

UNIFIED FACILITIES CRITERIA (UFC)

SECURITY ENGINEERING: WATERFRONT SECURITY



UNIFIED FACILITIES CRITERIA (UFC)

SECURITY ENGINEERING: WATERFRONT SECURITY

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

U.S. ARMY CORPS OF ENGINEERS

NAVAL FACILITIES ENGINEERING COMMAND (Preparing Activity)

AIR FORCE CIVIL ENGINEER CENTER

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

Change No.	Date	Location



FOREWORD

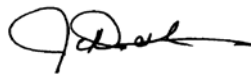
The Unified Facilities Criteria (UFC) system is prescribed by MIL-STD 3007 and provides planning, design, construction, sustainment, restoration, and modernization criteria, and applies to the Military Departments, the Defense Agencies, and the DoD Field Activities in accordance with [USD \(AT&L\) Memorandum](#)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

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

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

- Whole Building Design Guide web site <http://dod.wbdg.org/>.

Hard copies of UFC printed from electronic media should be checked against the current electronic version prior to use to ensure that they are current.



JAMES C. DALTON, P.E.
Chief, Engineering and Construction
U.S. Army Corps of Engineers



JOSEPH E. GOTT, P.E.
Chief Engineer
Naval Facilities Engineering Command



SCOTT HARTFORD, Col, USAF, P.E.
Acting Director
Facilities Engineering Center of Excellence
Air Force Civil Engineer Center



MICHAEL McANDREW
Director, Facilities Investment and Management
Office of the Deputy Under Secretary of Defense
(Installations and Environment)

**UNIFIED FACILITIES CRITERIA (UFC)
NEW DOCUMENT SUMMARY SHEET**

Document: UFC 4-025-01 *Security Engineering: Waterfront Security*

Superseding: None

Description: Provide a unified approach to the development of waterfront protective measures intended to protect waterside assets.

Reasons for Document:

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

Impact:

- This document does not set the requirement for protection measures for the waterfront. No additional cost impacts are anticipated by the publication of this document. This document should reduce the design and coordination efforts for waterfront design.

Unification Issues

There are no unification issues.

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION	1
1-1 BACKGROUND.	1
1-2 PURPOSE.	1
1-3 APPLICABILITY.....	1
1-4 SCOPE.	1
1-5 VULNERABILITY AND RISK ASSESSMENT.	1
1-6 POLICY REQUIREMENTS.....	2
1-6.1 Department of Defense.....	2
1-6.2 Geographic Combatant Commander (GCC) Requirements.....	2
1-6.3 Service Requirements.	3
1-6.4 Installation Specific Requirements.....	3
1-7 CONSIDERATIONS.	3
1-7.1 Security.....	3
1-7.2 Port Operations.....	4
1-7.3 Safety.....	4
1-7.4 Appearance.	4
1-7.5 Environmental Impact.	4
1-8 CORROSION PREVENTION AND CONTROL.....	4
1-9 REFERENCES.	4
1-10 GLOSSARY.....	4
1-11 GENERAL BUILDING REQUIREMENTS.	4
1-12 SECURITY ENGINEERING UFC SERIES.	5
1-12.1 DoD Minimum Antiterrorism Standards for Buildings.....	5
1-12.2 DoD Security Engineering Facilities Planning Manual.	5
1-12.3 DoD Security Engineering Facilities Design Manual.....	5
1-12.4 Security Engineering Support Manuals.....	6
1-12.5 Security Engineering UFC Application.....	6
CHAPTER 2 OVERVIEW.....	9
2-1 OVERVIEW.	9
2-2 WATERFRONT SECURITY SYSTEM.....	9
2-2.1 Waterfront Assets.	9
2-2.2 Waterfront.....	9

2-2.3	Physical Security System.....	10
2-3	PLANNING.....	12
2-3.1	Establish Requirements.....	12
2-3.2	Design Basis Threat (DBT).....	12
2-3.3	Level of Protection (LOP).....	12
2-3.4	Future Development Plans.....	13
2-3.5	Document Requirements.....	13
CHAPTER 3	DESIGN STRATEGY.....	15
3-1	INTRODUCTION.....	15
3-2	DESIGN STRATEGY.....	15
3-2.1	Detect, Delay, and Respond.....	16
3-3	SYSTEM EFFECTIVENESS.....	17
3-4	ESTABLISH PERIMETER.....	17
3-4.1	Landside Perimeter.....	18
3-4.2	Waterside Perimeter.....	18
3-5	SECURITY LIGHTING.....	18
3-6	SIGNAGE.....	18
3-6.1	Access Control Point (ACP) Signage.....	18
3-6.2	Restricted area signage.....	19
3-6.3	Boat Barrier Signage.....	19
CHAPTER 4	LANDSIDE.....	21
4-1	INTRODUCTION.....	21
4-2	GENERAL DESIGN STRATEGY.....	21
4-3	LANDSIDE ACCESS CONTROL.....	22
4-4	LANDSIDE STANDOFF.....	24
4-5	ACCESS CONTROL LAYER I: INSTALLATION PERIMETER.....	24
4-6	ACCESS CONTROL LAYER II: WATERFRONT ENCLAVE.....	24
4-6.1	Layer II: Vehicle ACPs.....	24
4-6.2	Layer II: Pedestrian ACPs.....	24
4-6.3	Layer II: Fence.....	25
4-6.4	Layer II: Vehicle Barriers.....	25
4-7	ACP LAYER III: FOOT OF PIER.....	25
4-7.1	Layer III: Vehicle Barriers.....	25

4-7.2	Layer III: Guard Booth.	26
4-8	ELECTRONIC SECURITY SYSTEMS (ESS).....	26
4-9	SECURITY LIGHTING.....	27
4-9.1	Perimeter Lighting.....	27
4-9.2	Vehicle ACP Lighting.	27
4-9.3	Pedestrian ACP Lighting.....	27
CHAPTER 5	WATERSIDE	29
5-1	INTRODUCTION.	29
5-2	DESIGN STRATEGY.....	29
5-2.1	General Design Strategy.....	29
5-3	WATERSIDE STANDOFF.....	30
5-4	PERIMETER.....	30
5-4.1	Waterside Perimeter.	30
5-4.2	Waterside Restricted Area.	31
5-4.3	Line of demarcation (LOD).....	31
5-4.4	Boat Barrier System.....	31
5-5	GUARD TOWERS.....	32
5-5.1	Communication and Information Technology.....	33
5-5.2	Central Duress Alarm.	33
5-5.3	Guard Tower Lighting.	33
5-6	WATERFRONT SECURITY LIGHTING.	34
5-6.1	Water surface Lighting.....	34
5-6.2	Underwater Lighting.....	34
5-6.3	Under deck Lighting.....	34
5-6.4	Lighting Interference.	34
5-7	ELECTRONIC HARBOR SECURITY SYSTEMS (EHSS).....	35
5-7.1	Surface Detection and Assessment.....	35
5-7.2	Subsurface Detection and Assessment.	38
5-7.3	Command, Control, Communication and Display (C3D).....	38
5-7.4	Infrastructure.....	39
APPENDIX A	REFERENCES.....	43
APPENDIX B	GLOSSARY	45

FIGURES

Figure 1-1 Security Engineering UFC Application	7
Figure 2-1 Waterfront	10
Figure 2-2 Diagram of Physical Security System Functions.....	11
Figure 2-3 Project Process.....	13
Figure 3-1 Zone Concept	16
Figure 3-2 ACP Sign Example	19
Figure 3-3 Restricted Area Sign Example	19
Figure 4-1 Landside Security Zones Adjacent to Piers.....	22
Figure 4-2 Landside Access Control Transitions.....	23
Figure 4-3 Waterfront Access Control	23
Figure 4-4 Pier ACP	25
Figure 5-1 Waterside Security Zones	30
Figure 5-1 Floating Line of Demarcation	32
Figure 5-2 Boat Barrier System (Port Security Barrier)	32
Figure 5-3 Guard Tower on Pier.....	34
Figure 5-4 Radar Antenna.....	36
Figure 5-5 Sound Transducer Being Lowered into the Water	38
Figure 5-6 Roof Mounted Equipment	40
Figure 5-7 EHSS Configuration.....	41

TABLES

Table 2-1 Waterfront Security Elements.....	11
Table 5-2 Visual-Imaging Element Technologies	37

CHAPTER 1 INTRODUCTION

1-1 BACKGROUND.

Terrorist attacks on waterside assets such as the USS Cole emphasize the need for increased antiterrorism (AT) and physical security protective measures for waterfront assets.

1-2 PURPOSE.

Present a unified approach for AT and physical security systems that protect waterfront assets. Commanders, security personnel, planners, designers, architects, and engineers shall use this document when considering AT and physical security systems that protect waterfront assets.

1-3 APPLICABILITY.

This document provides planning and design criteria for DoD components and participating organizations. This document applies to all construction, renovation, and repair projects including expeditionary or temporary construction of waterfront facilities associated with waterfront assets onboard DoD installations. This document does not apply to ports of call.

1-4 SCOPE.

This document provides a methodology to design AT and physical security systems required to protect waterfront assets. It focuses on the protection of military warships and support vessels but the concepts within may be adopted for the protection of all DoD waterfront assets such as airfields, shore facilities, or other structures immediately adjacent to water.

The examples provided are for illustration only and should be modified and adapted to satisfy installation specific constraints. Issues such as tactics, techniques, and operational procedures are not addressed. However, a well-designed physical security system should not hinder operations and capabilities.

1-5 VULNERABILITY AND RISK ASSESSMENT.

In accordance with DOD O-2000.12H Antiterrorism handbook, a vulnerability and risk assessment must be conducted prior to beginning any security project. Upon identifying facility or asset vulnerabilities to threats, physical security measures such as fences, gates, and Electronic Security Systems (ESS) may be deployed to reduce vulnerabilities. In summary, this document assumes the pre-design phases, including the risk analysis, are complete prior to beginning design. For information on Security Engineering Planning and Design process, refer to UFC 4-020-01 and UFC 4-020-02 (described in the section "Security Engineering UFC Series" in this chapter). The engineering risk analysis conducted as part of UFC 4-020-01 should be consistent with the terrorism risk analysis conducted by the installation security/AT staff.

1-6 POLICY REQUIREMENTS.

The requirement to protect waterfront assets comes from DoD Instruction/Directives, Geographic Combatant Commander (GCC) Instructions, Service Instruction/Directives, and Regional or Installation requirements. Consult Headquarters, Major Command, Regional, and Installation personnel to established waterfront asset protection requirements.

1-6.1 Department of Defense.

There are several instructions and publications within the Department of Defense that establish requirements for access control and physical security for waterfront assets.

- DOD 5200.8-R: Requires DOD Components to determine the necessary access control based on the requirements of a developed physical security program. Emergency planning is specified to include establishment of a system for positive identification of personnel and equipment authorized to enter and exit the installation and maintenance of adequate physical barriers that will be deployed to control access to the installation. Planning will also include increasing vigilance and access restrictions during higher force protection conditions.
- DODD 2000.12: Provides DOD policies for ATFP and assigns responsibilities for implementing the procedures for the DOD ATFP Program. It authorized the publication of DOD 2000.16 Antiterrorism Standards as the DOD standards for ATFP and DOD O-2000.12-H DOD Antiterrorism Handbook as guidance for the DOD standards.
- DOD O-2000.12H: Defines the DOD Force Protection Condition (FPCON) System, which describes the potential threat levels and the applicable FPCON measures to be enacted for each level. FPCON measures in the 12-H were modified in DoDI 2000.16, Change 2 of 08 Dec 2006. DOD O-2000.12H also requires Commanders to develop and implement Random Antiterrorism Measures (RAM) as an integral part of their AT Program.
- DODI 2000.16: This instruction requires the installation or activity Commanding Officer to define the access control measures at installations. Additionally, DOD 2000.16 requires Commanders at all levels to develop and implement a comprehensive Antiterrorism (AT) Program, which should define the necessary action sets, including identification and inspection procedures, at each of the potential Force Protection Condition (FPCON) levels and lists the most current approved FPCONS.

1-6.2 Geographic Combatant Commander (GCC) Requirements.

GCC issue requirements for Antiterrorism and physical security for installations within their area of responsibility. Ensure any such requirements are incorporated in addition to the requirements found in DoD and Service Directive/Instructions. Resolve any differences in the requirements for the design of a waterfront security by applying the most stringent requirement.

1-6.3 Service Requirements.

Department of Navy.

- OPNAVINST 5530.14, Chapter 10 identifies the requirements for installation and restricted area access control. APPENDIX VIII identifies Waterside and Waterfront physical security requirements.
- NTTP 3-07.2.3 provides guidance for the physical security for Naval Installations to include Restricted Areas and Waterfront Security.

1-6.4 Installation Specific Requirements.

As required by DODI 2000.16 and service directives, each installation must have an Antiterrorism Plan. The plan provides procedures and recommendations for reducing risk and vulnerability of DOD personnel, their family members, facilities, and assets from acts of terrorism. As such, the installation AT plan reflects the foundation for requirements determination. Installation specific requirements need to be factored into all capital improvement initiatives.

1-7 CONSIDERATIONS.

The objective of waterfront security system is to secure the waterfront from unauthorized access and to detect and neutralize threats while minimizing impacts to port operations and the environment. Design considerations are:

- Security
- Port Operations
- Safety
- Appearance
- Environmental impact

1-7.1 Security.

Installations should focus first on threats at the first line of defense – the installation perimeter. Consideration of the waterfront is extremely important to defense-in-depth and effective risk mitigation.

The first priority of a waterside security system is to maintain perimeter security. The waterfront:

- is a part of the installation perimeter and a legal line of demarcation

- must be able to accommodate Random Antiterrorism Measures (RAMS) employment for sustained operations in order to validate installation's ability to affect directed security posture.
- must be able to operate at all FPCONs; and must have security features that protect against landside and waterside threats and unauthorized entry

1-7.2 Port Operations.

Design the waterfront security systems to maximize security while minimizing the impact on port operations. Ships must be able to sortie effectively without compromising safety, security, or causing undue delays that may affect port or fleet operations.

1-7.3 Safety.

Waterfronts must have a working environment that is both safe and effective for security forces and personnel working in the waterfront area. Safety includes provisions for personal protection against attack and mishaps.

1-7.4 Appearance.

Design waterfront security systems to impart an immediate impression of professionalism and convey the DOD's commitment to the security of DOD personnel and its mission critical assets, facilities, and resources.

1-7.5 Environmental Impact.

Design waterfront security systems to minimize environmental impact on the adjacent waterway. Include environmental representatives in the initial planning, design and construction of applicable projects to ensure there are no compliance issues, and that all regulatory approvals are received in a timely manner.

1-8 CORROSION PREVENTION AND CONTROL.

Design strategies for waterfront security structures and equipment shall consider corrosion prevention and control (CPC) preservation techniques for long term maintainability throughout their life cycle. Trade-off decisions involving cost, useful service life, and effectiveness shall address corrosion prevention and mitigation.

1-9 REFERENCES.

Appendix A contains a list of references used in this document. The publication date of the code or standard is not included in this document. In general, the latest available issuance of the reference is used.

1-10 GLOSSARY.

Appendix B contains acronyms, abbreviations, and definitions of terms.

1-11 GENERAL BUILDING REQUIREMENTS.

UFC 1-200-01, "General Building Requirements", provides applicability of model building codes and government-unique criteria for typical design disciplines and building systems, as well as for accessibility, antiterrorism, security, sustainability, and safety. Use this UFC in addition to UFC 1-200-01 and the UFCs and government criteria referenced therein.

1-12 SECURITY ENGINEERING UFC SERIES.

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

1-12.1 DoD Minimum Antiterrorism Standards for Buildings.

UFC 4-010-01 and 4-010-02 establish standards that provide minimum levels of protection against terrorist attacks for the occupants of all DoD inhabited buildings. These UFCs are intended to be used by security and antiterrorism personnel and design teams to identify the minimum requirements that must be incorporated into the design of all new construction and major renovations of inhabited DoD buildings. They also include recommendations that should be, but are not required to be incorporated into all such buildings.

1-12.2 DoD Security Engineering Facilities Planning Manual.

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

1-12.3 DoD Security Engineering Facilities Design Manual.

UFC 4-020-02 provides interdisciplinary design guidance for developing preliminary systems of protective measures to implement the design criteria established using UFC 4-020-01. Those protective measures include building and site elements, equipment, and the supporting manpower and procedures necessary to make them all work as a system. The information in UFC 4-020-02 is in sufficient detail to support concept level project development, and as such can provide a good basis for a more detailed design.

The manual also provides a process for assessing the impact of protective measures on risk. The primary audience for the Security Engineering Design Manual is the design team, but it can also be used by security and antiterrorism personnel.

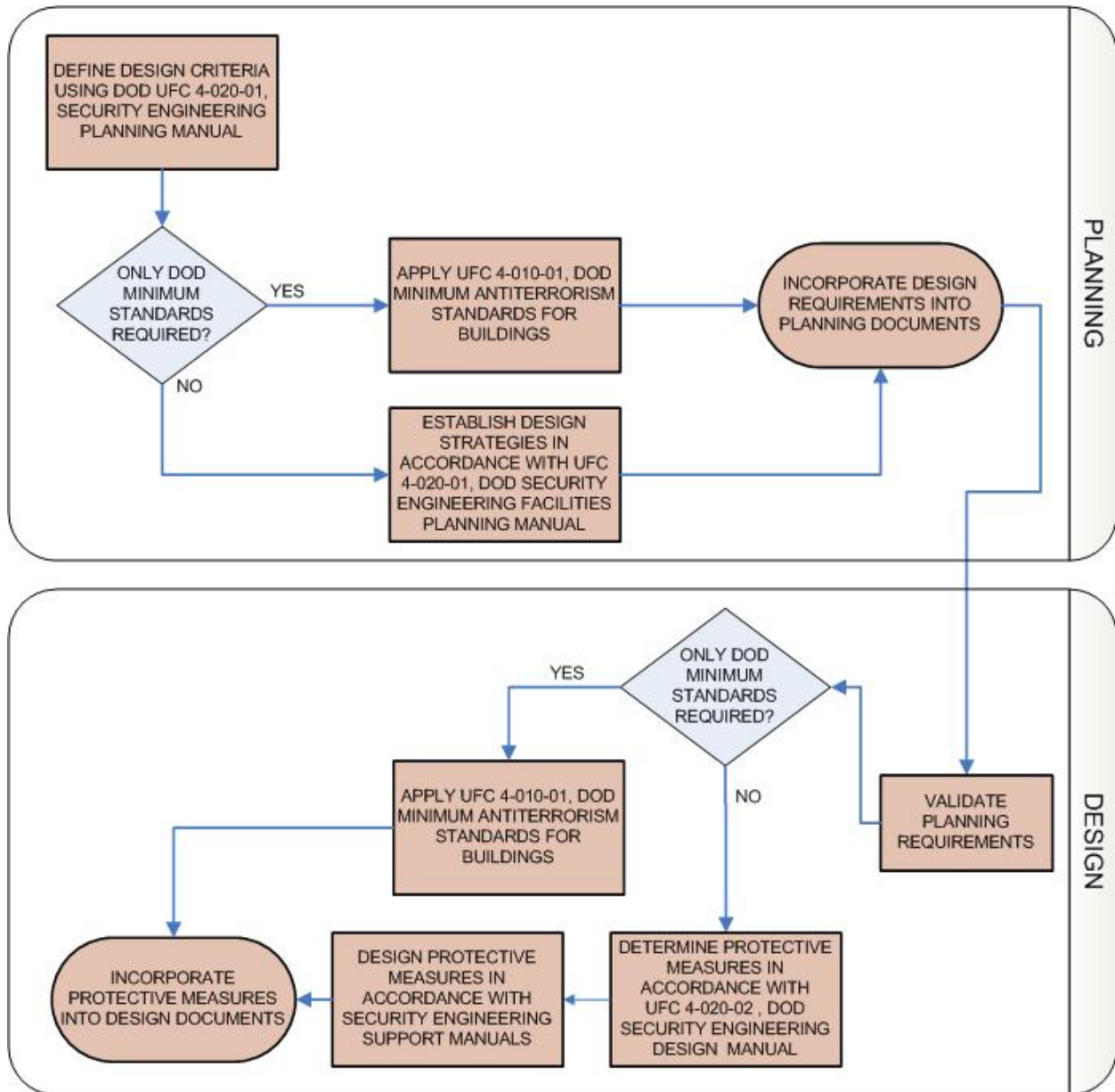
1-12.4 Security Engineering Support Manuals.

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

1-12.5 Security Engineering UFC Application.

The application of the security engineering series of UFCs is illustrated in Figure 1-1. UFC 4-020-01 is intended to be the starting point for any project that is likely to have security or antiterrorism requirements. By beginning with UFC 4-020-01, the design criteria will be developed that establishes which of the other UFCs in the series will need to be applied. The design criteria may indicate that only the minimum standards need to be incorporated, or it may include additional requirements, resulting in the need for application of additional UFCs. Even if only the minimum standards are required other UFCs may need to be applied if sufficient standoff distances are unavailable. Applying this series of UFCs in the manner illustrated in Figure 1-1 will result in the most efficient use of resources for protecting assets against security and antiterrorism related threats.

Figure 1-1 Security Engineering UFC Application



This Page Intentionally Left Blank

CHAPTER 2 OVERVIEW

2-1 OVERVIEW.

DoD installations located adjacent to bodies of water face all the threats of land –locked installations. In addition, waterfront installations must defend against the waterside threat. Waterside attacks pose additional challenges for security forces and the installation’s overall physical security system and include either surface (boat or swimmer) or subsurface (scuba diver or submersible) threats. Physical security systems protecting waterfront assets must enable/facilitate threat detection, assessment, delay, response, and threat neutralization for both waterside and landside threats.

2-2 WATERFRONT SECURITY SYSTEM.

Waterfront security system is that subset of an Installation’s physical security system specifically designed to safeguard waterfront assets against espionage, sabotage, damage, or theft.

2-2.1 Waterfront Assets.

Waterfront assets are vessels, personnel, and facilities such as piers, wharves, docks or similar structures used to berth vessels.

2-2.2 Waterfront.

The area of the DoD installation adjacent to a body of water. This area comprises waterfront assets and the surrounding area including the adjacent waterway, land, facilities, parking, and roadways. This area may be designated as a restricted or controlled areas per DoD 5200.8-R. Within the controlled or restricted area, the waterfront is divided into the two areas of waterside and landside. See Figure 2-1.

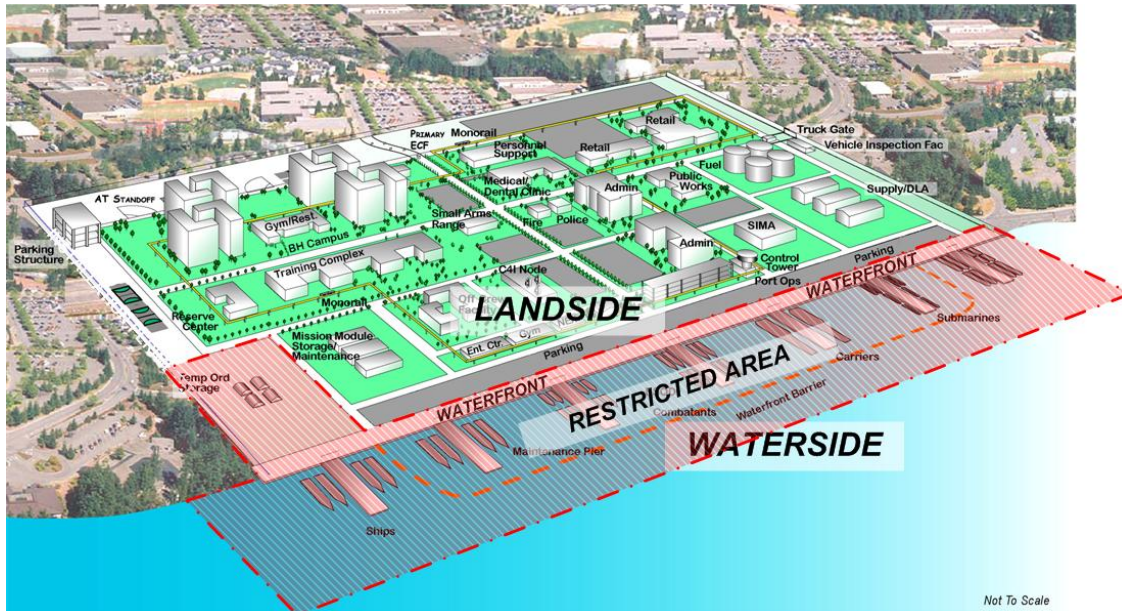
2-2.2.1 Waterside.

The body of water (waterway) adjacent to the DoD installation that is monitored and or controlled by the Installation. The waterside includes the piers and similar structures built out into the water.

2-2.2.2 Landside.

The land within the controlled or restricted area adjacent to the body of water. This includes facilities such as wharves or similar structures and includes the adjacent, facilities, parking and roadways.

Figure 2-1 Waterfront



2-2.3 Physical Security System.

A system of integrated protective measures comprised of people, equipment, and operational procedures that control access to facilities or assets.

Design physical security systems to ensure protective measures work as an integrated system rather than separate elements. The system must detect threats, delay threats, and then respond to threats. This concept is referred to as of detect, delay, and respond or detect, delay, and defend. To create an effective system, the time between detection and response by response capability must be less than the time it takes the threat to compromise the asset. Physical security systems accomplish this by detecting threats at the farthest possible distance from the asset and providing delays between the detection points and the asset giving the response capability time neutralize threat. This presents a challenge on the waterside due to limited distances between waterfront assets and unrestricted waterways.

Figure 2-2 diagrams the functions of a physical security system. Table 2-1 depicts the physical security protection measures of a waterfront security system.

Figure 2-2 Diagram of Physical Security System Functions

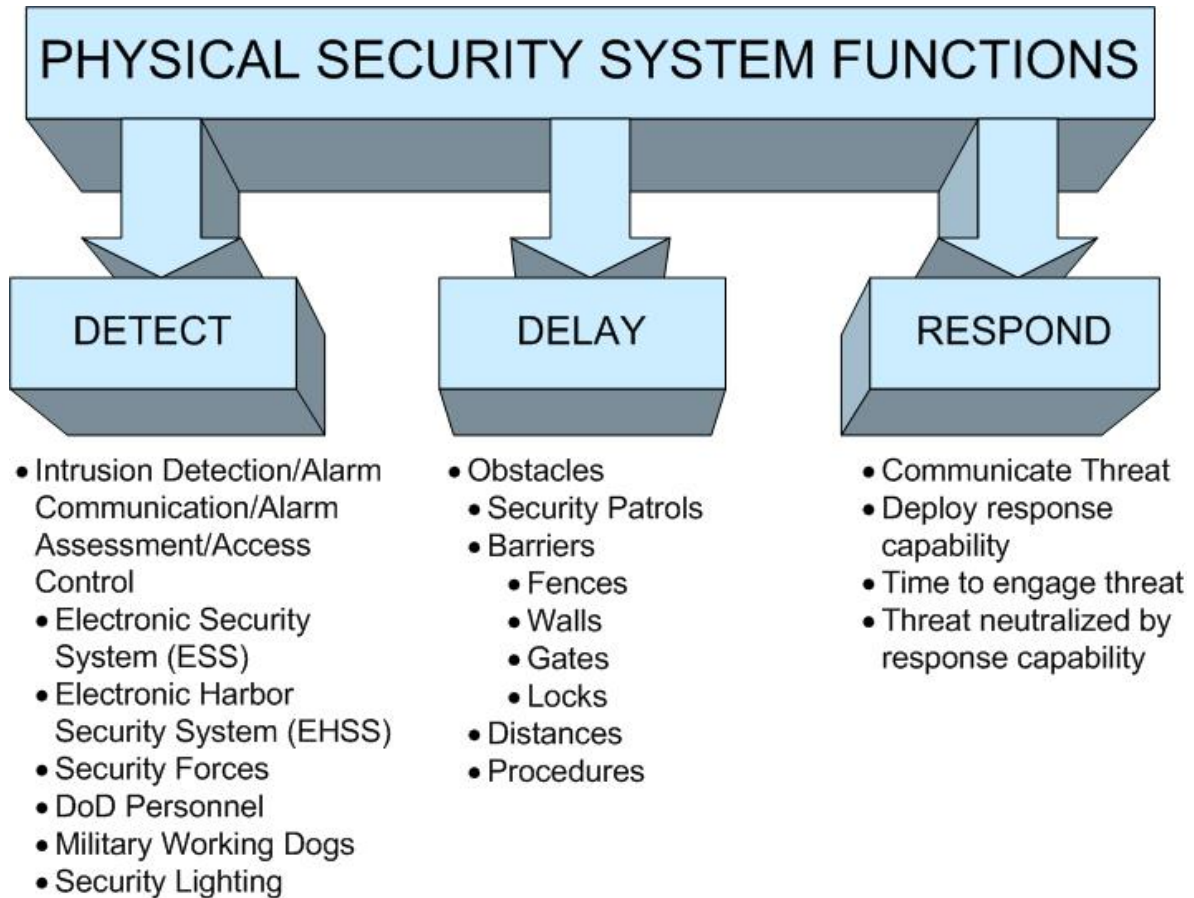


Table 2-1 Waterfront Security Elements

WATERSIDE	LANDSIDE	
WATER	PIERS/ WHARFS	LAND
Channel Markers Buoy line Barriers Signage Patrol Boats Electronic Harbor Security System (EHSS) <ul style="list-style-type: none"> • Surface detection/assessment <ul style="list-style-type: none"> ○ Cameras ○ Thermal Imagers ○ Radar ○ Video Analytics • Subsurface detection/assessment • Sonar 	Guard Towers Security Lighting Access Control Point <ul style="list-style-type: none"> • Vehicle • Pedestrian Giant Voice	Fences Access Control Point <ul style="list-style-type: none"> • Vehicle • Pedestrian Security Lighting Electronic Security System (ESS) <ul style="list-style-type: none"> • Camera • Intrusion Detection • Access Control Giant Voice

2-3 PLANNING.

2-3.1 Establish Requirements.

For some waterfront assets, the minimum security measures are established by policy or regulation. See OPNAVINST 5530.14 for security measures associated with waterfront assets in U.S. Navy controlled ports. Always determine requirements for waterfront asset protection early in the project planning process.

Establish an interdisciplinary planning team with local considerations to include the following:

- Supported Command
- Security forces
- Port Operations
- Installation/Regional Anti-terrorism Officer (ATO)
- Communications Officers
- Safety Officers
- Engineering
- Environmental
- Planning
- Local, state, Federal, or host nation officials to ensure integrity of restrictive access to the installation and reduce the potential adverse effects on surrounding communities.

The interdisciplinary planning team will use the process in UFC 4-020-01 to identify the design criteria, which includes the assets to be protected, the threats to those assets, and the levels of protection required for the assets against the identified threats. The planning team may also consider user constraints such as appearance, operations, manpower requirements or limitations, and sustainment costs when determining the requirements for asset protection and components of the overall security solution.

2-3.2 Design Basis Threat (DBT).

The DBT links aggressor with tactic. It includes the aggressor tactics and the associated weapons such as explosives, tools, and agents. The DBT must be determined to plan and design the protective measures required to protect the assets from compromise.

The waterfront should have a DBT for the landside protection measures, and a different DBT for the waterside. For example, the landside may be a stationary vehicle bomb consisting of a 4,000 lb (1814 kg) vehicle containing a Type II explosive. The waterside may be a 2,000 lb (907 kg) powerboat containing a Type I explosive.

2-3.3 Level of Protection (LOP).

Defines the degree to which an asset is protected against DBT.

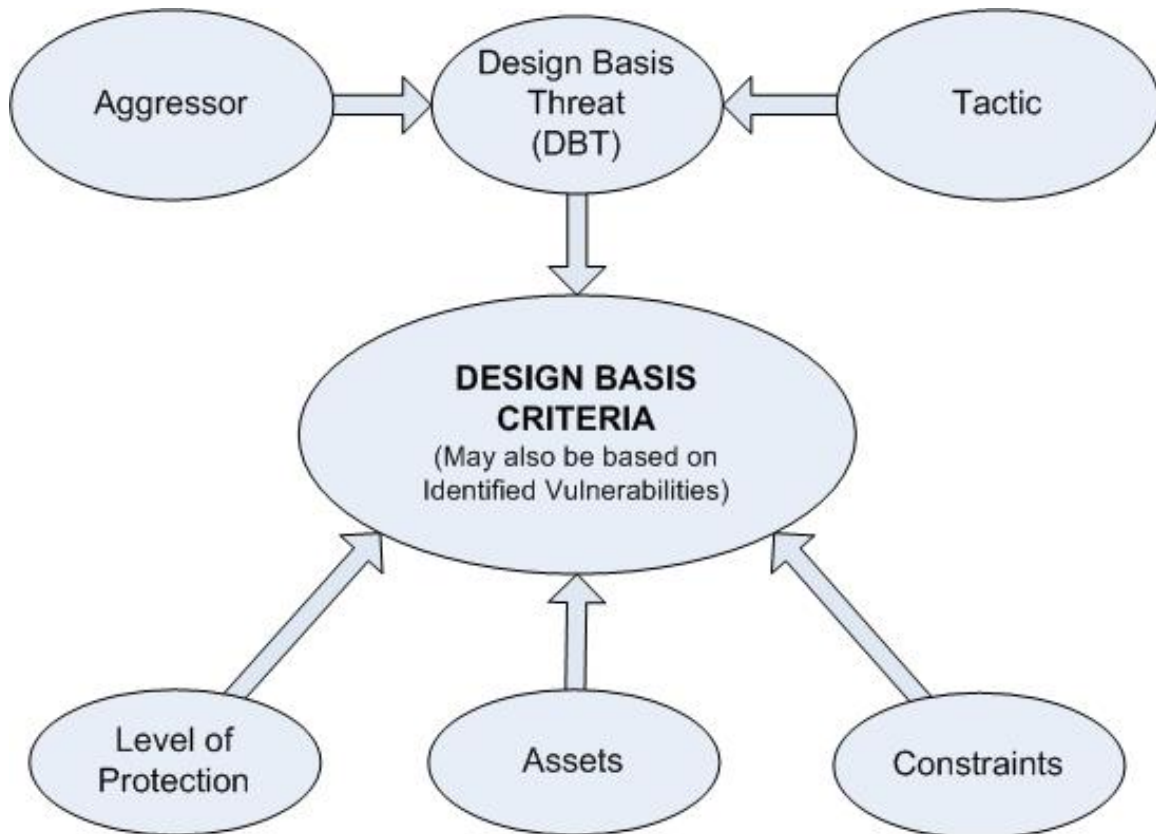
2-3.4 Future Development Plans.

The planning team must carefully evaluate future development plans for the installation and the surrounding community. All waterfront security development plans should accommodate future modifications necessitated by increased demand, additional assets, additional facilities, or revised security measures.

2-3.5 Document Requirements.

Document the planning requirements for endorsement by the Installation ATO and Port Ops Officers to ensure protective measures support the installation's physical security system, AT plan, and waterfront operations. Figure 2-3 provides a simplified flow chart of the overall process.

Figure 2-3 Project Process



This Page Intentionally Left Blank

CHAPTER 3 DESIGN STRATEGY

3-1 INTRODUCTION.

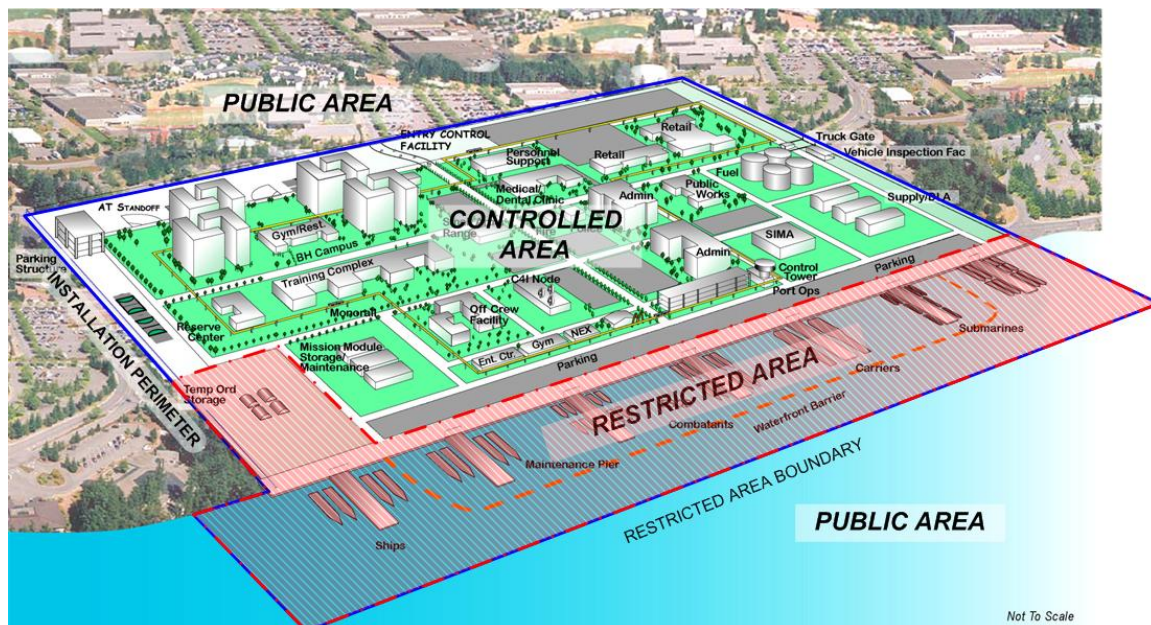
This chapter presents information to design a system of protective measures deployed on an installation that protect the waterfront from unauthorized access using the processes in UFC 4-020-01 and UFC 4-020-02 (delineated in Figure 2-3) to identify the design requirements. It assumes the waterfront is a controlled or restricted area (enclave), onboard a DoD installation with protective measures deployed on the installation and at the entry control points. It also does not address protective measures outside the waterfront area.

3-2 DESIGN STRATEGY.

All protective measures must support the concept of detect, delay and respond and facilitate security force's ability to determine capability, opportunity, and intent of would be aggressors. When possible, physical security systems shall use a defense-in-depth approach, which effectively employs human and other physical security measures throughout the installation to create a layered defense against potential threats. Defense-in-depth insures that no single point of failure would render assets vulnerable to compromise. This strategy utilizes a zone concept that establishes areas within the installation and their associated security measures. An installation must establish clearly defined sequence of boundaries through which personnel must pass to reach the restricted area. Security measures and access controls must increase as personnel transition from lower to higher security areas and personnel must understand the consequences associated with entering the restricted area. Figure 3-1 graphically describes this concept. This document will focus on the restricted area of the waterfront sometimes referred to as the waterfront enclave.

In the case of waterfront security, the first layer of defense is the Installation's perimeter including the Access Control Points (ACPs). For the landside, the installation's ACPs provide the first opportunity to detect and engage threats away from the critical assets. Access control at the installation's perimeter is extremely important to the defense-in-depth concept and effective risk mitigation. For the waterside, the first layer of defense may be the restricted area (waterway) boundary. The waterside restricted area should be visibly delineated in order to facilitate security force's ability to determine the intent of would be aggressor.

Figure 3-1 Zone Concept



- **Public Area:** Area outside an installation or controlled perimeter where the public has unrestricted access.
- **Access Control Area:** The installation's entry control points where authorized personnel transition from public zone to the DoD installation.
- **Controlled Area:** The area within the installation's controlled perimeter where authorized personnel have access. Installations are considered controlled areas for the purposes of national defense.
- **Restricted Area:** A defined area established to protect critical assets by providing a higher level of security than that afforded elsewhere on the installation.

3-2.1 Detect, Delay, and Respond.

A physical security system must operate on the principle of Detect, Delay, and Respond. To be effective, the time between detection of an intrusion and response by security forces must be less than the time it takes to damage or compromise the protected asset.

3-2.1.1 Detect.

Detection and assessment of the potential threats may be accomplished through ESS, electronic harbor security system (EHSS), security lighting, security forces, DoD personnel, military working dogs. Training and operational procedures are critical to detection and assessment as they improve personnel capabilities and support application of consistent concepts and practices. Security lighting, ESS and EHSS greatly enhance the probability of detection, reduce the time it takes to assess the

threat, improve classification of potential threats, and may reduce the manpower required to accomplish these functions.

3-2.1.2 Delay.

Delay is the time it takes for the aggressor to get from the point of detection to compromising the protected asset. Physical security systems may deploy roving security patrols, barriers, or increase standoff distance to create obstacles to increase delay. The time delay that a physical security system provides is critical to asset security. The time delay of the system must be synchronized with security force response time to ensure that maximum security is afforded to critical assets.

3-2.1.3 Response.

Response is the time it takes for the response capability to interrupt or neutralize a threat. This includes communication, mobilization, travel time, and tactics.

3-3 SYSTEM EFFECTIVENESS.

A well designed physical security system will:

- Provide defense-in-depth
- Provide continuous protection
- Enhance detect, delay, and response function

Effective waterfront security systems must be compatible with the installation's operational and security procedures. Measures that are excessive, inappropriate may eventually be eliminated or bypassed. Poorly placed fencing or barriers can reroute cranes, forklifts or container carriers to pavement areas not designed for heavy loads. Forklift tines and crane hooks can damage security equipment rendering the system inoperable. Minimize impediments to waterfront operations and security hardware by placement and consolidation.

3-4 ESTABLISH PERIMETER.

To protect waterfront assets from unauthorized access, it is important to establish and maintain a defined perimeter. Before a person proceeds into the waterfront restricted area, they must perceive the area boundary and understand the consequences associated with crossing it. The use of ESS on the landside and EHSS on the waterside enhance:

- Detection of unauthorized access with an intrusion detection system (IDS)
- Improve the validation of credentials with access control systems (ACS)
- Threat detection, alarm assessment, surveillance, and archiving with video imaging.

The easiest and least costly opportunity for achieving the appropriate levels of protection against terrorist threats is to incorporate sufficient standoff distance to mitigate the defined threat. While sufficient standoff distance is not always available, maximizing the available standoff distance always results in the most cost-effective solution.

3-4.1 Landside Perimeter.

The landside perimeter of the enclave may consist of fences, walls, signage, natural barriers, and ACPs for authorized vehicles and pedestrians. In addition, a final denial boundary may be established at the foot of a pier creating defense-in-depth. See chapter 4 for Landside protection measures.

3-4.2 Waterside Perimeter.

The waterside boundary of the enclave may consist of channel markers, buoys, float lines, signage, or boat barriers. The transition from the public area to the restricted area may not go through additional areas or zones. Therefore, the boundary on the waterside may have to provide a higher LOP (delay) for critical assets than the landside counterparts to ensure critical assets are not compromised. See chapter 5 for Waterside protection measures.

3-5 SECURITY LIGHTING.

Security lighting or protective lighting provides illumination during periods of darkness or in areas of low visibility to aid in the detection, delay, and respond functions of a physical security system. Coordinate security lighting requirements with security personnel. Refer to UFC 3-530-01 for lighting design criteria and the Landside and Waterside Chapters of this UFC for specific security lighting guidance.

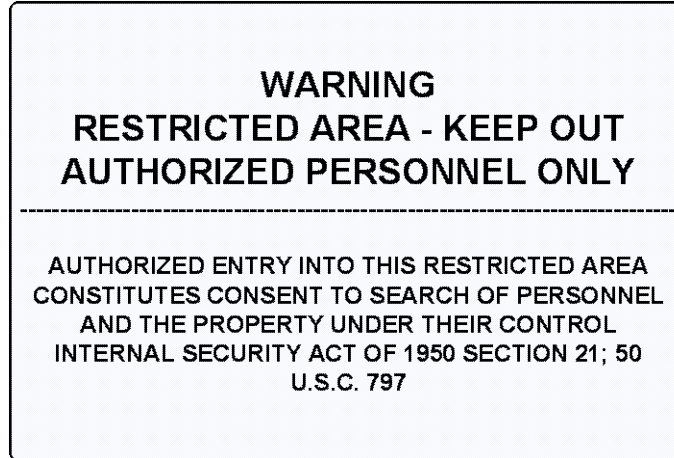
3-6 SIGNAGE.

Coordinate size, placement, wording, and use with security personnel. Signage should be consistent with applicable DoD/Service specific requirements. Any language in addition to English should be appropriate for the stated purpose.

3-6.1 Access Control Point (ACP) Signage.

Post reflective signs at all waterfront vehicle and pedestrian ACPs. For example see Figure 3-2.

Figure 3-2 ACP Sign Example



3-6.2 Restricted area signage.

Post reflective signs at intervals no greater than 100 feet (30.5 m) along the entire perimeter of the restricted area and where boundaries make abrupt changes in direction. For example see Figure 3-3.

3-6.3 Boat Barrier Signage.

Post reflective signs at intervals no greater than 100 feet (30.5 m) along the entire boat barrier perimeter and on moorings. For example see Figure 3-3.

Figure 3-3 Restricted Area Sign Example



This Page Intentionally Left Blank

CHAPTER 4 LANDSIDE

4-1 INTRODUCTION.

This chapter presents information to design a system of protective measures deployed on the landside of an installation intended to protect waterfront assets.

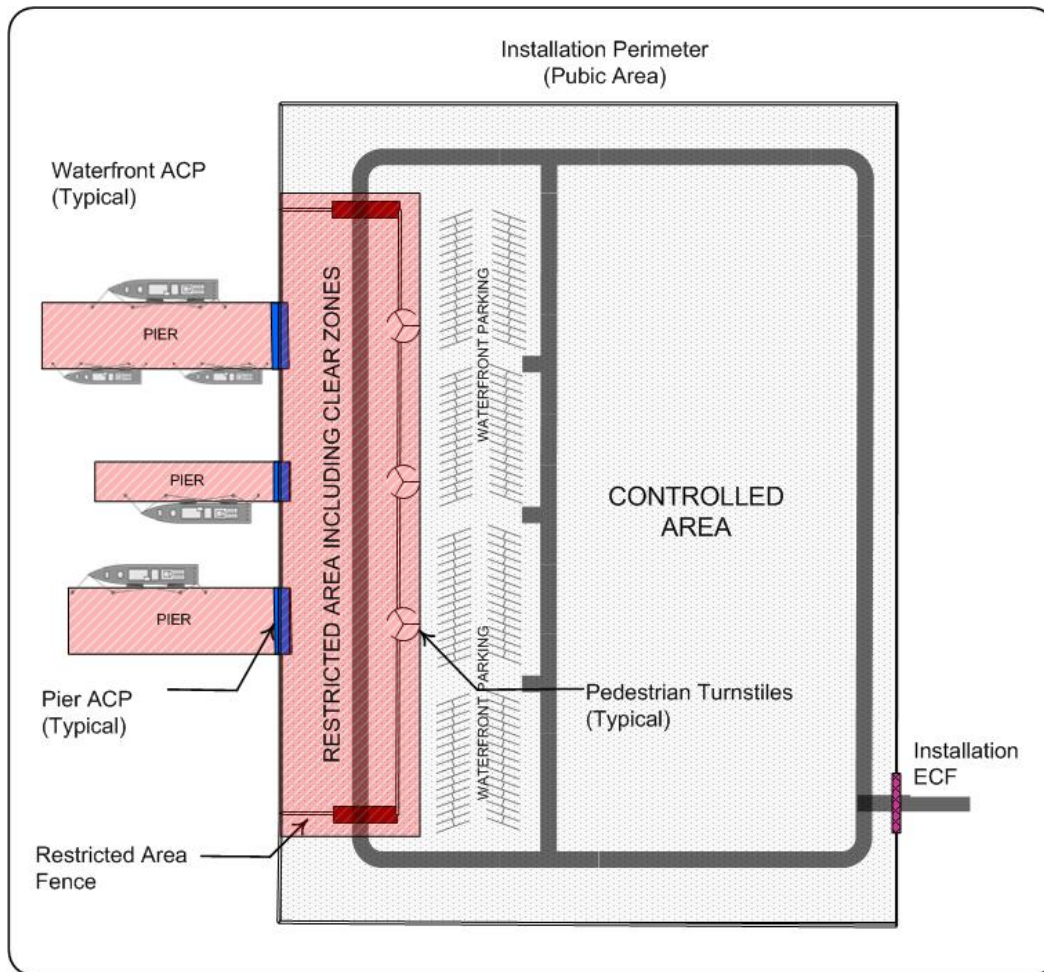
4-2 GENERAL DESIGN STRATEGY.

For the purposes of this chapter, threats are from the landside. The design strategy for the landside must be based on the concept of defense-in-depth. Establish multiple perimeters, boundaries, or zones through which unauthorized personnel must pass to access protected assets. Configuration of the physical perimeter and the LOP are dependent on assets to be protected and the DBT. In the case of the landside security, the Installation's controlled perimeter may be the first layer of defense.

The general design strategy for the landside is to establish and maintain defense in depth through the application of standoff, barriers, access control, operational procedures, and security zones, see Figure 4-1. The security zones or areas are defined as follows:

- **Asset location:** The area where the protected asset is located. For vessels, this would be a pier, wharf or dry dock.
- **Waterfront Restricted Area (enclave):** A defined waterfront area in which there are special measures employed to prevent unauthorized entry. Restricted areas may be of different types depending on the nature and varying degree of importance of the protected asset and may extend beyond the piers or wharfs to the surrounding areas. Restricted areas must be authorized by the installation commander, properly posted, and employ physical security measures.
- **Controlled Area:** The area within the installation's controlled perimeter where authorized personnel have access.

Figure 4-1 Landside Security Zones Adjacent to Piers



4-3 LANDSIDE ACCESS CONTROL.

Access control is established to prevent unauthorized access to restricted areas. As with any element of a physical security system, design must be based on the concepts of defense-in-depth. Design of the access control system begins at the Installation's perimeter and ACPs. Vehicles and personnel travel from one zone to another through the system to reach the restricted area. Physical security measures, including access control must increase from lower to higher security areas. The pier or wharf where critical assets are berthed are considered the final denial and should have the highest access control measures in the system, see Figures 4-2 and 4-3.

Figure 4-2 Landside Access Control Transitions

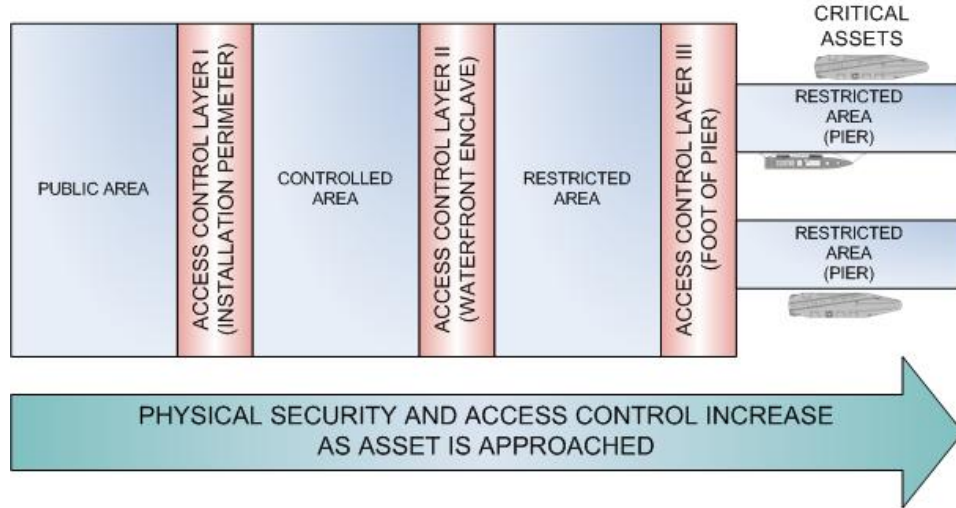
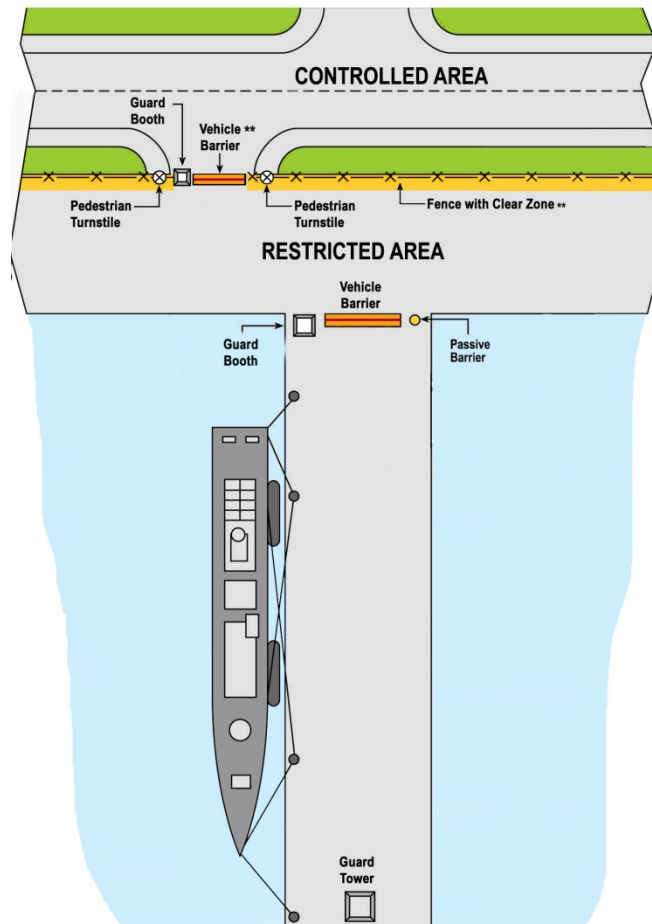


Figure 4-3 Waterfront Access Control



** If standoff from the asset is achieved at the foot of pier for the DBT, vehicle rated barriers at the restricted area boundary may not be required.

4-4 LANDSIDE STANDOFF.

While sufficient distance is not always available to provide the standoff required for a high LOP, maximizing the available standoff distance always results in the most cost-effective solution and also ensures that there is opportunity in the future to upgrade to meet increased threats or to accommodate higher force protection conditions (FPCON).

4-5 ACCESS CONTROL LAYER I: INSTALLATION PERIMETER.

The Installation's controlled perimeter and its related entry control points are not within the scope for this document. However, the Installation controlled perimeter, ACPs, and the related security procedures must be considered when determining the DBT and the resulting protective measures for the waterfront.

4-6 ACCESS CONTROL LAYER II: WATERFRONT ENCLAVE.

The access control and protection features for Layer II should be determined based on asset to be protected, DBT, and desired LOP. Coordinate requirements with supported command, ATO, and security personnel. To protect waterfront assets from unauthorized access, it is important to establish and maintain a defined perimeter. Before a person or vehicle proceeds into the waterfront restricted area (enclave), there must be a perceived perimeter boundary and an understanding of the consequences associated with crossing it. Design ACPs in accordance with UFC 4-022-01.

4-6.1 Layer II: Vehicle ACPs.

Minimize the number of vehicle ACPs into the waterfront to reduce operational requirement. However, provide a minimum of two gates for flexibility.

4-6.2 Layer II: Pedestrian ACPs.

Some waterfronts enclaves are very large and have a significant amount of pedestrian traffic. When pedestrian access control is required, ensure that proper sidewalk and safety provisions direct pedestrian traffic to the ACP separate from vehicular traffic. For pedestrian ACP at vehicular ACP, design pedestrian access to ensure security personnel maintain visual contact with the pedestrians as they approach the vehicular ACPs. If passive barriers are required, breaks in the passive barrier system for pedestrian access to the waterfront should not exceed 3.3 feet (1 m) in width for traffic having a 90-degree approach and 4.1 feet (1.25 m) in width for traffic paralleling the barrier.

Where warranted by pedestrian usage and size of the waterfront, incorporate turnstiles or similar devices in areas of high pedestrian traffic that can be automated to facilitate access control system. Provide infrastructure required to support automation to include a card reader, intercom, and video monitoring at each turnstile. Other considerations in the selection of turnstiles or similar access control devices include the control of potential tailgating and the likelihood that personnel will have equipment or luggage, which may require additional space in the turnstile. Consider if pedestrian inspection areas will be required based on pedestrian demand and any requirement to search

personnel and packages. Design elements for pedestrians should be compliant with *ABA Accessibility Standard for Department of Defense Facilities*.

4-6.3 Layer II: Fence.

Fences, clear zones, signage, or other lines of demarcation shall delineate the waterfront restricted area. When required, design the fence and associated gates in accordance with UFC 4-022-03. Buildings, structures, and other barriers may be used as a part of a security fence line as long as they provide equivalent protection to the fencing enclosing the restricted area.

4-6.4 Layer II: Vehicle Barriers.

Vehicle rated barriers are only required for the moving vehicle threat. Consider the regional threat environment and coordinate with installation Antiterrorism Officer (ATO) to determine DBT. Depending on the DBT, reinforcement of the waterfront enclave may not be required if the standoff provided by the final denial barrier at the foot of the pier is adequate to meet the LOP. If vehicle rated barriers are required, conduct a site survey to determine where reinforcement of the waterfront enclave is required. Some areas may not require reinforcement due to existing site elements such as ditches, bio swales, or retaining walls. Design barriers in accordance with UFC 4-022-02.

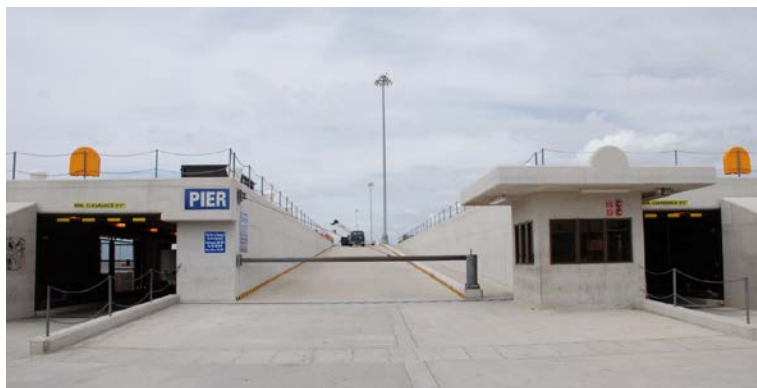
4-7 ACP LAYER III: FOOT OF PIER.

The access control and protection features for Layer III should be determined based on assets to be protected, DBT, and desired LOP. Coordinate requirements with supported command, ATO, and security personnel. For high value assets, the ACP for a pier shall have a guard booth, barriers, security lighting, and signage.

4-7.1 Layer III: Vehicle Barriers.

Barriers may consist of either passive or active barriers designed to prevent vehicles or personnel from accessing the protected area. Active barrier systems are not recommended due to the extreme environmental conditions at the waterfront. For double deck piers, access for both the upper and lower decks must be controlled. See Figure 4-4 for an example of a double deck pier ACP.

Figure 4-4 Pier ACP



4-7.2 Layer III: Guard Booth.

A guard booth is a structure that provides a protected position to facilitate surveillance, assessment, and response to threats. It may be fixed or temporary/portable. Manning of the watch position will be in accordance with the installation physical security and AT plans. Location and elevation of the guard booth must enhance the ability of security personnel to process vehicles and personnel, observe and determine capability, opportunity, and intent of threats, initiate alarms, coordinate response, and attack with force if necessary and authorized. Coordinate the manning requirements of the guard booth with security personnel. Design the guard booth to provide maximum visibility of the approach to the guard position and pier deck from the interior. Provide overhangs sized to reduce glare on glazing, facilitate mounting of exterior lighting, and provide cover from the elements for security personnel. Refer to UFC 4-023-02 for ballistic design and other requirements. See Figure 4-4 for an example of a guard house at the foot of a double deck pier.

4-7.2.1 Communication and Information Technology.

Each guard booth should have at least two means of communication to a central monitoring point, e.g. installation emergency control center, central dispatch, or similar designated location. Coordinate the communication requirements with the installation. Provide a minimum of two 1 inch (2.54 cm) empty conduit raceways from the watch position to the roof to facilitate future roof mounted communication equipment.

4-7.2.2 Central Duress Alarm.

Provide a central duress alarm, which signals other guard positions and the central monitor point. Provide an enunciator in the guard tower to alert security personnel of alarm triggered at any other waterfront guard position or tower.

4-7.2.3 Guard Booth Lighting.

Lighting inside the guard booth must not degrade security personnel's nighttime vision. All luminaires must be dimmable and should be mounted at or near desk level. Switch task and general lighting separately. When colors are not used to distinguished tasks (colored lights or controls for alarm annunciators), consider red light sources for task lighting to reduce adaptation problems. Lighting controls must be under the direct control of security personnel.

4-8 ELECTRONIC SECURITY SYSTEMS (ESS).

The need for an intrusion detection system (IDS) and video monitoring for the landside perimeter will be based on assets to be protected, threat environment, desired LOP, and defense-in-depth. Coordinate requirements with supported command, ATO, and security personnel. Design systems in accordance with UFC 4-021-02NF.

When turnstiles are provided for pedestrian access control, provide infrastructure required to support automation of turnstiles. Include lighting, card reader, intercom, and video monitoring at each turnstile.

4-9 SECURITY LIGHTING.

Security lighting aids in the detection of aggressors and assists personnel in the assessment and response to potential threats. The type of site lighting system provided depends on the installation environment and intended use. Provide full cut-off or fully shielded fixtures to limit glare. In general, high mast lighting provided for waterfront operations supply adequate illuminance for security requirements. Design lighting in accordance with UFC 3-530-01.

4-9.1 Perimeter Lighting.

The need for lighting for the landside perimeter will be based on assets to be protected, threat environment, desired LOP, and defense-in-depth. Coordinate requirements with supported command, ATO, and security personnel. Illumination of a restricted area perimeter includes the exterior and interior clear zones adjacent to the fence or, in some applications, the area between multiple fences. Provide poles, power circuits, and transformers within the protected area. Coordinate pole locations with the user to ensure that the applicable egress requirements and patrol routes of the clear zone are not violated. The distance of poles from the fence shall not be less than 5 feet.

4-9.2 Vehicle ACP Lighting.

For most of the ACPs (access zone), full cutoff or fully shielded luminaires will provide adequate lighting for most visual tasks. However, vertical illuminance on motorists' faces can be improved with the use of low brightness light sources (less than 3500 lumen lamp output). Luminaires mounted to the side and behind security personnel will improve identification tasks.

4-9.3 Pedestrian ACP Lighting.

Illuminate pedestrian zones for both pedestrians and security personnel. Pedestrians must have a clear view of gates and card access readers and security personnel must be able to see pedestrians approaching the ACP. Provide full cutoff or fully shielded luminaires mounted in the horizontal plane to minimize glare.

This Page Intentionally Left Blank

CHAPTER 5 WATERSIDE

5-1 INTRODUCTION.

This chapter presents information to design a system of protective measures deployed on the waterside of an installation.

5-2 DESIGN STRATEGY.

For this chapter, threats are from the waterside. As with Landside, the design strategy for the waterside must be based on the concept of defense-in-depth by establishing multiple boundaries or zones in which unauthorized watercraft or personnel (i.e. diver or swimmer) must pass to access protected assets. Configuration of the physical perimeter and the LOP are dependent on assets to be protected and the DBT. The primary protective measure is maintaining stand-off through detection and delay of surface and subsurface threats.

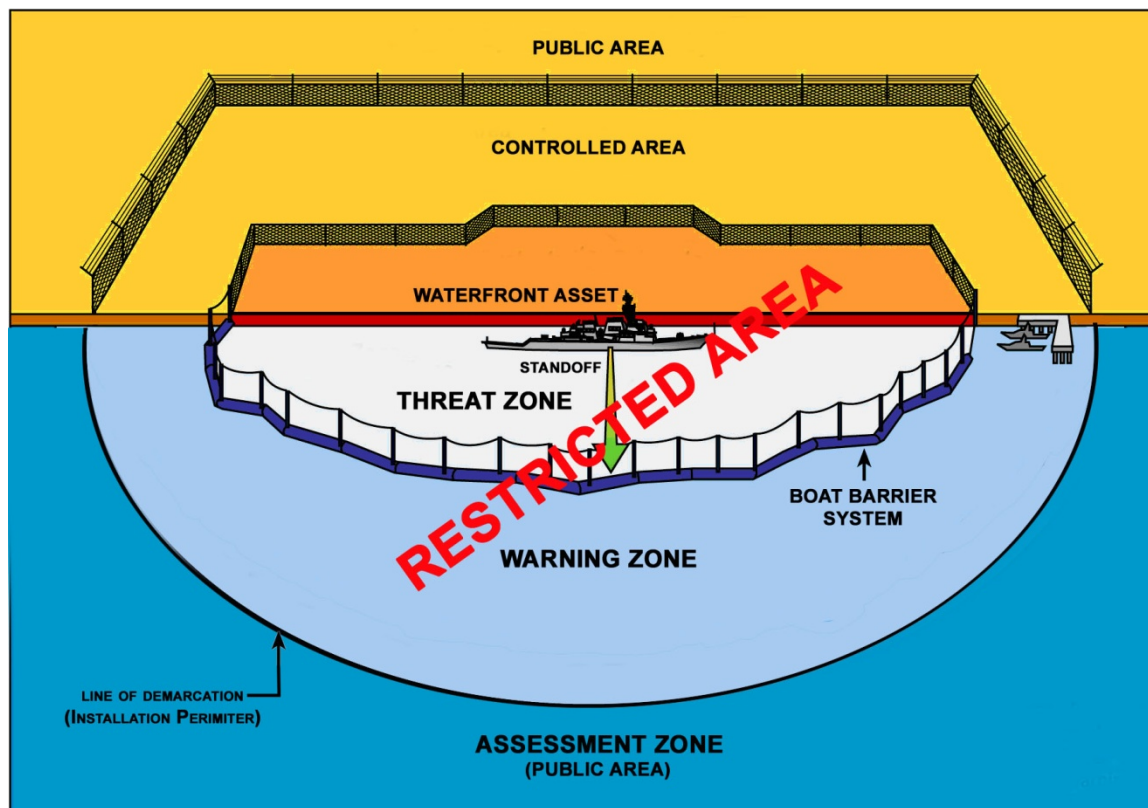
5-2.1 General Design Strategy.

Prevent waterfront attack by creating standoff and applying the defense in depth concept. Establish security zones with barriers, electronic harbor security systems (EHSS), and operational procedures from the high water mark to the waterside, installation perimeter. The security zones are defined as follows:

- **Waterside Assessment Zone:** An area beyond the DoD's property line from where surface and subsurface threats approaching the waterside warning zone may be detected, monitored, and tracked.
- **Waterside Warning Zone:** The area just outside the Threat Zone and within the waterside installation perimeter. In some locations a large warning zone is not feasible due to channel constraints.
- **Waterside Threat Zone:** The area between a line of floating barriers and an asset.

The Threat and Warning zones are determined by the Installation Commander.

Figure 5-1 Waterside Security Zones



Note: Restricted Area may extend out to the installation perimeter at some locations.

5-3 WATERSIDE STANDOFF.

Establish waterside standoff based on DBT. Ideally, this standoff distance extends from the protected assets to the maximum range of anticipated DBT (25 meters for small explosives to several thousand meters for portable anti-tank weapons). Security forces should endeavor to prevent the entry of surface and subsurface threats into the waterside standoff.

5-4 PERIMETER.

Establishing a perimeter is an important protective measure meant to deter and prevent unauthorized personnel from entering a DoD installation.

5-4.1 Waterside Perimeter.

Delineate the waterside perimeter by issuing a notice to mariners and with floating signage, signs on piles or other lines of demarcation to prevent innocent vessels from entering the Warning Zone. Methods of demarcation depend on the waterfront geography and the relation between installation and the navigational channel.

5-4.2 Waterside Restricted Area.

This is the designated restricted area in which special measures are employed to prevent unauthorized entry. The waterside restricted area may be the waterside perimeter or an enclave within that perimeter (Threat Zone). Identify waterside restricted area(s) with buoys and signs. Consider using a floating line of demarcation (LOD) to identify the waterside restricted area.

5-4.3 Line of demarcation (LOD).

A LOD is a system used to identify restricted waters, standoff distance, or an installation's waterside perimeter. It must be clearly visible to vessel operators in most weather conditions and be interspersed with signage indicating access control measures. LOD may be located at the perimeter of the Threat or Warning Zone. Coordinate location and requirement on floating LOD with installation. Figure 5-1 illustrates basic floating LOD.

5-4.4 Boat Barrier System.

A boat barrier system is a continuous, modular LOD intended to stop and/or delay waterborne threats. When required by DOD, GCC, or Service Instruction, provide boat barriers at the Threat Zone perimeter to prevent direct unchallenged access to waterfront assets. The boat barrier system's capability and configuration will depend upon the assets to be protected, DBT, port configuration, operations tempo, environmental constraints, and response capability. Attempting to cross a boat barrier establishes intent and provides time for security forces to arrive and escort the threat out of the area. Many DoD controlled waterfronts do not allow comprehensive waterside security layering due to proximity of waterfront restricted area to shipping channels. Therefore, the delay time afforded by the barrier system should be synchronized with other physical security system capabilities to ensure a comprehensive security. Figure 5-2 illustrates a boat barrier system. For more information on boat barrier systems and related products contact:

Waterfront Security Manager
Naval Facilities Engineering Service Center, Code 55
720 Kennon St SE Suite 333
Washington Navy Yard DC 20374-5063

Figure 5-1 Floating Line of Demarcation



Figure 5-2 Boat Barrier System (Port Security Barrier)



5-5 GUARD TOWERS.

Guard towers provide an elevated protected position to facilitate surveillance, assessment, and response to waterside threats. This position may be fixed or temporary/portable. Guard towers are not required at all locations. When required, there should be enough guard towers on the waterfront to ensure complete overlapping coverage of the protected area. Coverage should be such that the elimination of one guard tower does not preclude complete coverage.

Manning of the watch position will be in accordance with the installation physical security and AT plans. Locate and set the elevation of the guard tower to enhance the ability of security personnel to observe and assess threats, initiate alarms, coordinate response, and attack with force, if necessary and authorized. Coordinate the number and location guard towers with security personnel, waterfront operations, and EHSS infrastructure. Ensure towers have proper line of sight, are suitable for port operations, account for variations in port loading, and are suitable for port operations. In most cases, locate the guard tower at or near the end of the pier (head) to maximize visibility of the waterside restricted area. Provide 360-degree visibility from the interior of the guard tower and an open observation deck with overhang to facilitate assessment and engagement of threat, maintenance of watch position glazing, and access to roof mounted equipment. Size the overhang to reduce glare on glazing and provide cover from the elements for security personnel. Refer to UFC 4-023-02 for ballistic design and other requirements. See Figure 5-3 for an example of a guard tower at the head of a pier.

5-5.1 Communication and Information Technology.

Each guard tower should have at least two means of communication to a central monitoring point, e.g. installation emergency control center, central dispatch, or similar designated location. Coordinate the communication requirements with the installation. Provide a minimum of two 1 inch (2.54 cm) empty conduit raceways from the watch position to the roof to facilitate future roof mounted communication equipment.

5-5.2 Central Duress Alarm.

Provide a central duress alarm, which signals other guard towers and the central monitor point. Provide an enunciator in the guard tower to alert security personnel of alarm triggered at any other waterfront guard facility or towers.

5-5.3 Guard Tower Lighting.

Lighting inside the guard towers must not degrade security personnel's nighttime vision. All luminaires must be dimmable and should be mounted at or near desk level. Switch task and general lighting separately. When colors are not used to distinguished tasks (colored lights or controls for alarm annunciations), consider red light sources for task lighting to reduce adaptation problems. A manually operated roof mounted searchlight may be required to assist security personnel to locate and assess waterside threats. Lighting controls must be under the direct control of security personnel.

Figure 5-3 Guard Tower on Pier



5-6 WATERFRONT SECURITY LIGHTING.

Provide full cut-off or fully shielded fixtures to limit glare. In general, high mast lighting provided for waterfront operations supply adequate illuminance for security requirements. Coordinate number, height, and location of poles and the associated concrete pedestals to minimize obstructions to pier and wharf operations. Refer to UFC 4-152-01 for Pier and Wharf operational lighting requirements and UFC 3-530-01 for lighting design criteria. Additional lighting (fully shielded or full cutoff) may be required on guard tower (below observation deck) to illuminate egress and the area on the opposite side from high mast lighting. Coordinate security lighting requirements with security personnel.

5-6.1 Water surface Lighting.

High mast lighting on piers and wharfs provide adequate illumination for security requirements. Glare, poor distribution, and excessive light levels reduce security personnel's ability to assess surface and subsurface threats.

5-6.2 Underwater Lighting.

Underwater lighting is not normally required for detection of subsurface threats and is discouraged due to limited benefit, high installation cost, and maintenance issues.

5-6.3 Under deck Lighting.

Dedicated luminaires located beneath the pier are not normally required and are discouraged due to limited benefit, high installation cost, and maintenance issues.

5-6.4 Lighting Interference.

Security lighting can visually interfere with lighting used as aids to navigation (ATON) by ships. Lighting ashore can camouflage, outshine, or otherwise conceal ATON. Ensure that lighting ashore and in the waterfront restricted area does not conflict with or otherwise conceal the ATON lights. Coordinate security lighting requirements with Port Operations

5-7 ELECTRONIC HARBOR SECURITY SYSTEMS (EHSS).

EHSS is provided when required by DOD, GCC, or Service Instruction. EHSS integrates electronic sensors and video systems to detect, assess, track, and archive capabilities for waterside surface and subsurface threats. The type of system utilized shall be based on assets to be protected and risk.

The EHSS can be configured to integrate all sensor and video information to provide a graphical display of all threats within waterside security zones to be protected (protected area). The waterside security zones may be programmed to generate alarm conditions dependant on location of threat relative to protected assets. As with all protection measures, the capability and configuration of the EHSS is dependent on the assets to be protected, DBT, port configuration, operations tempo, environmental constraints, and response capability. For more information on related products contact:

Waterside Security Systems
Space and Naval Warfare Systems Center, Code 71742
53560 Hull Street
San Diego, CA 92152-5001

waterside@spawar.navy.mil

(619) 553-5033 voice

(619) 553-6553 fax

5-7.1 Surface Detection and Assessment.

Radar and video equipment are used to detect, track and assess surface threats within the protected area. Radar and video systems should be located based on site specific conditions such as landside and waterside operations, landside and waterside terrain, climate, available power and communications, and technology capabilities. When available, equipment should be roof mounted on the guard towers to provide a solid elevated mounting platform and enclosed space for the related equipment.

5-7.1.1 Radar.

The radar element is the primary means for detecting surface threat. Systems include a radar set, tracking processor, and display. The tracking processor has acquisition zones that can be configured for each site based on local geography, port activity, and the installation's security protocols. The radar element should

utilize multiple radar transponders installed at various locations to provide a complete picture of the protected zone. See Figure 5-4.

5-7.1.2 Identification Friend or Foe (IFF).

This system provides the capability identify “friend” vessels authorized to be in the area and assists in determining bearing and range when vessels are equipped with IFF transponder.

Figure 5-4 Radar Antenna



5-7.1.3 Video Imaging.

The imaging system is a collection of cameras, recorders, switches, keyboards, and monitors that allow assessment and recording of security events. The imaging system is normally integrated into the overall EHSS and monitored at operator workstation. Capabilities of the imaging systems include assessment of alarm conditions, surveillance of the protected area, and archiving of events. The imaging system must have a minimum of 30 days storage capacity. When integrated with video analytics the imaging system can have a detection capability. Refer to UFC 4-021-02NF for the design of imaging systems.

For EHSS, the basic imaging element consists of two cameras. Provide one low light color; pan, tilt, zoom (PTZ) camera for daytime assessment and one PTZ night vision camera or imaging device at each location. Multiple technologies must be deployed to ensure adequate coverage of the waterside area. Available technologies include low-light cameras, infrared cameras, thermal imagers, and near infrared laser-camera systems. Table 5-2 provides a summary the various technologies.

Table 5-2 Visual-Imaging Element Technologies

Technology	Range (Nominal)	Light Source	Support	Cost	Advantages	Disadvantages
Low-light camera	Short 100 to 300 yards (90 to 275 m)	Visible light (sunlight, moonlight, artificial light)	Camera power, video cable	\$3k to \$5k	Low cost Uses available light	Unable to provide coverage in new moon (no moon) and dark or cloudy conditions
Infrared camera (camera with infrared illuminators)	Short 100 to 300 yards (90 to 275 m)	Infrared illuminators	Power for camera and illuminator, video cable Illuminators	\$3k to \$5k camera \$1k per illuminator	100 percent night vision capable Low total cost of ownership	Limited to the range of the associated infrared illuminators Short range
Near-infrared system	Medium 1,000 to 3,000 yards 900 to 2700 m)	Near-infrared laser	Composite system of laser and camera	\$50k to \$90k	No interference from heat and visible light Natural-contrast night image	Performs best as synchronized system
Thermal camera (uncooled)	Long 1,000 to 5,000 yards (900 to 4500 m) (height of eye)	Heat energy emitted from object/scene	Camera power Internal temperature-adjusting controls	\$7k to \$20k	Autonomous system; does not require visible light or supporting illumination system	Non-natural image Requires trained operator to interpret thermal images
Thermal camera (cooled)	Long 1,000 to 10,000 yards (900 to 9000 m) (height of eye)	Heat energy emitted from object/scene	Camera power Internal refrigerant system	\$100k plus	Highest detection sensitivity Autonomous system	High cost Periodic maintenance of coolant system Non-natural image

5-7.2 Subsurface Detection and Assessment.

The subsurface element detects an underwater threat. Current designs make use of underwater soundheads connected to signal processors for eventual display. Ensure proper EV permitting has been obtained to ensure conformance with the “Marine Mammal Protection Act (MMPA).

5-7.2.1 Sonar.

The sonar transponders are the primary means for detecting subsurface targets. Submerged non-visual elements include the use of sonar transponders installed at various underwater locations feeding their inputs to a central display (operator workstation). The soundhead can be bottom-mounted, side-mounted, or moored, See Figure 5-5. The sonar track processor evaluates contacts and assigns tracks to those exceeding preset levels. The use of multiple transponders helps eliminate holes and shadows in the non-visual submerged surveillance picture. Locate the devices so that they are not shrouded by berthed ships, and provide adequate coverage of the underwater approaches. Poorly placed devices can create hazards to shipping, interfere with dredging operations and can be difficult to maintain. An environmental assessment must be completed prior to the deployment of any sonar transponders.

Figure 5-5 Sound Transducer Being Lowered into the Water



5-7.3 Command, Control, Communication and Display (C3D).

The C3D element provides a situational display of the waterside. Multiple displays provide an overview of the waterside and include display of EHSS subsystem elements for surface and subsurface detection, assessment, and tracking.

5-7.4 Infrastructure.

Infrastructure includes the permanent facilities necessary to support the EHSS including mounting structures, power, communication cabling (connectivity), pathways, and space for workstations and rack mounted equipment.

Vehicles including forklifts and container carriers operate in all areas of a pier. Electrical gear located on pier decks have suffered casualty due to forklift tines and crane hooks. Minimize equipment mounted on the operational pier deck. Any deck mounted equipment must be approved by the Port Ops Officer.

5-7.4.1 Location.

For double deck piers, the generator and electronic equipment enclosure shall be located to the lower deck, within the guard tower, or located on the offshore side of the guard tower to minimize the total footprint, and enable the guard tower walls to be used for mounting the conduit system.

Do not mount equipment or conduits near cleats or bollards. Crews must haul mooring lines past these deck fittings in order to secure the ship. Equipment located in close proximity to these deck fittings create safety hazards for the crew and is subject to damage by the lines.

5-7.4.2 Space.

Space must be reserved in multiple locations to support the equipment and operation of the EHSS. This includes locations such as guard towers, piers, wharfs, and a central monitoring location.

5-7.4.3 Guard Towers.

Provide space for roof mounted equipment and weather tight pathways from the roof to the sensor equipment cabinet for associated communication and power cabling, See Figure 5-6. Provide a minimum of two 2 inch (50 mm) conduit per element (imaging, radar, and/or sonar) from sensor equipment cabinet to element location.

Provide space for a 19 inch (48 cm) telecommunications cabinet (sensor equipment cabinet) sized for the associated EHSS equipment. Consider providing space on first floor of guard tower for EHSS generator and controls. If the generator is located in guard tower, provide ventilation, vibration, an acoustic isolation from guard position.

Figure 5-6 Roof Mounted Equipment



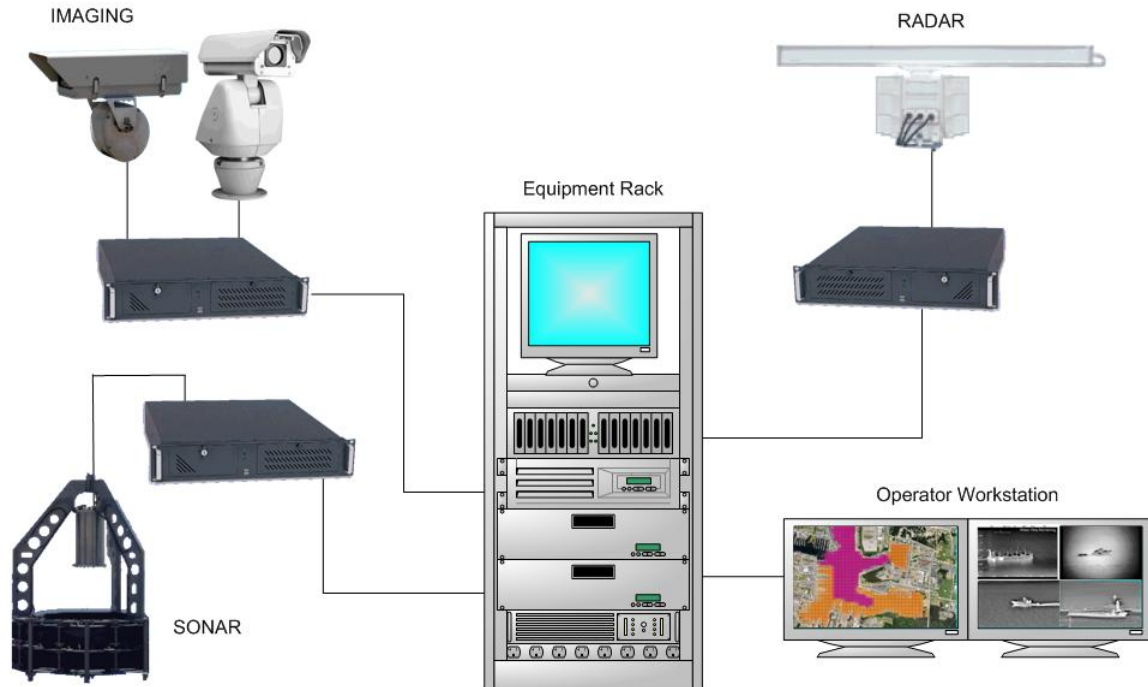
5-7.4.4 Piers and Wharfs.

Provide a dry location for a sensor equipment cabinet (19 inch (48 cm) telecommunications cabinet) sized for the EHSS equipment deployed. The preferred location is directly underneath or adjacent to the surface detection and assessment equipment mounting structure.

5-7.4.5 Central Monitoring Location.

Provide space for a full height freestanding 19 inch (48 cm) telecommunications cabinet, operator workstation, and multiple displays. Provide space, connectivity, and power receptacles for operator workstation including multiple desktop displays. Provide wall space, connectivity, and power receptacles for EHSS multiple large format flat panel displays EHSS subsystems monitoring. Reserve additional wall space for nautical chart displays. See Figure 5-7 for a notional configuration of the equipment associated with an EHSS.

Figure 5-7 EHSS Configuration



5-7.4.6 Backup Power.

EHSS systems require a backup generator. The supporting generator is normally located pierside in a weather-protected location or enclosure. Reserve a minimum of 8 foot 6 inch (259 cm) space x 3 foot 6 inch (107 cm) space for generator and associated controls. Coordinate actual space requirements with equipment provider. Do not locate generators on the upper (operational) deck of a double deck pier unless they are located on the offshore side of the guard tower.

5-7.4.7 Conduit Infrastructure.

Coordinate conduit requirements with equipment provider. At a minimum, provide one conduit per element (imaging, radar, and/or sonar) from sensor equipment cabinet to element location.

5-7.4.8 Communication and Information Technology.

Connectivity is required from each sensor equipment cabinet to the central monitoring location. Provide a minimum of one 12-strand, single mode, optical fiber cable from sensor equipment cabinet to the central monitoring station. Coordinate point of service with installation.

This Page Intentionally Left Blank

APPENDIX A REFERENCES

GOVERNMENT PUBLICATIONS

ABA Accessibility Standard for Department of Defense Facilities,
<http://www.access-board.gov/ada-aba/aba-standards-dod.cfm>

DEPARTMENT OF DEFENSE <http://www.dtic.mil/whs/directives/>
DOD 5200.8-R *Physical Security Program*

DODD 2000.12 *DOD Antiterrorism (AT) Program*

DODI 2000.16 *DOD Antiterrorism (AT) Standards*

DOD O-2000.12-H *Antiterrorism Handbook (FOUO)*

DEPARTMENT OF THE NAVY

OPNAVINST 5530.14 *Navy Physical Security and Law Enforcement Program*
<http://www.fas.org/irp/doddir/navy/opnavinst/>

NTTP 3-07.2.3 *Navy Tactics, Techniques, and Procedures Law Enforcement and Physical Security*

UNIFIED FACILITIES CRITERIA http://www.wbdg.org/ccb/browse_cat.php?o=29&c=4

UFC 3-530-01 *Design: Interior and Exterior Lighting and Controls*

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

UFC 4-010-02 *DoD Minimum Antiterrorism Standoff Distances for Buildings (FOUO)*

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

UFC 4-020-02 *DoD Security Engineering Facilities Design Manual*, currently in Draft and unavailable

UFC 4-021-02NF *Security Engineering Electronic Security Systems*

UFC 4-022-01 *Security Engineering: Entry Control Facilities / Access Control Points*

UFC 4-022-02 *Design and Selection and Application of Vehicle Barriers*

UFC 4-023-02 *Security Engineering: Fences, Gates and Guard Facilities*, currently in Draft and unavailable. Utilize MIL-HDBK 1013/10 *Design Guidelines for Security Fencing, Gates, Barriers, and Guard Facilities* until UFC is published.
(http://www.wbdg.org/ccb/NAVFAC/DMMHNAV/1013_10.pdf)

UFC 4-152-01 *Design: Piers and Wharves*

This Page Intentionally Left Blank

APPENDIX B GLOSSARY

ACRONYMS

ACP	Access Control Point
AT	Antiterrorism
ATON	Aids to Navigation
CCTV	Closed Circuit Television
DBT	Design Basis Threat
EHSS	Electronic Harbor Security System
ESS	Electronic Security System
ESSC	Electronic Security System Console
FP	Force Protection
FPCON	Force Protection Condition
GCC	Geographic Combatant Commander
IDS	Intrusion Detection System
LOD	Line of Demarcation
LOP	Level of Protection
RAM	Random Antiterrorism Measures

DEFINITION OF TERMS

Controlled Area. A space extending upward and outward from a specified point. This area is typically designated by a commander or director, wherein sensitive information or operations occur and requires limitations of access.

Design basis threat (DBT) The threat against which an asset must be protected and upon which the protective system's design is based. It is the baseline type and size of threat that buildings or other structures are designed to withstand. The DBT includes the tactics aggressors will use against the asset and the tools, weapons, and explosives employed in these tactics.

Dispatch Center. The space that serves as a central monitoring and assessment facility for the ACS, CCTV, and IDS systems. The key components of a Dispatch Center include consoles, monitors, and printers. Normally, the Dispatch Center is staffed 24 hours a day, seven days a week by trained personnel. Other names for the Dispatch Center include Regional Dispatch Center (RDC), Security Operations Center (SOC), Security Command Center and Security Control Center (SCC), Central Monitoring Station, Data Transmission Center (DTC), and Alarm Control Center (ATC).

Electronic Harbor Security System (EHSS). An electronic system that integrates surface detection, subsurface detection, and video systems to detect, assess, track, and archive waterside threats.

Electronic Security System (ESS). The integrated electronic system that encompasses interior and exterior Intrusion Detection Systems (IDS), Closed Circuit Television (CCTV) systems for assessment of alarm conditions, Automated Access Control Systems (ACS), Data Transmission Media (DTM), and alarm reporting systems for monitoring, control, and display.

Electronic Security System Console (ESSC). While not always specifically referred to as the ESSC, most security systems have a console that houses monitoring and server interface equipment. Generally, this console is located in the Dispatch Center.

Foot of pier. The landside end of the pier

Force Protection (FP). Actions taken to prevent or mitigate hostile actions against DoD personnel (including family members), resources, facilities, and critical information.

Force Protection Condition (FPCON). A DoD-approved system standardizing the Department's identification, recommended preventive actions, and responses to terrorist threats against U.S. personnel and facilities.

Head of pier. The waterside end of the pier sometimes referred to as the pier head.

Installations. Real DoD properties including bases, stations, forts (including National Guard and Federal Reserve Centers), depots, arsenals, plants (both contractor and Government operated), hospitals, terminals, and other special mission facilities, used primarily for military purposes.

Level of protection. The degree to which an asset is protected against compromise.

Physical Security. That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft.

Ports of Call. A port not located on a DoD installation where ships dock in the course of deployment to load or unload cargo, obtain supplies, liberty, or undergo repairs.

Restricted Area. An area under military jurisdiction in which special security measures are employed to prevent unauthorized entry.

Waterside Security. Measures or actions taken to prevent or guard against the use of a waterside approach to a waterfront facility or vessel by persons or vessels intent on theft, sabotage, terrorism, and/or belligerent acts