



UFC 4-025-01 Waterfront Security

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

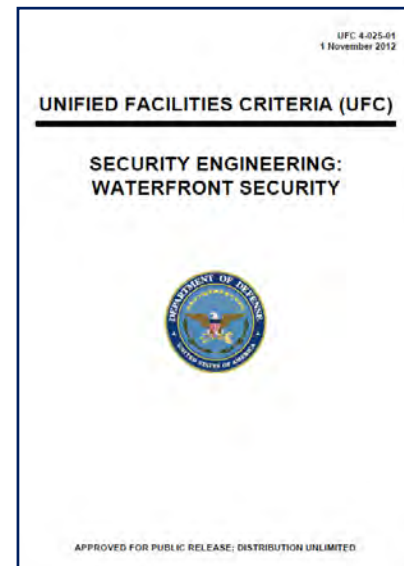
October 2024

5 Aircraft Carriers in Port - Replacement cost @ \$13 billion each



UFC 4-025-01, WATERFRONT SECURITY

- **Purpose:**
 - Present a unified approach for AT and protective systems that protect waterfront assets.
- **Applicability:**
 - Applies to all construction, renovation, and repair projects including expeditionary or temporary construction of waterfront facilities onboard DoD installations.
 - This document does not apply to ports of call.
- **Lead Agency: NAVFAC**
 - Point of contact: John Lynch
- **Current Document Status:**
 - First Published November 2012
 - Revision currently up for signature



Definitions

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

Definitions

- **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.
- **Level of protection**
 - The degree to which an asset is protected against compromise
- **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
- **Restricted Area**
 - An area under military jurisdiction in which special security measures are employed to prevent unauthorized entry.

Policy Based 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.
- **Department of Defense**
 - DoD 5200.8-R: Requires DoD Components to determine the necessary access control based on the requirements of a developed physical security program. Establishes procedures and responsibilities for security of weapon systems, including platforms, such as armored fighting vehicles, fixed- and rotary-wing aircraft, and ships in port.
 - DoDD 2000.12: Provides DoD policies for ATRP and assigns responsibilities for implementing the procedures for the DoD ATRP Program
 - DoDI 2000.16: This instruction requires the installation or activity Commanding Officer to define the access control measures at installations.
 - DoDM 5200.08 Vol 3: Establishes DoD access control policy and the minimum DoD security standards for controlling entry onto DoD installations.

Policy Based Requirements

- **Geographic Combatant Commander (GCC)**
 - 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.
- **Department of the Navy**
 - OPNAVINST 5530.14E: Provides the physical security requirements for the installation and restricted area access control. Provides Waterfront security requirements and waterway access control.
 - NTPP 3-07.2.3: Provides guidance for the physical security for Naval Installations to include Restricted Areas and Waterfront Security.

OPNAVINST 5530.14E NAVY PHYSICAL SECURITY AND LAW ENFORCEMENT PROGRAM TABLE 2-3

Priority	Asset	Security Measures (Accumulative from low to high)
A (Highest)	SSBN	Per SECNAVINST S8126.1 and at non-home ports (Highest) where cumulative asset in port time exceeds more than 120 days in a calendar year, use water barriers to stop small boat threat.
B (High)	Carriers, other submarines, and large-deck amphibious	<ul style="list-style-type: none">— Electronic water/waterside security system (closed-circuit television, associated alarms, surface craft or swimmer detection, underwater detection) .— Use water barrier(s) to prevent direct unchallenged access from small boat attacks.— Submarines and aircraft carriers shall receive an armed escort during ingress and egress.
C (Medium)	Surface combatants, other auxiliary, MSC SSS, ammunition ships, mine Warfare	<ul style="list-style-type: none">— Establish security zone with the USCG, where possible.— Use water barrier(s) where appropriate amphibious, and/or practical, harbor patrol boat (s) with bullhorn, night vision device, spotlight, marine flares, and lethal and non-lethal weapons.— Arrange patrol boat backup support from harbor operations, USCG, or other (tenant boat units, small craft from ships) .
D (Low)	Patrol coastal MSC SSS (reduced Operational status) , pier facilities	<ul style="list-style-type: none">— Adjacent landside security (patrols, surveillance, pier access control) , no special requirement in waterways— Identify restricted area waterway(s) with buoys and signs.

Policy Based Requirements

- **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 required by OPNAVINST 5530.14E, Installation Commanding Officers shall ensure that Physical Security surveys of their activities are conducted annually and the results addressed as a part of a command review and assessment program.**
 - Surveys will serve to update the command on what needs protecting, what security measures are in effect, what needs improvement, and what the security priorities are.
- **The installation AT plan and Physical Security survey reflects the foundation for security requirements determination. Installation specific requirements need to be factored into all capital improvement initiatives.**

Considerations

- **The objective of waterfront security system is to secure the waterfront from unauthorized access and detect and neutralize threats while minimizing impacts to port operations and the environment. Design considerations are:**
 - **Security**
 - **Port Operations**
 - **Safety**
 - **Appearance**
 - **Environmental impact**

Considerations

- **Security**

- Installations should focus first on threats at the first line of defense – the installation perimeter.
- The first priority of a waterside security system is to establish and 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

- **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.

Considerations

- **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.

- **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.

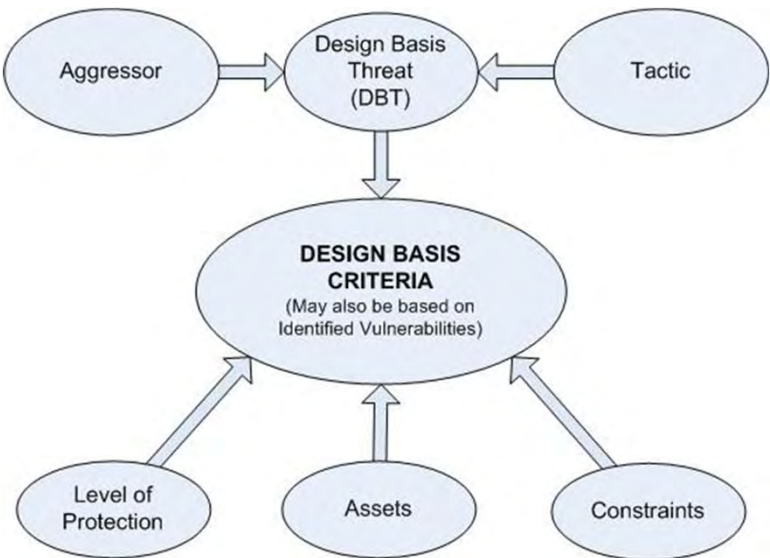
- **Environmental Impact**

- 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.

Establish Requirements

- 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.
- For some waterfront assets, the minimum security measures are established by policy or regulation.

Key Inputs



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.

Establish Requirements

- Future Development Plans
 - 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.
- 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.

Key Inputs

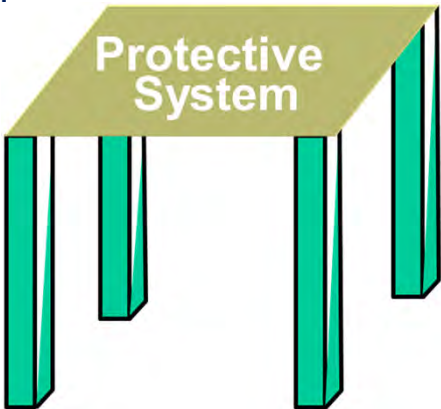
- **Design Basis Threat (DBT)**
 - The DBT links aggressor with tactic.
 - It includes the aggressor tactics and the associated weapons such as explosives, tools, and agents.
 - The DBT must be determined to plan and design the protective measures required to protect the assets from compromise.
- **Waterfront may have a DBT for the landside and different DBT for the waterside. For example :**
 - Landside: placed or stationary vehicle bomb consisting of Type II explosive.
 - Waterside: 2,000 lb. (907 kg) powerboat containing a Type I explosive.

Design Strategy

- All protective measures/systems 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 (aka security-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.

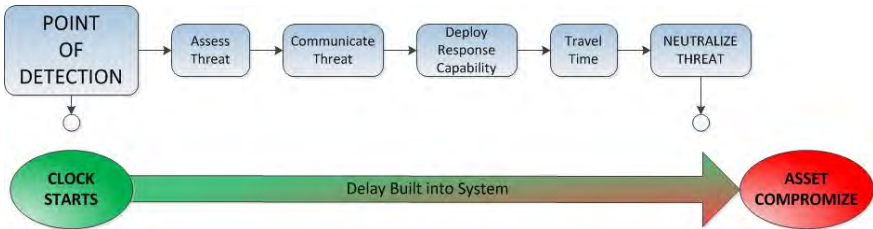
Design Strategy – Protective Systems

- An integrated system of protective measures and operational procedures designed to protect assets against threats to specific level of protection.
 - Sitework Elements
 - Building Elements
 - Equipment
 - Manpower/ Operational Procedures
- Components should complement each other and correct for vulnerabilities.
- Components of the system should be coordinated to minimize gaps in responsibilities and performance.

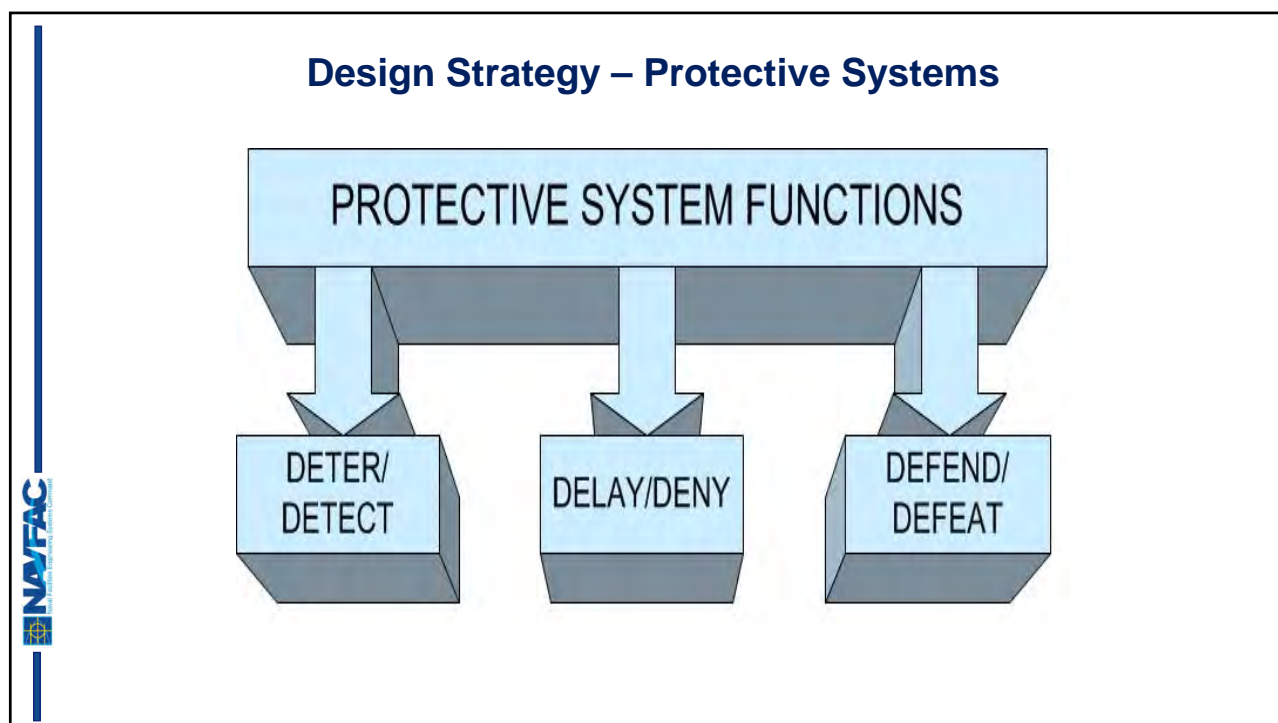


Design Strategy – Protective Systems Timeline

- 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.
 - This is accomplished 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.



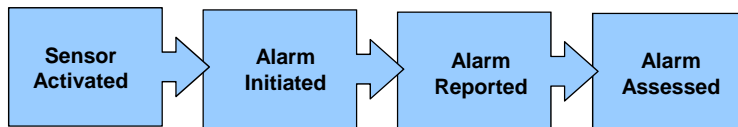
- This presents a challenge on the waterside due to limited distances between waterfront assets and unrestricted waterways.



Design Strategy – Protective Systems - Deter

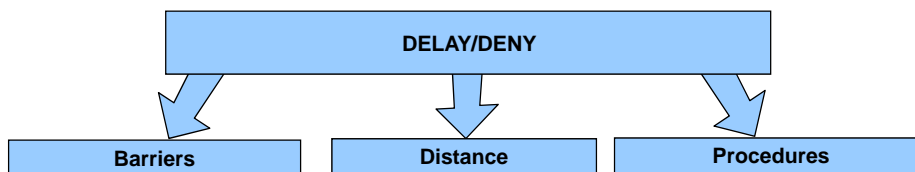
- The deter function is when the potential aggressor perceives that a protection system may be too difficult to defeat or the risk of any attempted attack would outweigh any potential benefit.
 - The deter function cannot be measured or relied upon with regards to 'time'.
 - Deter has no benefit if the aggressor intends to attack despite the protection measures in place.
 - Deter is considered a secondary function and should not be evaluated when determining the elements of a protective systems.

Design Strategy – Protective Systems - Detect



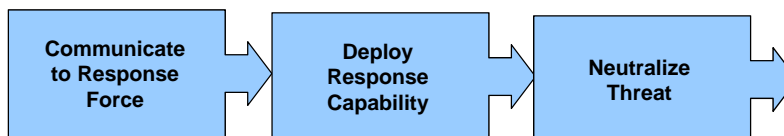
- Detect the presence of an aggressor
- Assess the validity of the threat
- Communicate the appropriate information to the response capability

Design Strategy – Protective Systems – Delay/Deny



- Delay is the TIME it takes for the aggressor to get from the point of detection to the point where the response capability interrupts or neutralizes the aggressor.
- Provide protective measures intended to hinder aggressor from reaching asset before response capability/forces can intervene.
- Delay must be synchronized with security force response time to ensure assets are protected from compromise.

Design Strategy – Protective Systems – Defend/Defeat



- Sometimes referred to as response, is the TIME it takes for the response capability to delay or defeat a threat. This includes:

- Communication
- Mobilization
- Travel time
- Tactics
- Security Police
- Military Police
- Military Working Dogs
- Rapid Response Force
- Passive Barriers
- Active Barriers
- Waterfront Barriers

Design Strategy – Protective Systems - SID

- **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**

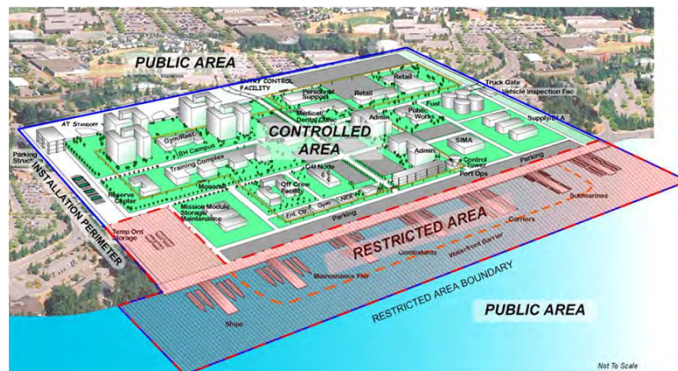
- The area within the installation's controlled perimeter where authorized personnel have access. Installations are considered controlled areas for the purposes of national defense.

- **Restricted Area**

- A defined area established to protect critical assets by providing a higher level of security than that afforded elsewhere on the installation.

Design Strategy – Protective Systems - SID

- An installation must establish clearly defined sequence of boundaries and access control points 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.



Security/Defense in Depth (SID/DID)

- Combination of layered and complementary security controls sufficient to deter, detect, and document unauthorized entry and movement within the installation and/or facility and the ability to delay/deny and defend/defeat/respond with force.
 - Incorporating SID ensures that no single point of failure will render assets vulnerable to compromise.
 - SID strategy should establish a clearly defined sequence of boundaries and zones through which aggressors must pass to reach the protected asset.
 - Security measures and access controls should increase as aggressors approach the protected asset and transition from lower to higher security zones.

Establish Perimeter

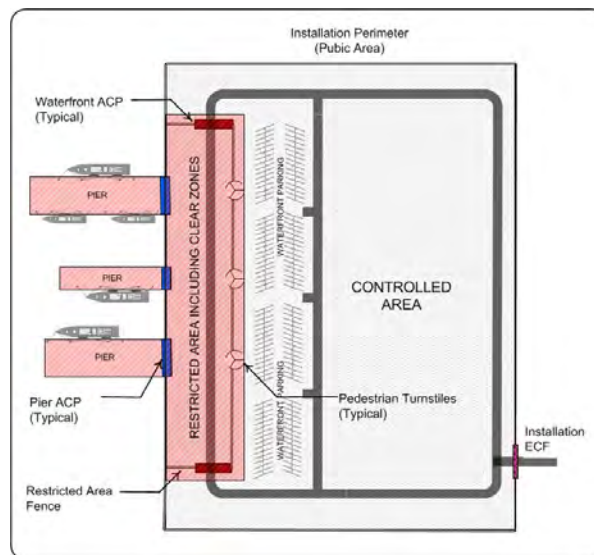
- To protect waterfront assets from unauthorized access, it is important to establish and maintain a defined perimeter.
- Before a person proceeds into the waterfront restricted area, they must perceive the area boundary and understand the consequences associated with crossing it.
- Landside
- Waterside
- 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.

LANDSIDE

• GENERAL DESIGN STRATEGY

- The general design strategy for the landside is to establish and maintain defense in depth through the application of standoff, barriers, access control, security zones, and operational procedures. 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 protective measures.
 - **Controlled Area:** The area within the installation's controlled perimeter where authorized personnel have access.
- 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.

LANDSIDE: Security Zones



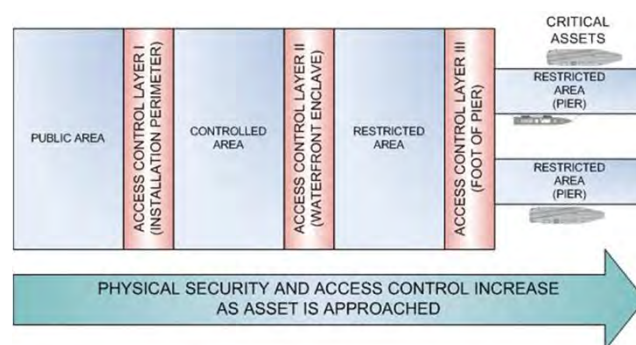
Design Strategy – Landside Perimeter

- **Landside Perimeter**
 - The landside perimeter of the enclave may consist of fences, walls, buildings, 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.

LANDSIDE ACCESS CONTROL

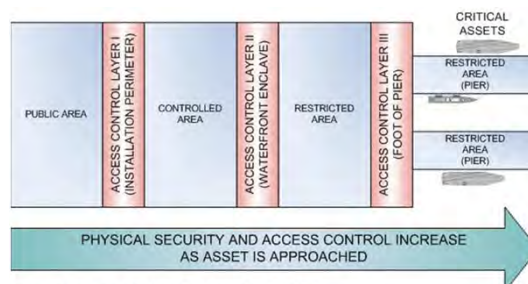
- Design of the access control system begins at the Installation's perimeter and access control points.
- Vehicles and personnel travel from one zone to another through the system to reach the restricted area.
- Physical security measures, including access control must increase from lower to higher security 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

LANDSIDE: Access Control Layers



- **LAYER I: INSTALLATION PERIMETER**
 - The Installation's controlled perimeter, access control points, and the related security procedures must be considered when determining the design basis threat and the resulting protective measures for the waterfront.

LANDSIDE: Access Control Layers



- **LAYER II: WATERFRONT ENCLAVE**

- Coordinate requirements with supported command, ATO, and security personnel.
- The access control and protection features for Layer II should be determined based on asset to be protected, DBT, and desired LOP.
- 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.

LANDSIDE: Access Control Layers

- **LAYER II: Vehicle Access Control Points**

- Design ACPs in accordance with UFC 4-022-01
- Minimize the number of vehicle ACPs into the waterfront to reduce operational requirement.
- Provide a minimum of two gates for flexibility.



LANDSIDE: Access Control Layers

- **LAYER II: Pedestrian Access Control Points**
 - When pedestrian access control is required, ensure that proper sidewalk and safety provisions direct pedestrian traffic to the ACP separate from vehicular traffic.
- **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.

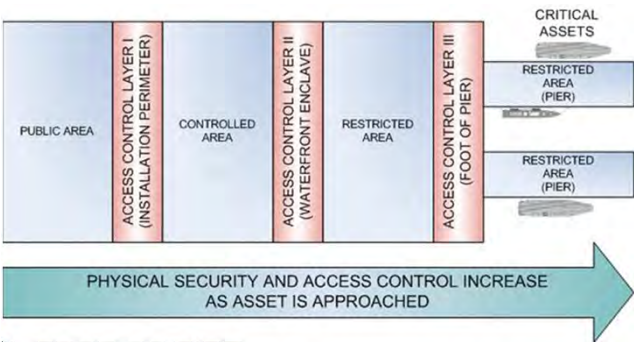


LANDSIDE: Access Control Layers

- **Layer II: Vehicle Barriers**
 - When pedestrian access control is required, ensure that proper sidewalk and safety provisions direct pedestrian traffic to the ACP separate from vehicular traffic.
 - 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.

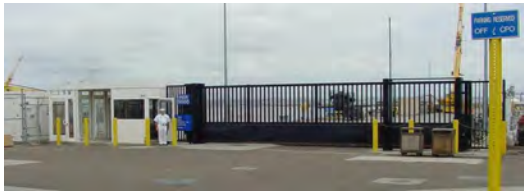
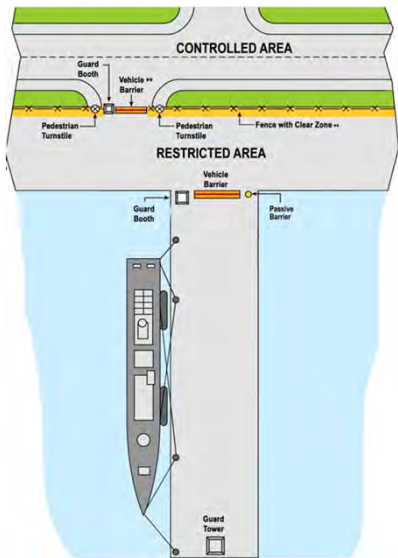


LANDSIDE: Access Control Layers



- **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.

LANDSIDE: Access Control



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

LANDSIDE: Access Control Layers

- **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.



LANDSIDE: Access Control Layers

- **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.
 - At a minimum, provide ballistic protection equivalent to Underwriters Laboratories (UL) 752 Level 3 (low threat severity) for all guard facilities. Consult with COCOM/Service policy if protection from a higher threat severity is required.
- Location and elevation of the guard booth must enhance the ability of security personnel to process vehicles and personnel.
- Design 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.



Design Strategy - Signage

- **Signage**
 - **Access Control Point (ACP) Signage.**
 - Post reflective signs at all waterfront vehicle and pedestrian ACPs
 - **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.
 - **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.



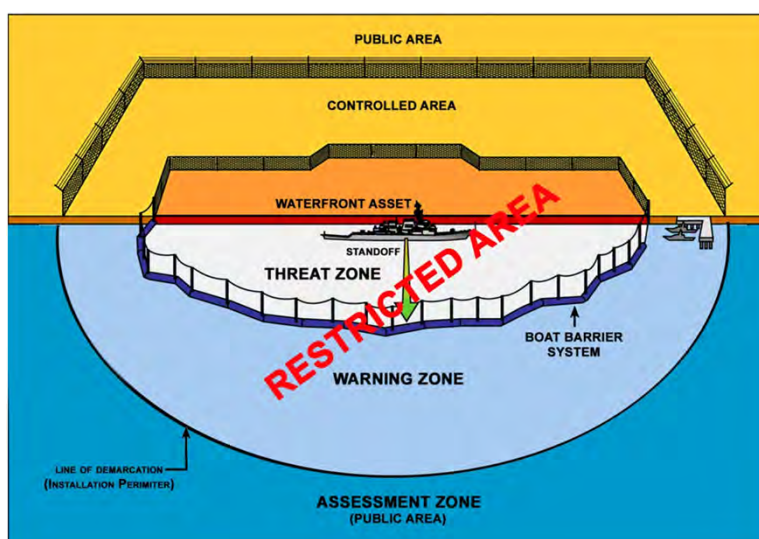
Waterfront Attack



Waterside: General Design Strategy

- Prevent waterfront attack by defining a perimeter and applying the defense in depth concept.
- Establish security zones from the high water mark to the waterside installation perimeter and beyond. 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 Installation Commander defines the limits of the Threat and Warning zones.

Waterfront Zones



Design Strategy – Waterside Perimeter

- **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.

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.
 - At a minimum, provide ballistic protection equivalent to Underwriters Laboratories (UL) 752 Level 3 (low threat severity) for all guard facilities. Consult with COCOM/Service policy if protection from a higher threat severity is required.
- 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.
 - 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.

GUARD TOWERS

- 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.
- Size the overhang to reduce glare on glazing and provide cover from the elements for security personnel.



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 dependent on location of threat relative to protected assets.

ELECTRONIC HARBOR SECURITY SYSTEMS (EHSS)

- **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.

- **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.

ELECTRONIC HARBOR SECURITY SYSTEMS (EHSS)

Surface Detection



ELECTRONIC HARBOR SECURITY SYSTEMS (EHSS)

• Video Imaging

- Imaging system is a collection of cameras, recorders, switches, keyboards, and monitors that allow assessment and recording of security events.
- 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.
- When integrated with video analytics the imaging system can have a detection capability.
- The basic imaging element consists of two cameras. 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.

ELECTRONIC HARBOR SECURITY SYSTEMS (EHSS)

• 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 Environmental permitting has been obtained to ensure conformance with the “Marine Mammal Protection Act (MMPA).”

• 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).
- An environmental assessment must be completed prior to the deployment of any sonar transponders.



ELECTRONIC HARBOR SECURITY SYSTEMS (EHSS)

• 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.

• 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.

ELECTRONIC HARBOR SECURITY SYSTEMS (EHSS)

• 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.

• 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.

ELECTRONIC HARBOR SECURITY SYSTEMS (EHSS)

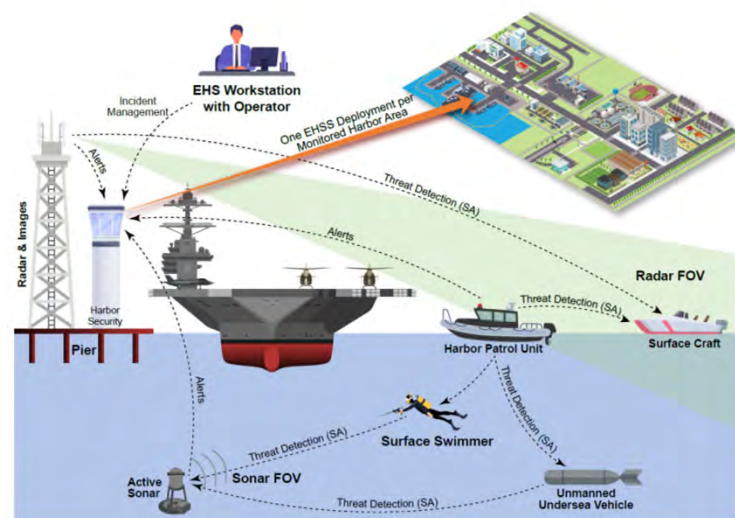
- **Backup Power**
 - EHSS systems require a backup generator. The supporting generator is normally located pier side in a weather-protected location or enclosure. Reserve a minimum of 8 foot 6 inch (259 cm) space x 3 foot 6 inch (107 cm) space for generator and associated controls. Coordinate actual 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
- **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.
- **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.

ELECTRONIC HARBOR SECURITY SYSTEMS (EHSS)

- **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
Naval Information Warfare Center
53560 Hull Street
San Diego, CA 92152-5001
EHSS_Action@us.navy.mil
(619) 553-5033 voice**

ELECTRONIC HARBOR SECURITY SYSTEMS (EHSS)



Waterside: Design Strategy

- **Waterside Restricted Area**
 - 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.

Booms for Setting Boundaries

Line of Demarcation



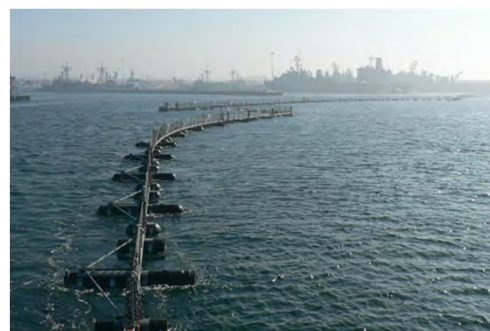
NAVFAC

Waterside: Design Strategy

- **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.

- 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.



NAVFAC

Barriers



Dunlop Barrier



Barriers to Stop Rapidly Moving Boats



Port Security Barrier (PSB)



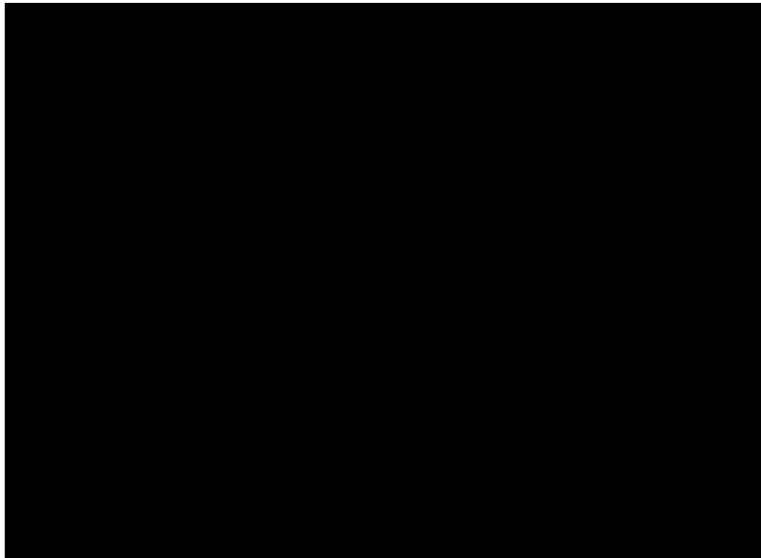
Port Security Barrier (PSB)



Port Security Barrier (PSB)



Port Security Barrier (PSB)



DoD Waterfronts – NAS North Island





DoD Waterfronts – NAVSTA Norfolk



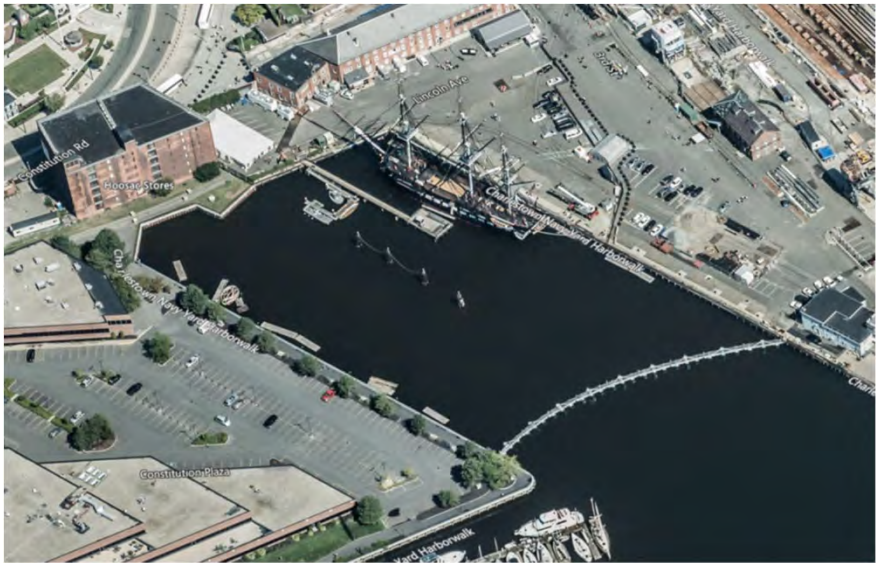
DoD Waterfronts – NAVSTA Mayport



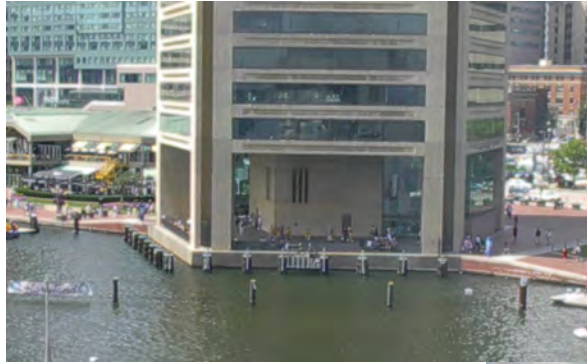
DoD Waterfronts – NAVSTA Yokosuka



DoD Waterfronts – USS Constitution



Fixed Waterfront Barriers



Boat Barrier Systems

For more information on boat barrier systems and related products contact:

**Water Barrier Program Management Office
Naval Sea Systems Command, PMS 300
1333 Isaac Hull Avenue, SE
Washington Navy Yard DC 20376-0005**



LANDSIDE: Security Lighting

- **Security Lighting**
 - Security lighting aids in the detection of aggressors and assists personnel in the assessment and response to potential threats.
 - Design lighting in accordance with UFC 3-530-01.
 - 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.
- **Perimeter Lighting**
 - 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.

LANDSIDE: Security Lighting

- **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.
- **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.

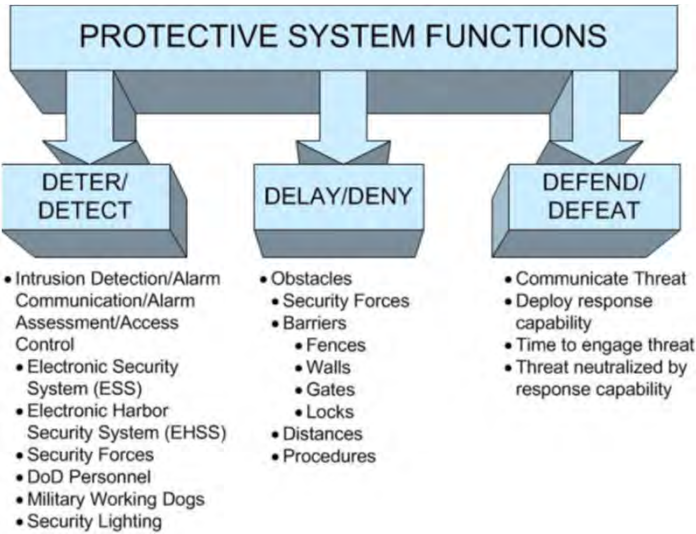
WATERFRONT: Security Lighting

- In general, high mast lighting provided for waterfront operations supply adequate illuminance for security requirements.
- Provide full cut-off or fully shielded fixtures to limit glare.
- 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.

WATERFRONT: Security Lighting

- **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.
- **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.
- **Under deck Lighting**
 - Dedicated luminaires located beneath the pier are not normally required and are discouraged due to limited benefit, high installation cost, maintenance cost and environmental issues.

WATERFRONT PROTECTIVE SYSTEMS



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

Summary

- Key to Waterfront protection is keeping threat away from assets
- Protect the waterside and the landside
- Detection on the waterside may be both over and under water
- Maintaining controlled area requires some form of barriers
- Response is critical

QUESTIONS?



Thanks!

NAVFAC PDCC:

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

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

