
FLIR MilRecon Cam	Short to medium range thermal camera.	5855-01-DTQ-2834
OPAL	Used to detect weapons and bomb vest under clothing.	5855-01-531-3097

Figure G-35. MilCAM Recon III Lite

Figure G-36. RDISS

Table G-28. Communications

Item	Description	NSN/GSA/POC
MBITR AN/PRC 148 Radio (Figure G-37)	Personal size radio that can be used to provide the ECP with communication throughout the base.	5810-01-460-1605

Figure G-37. MBITR AN/PRC 148 Radio

This page intenionally blank

Appendix H
Soil-Filled Container Application

Soil-filled containers have proliferated in current theaters of operation. Further, the term soil-filled containers collectively describe two general containers types, wire and fabric, and metal. The US Army Engineer Research and Development Center (ERDC) designed numerous soil-filled container applications. These designs include specific layout configurations and employ multiple soil container units. This appendix details the soil-filled container applications listed in Figure H-1. Where applicable, bills-of-material and construction techniques for the various structures are provided. Before modification to these designs or development of others, consult a structural engineer with weapons effects mitigation experience.

Annex	Application	Page
Annex H-1	Small Observation Post	H-12
Annex H-2	Large Observation Post (Wire and Fabric Container Version)	H-16
Annex H-3	Large Observation Post (Metal Container Version)	H-20
Annex H-4	Aboveground Single-Bay Fighting Position	H-26
Annex H-5	Aboveground Two-Bay Fighting Position	H-30
Annex H-6	Aboveground 20 foot ISO/MILVAN Personnel Bunker	H-34
Annex H-7	HEMTT-LHS/PLS Bunker	H-37
Annex H-8	Helicopter Revetments	H-41

Figure H-1. Soil-Filled Containers Applications

Wire and fabric soil-filled containers are manufactured in several basic units, distinguished by fabric material and color, wire basket dimensions, and the number of bays contained within the units. Wire and fabric container units are manufactured in green, desert tan, and gray. The fabric dyes react differently to ultraviolet (UV) radiation. Current data indicate the gray fabric deteriorates most quickly. Based on this susceptibility to UV deterioration, gray fabric is not recommended. Metal containers are not subject to UV light degradation.

Site Selection and Preparation. The performance of soil-filled container structures, as with any conventional structure, depends on proper site selection and preparation. Soil-filled container structures rely heavily on near-surface soil strength for overall structural stability. Near surface material conditions might deteriorate due to elevated moisture levels, soil erosion, freeze/thaw cycles, organic matter decay, and compression of weak soils. Therefore, the site evaluation process should consider site drainage patterns and existing soil conditions. FM 5-34, *Engineer Field Data* details soil evaluation procedures.

Construct soil-filled containers on a flat foundation that will support the structure over its intended life. If construction cannot take place on an improved surface (concrete, asphalt, or stabilized soil) the foundation area must be improved (Figure H-2).

Site Preparation and Foundation Considerations

- □ Has the foundation site been leveled?
- □ Have organic materials and loose surface soils been removed?
- □ Has exposed foundation material been tested for stability? (FM 5-34 details soil foundation tests)
- □ If exposed foundation material will not provide a stable foundation, or if the structure's life expectancy exceeds 6 months, has an improved foundation been constructed to prevent future settlement and shifting?

Figure H-2. Site Preparation and Foundation Considerations

To construct an improved foundation (Figure H-3), excavate a trench 20 in. (508 mm) deep beneath structure walls. Extend the trench width 20 in. (508 mm) beyond each wall edge. After excavation, line the trench with a geotextile cloth (minimum weight 200 g/sq. m) and backfill the trench with a well compacted layer of coarse-graded fill material or crushed rock. Prior to construction, test the improved foundation for strength and stability.

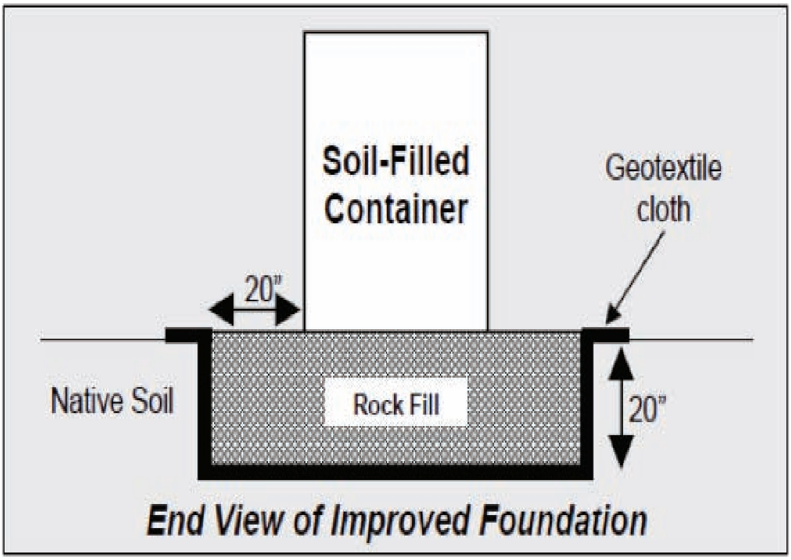


Figure H-3. Typical Improved Foundation

Wire and Fabric Containers. Wire and fabric container kits consist of bins, connecting pins, and plastic ties. The bins come in multiple sizes and consist of collapsible wire mesh lined with geotextile fabric. The bins are corner-connected with spiral wire hinges that allow wall sections to be expanded from a compact, folded storage configuration (Figure H-4). This allows the walls to be transported at only 5 percent of constructed volume.

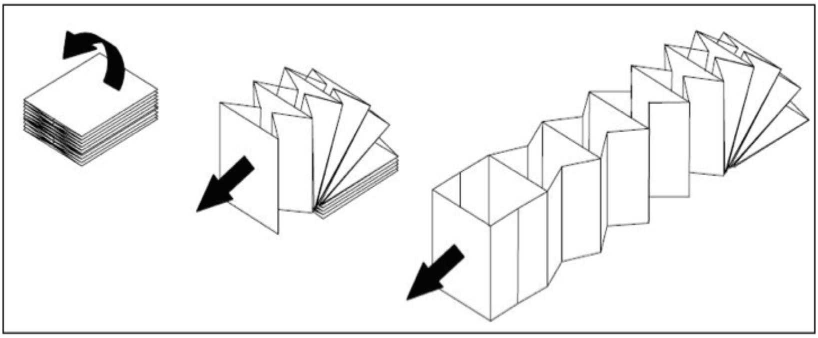


Figure H-4. Wire and Fabric Container Expansion

Layout and Connection. Position wall units so that attached plastic wire ties are located at the top. This allows connection to additional container unit layers. In most applications, multiple container units are necessary to achieve the desired shape and dimensions. Secure multiple units in a single layer for structural continuity.

Container units can be connected together to increase overall structure length or form corners and tees (Figure H-5). Units are connected end-to-end by connecting the coil hinges at the ends of the units to be joined and connecting the common wall with plastic ties. Units are connected end-to-side by connecting the coil hinges at the common corners between units, and connecting the common wall with plastic ties.

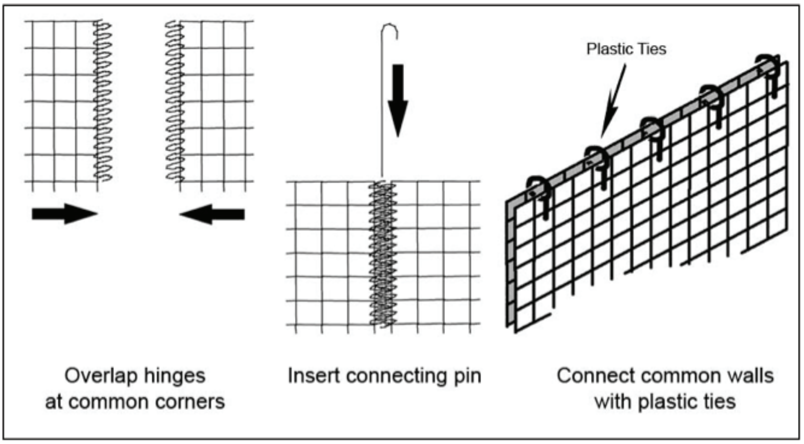


Figure H-5. Wire and Fabric Container Connection Technique

In addition to forming corners in an end-to-side fashion, corners can be formed by manipulating a single container unit. To create a single-unit corner, the unit must contain coil hinges at the center of each sidewall. To form a corner (Figure H-6), locate two adjacent bays where the corner is intended. Push the coil hinges at the center of each bay's sidewall inward, and bring all three coil hinges located at the bay corners together. While bringing the three corner hinges together, rotate the unit end to form the corner. After bringing the coil hinges together, connect the coil hinges with a standard coil hinge connection pin.

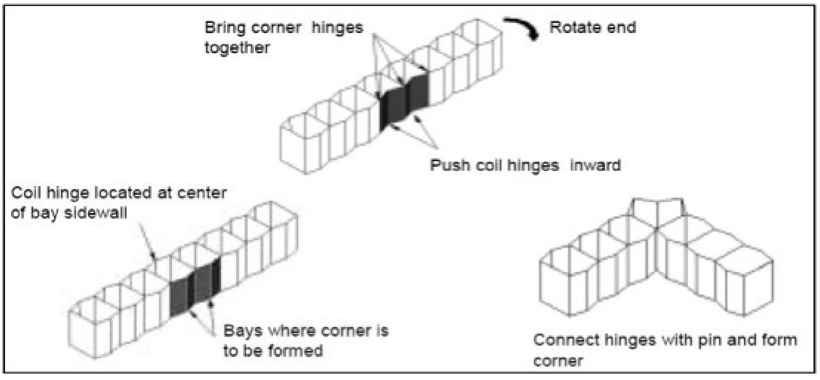


Figure H-6. Wire and Fabric Container Corner Formation Technique

Depending on the structure's height or desired wall thickness, two units might be placed side-to-side. In this case, connect the coil hinges at the unit's common corners with standard coil hinge connections. To prevent fill spill between units (which may affect structure stability), connect common walls along the full length of units with plastic ties.

Modifications. Structures of non-standard unit length may be necessary. Break container units into smaller units by unscrewing the coil hinges at the center of a single bay's sidewalls. Cut the fabric liner, fold in the loose ends, and secure with the removed coil hinges. Note that some units are manufactured with connection pins inserted into overlapped coil hinges. Units can be separated by removing the connection pin (Figure H-7).

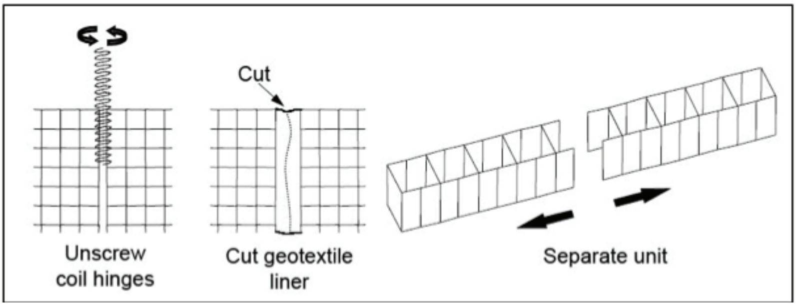


Figure H-7. Wire and Fabric Container Modification Technique

Fill Placement. The ideal fill material is a sand/gravel mix. A basic advantage of wire and fabric containers is the ability to create a structural framework, and then fill the framework to obtain structural strength. These container structures rely on proper fill and fill placement for optimum performance. Closely follow fill guidelines.

Prior to fill, connect single-layer units and adjust to the desired layout. Begin fill at the corner bays, and then every 8th to 12th bay thereafter, with one foot of compacted fill placed in two 6 in. lifts. This anchors the entire layer for remaining fill activities. Fill the remaining bays with uniformly distributed material. Do not fill one bay while an adjacent bay is completely empty.

As fill is placed in the bays, the material exerts lateral outward pressure. Container walls reach capacity by outward expansion. This expansion confines the fill material to the widest, shortest volume of space, reducing the potential for future movement and failure. Expansion also increases wall width, which further increases stability.

Do not place restraint mechanisms on container walls. As bays are filled, outward pressure induces stress concentrations in restraint mechanisms that can lead to restraint failure. When restraints fail, the container walls move outward to maximum deformation. As fill material occupies the void created by the moving wall, material also moves downward. This outward/downward fill movement induces wall settlement, load shifting, and potential structural failure.

To accommodate deformation/expansion, the center coil hinges on each side of every bay must be pulled out approximately 4 in. during initial fill. If coil hinges are not present, pull the sides of each bay outward to create a slightly curved side wall for each bay. This assists the bay in expanding as necessary during fill.

After adjusting the base, fill the bays (Figure H-8). Unless otherwise specified, place fill in lifts no greater than 9 inches thick, followed by foot compaction. Fully compact the fill along the outer walls and corners. Proper compaction prevents future fill settlement.

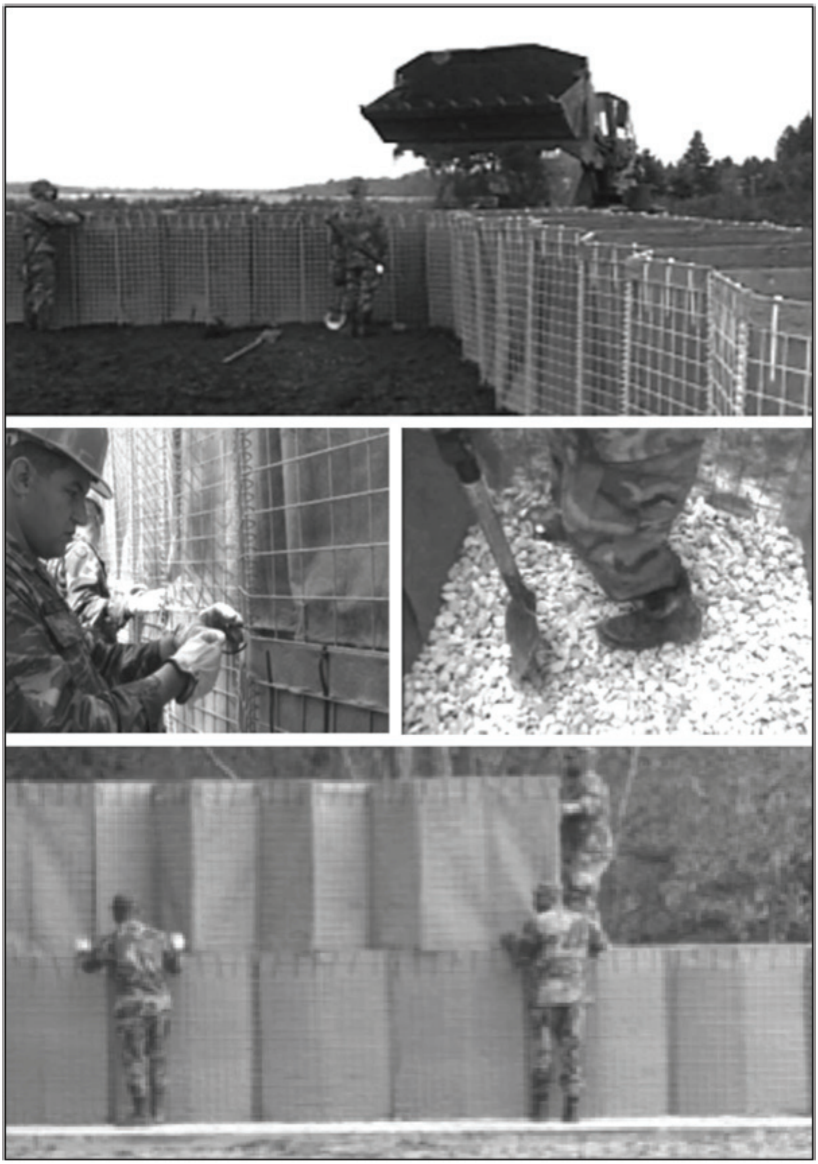


Figure H-8. Wire and Fabric Container Fill Procedure
(clockwise from top: place and fill first layer; compact fill into sides and corner; place second layer; connect layers together with plastic ties)

If a second layer is to be placed on top of the first, stop the bottom layer fill approximately 4 in. below its top edge. The second layer must then be correctly aligned on top of the first. Place the second layer so that the bay corners are directly above the bottom-layer corners. Proper positioning of the second layer prevents excessive fill leakage and enhances structural stability. After positioning the second layer, seal wall junctions with the geotextile flaps located on the bottom of the second layer. Connect the layers with pre-positioned plastic ties. Fill the second layer exactly as the first.

Durability. UV light degradation is the primary environmental factor affecting container durability. Fabric liners deteriorate with prolonged exposure to sunlight and begin to release fill material. The fabrics are colored with dyes that affect UV resistance. The expected life of available fabric colors are: Gray – 1 to 2 years; Green – greater than 6 years; Tan – no data available.

In windy environments, fill material can be scoured away. This undermines soil surfaces that support roof structures. In such conditions, cap the exposed fill material with sand bags to mitigate wind action.

In rainy environments, moisture infiltration may affect container durability. Moisture induces fill settlement and weakens the wall's load capacity. Moisture can also hasten fabric liner decay. In high-moisture environments, a waterproofing mechanism (such as a paint or membrane) over exposed surfaces may mitigate water infiltration. Additional drainage may be necessary for runoff. Also, waterproofing should not affect the wall's structural integrity.

Metal Containers. Metal containers or revetments provide sidewall protection (Chapter 8). The containers are shipped flat and unassembled. Each kit consists of four panels (side, end, cross, and brace), connecting pins, flaring tools, and corner containment materials (wire mesh and poly film).

Metal container side panels are typically 8 ft. (2.4 m) long. End and cross panels are 2, 4, or 6 ft. (0.6, 1.2, or 1.8 m) long. Brace panels are 4 ft. (1.2 m) long. Panel heights vary depending on material thickness: 16 gauge metal is 2 ft. (0.6 m) and 18 gauge metal is 3 ft. (0.9 m) high.

As with wire and fabric containers, metal container performance and lifespan depends on site selection and preparation. A well-prepared foundation enhances performance and durability.

Layout and Construction. Place all metal panels short leg down with notches at the top (Figure H-9). Place side panels with the large corrugations outward. If both 16 gauge and 18 gauge materials are used, place 16 gauge materials at the bottom.

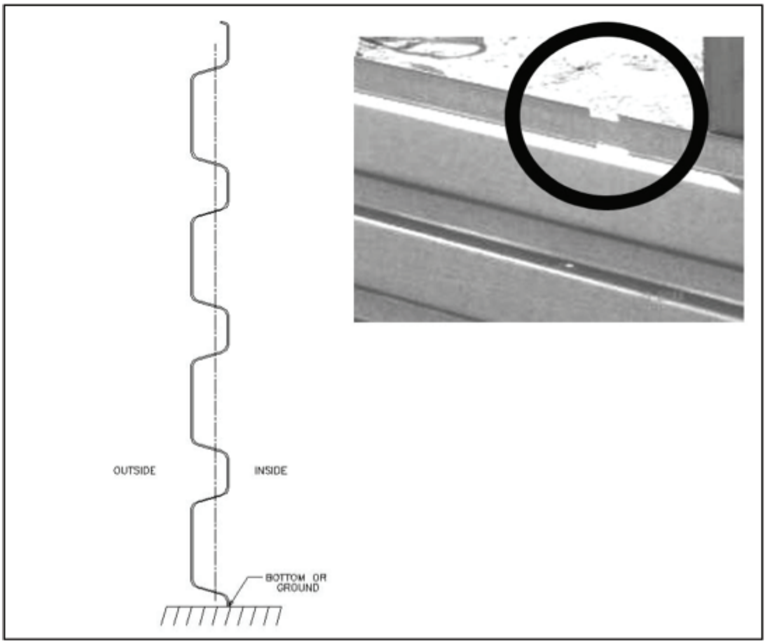


Figure H-9. Panel Orientation Panel Notch at Top Shown in Inset

Flare the top and bottom panels with a flaring tool or pliers prior to installation (Figure H-10). Safety gloves are recommended during construction.

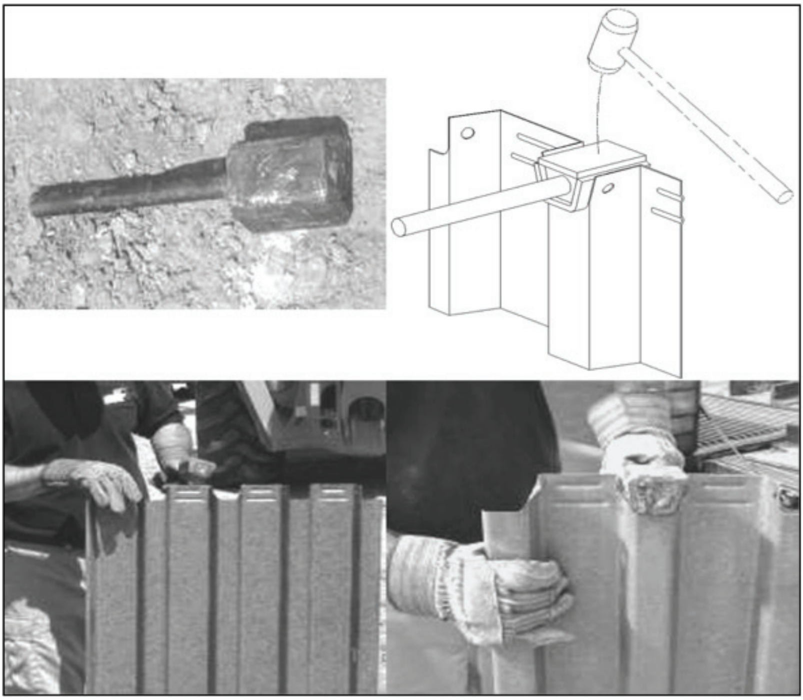


Figure H-10. Panel Flaring Methods
(clockwise from top left: flaring tool; flaring tool and Hammer; flaring tool only; pliers)

After surface and foundation preparation, metal container assembly consists of five steps.

Step 1. Assemble end and side panels. Begin assembly from left to right with the small panel legs facing down. Pin the side panel to the end panel with the provided connecting pin (Figure H-11).

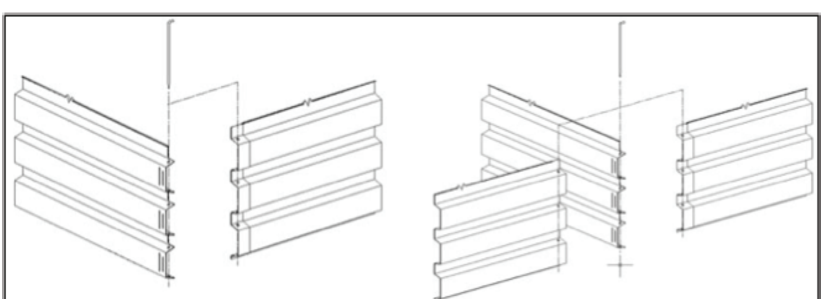


Figure H-11. Panel Connection Technique
(left: end and side panels; right: side and cross panels)

Step 2. Add end and brace panels. Face the small corrugations toward each other for proper alignment.

Step 3. Add side and cross panels (Figure H-11). Face all cross panels in the same direction. Install side panels from left to right to allow proper overlap. Repeat as needed to obtain the required length.

Step 4. Attach side panels on opposite side. Install side panels from left to right to allow proper overlap.

Step 5. Install wire mesh and poly film to minimize fill material leakage. Place poly film and wire mesh in corners. Add fill material (Figure H-12). Repeat as needed to reach the required height.

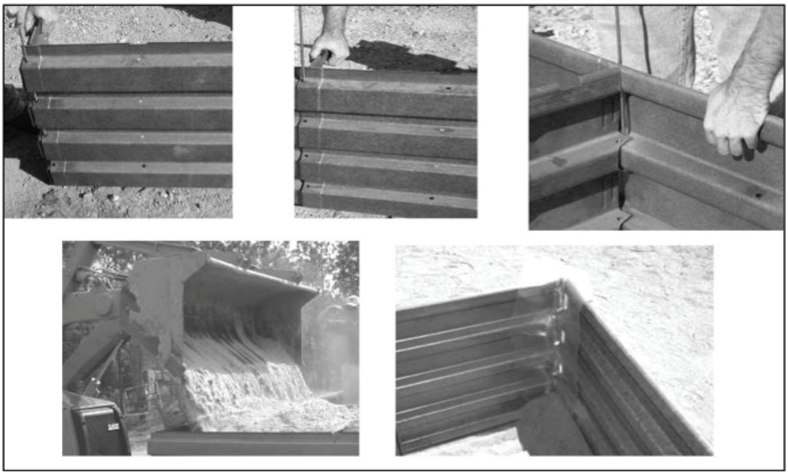


Figure H-12. Metal Container Fill Procedure
(clockwise from top left: assemble end and side panels; add cross panels; add brace panels; add poly film and wire mesh; add fill material)

Fighting Positions, Observation Positions, and Bunker Applications. Fighting and observation positions allow enemy engagement and provide some level of protection against small arms, VBIED, and RAM. These positions enhance FOB perimeter security and ECP overwatch positions.

Bunker applications protect against larger weapons. Bunker designs were developed and tested at the request of the Directorate of Training, US Army Engineer School, Fort Leonard Wood, MO. Constructed properly, bunkers protect against direct-hit 81/82-mm mortar, and the above-ground bunkers sidewalls defeat fragmentation from near-contact burst of up to 120-mm mortar, 122-mm rockets and 155-mm artillery rounds. Overhead cover for bunker positions consist of roof systems covered with 24 in. of fill material. Smaller roof systems are constructed with composite fiberglass panels; larger systems are constructed with steel sheet piling (Figure H-13). Improvised roof systems can be constructed if specified roof materials are unavailable. Possible alternatives for the composite fiberglass include runway landing mats or wooden stringer roofs. Design and construct wooden roofs in accordance with FM 5-103, *Survivability*, Appendix B “Bunker and Shelter Roof Design.”

For larger structures, sheet steel piling cannot simply be replaced with wooden stringers. Improvised roof systems for these positions might include steel beams to span the structure and a wooden roof deck placed over the beams. A structural engineer should design improvised roof systems to ensure adequate load capacity.

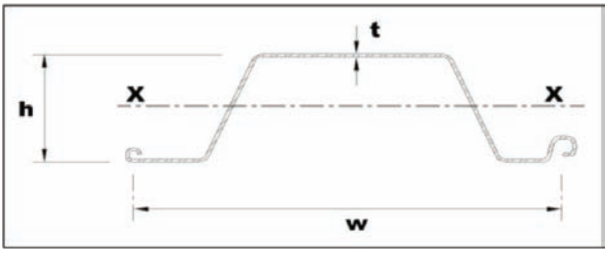


Figure H-13. Sheet Piling Material Requirements
(material is ASTM A572, grade 50 steel; prime and paint all piling as required; minimum section properties are Thickness (t) = 0.2 in.; Height (h) = 6 in.; Width (w) = 27.5 in.; and X-axis section modulus (x) = 6.3 cubic in/ft.)

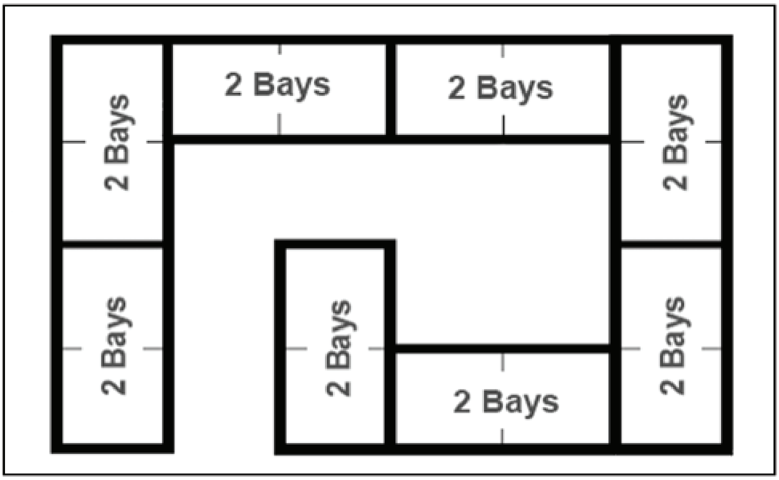
Planning estimates for equipment, personnel, assets, and construction time are provided for annex designs. In many cases, multiple equipment types can accomplish the same task, and are listed as alternatives. Give planning consideration to such issues as equipment and operator availability, topography, work area limitations, and maneuverability. Based on foundation type and fill material, certain tasks and equipment may be unnecessary. Only heavy equipment is listed below. Hand tools such as shovels, rakes, pliers, and wire cutters are also necessary.

The indicated construction time includes foundation preparation and position construction. Many factors such as threat based urgency, equipment and material availability, experience, and knowledge of construction techniques can affect time requirements. Construction times are estimates.

Annex H-1

Small Observation Post

The construction materials for this position are available in a pre-assembled package (NSN 5680-01-501-1462). If the materials are not ordered as a package, use the bill of materials listed in the table below.



Section Layout

Bill of Materials

Item Description	NSN	Quantity
Wire and Fabric Container (2 ft. x 2 ft. x 4 ft.)	5680-99-001-9397 (Green) 5680-99-968-1764 (Sand)	30
Composite Material Panels (12 ft. length)	5675-01-500-2803	4
Composite Material Panels (8 ft. length)	5675-01-500-2729	3
Toggle connectors (12 ft. length)	Incl. in NSN 5675-01-500-2803	3
Waterproof membrane (16 ft. x 20 ft.)	5650-01-504-5373	1
Fill material (cubic yards)	N/A	24

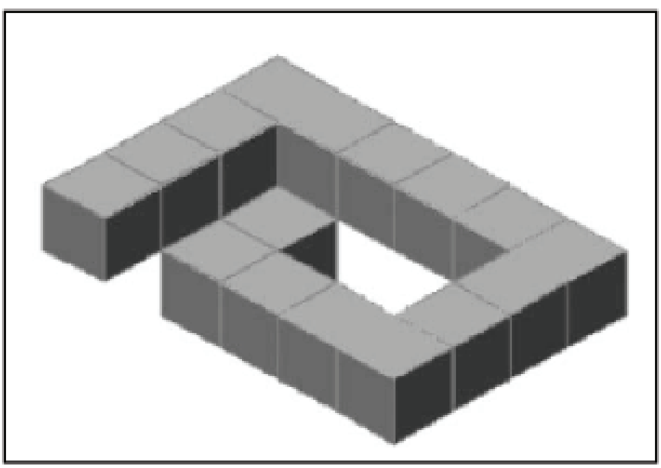
Equipment, Personnel, and Time Estimate

Task	Equipment Required	Personnel Required*	Time Required
Site preparation and foundation leveling	bulldozer, DEUCE, ACE, front-end loader, skid-steer loader, SEE, HMEE	2	30 min/person x 2 = *1man- hour*
Foundation compaction	vibratory roller (smooth drum or pad feet), HSC	2	30 min/person x 2 = *1 man-hour*
Haul fill material to site	dump trucks	varies	varies
Erect structure and place fill	front-end loader, skid-steer loader, SEE, HMEE	4	5 hrs/person x 4 = *20 man-hours*
Total manpower			*22 man-hours*

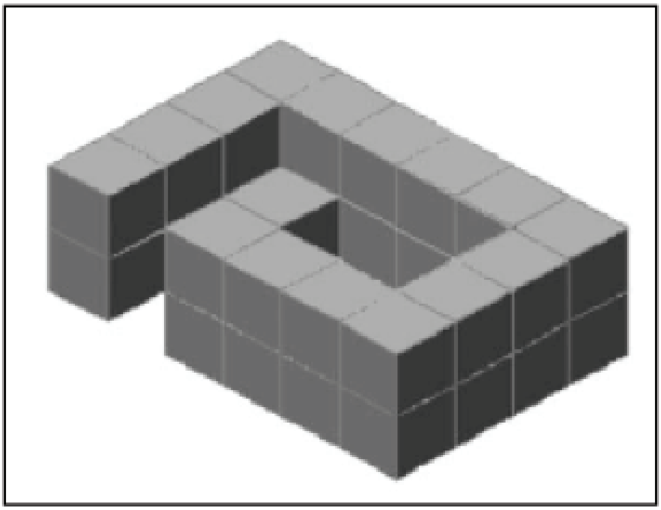
*Excludes equipment operators

General Construction Steps for Small Observation Post

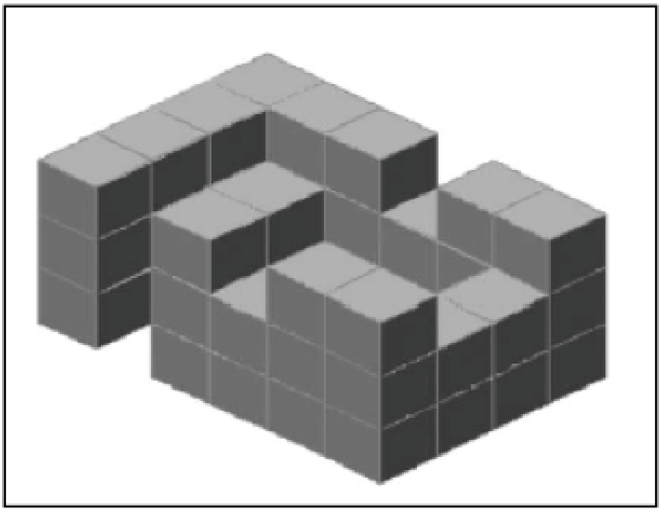
1. Place and fill first layer



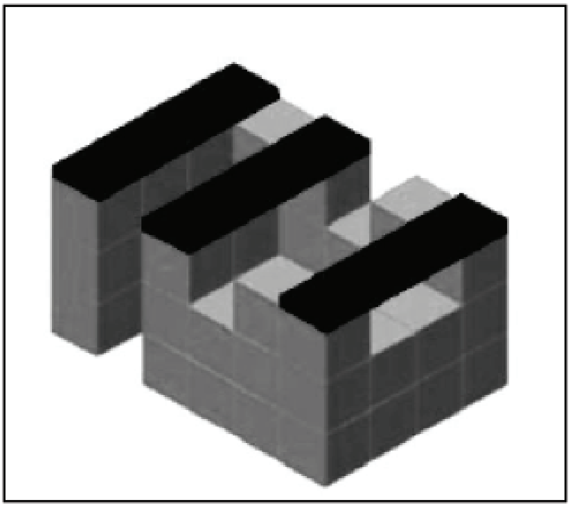
2. Place and fill second layer



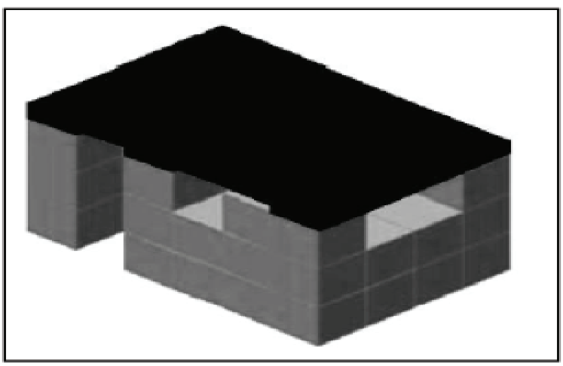
3. Place and fill third layer



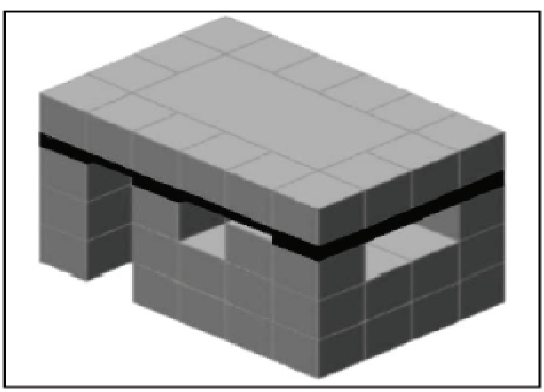
4. Add roof support



5. Add roof layer

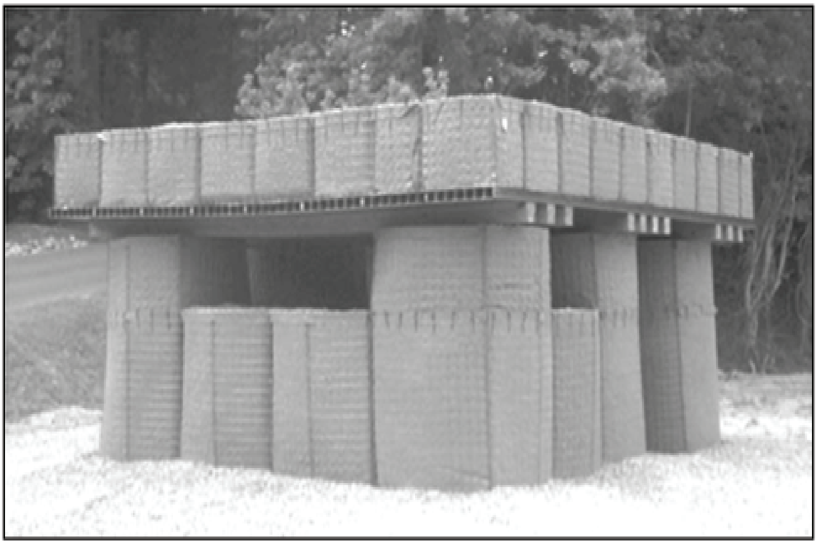


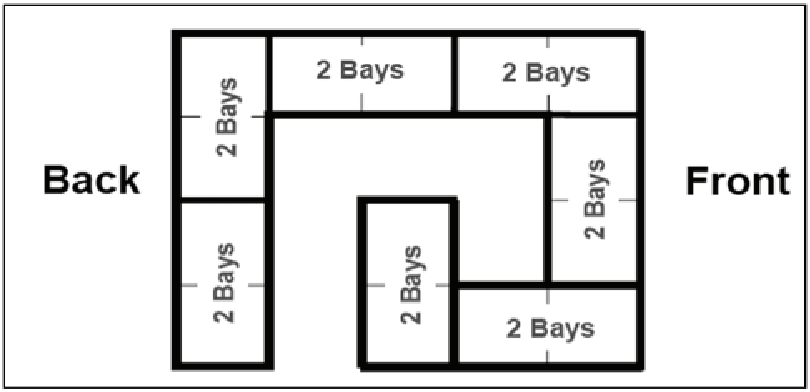
6. Add and fill overhead cover



Annex H-2

Large Observation Post (Wire and Fabric Container Version)





Section Layout

Bill of Materials

Item Description	NSN	Quantity
Wire and Fabric Container (modified to 4.5 ft. H, 3.5 ft. W, 7 ft. L)	5680-99-001-9396 (Green) 5680-99-835-7866 (Sand)	7
Wire and Fabric Container (modified to 2 ft. H, 3.5 ft. W, 3.5 ft. L)	5680-99-001-9396 (Green) 5680-99-835-7866 (Sand)	6
Wire and Fabric Container (2 ft. x 2 ft. x 4 ft.)	5680-99-001-9397 (Green) 5680-99-968-1764 (Sand)	16
Timbers (6 in. x 6 in. x 16 ft. length)	-	10
Composite Material Panels (20 ft. length)	5675-01-496-4896	8
Toggle connectors (20 ft. length)	Incl. in NSN 5675-01-496-4896	7
Waterproof membrane (16 ft. x 20 ft.)	5650-01-504-5373	1
Fill material (cubic yards)	N/A	70

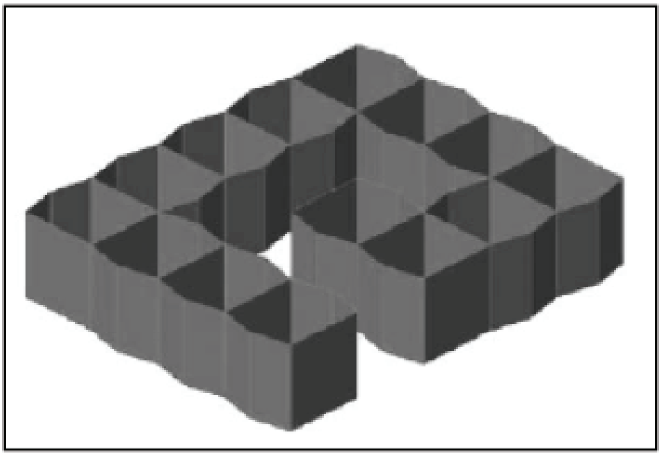
Equipment, Personnel, and Time Estimate

Task	Equipment Required	Personnel Required*	Time Required
Site preparation and foundation leveling	bulldozer, DEUCE, ACE, front-end loader, skid-steer loader, SEE, HMEE	2	1 hr/person x 2 = *2 man-hours*
Foundation compaction	vibratory roller (smooth drum or pad feet), HSC	2	30 min/person x 2 = *1 man-hour*
Haul fill material to site	dump trucks	varies	varies
Erect structure and place fill	front-end loader, skid-steer loader, SEE, HMEE	6	7 hr/ person x 6 = *42 man-hours*
Total Manpower			*45 man-hours*

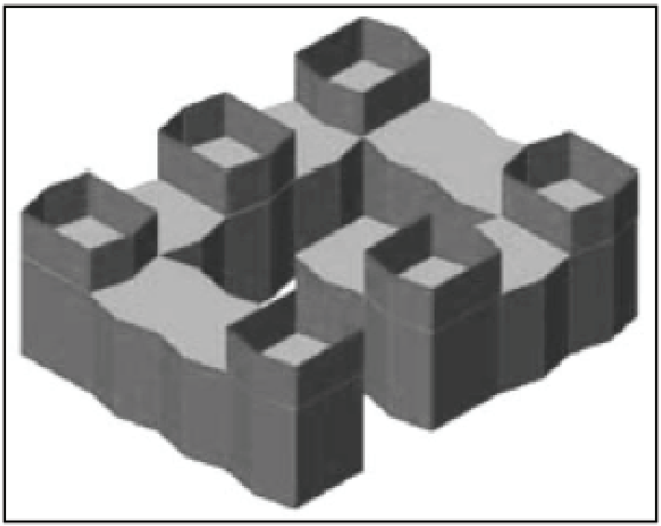
*Excludes equipment operators

Construction Steps for Large Observation Post (Wire and Fabric Container Version)

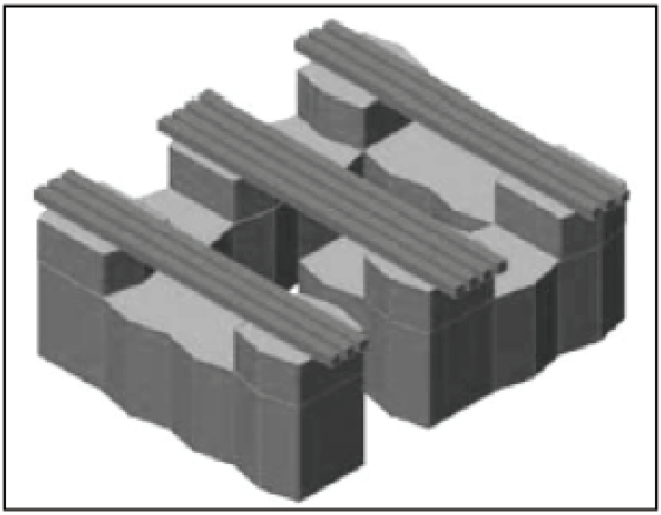
1. Arrange and fill first layer



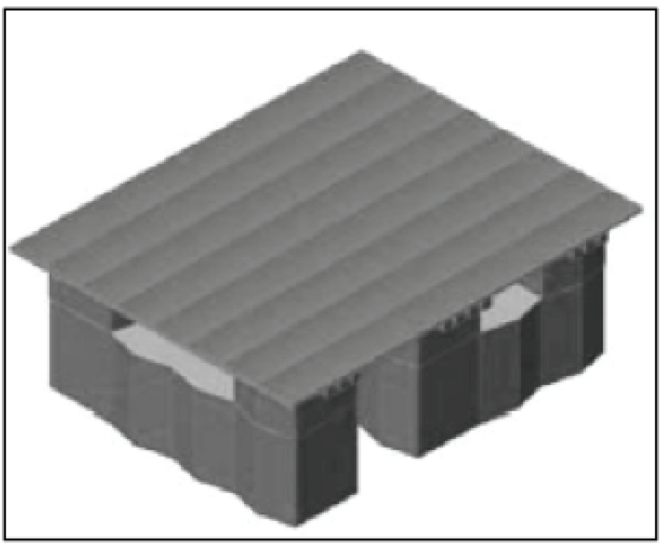
2. Arrange and fill second layer



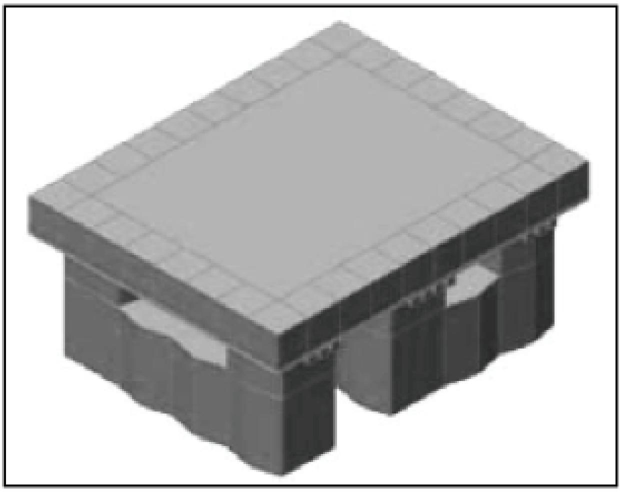
3. Add timbers for roof support



4. Add roof layer

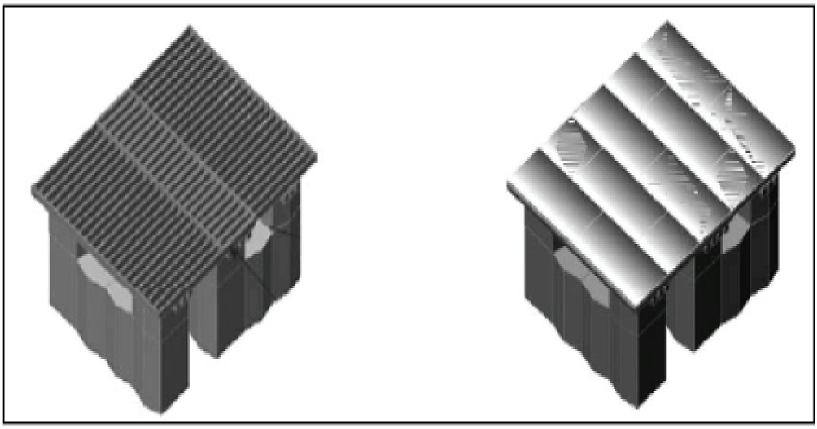


5. Arrange and fill overhead cover

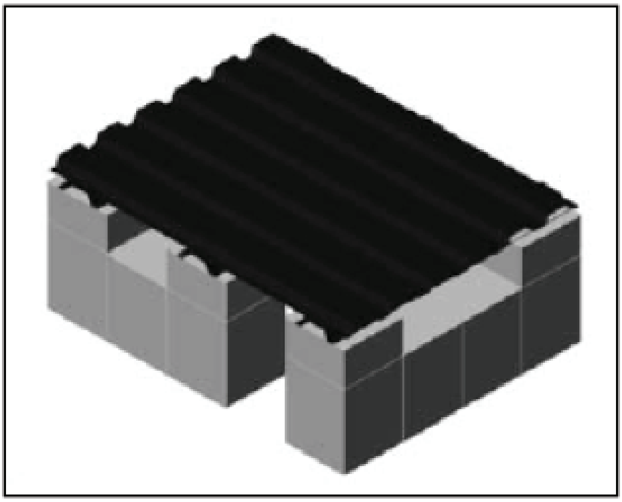


Configuration Options:

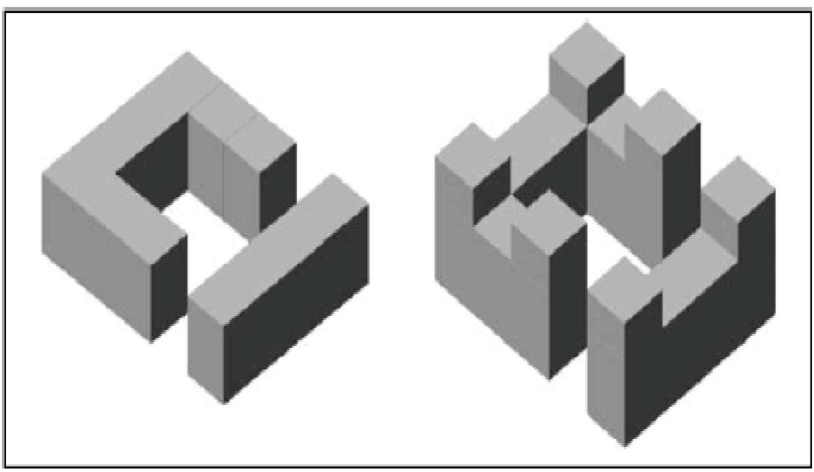
Wooden Roof constructed with 2 x 6 timbers (left) and ¾ in. plywood (right)



Sheet Pile Support and Roof constructed with sheet pilings



Entry Control Point or Guard House (modified layout for additional entrance)



Annex H-3

Large Observation Post (Metal Container Version)

Bill of Materials

Item Description	NSN	Quantity
Metal Revetment Protective Position Kit	Contact USACE ERDC	1
Steel Column □W8x10 (7 ft.-1 in.)	N/A	6
Steel Beam □W8x10 (18 ft.)	N/A	6
Steel Base Plate (3□x3 ft. x1/2 in.)	N/A	6
Steel Cap Plate (2 ft. x2 ft. x1/2 in.)	N/A	6
Steel Angle (3 in.x3 in. x1/4 in.), 2-ft. long	N/A	12
Steel Angle (3 in. x3 in. x 1/4 in.), 5□in. long	N/A	12
Composite Material Panel w/Toggle Connector, 22 ft. long	5675-01-496-4896	9
Waterproof Membrane (18 ft. x 22 ft.)	5650-01-504-5373	1
Fill Material, cubic yard	N/A	70
Revetment Kit, 4 ft. x8 ft. x64 ft. length	5450-01-535-7952	□
Revetment Kit, 2 ft. x6 ft. x104 ft. length	5450-01-535-7955	□
Revetment Kit, 4 ft. x10 ft. x48 ft. length	5450-01-537-7061	□
If individual kit components are not available, fashion the following kit pieces:		
16 Ga Side Panel, 2 ft. H x 8 ft. L	□ -	44
16 Ga End Panel, 2 ft. H x 2 ft. L	□ -	24
16 Ga End Panel, 2 ft. H x 4 ft. L	□ -	42
16 Ga Brace Panel, 2 ft. H x 4 ft. L	□ -	22
18 Ga Side Panel, 3 ft. H x 4 ft. L	□ -	24
18 Ga End Panel, 3 ft. H x 4 ft. L	□ -	8
2 ft. Connecting Pin	□ -	190
3 ft. Connecting Pin	□ -	30

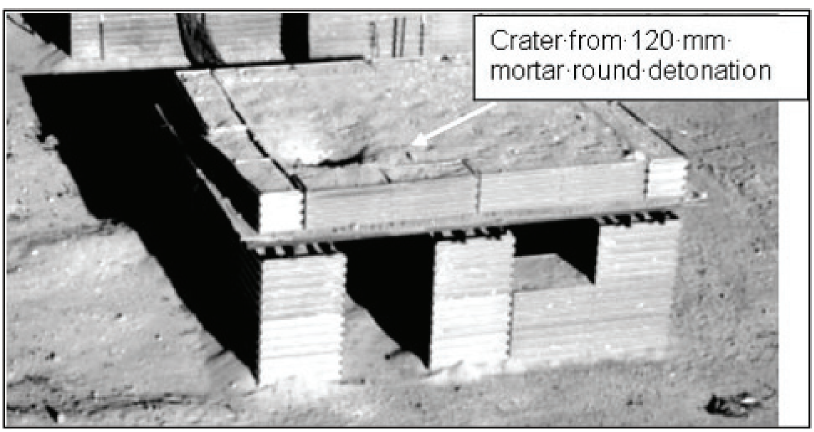
Equipment and manpower requirements are similar to those for the Wire and Fabric Version.

Equipment, Personnel, and Time Estimate

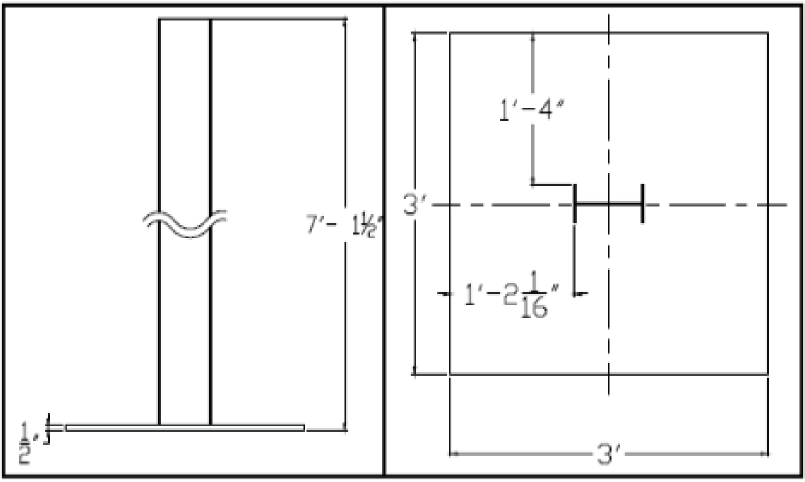
Task	Equipment Required	Personnel Required*	Time Required
Site preparation and foundation leveling	bulldozer, DEUCE, ACE, front-end loader, skid-steer loader, SEE, HMEE	2	1 hr/person x 2 = *2 man-hours*
Foundation compaction	vibratory roller (smooth drum or pad feet), HSC	2	30 min/person x 2 = *1 man-hour*
Haul fill material to site	dump trucks	varies	varies
Erect structure and place fill	front-end loader, skid-steer loader, SEE, HMEE	6	8 hr/person x 6 = *48 man-hours*
Total Manpower			*51 man-hours*

*Excludes equipment operators

Results of ERDC static and live-fire tests showed this bunker design will protect from direct-hit 82-mm and 120-mm mortars and near-miss (4 ft.) 122-mm rockets with no significant structural damage and no fragment penetration through the sidewalls or roof.

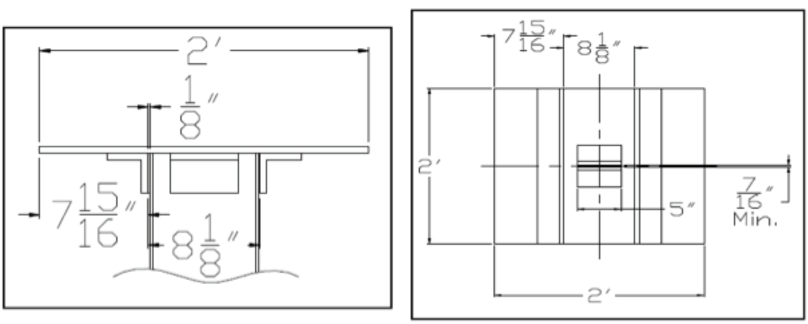


Six (6) columns are needed to construct this position. Fabricate with one (1) 3 in. x 3 in. x ½ in. plate and one (1) WBx10, 7 ft.-1 in. length column. Fillet weld (minimum 3/16 in.) all locations. Column and base plate steel details are shown below.



Left: Column and Base Plate; Right: Base Plate Details

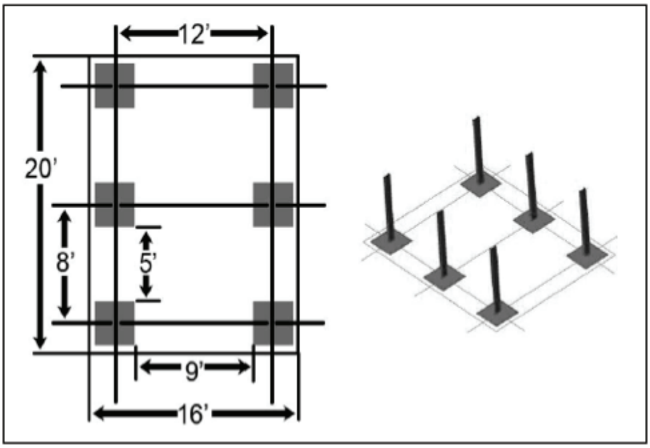
Six (6) cap plates are required, one for each column. Fabricate with one (1) 2 ft. x 2 ft. x 1/2 in. plate, two (2) 3 in. x 3 in. x 1/2 in. 2-ft. angle iron, and two (2) 3 in. x 3 in. x 1/2 in. 5-in. length angle iron. Fillet weld (minimum 3/16 in.) all locations. Cap plate details are shown below.



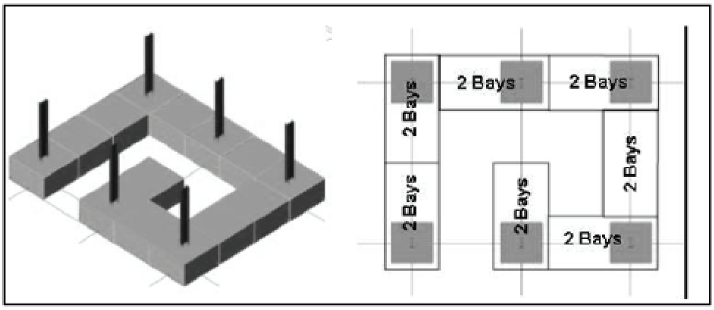
Left: Cap Plate on Column Detail; Right: Cap Plate Details

Construction Steps for Large Observation Post (Metal Container Version)

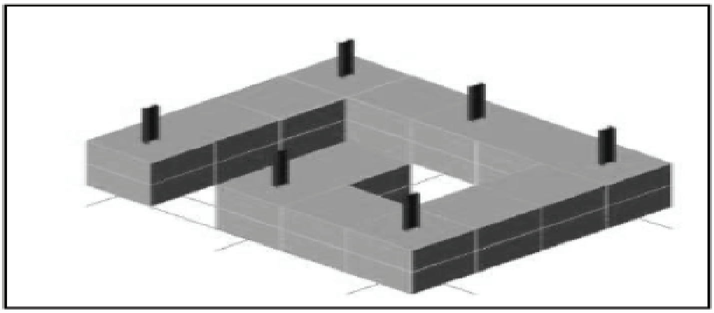
1. Flatten surface, locate and place columns. Columns are important for stability.



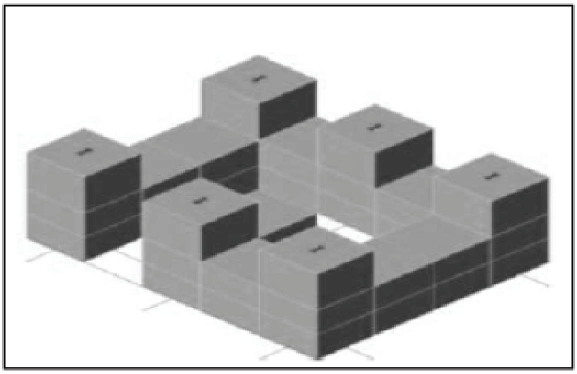
2. Arrange and fill first layer (section layout shown at right) starting with the shaded bins.



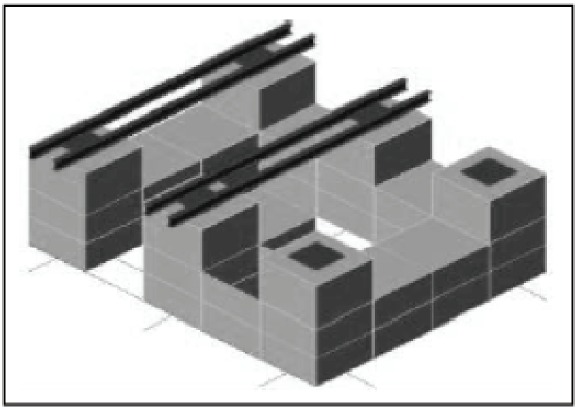
3. Arrange and fill second layer



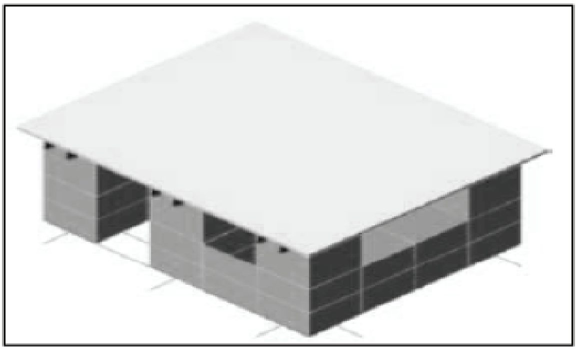
4. Arrange and fill third layer



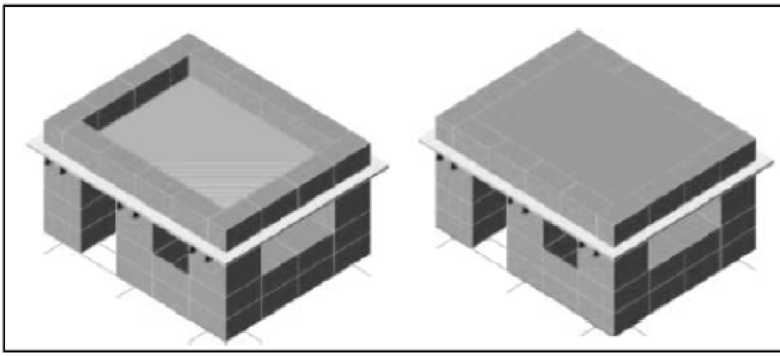
5. Add cap plates and add roof support



6. Add composite roof

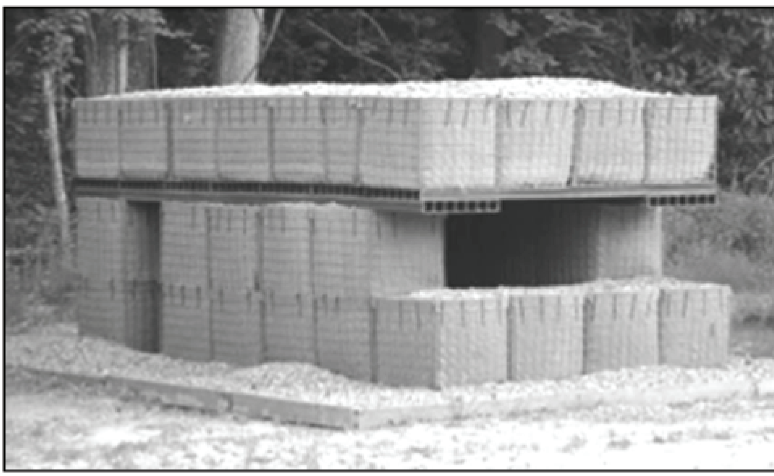


7. Arrange and fill overhead cover

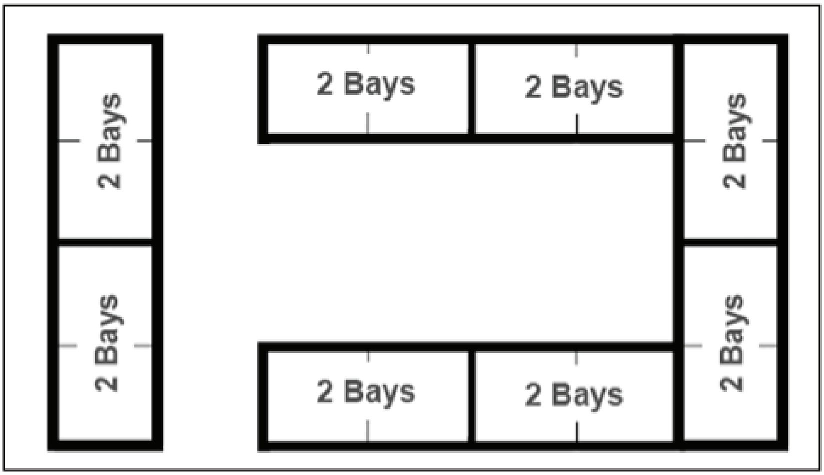


Annex H-4

Aboveground Single-Bay Fighting Position



The required construction materials for this position are available in a pre-assembled package (NSN 5680-01-501-1235). If the materials are not ordered as a package, use the bill of materials listed in the table below.



Section Layout

Bill of Materials

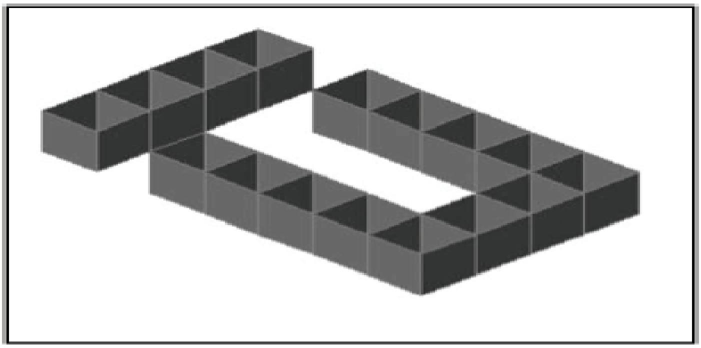
Item Description	NSN	Quantity
Wire/Fabric Container (2 ft. x 2 ft. x 4 ft.)	5680-99-001-9397 (Green) 5680-99-968-1764 (Sand)	23
Composite Material Panels (14 ft. length)	5675-01-500-2808	2
Composite Material Panels (8 ft. length)	5675-01-500-2729	7
Toggle connectors (8 ft. length)	Incl. in NSN 5675-01-500-2729	6
Waterproof membrane (8 ft. x 14 ft.)	5650-01-504-5373	1
Fill material (cubic yards)	N/A	20

Equipment, Personnel, and Time Estimate

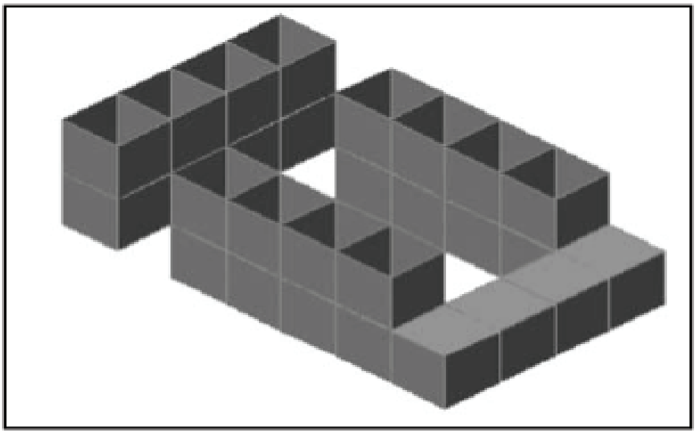
Task	Equipment Required	Personnel Required*	Time Required
Site preparation and foundation leveling	bulldozer, DEUCE, ACE, front-end loader, skid-steer loader, SEE, HMEE	2	30 min/person x 2 = *1 man-hour*
Foundation compaction	vibratory roller (smooth drum or pad feet), HSC	2	30 min/person x 2 = *1 man-hour*
Haul fill material to site	dump trucks	varies	varies
Erect structure and place fill	front-end loader, skid-steer loader, SEE, HMEE	2	6 hr/person x 2 = *12 man-hours*
Total Manpower			*14 man-hours*

Construction Steps for Aboveground Single-Bay Fighting Position

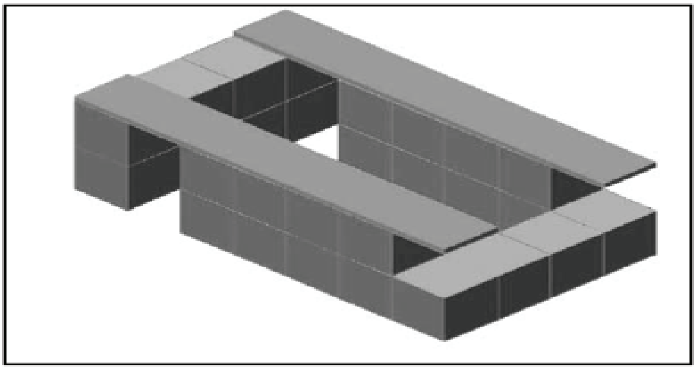
1. Arrange and fill first layer



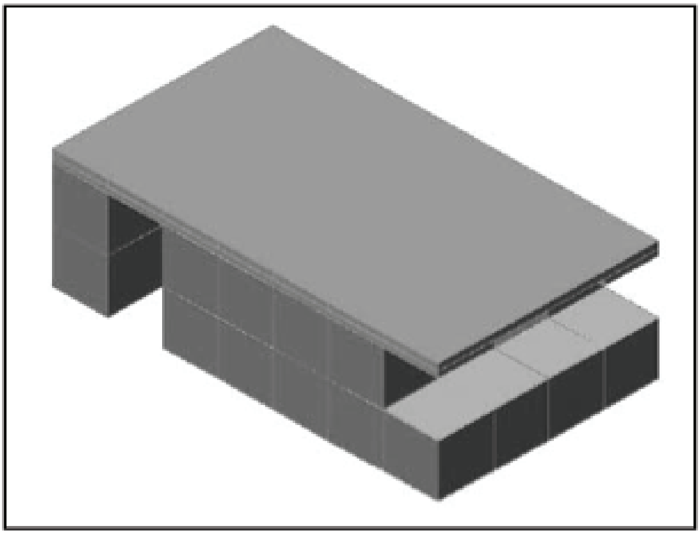
2. Arrange and fill second layer



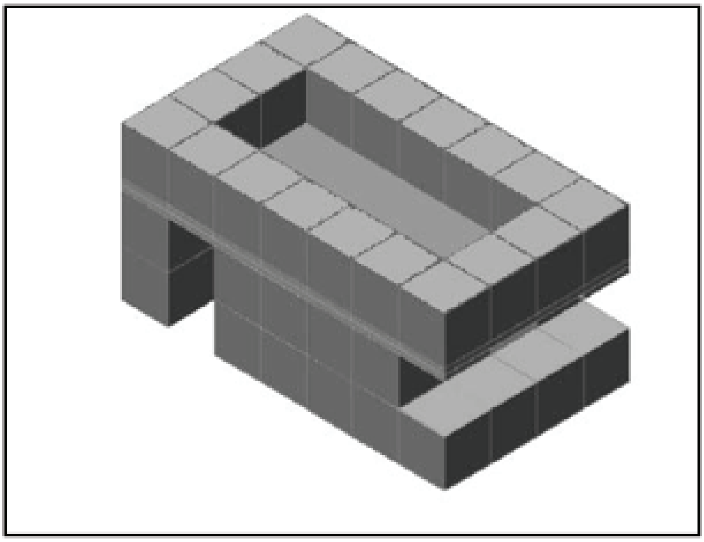
3. Add roof support



4. Add roof panels

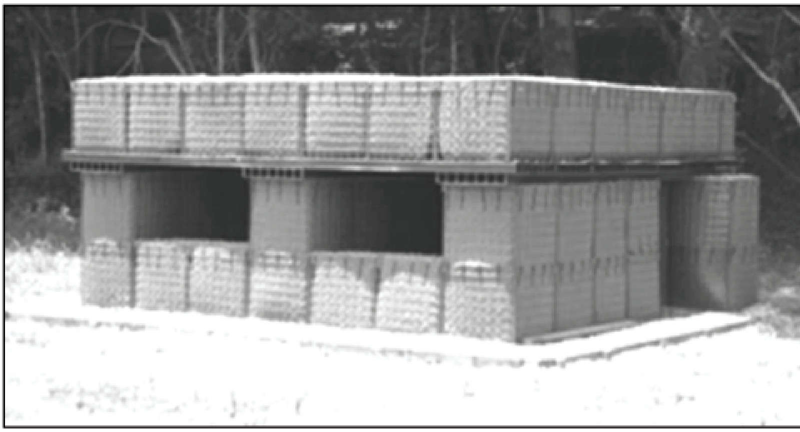


5. Add and fill overhead cover

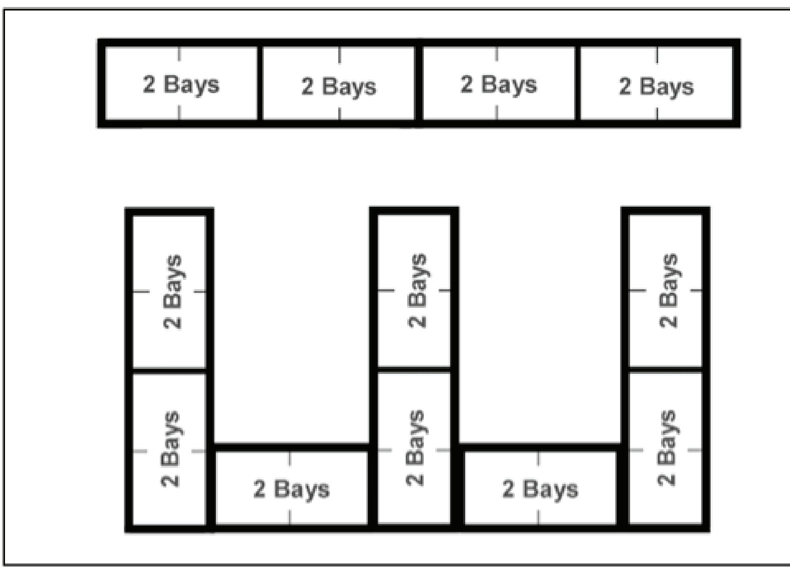


Annex H-5

Aboveground Two-Bay Fighting Position



The material required to construct this position are available in a pre-assembled package (NSN 5680-01-501-1357). If the materials are not ordered as a package, use the bill of materials listed in the table below.



Section Layout

Bill of Materials

Item Description	NSN	Quantity
Wire/Fabric Container (2 ft. x 2 ft. x 4 ft.)	5680-99-001-9397 (Green) 5680-99-968-1764 (Sand)	33
Composite Material Panels (14 ft. length)	5675-01-500-2808	6
Composite Material Panels (12 ft. length)	5675-01-500-2803	3
Toggle connectors (14 ft. length)	Incl. in 5675-01-500-2808	5
Waterproof membrane (14 ft. x 12 ft.)	5650-01-504-5373	1
Fill material (cubic yards)	N/A	30

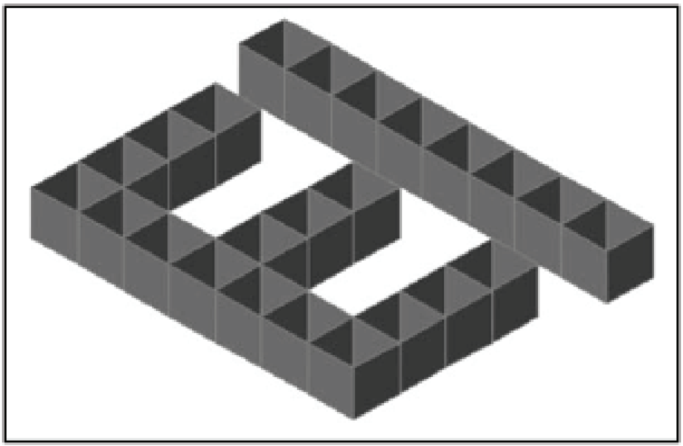
Equipment, Personnel, and Time Estimate

Task	Equipment Required	Personnel Required*	Time Required
Site preparation and foundation leveling	bulldozer, DEUCE, ACE, front-end loader, skid-steer loader, SEE, HMEE	2	30 min/person x 2 = *1 man-hour*
Foundation compaction	vibratory roller (smooth drum or pad feet), HSC	2	30 min/person x 2 = *1man- hour*
Haul fill material to site	dump trucks	varies	varies
Erect structure and place fill	front-end loader, skid-steer loader, SEE, HMEE	4	6 hr/person x 4 = *24 man-hours*
Total Manpower			*26man- hours*

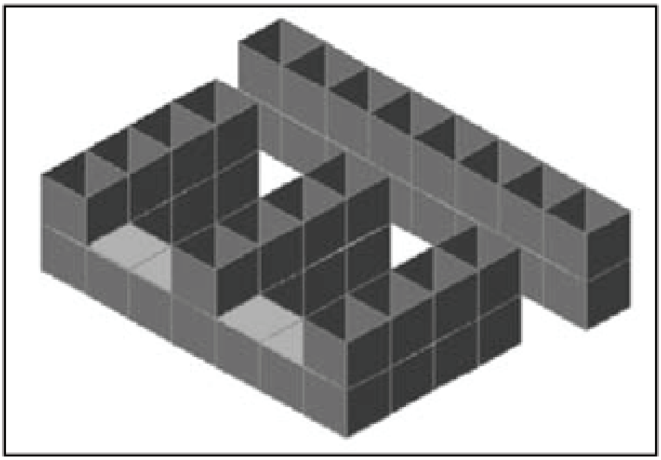
*Excludes equipment operators

Construction Steps for Aboveground Two-Bay Fighting Position

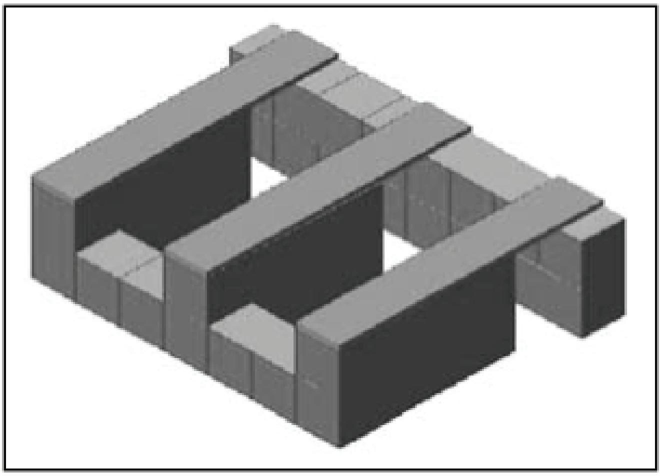
1. Arrange and fill first layer



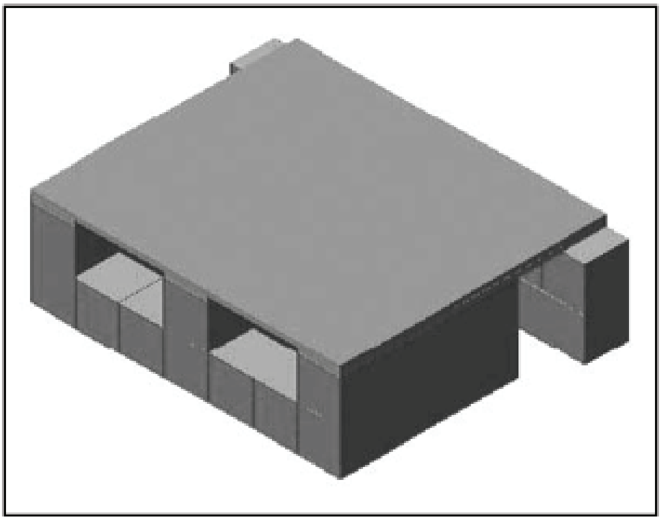
2. Arrange and fill second layer



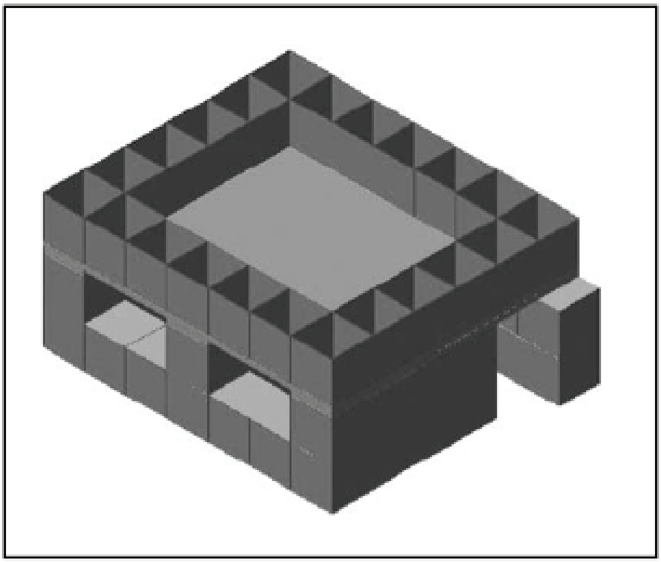
3. Add roof support



4. Add roof panels



5. Add and fill overhead cover



Annex H-6

Aboveground 20 foot ISO/MILVAN Personnel Bunker

These bunkers are designed to protect a standard 20 foot ISO/MILVAN container. The bunker roof requires sheet piling. If a piling of different width is used, the required number of pieces in the bill of materials may change.

Bill of Materials

Item Description	NSN	Quantity
Wire and Fabric Container (4.5 ft. x 3.5 ft. x 32 ft.)	5680-99-001-9396 (Green) 5680-99-835-7866 (Sand)	6
Wire and Fabric Container (2 ft. x 2 ft. x 4 ft.)	5680-99-001-9397 (Green) 5680-99-968-1764 (Sand)	22
Sheet piling-18 ft. length (Skyline Steel CS 55 steel sheet piling or equivalent)	N/A	19
Sandbags Poly (Cloth or Acrylic material also available)	8105-00-142-9345 (Green) 8105-01-336-6163 (Sand)	100
Waterproof membrane (44 ft. x 18 ft.)	5650-01-504-5373	1
Fill material (cubic yards)	N/A	180

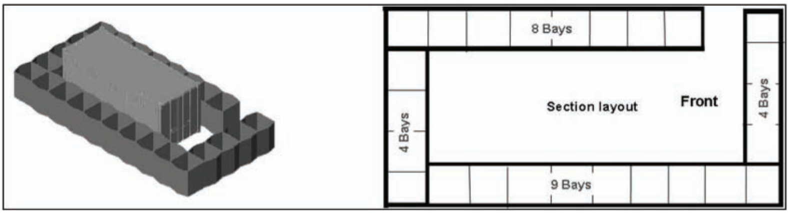
Equipment, Personnel, and Time Estimate

Task	Equipment Required	Personnel Required*	Time Required
Site preparation and foundation leveling	bulldozer, DEUCE, ACE, front-end loader, HMEE	2	1 hr/person x 2 = *2 man-hours*
Foundation compaction	vibratory roller (smooth drum or pad feet), HSC	2	30 min/person x 2 = *1 man-hour*
Haul fill material to site	dump trucks	varies	varies
Place ISO container	crane, forklift	2	30 min/person x 2 = *1 man-hour*
Construct roof	front-end loader, HMEE	6	5 hr/person x 6 = *30 man-hours*
Construct roof & place fill	forklift, crane (w/clamshell bucket for fill), HYEX	6	6 hr/person x 6 = *36 man-hours*
Total Manpower			*70 man-hours*

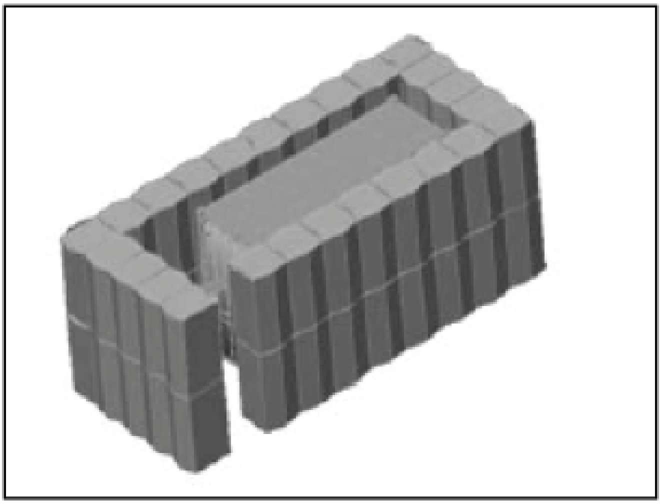
* Excludes equipment operators

Construction Steps for aboveground ISO/MILVAN Personnel Bunker

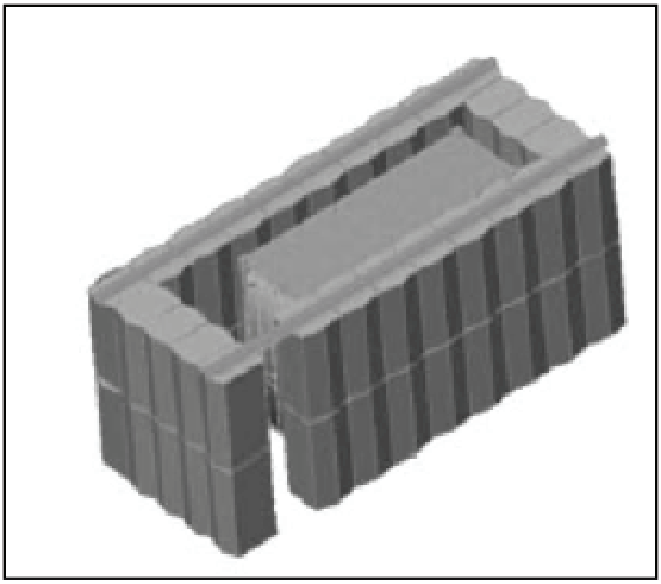
1. Arrange and fill first layer (section layout shown at right)



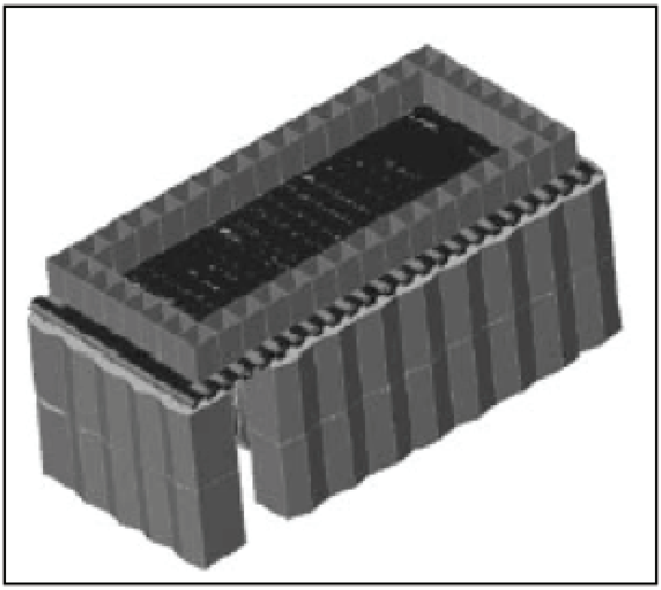
2. Arrange and fill second layer



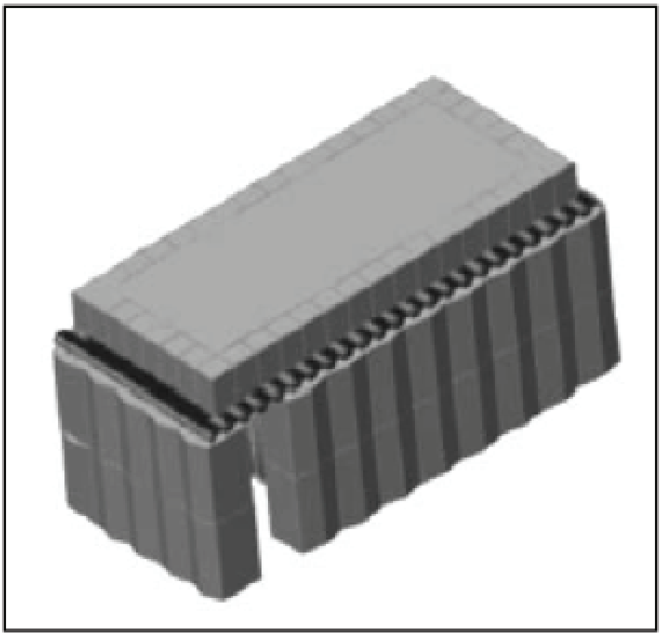
3. Add sheet piling roof support



4. Add roof layer

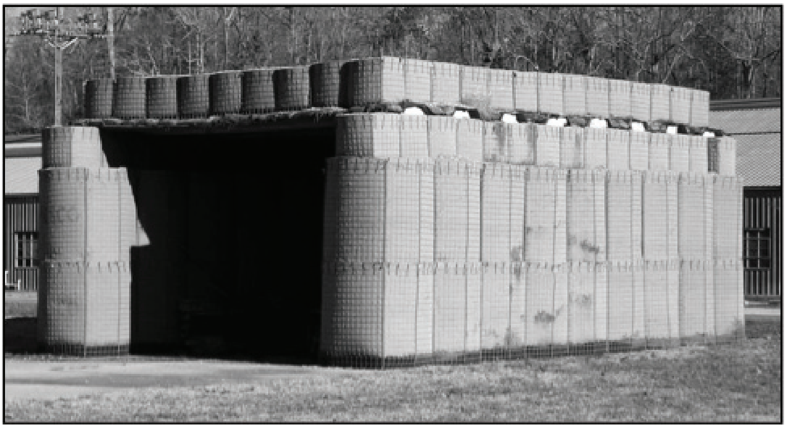


5. Fill overhead cover



Annex H-7

HEMTT-LHS/PLS Bunkers



These bunkers were designed to protect Heavy Expanded Mobility Tactical Truck – Load Handling System (HEMTT-LHS) and Palletized Loading System (PLS) vehicles. These bunkers will also protect any equipment and materials that will fit inside (for example, the US Marine Corps Logistics Vehicle System).

HEMTT-LHS Bunker dimensions: 49 ft. L x 28 ft. W x 16 ft. H (14.9m x 8.5m x 4.9m)

PLS Bunker dimensions: 32 ft. L x 21 ft. W x 14 ft. H (9.8m x 6.4m x 4.3m)

Bill of Materials

Item Description	NSN	Quantity	
		HEMTT	PLS
Wire and Fabric Container (4.5 ft. x 3.5 ft. x 32 ft.)	5680-99-001-9396 (Green) 5680-99-835-7866 (Sand)	18	5
Wire and Fabric Container (2 ft. x 2 ft. x 4 ft.)	5680-99-001-9397 (Green) 5680-99-968-1764 (Sand)	31	40
Sheet piling-18 ft. length Skyline Steel CS 55 steel sheet piling or equivalent	N/A	19	13
Sandbags Poly (Cloth or Acrylic material also available)	8105-00-142-9345 (Green) 8105-01-336-6163 (Sand)	136	96
Waterproof membrane (44 ft. x 18 ft.)	5650-01-504-5373	1	1
Fill material (cubic yards)	N/A	470	170

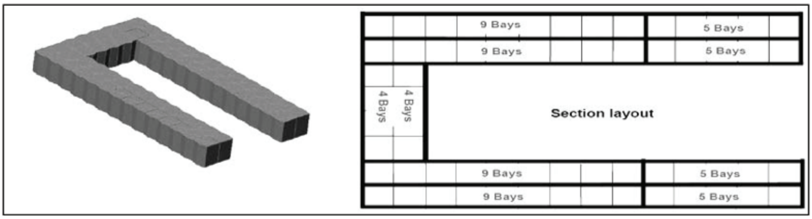
Equipment, Personnel, and Time Estimate

Task	Equipment Required	Personnel Required*	Time Required
Site preparation and foundation leveling	bulldozer, DEUCE, ACE, front-end loader, HMEE	2	1 hr
Foundation compaction	vibratory roller (smooth drum or pad feet), HSC	2	30 min/person x 2 = *1 man-hour*
Haul fill material to site	dump trucks	varies	varies
Erect walls and place fill	front-end loader, HMEE (lower level), crane w/clamshell or HYEX (upper levels)	8	10 hr/person x 8 = *80 man-hours*
Construct roof	crane, HYEX, front-end loader or HMEE (assist w/piling)	8	3 hr/person x 8 = *24 man-hours*
Construct overhead cover	crane (w/clamshell bucket for fill), HYEX	8	3 hr/person x 8 = *24 man-hours*
Total Manpower			*131 man-hours*

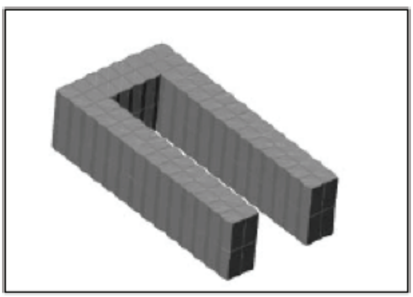
*Excludes equipment operators

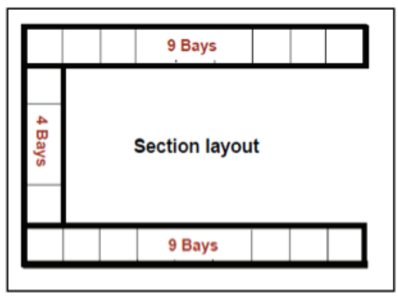
Construction Steps for HEMTT-LHS/PLS Bunker. Construction details are essentially the same for both bunkers. The section layout for each bunker differs as shown.

1. Arrange and fill first layer.



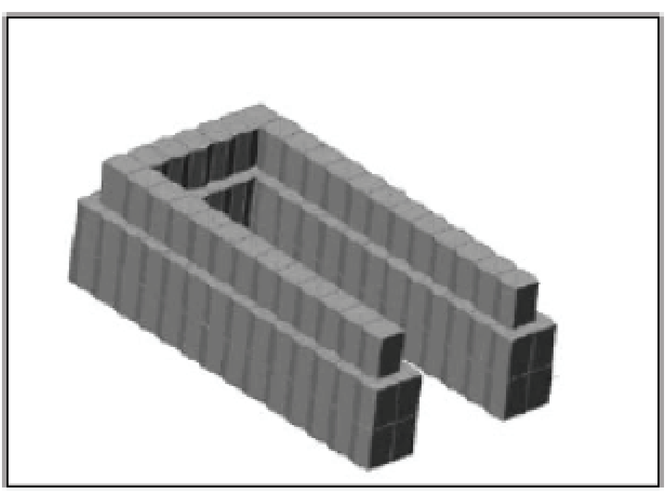
2. Arrange and fill second layer



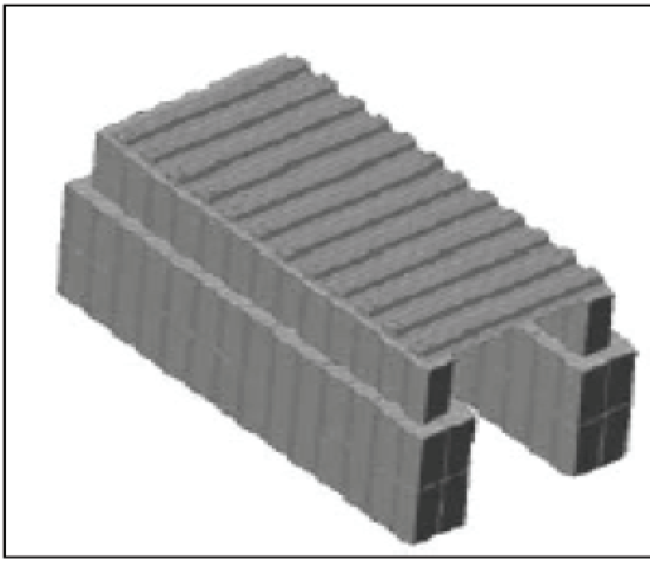


PLS Bunker Section Layout

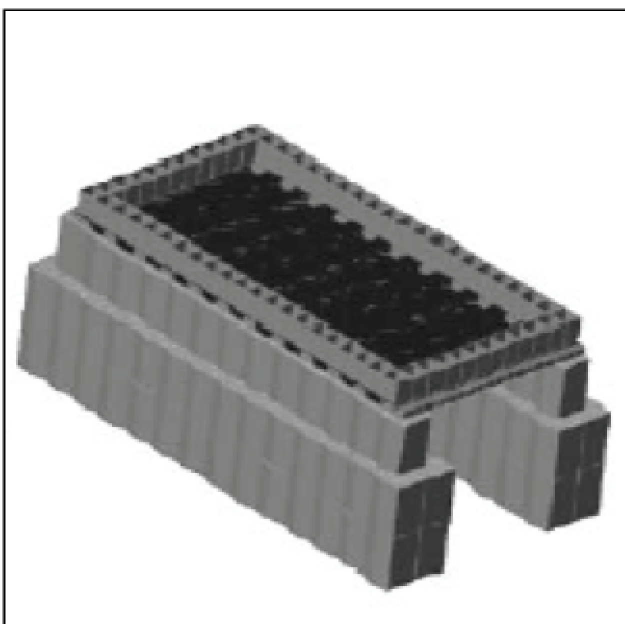
3. Arrange and fill third layer



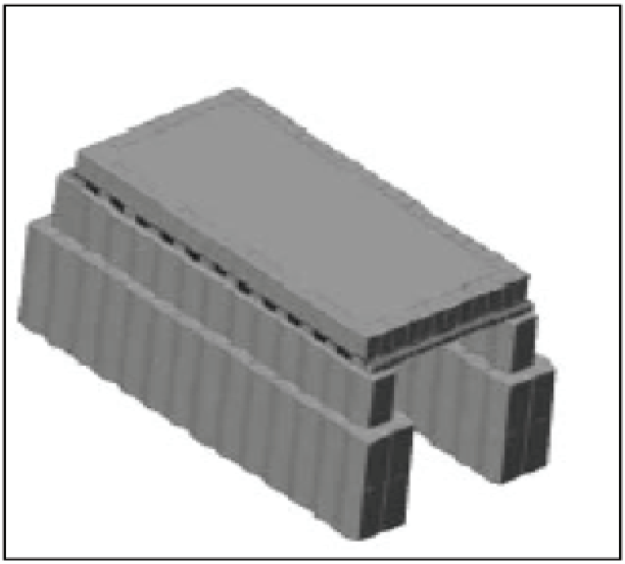
4. Add sheet piling roof support



5. Add roof layer

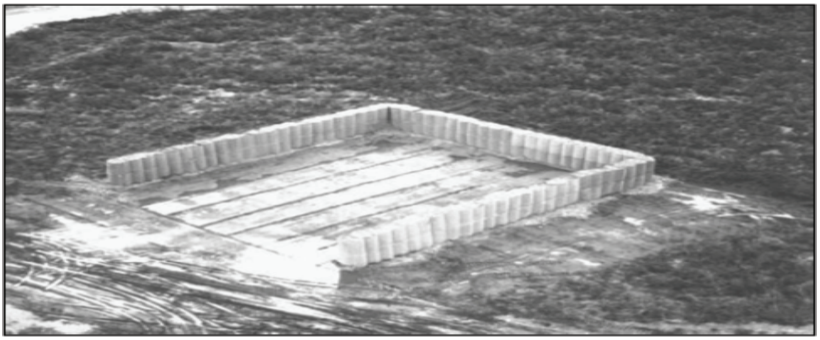


6. Fill overhead cover



Annex H-8

Helicopter Revetments



These soil-filled wire and fabric structures protect helicopters from near-miss RAM. Such positions can also protect stored equipment that does not require overhead cover.

The indicated construction time includes basic foundation preparation and position construction. Other factors such as threats, equipment and material availability, poor foundation soils, and construction expertise can impact time requirements. The indicated time is an estimate and should only be utilized when actual performance data for similar positions is unavailable.

These revetments can also be constructed from metal containers of similar size. However, materials quantities may differ from the listed bills of materials. This results from dimensionality differences for equivalent metal containers.

Bill of Materials for Various Soil-Filled Wire and Fabric Helicopter Revetments

Item Description	NSN	AH-64 Apache/UH-60 Blackhawk	OH-58 Kiowa Warrior	AH-1 Cobra	UH-1 Iroquois (Huey)	CH-47 Chinook	CH-53 Super Stallion
Wire and Fabric Container (4.5 ft. x 3.5 ft. x 32 ft.)	5680-99-001-9396 (Green) 5680-99-835-7866 (Sand)	16	11	14	14	11	11
Wire and Fabric Container (7.5 ft. x 7 ft. x 91 ft.)	5680-99-126-3716 (Green) 5680-99-169-0183 (Sand)	□	□	□	□	4	4
Fill material (cubic yards)	N/A	340	230	300	290	1000	1000

Equipment, Personnel and Time Estimates

Aircraft	Task	Equipment Required	Personnel Required (excluding operators)	Time Required.
AH-64 Apache/ UH-60 Blackhawk	1	A	2	45 min
	2	B	varies	varies
	3	C	8	8 hr
OH-58 Kiowa Warrior	1	A	2	30 min
	2	B	varies	varies
	3	C	6	8 hr
AH-1 Cobra	1	A	2	45 min
	2	B	varies	varies
	3	C	8	7 hr
UH-1 Iroquois (Huey)	1	A	2	45 min
	2	B	varies	varies
	3	C	8	7 hr
CH-47 Chinook	1	A	2	1 hr 30 min
	2	B	varies	varies
	3	D	10	16 hr
CH-53 Super Stallion	1	A	2	1 hr 30 min
	2	B	varies	varies
	3	D	10	16 hr

KEY:

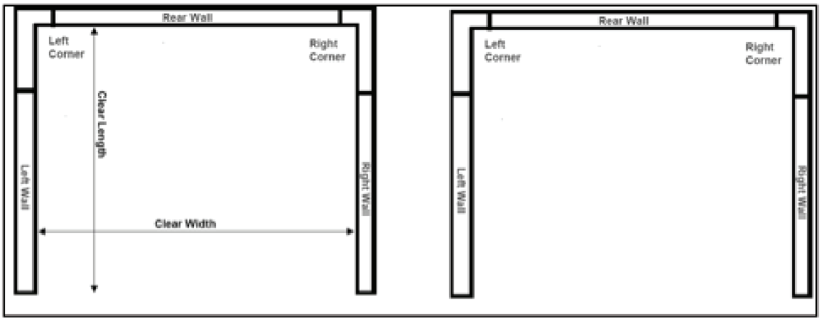
Task:
1. Prepare site and level foundation
2. Haul fill material to site
3. Erect walls and place fill

Equipment Required:
A. Bulldozer, DEUCE, ACE
B. Dump Trucks
C. Front-end loader, HMEE
D. Front-end loader w/clamshell bucket, HYEX

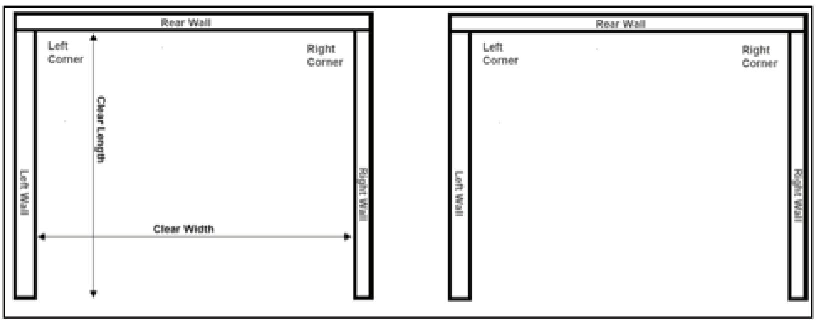
Layout Dimensions for Various Helicopters

Helicopter	Wire and Fabric Container Size	Quantity	Clear Length (ft)	Clear Width (ft)
Blackhawk/Apache	4.5 x 3.5 x 32 ft.	16	82	78
Kiowa	4.5 x 3.5 x 32 ft.	11	53	57
Cobra	4.5 x 3.5 x 32 ft.	14	78	64
Iroquois (Huey)	4.5 x 3.5 x 32 ft.	14	67	71
Chinook	7.25 x 7 x 91 ft.	4	126	91
2nd layer	4.5 x 3.5 x 32 ft.	11	□	□
Super Stallion	7.25 x 7 x 91 ft.	4	112	112
2nd layer	4.5 x 3.5 x 32 ft.	11	□	□

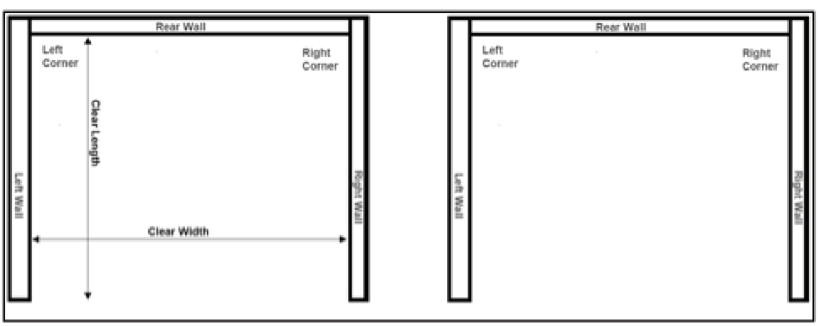
Section Layouts. Specific layouts for different aircraft types are provided below. Regardless of the revetment design, proper place and fill of container units is important.



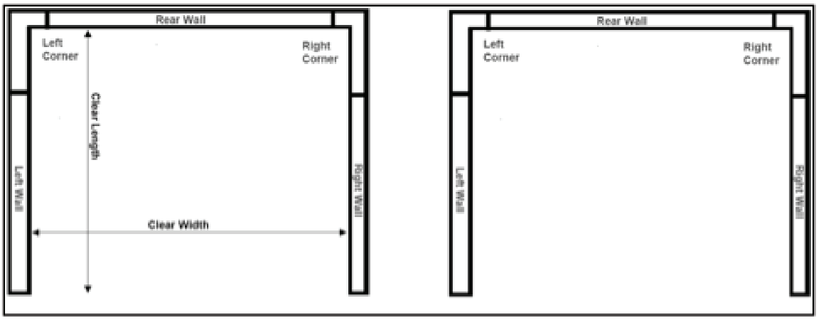
AH-64 Apache/ UH-60 Blackhawk (left: first layer; right: second layer)



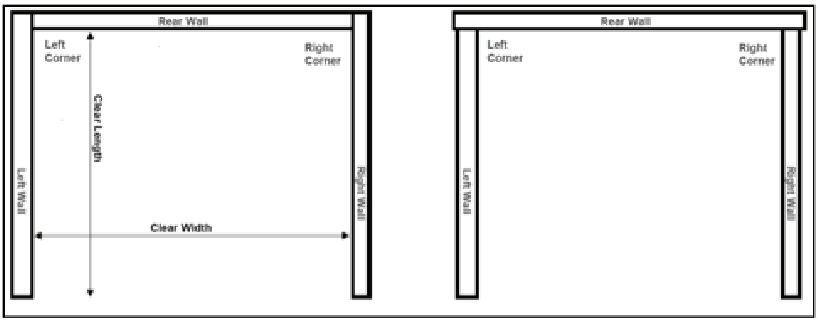
OH-58 Kiowa (left: first layer; right: second layer)



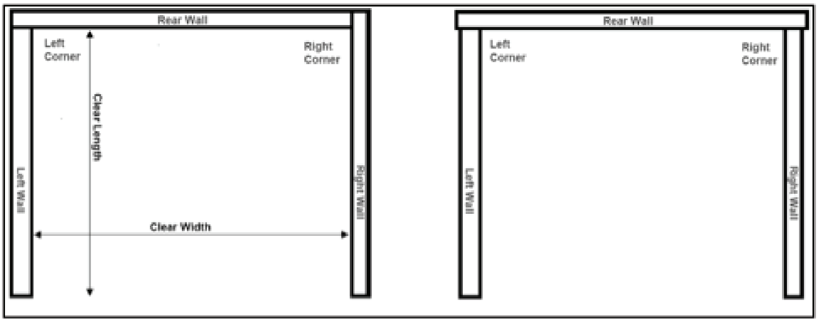
AH-1Cobra (left: first layer; right: second layer)



UH-1 Iroquois “Huey” (left: first layer; right: second layer)



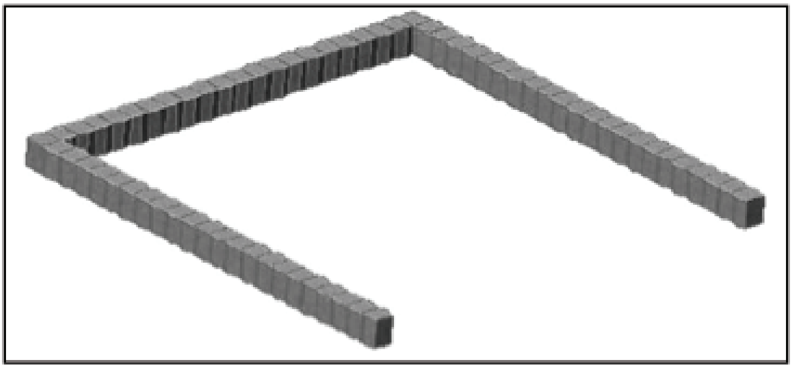
CH-47 Chinook (left: first layer; right: second layer)



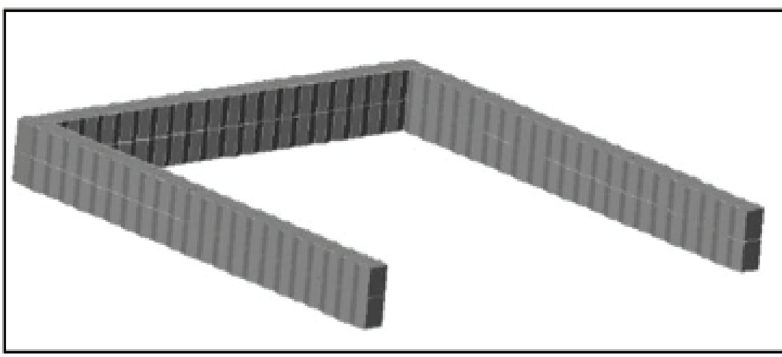
CH-53 Super Stallion (left: first layer; right: second layer)

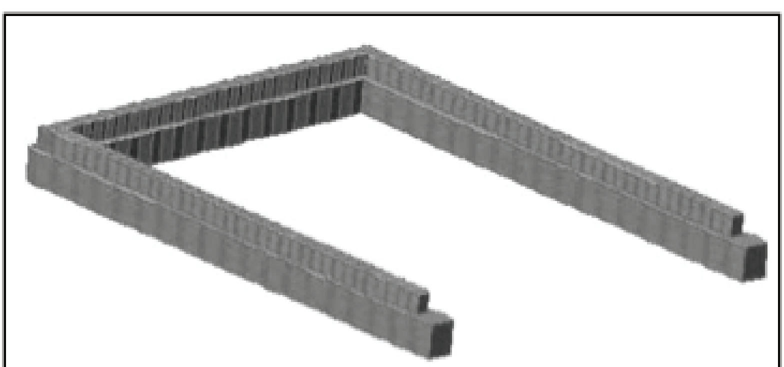
Construction Steps for Helicopter Revetments

1. Arrange and fill first layer



2. Arrange and fill second layer (first: Apache, Blackhawk, Kiowa, Cobra, Huey; second: Chinook and Super Stallion)





References:

FM 5-34. *Engineer Field Data*, 19 July 2005.

ERDC *Concertainer Construction Techniques*. May 2003.

ERDC M*etal Revetment Assembly Construction Guide*, November 2005.

ERDC Fact Sheet: *Field Expedient Protective Positions*, June 2003.

ERDC/USAES *Construction Guide for Small Observation Post*, May 2003.

ERDC/USAES *Construction Guide for Aboveground Large Observation Post*, May 2003.

ERDC/USAES *Construction Guide for Single-Bay Aboveground Fighting Position*, May 2003.

ERDC/USAES *Construction Guide for Two-Bay Aboveground Fighting Position*, May 2003.

ERDC/USAES *Construction Guide for Aboveground 20' Milvan Bunker, May* 2003.

ERDC/USAES *Construction Guide for HEMTT-LHS/PLS Bunker, May 2003*.

ERDC/USAES *Construction Guide for PLS Cargo Bunker.*

ERDC/USAES *Construction Guide for Helicopter Revetment.*

This page intenionally blank

Department of Defense

Defense Federal Acquisition Regulation Supplement: The 1998 Edition (including DACs 91-1 through 91-13 and Departmental Letters 98-001 through 98-021), 17 August 1998 (Revised 29 July 2009). (available at http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html) .

DoDI 2000.16. *DoD Antiterrorism (AT) Standards,* 2 October 2006 (including Change 2, 8 December 2006).

DoDI 3020.45. *Defense Critical Infrastructure Program (DCIP) Management,* 21 April 2008.

DoDI 5400.13. *Public Affairs (PA) Operations*, 15 October 2008.

DoD O-2000.12-H. *DoD Antiterrorism Handbook*, February 2004.

National Defense Strategy. Washington DC: Department of Defense, June 2008.

The National Military Strategy of the United States of America: 2011. Washington DC: Joint Chiefs of Staff, 8 February 2011.

Chairman of the Joint Chiefs of Staff

CJCSI 3470.01. *Rapid Validation and Resourcing of Joint Urgent Opera¬tional Needs (JUONS) in the Year of Execution,* 15 July 2005 (Current as of 9 July 2007).

CJCSI 5261.01F. *Combating Terrorism-Readiness Initiative Fund (CbT-RIF)*, 21 October 2008.

CJCSI 7401.01E. *Combatant Commander Initiative Fund (CCIF),* 01 July 2009.

CJCSM 3122.01A. *Joint Operation Planning and Execution System (JOPES) Volume I (Planning Policies and Procedures),* 29 September 2006 (Current as of 11 October 2008).

CJCSM 3122.02D. *Joint Operation Planning and Execution System (JOPES) Volume III (Crisis Action Time-Phased Force and Deployment*

Data Development and Deployment Execution),01 April 2011.

CJCSM 3122.03C. *Joint Operation Planning and Execution System Volume II, Planning Formats and Guidance*, 17 August 2007.

Joint Publications

Contingency Contracting: A Joint Handbook (YFV 08-01 Jan 08), January 2008.

Joint Antiterrorism Program Manager's Guide (JAT Guide) Version 3.0, August 2008.

JP 1-02. *DOD Dictionary of Military and Associated Terms,* 12 April 2001 (As amended through 19 August 2009).

JP 1-04. *Legal Support to Military Operations,* 01 March 2007

JP 2-0. *Joint Intelligence*, 22 June 2007.

JP 2-01.3. *Joint Intelligence Preparation of the Operational Environment,* 16 June 2009.

JP 3-0. *Joint Operations*, 17 September 2006 (Incorporating Change 1, 13 February 2008).

JP 3-01. *Countering Air and Missile Threats*, 5 February 2007.

JP 3-07.2. *Antiterrorism*, 14 April 2006.

JP 3-09. *Joint Fire Support*, 30 June 2010.

JP 3-10. *Joint Security Operations in Theater*, 03 February 2010.

JP 3-11. *Operations in Chemical, Biological, Radiological, and Nuclear (CBRN) Environments*, 26 August 2008

JP 3-13.3. *Operations Security,* 29 June 2006.

JP 3-15. *Barriers, Obstacles, and Mine Warfare for Joint Operations*, 17 June 2011.

JP 3-16. *Multinational Operations*, 7 March 2007.

JP 3-28. *Civil Support,* 14 September 2007

JP 3-31. *Command and Control for Joint Land Operations*, 29 June 2010.

JP 3-34. *Joint Engineer Operations,* 30 June 2011.

JP 3-34.170. *Engineer Reconnaissance*, March 2008

JP 3-40. *Combating Weapons of Mass Destruction,* 10 June 2009.

JP 3-50. *Personnel Recovery*, 5 January 2007.

JP 3-52. *Joint Doctrine for Airspace Control in the Combat Zone*, 20 May 2010.

JP 3-57. *Civil-Military Operations*, 8 July 2008.

JP 4-0. *Joint Logistics,* 18 July 2008.

JP 4-02. *Health Service Support,* 31 October 2006.

JP 4-03. *Joint Bulk Petroleum and Water Doctrine,* 09 December 2010.

JP 5-0. *Joint Operation Planning*, 11 August 2011.

JP 6-0. *Joint Communication Systems*, 10 June 2010.

*Joint Sniper Defeat Handboo*k (GTA 90-01-013), August 2008.

Multiservice Publications

FM 3-24 / MCWP 3-33.5. *Counterinsurgency*, 15 December 2006.

FM 3-34.170/MWCP 3-17.4. *Engineer Reconnaissance*, 25 March 2008.

Air Force Publications

AFDD 2-4.1. *Force Protection,* 9 November 2004.

AFDD 2-4.4. Bases, Infrastructure, and Facilities, 13 November 1999.

AFH 10-222 V3. *Civil Engineer Guide to Expeditionary Force Protection*, 1 May 2008.

AFH 10-222 V14. *Civil Engineer Guide to Fighting Positions, Shelters, Obstacles, and Revetments*, 1 August 2008.

AFH 10-222v1. *Guide to Bare Base Development,* 01 February 2006.

AFH 10-2401. *Vehicle Bomb Mitigation Guide*, 1 September 2006.

AFI 90-901. *Operational Risk Management*, 1 April 2000.

AFMAN 10-401 V2. *Planning Formats and Guidance*, 1 May 1998.

AFPAM 90-902. *Operational Risk Management (ORM) Guidelines and Tools*, 14 December 2000.

U.S. Air Force Entry Control Facilities Design Guide, 18 February 2003.
Draft AFRL Report on Fuze Initiation, 2010.

Army Publications

AR 525-13. *Antiterrorism,* 11 September 2008.

AR 525-26. *Infrastructure Risk Management (Army)*, 22 June 2004.

DA Pam 190-51. *Risk Analysis for Army Property,* 30 September 1993.

DA Pam 420-11. *Project Definition & Work Classification,* 18 March 2010.

EP 500-1-2. *Emergency Employment of Army and Other Resources- Field Force Engineering- United States Army Corps of Engineers Support to Full Spectrum Operations*, 01 August 2010.

FM 3-0. *Operations*, June 2001.

FM 3-06.11. *Combined Arms Operations in Urban Terrain*, 28 February 2002.

FM 3-07. *Stability Operations*, 6 October 2008.

FM 3-19.30. *Physical Security,* 08 January 2001.

FM 3-34. *Engineer Operations*, 2 April 2009.

FM 3-37. *Protection*, September 2009

FM 3-90. *Tactics*, 4 July 2001.

FM 4-02. *Force Health Protection in a Global Environment*, 13 February 2003.

FM 4-02.2. *Medical Evacuation*, 8 May 2007 (w/Change 1, 30 July 2009).

FM 5-0. *The Operations Process,* 26 March 2010.

FM 5-19. *Composite Risk Management*, 21 August 2006.

FM 5-34. *Engineer Field Data*, 19 July 2005.

FM 3-34.400. *General Engineering*, 09 December 2008.

FM 5-415. *Fire-Fighting Operations,* 9 February 1999.

FM 6-0. *Mission Command: Command and Control of Army Forces,* 11 August 2003.

FM 6-99.2. *U.S. Army Report and Message Formats,* 30 April 2007.

FM 100-10-2. *Contracting Support on the Battlefield,* 4 August 1999.

FM 4-92, *Contracting Support Brigade,* 12 February 2010.

FM 5-103. *Survivability,* 10 June 1985.

FMI 4-93.2. *The Sustainment Brigade,* 04 February 2009.

TC 7-100. *Hybrid Threat*, November 2010.

Navy/Marine Corps Publications

MCO 3500.27B. *Operational Risk Management (ORM)*, 5 May 2004.

MCO P5530.14. *Marine Corps Physical Security Program Manual*, 21 December 2000.

MCWP 5-1. *Marine Corps Planning Process*, 5 January 2000 (w/Change 1, 24 September 2001).

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

MIL-HDBK-1013/10. *Military Handbook: Design Guidelines for Security Fencing, Gates, Barriers, and Guard Facilities,* 14 May 1993.

NWP 5-01. *Naval Operational Planning*, 1 January 2007.

OPNAV Instruction 3500.39B. *Operational Risk Management (ORM)*, 30 July 2004.

UG-2031-SHR. *User's Guide on Protection Against Terrorist Vehicle Bombs*, May 1998.

Unified Facilities Criteria

UFC 3-340-02. *Structures to Resist the Effects of Accidental Explosions,* 05 December 2008

UFC 3-530-01. *Design: Interior and Exterior Lighting and Controls*, 22 August 2006.

UFC 4-010-01. *DoD Minimum Antiterrorism Standards for Buildings*, 8 October 2003 (Including Change 1, 22 January 2007).

UFC 4-010-02. *DoD Minimum Antiterrorism Standoff Distances for Buildings,* 8 October 2003 (Including Change 1, 19 January 2007).

UFC 4-020-04FA / TM 5-853-4. *Security Engineering: Electronic Security Systems,* 1 March 2005.

UFC 4-020-01. *DoD security Engineering Facilities Planning Manual*, 11 September 2008

UFC 4-021-01. *Design and O&M: Mass Notification Systems,* 9 April 2008.

UFC 4-023-07. *Design to Resist Direct Fire Weapons Effects*, 07 July 2008

UFC 4-022-01. *Security Engineering: Entry Control Facilities / Access Control Points,* 25 May 2005.

UFC 4-022-02. *Selection and Application of Vehicle Barriers*, 8 June 2009, (w/change 1, 9August 2010).

USACE/ERDC Publications

ERDC/GSL TR-06-7 *Evaluation of the Current Vulnerability of Expeditionary Shelters to Airblast,* 2006.

ERDC/GSL *Fact Sheet: Field Expedient Fighting Positions.*

ERDC/GSL *Executive Summary: Investigation & Field Verification of Metal Revetments Systems Subjected to 80mm Mortar, 120mm Mortar, & 122mm Rocket*, November 2004.

ERDC/GSL *Quick Look Report: Protection from the Rocket Propelled Grenade.*

ERDC/GSL *Quick Look Report: ERDC Compartmentalization Techniques,* December 2004.

ERDC/GSL TR-10-10 *Development of the Modular Protective System: Validation of Protection from Direct Fire, Indirect Fire, and Bare Charge Threats,* 2010.

ERDC/GSL TR-10-33, *Physical Screening Protection Rapid Technology Transition Project : Direct and Indirect Fire Performance Evaluation*, September 2010.

ERDC/GSL TR-10-28, *Investigation into the Material Requirements for Mitigation of Indirect Fire Fragmentation from 82-mm and 120-mm Mortars,* 2010.

ERDC TR SL-90-5, *Penetration Tests of Masonry Walls with Small-Arms Ammunition*, April, 1990.

ERDC/EL TR-08-29, *Technical Guidelines for Environmental Dredging of Contaminated Sediments,* September 2008.

ERDC/GSL TR-02-18, *Fabric Retrofits of Concrete Masonry Exterior Walls – Blast Response Evaluation :* (*U.S.Israeli 1998 series, "Divine camel," Test 3)*, 2002.

ERDC/GSL *Executive Summary of Phase IV – Pre-Detonation and Fragment Shielding Experiments.*

ERDC/GSL *Installation Guidance for Plastic Bin, Soil Revetment Walls.*

ERDC/GSL *Experimental Validation of Compartmentalization Measures.*

ERDC *C-RAM Overhead Protection Quick Look Report.*

ERDC/GSL *Field Expedient Protective Positions.*

ERDC/USACE *Construction Guide for Reinforced Below-ground 40' Milvan Bunker*, May 2003.

ERDC *Concertainer Construction Techniques.* May 2003.

ERDC *Metal Revetment Assembly Construction Guide*, November 2005.

ERDC *Fact Sheet: Field Expedient Protective Positions*, June 2003.

ERDC/USAES *Construction Guide for Small Observation Post*, May 2003.

ERDC/USAES *Construction Guide for Aboveground Large Observation Post*, May 2003.

ERDC/USAES *Construction Guide for Single-Bay Aboveground Fighting Position*, May 2003.

ERDC/USAES *Construction Guide for Two-Bay Aboveground Fighting* Position, May 2003.

ERDC/USAES *Construction Guide for Aboveground 20' Milvan Bunker,* May 2003.

ERDC/USAES *Construction Guide for HEMTT-LHS/PLS Bunker*, May 2003.

ERDC/USAES *Construction Guide for PLS Cargo Bunker.*

ERDC/USAES *Construction Guide for Helicopter Revetment.*

Other

Contingency Contracting: A Joint Handbook for the 21st Century. Washington DC: Defense Procurement and Acquisition Policy Office (available at http://www.acq.osd.mil/dpap/pacc/cc/jcchb/index.html).

Larsen, Scott. "The Joint Combat Outpost Quick Reaction Test and the Revised Joint Forward Operations Base Handbook." *The Guardian*, Vol. 11, Issue 1, Summer 2009, pp. 19-24.

Lauritsen, Brad, and Aldo E. McKay. "Design and Evaluation of Novel Counter-Mobility Barrier Systems." San Antonio, TX: Advanced Technology Office, Applied Research Associates, Inc. (available at http://www.buildingsecurity.us/docs_pubs.php).

Magness, Thomas H., and James Ahern. "CTC Notes – 'SWEAT.'" *Engineer* Vol. 35, July-September 2005, pp. 18-19.

Peay, Binford J. H. III. "Correlating Medical Forces Forward." *Joint Force Quarterly* Vol. 14, Winter 1996-97, pp. 70-74.

Schumitz, Robert. "Operational Contracting in Support of Operation Iraqi Freedom," Briefing slides, 2005 Annual Army Contingency Contracting Conference, 20 April 2005.

Taylor, George P. Jr. "Air Force Capability-Based Medical Planning." *U.S. Medicine Issue* 58, January 2004.

Taylor, Scott R., Amy M. Rowe, and Brian M. Lewis. "Consequence Management in Need of a Timeout." *Joint Force Quarterly* Vol. 22, Summer 1999, pp. 78-85.

AASHTO, *American Association of State Highway and Transportation Officials.*

Small-Base Leader Entry Control Point Guide (ECP Guide).

Joint Entry Control Point & Escalation of Force Procedures (Jeep Handbook).

AASHTO WB-15M. *Policy on Geometric Design of Highways and Streets,* April 2003.

Defense Department. *Vehicle Inspection Guide,* 2007.

TSWG Desert Cobra Final Test Report, 2010.

Joint Forward Operations Base (JFOB)
Protection Handbook
GTA 90-01-011

SIXTH EDITION OCTOBER 2011