



Guidelines to Harden Vessels

(Second edition 2022)



Issued by the

Oil Companies International Marine Forum

29 Queen Anne's Gate

London SW1H 9BU

United Kingdom

Telephone: +44 (0)20 7654 1200

Email enquiries@ocimf.org

www.ocimf.org

Second edition 2022

© Oil Companies International Marine Forum

Illustrations in appendix C supplied with courtesy of the author Mr W Harrison

The Oil Companies International Marine Forum (OCIMF)

Founded in 1970, the Oil Companies International Marine Forum (OCIMF) is a voluntary association of oil companies having an interest in the shipment and terminalling of crude oil, oil products, petrochemicals and gas, and includes companies engaged in offshore marine operations supporting oil and gas exploration, development and production.

Our vision is a global marine industry that causes no harm to people or the environment.

Our mission is to lead the global marine industry in the promotion of safe and environmentally responsible transportation of crude oil, oil products, petrochemicals and gas, and to drive the same values in the management of related offshore marine operations. We do this by developing best practices in the design, construction and safe operation of tankers, barges and offshore vessels and their interfaces with terminals and considering human factors in everything we do.

Terms of Use

While the advice given in this information paper ("Paper") has been developed using the best information currently available, it is intended purely as guidance to be used at the user's own risk. No responsibility is accepted by the Oil Companies International Marine Forum ("OCIMF"), the membership of OCIMF or by any person, firm, corporation or organisation (who or which has been in any way concerned with the furnishing of information or data, the compilation or any translation, publishing or supply of the Paper) for the accuracy of any information or advice given in the Paper or any omission from the Paper or for any consequence whatsoever resulting directly or indirectly from compliance with, or adoption of or reliance on guidance contained in the Paper even if caused by a failure to exercise reasonable care.

Contents

Abbreviations	iv
Glossary	v
1 Introduction	1
1.1 Assessing threat and risk, detecting threats, defending the vessel	1
1.2 Scope	1
1.3 Layers of defence	1
2 Threat assessment	3
3 Risk assessment	4
3.1 Regional specific risks and advice	4
4 Threat detection	5
4.1 Tracking/monitoring and reporting	5
4.2 Radar	5
4.3 Automatic Identification System	5
4.4 Searchlights/lighting	5
4.5 Closed Circuit Television	6
4.6 Motion sensors	6
4.7 Mirrors	7
4.8 Watchkeepers	7
4.9 Pattern of life	7
5 First layer of defence	8
5.1 Preventing access to the vessel while at sea or offshore	8
5.2 Managing access to the vessel while in port or at anchor	10
5.3 Emerging technologies	11
6 Second layer of defence	12
6.1 Secondary doors	12
6.2 Monitoring	12
6.3 Door and door jambs	12
6.4 Windows	13
6.5 High strength glue	13
6.6 Staircases, hatches, vents and ladders	13
6.7 Pipework	13
7 Third layer of defence	14
7.1 Internal smoke cannon, strobe lights and noise makers	14
7.2 Lift shafts	14
7.3 Safe muster points and/or citadels	14

8	Vessel control and safety	16
8.1	Control of services	16
8.2	Security of fixed fire suppression systems	16
8.3	Navigation and engine control from the citadel – duplicate system	16
Appendix A	Designing security into new-build vessels	17
Appendix B	Training	19
Appendix C	Vessel Hardening Plan	21

Abbreviations

AIS	Automatic Identification System
BMP	Best Management Practice
CCTV	Closed Circuit Television
ECDIS	Electronic Chart Display and Information System
ECR	Engine Control Room
GPS	Global Positioning System
GRP	Glass Reinforced Plastic
HQ	Headquarters
IMO	International Maritime Organization
ISPS	International Ship and Port Facility Security (Code)
LRIT	Long Range Identification and Tracking
OCIMF	Oil Companies International Marine Forum
OOW	Officer of the Watch
PIR	Passive Infrared
PMSC	Private Military and Security Contractor
PPE	Personal Protective Equipment
RPG	Rocket Propelled Grenade
SATCOM	Satellite Communications
SOLAS	International Convention for the Safety of Life at Sea
SOP	Standard Operating Procedure
SSAS	Ship Security Alert System
SSP	Ship Security Plan
STCW	International Convention on Standards of Training, Certification and Watchkeeping for Seafarers
UKMTO	United Kingdom Maritime Trade Operations
VHF	Very High Frequency
VHP	Vessel Hardening Plan
WBIED	Water-borne Improvised Explosive Device

Glossary

Best Management Practice Methods determined to be the most effective and practical means by which companies and seafarers can detect, avoid, delay and report external threats to safety.

Best practice OCIMF views this as a method of working or procedure to aspire to as a part of continuous improvement.

Guidance Provision of advice or information by OCIMF.

Recommendation OCIMF supports and endorses a particular method of working or procedure.

Risk A measure of the likelihood that the harm from a particular threat will occur, taking into account the possible severity of the harm.

Risk assessment A systematic procedure for measuring and managing the likelihood that the harm from a particular threat will occur.

Ship Security Plan A plan developed to ensure the application of measures on board the ship designed to protect persons on board, cargo, cargo transport units, ship's stores or the ship from the risks of a security incident.

Threat The intent to cause damage or injury. Maritime threat is formed of capability, opportunity and intent.

Threat assessment The identification and evaluation of external factors that could intend to cause damage or injury, thereby adversely affecting the safe operation of a vessel.

Vessel hardening The physical measures taken to improve a vessel's security integrity.

Vessel Hardening Plan A plan to provide guidance to onboard personnel for equipment use, procedures and applicable points related to vessel's hardening.

1 Introduction

1.1 Assessing threat and risk, detecting threats, defending the vessel

This information paper brings together best practice both on board a vessel and for owners, operators, managers, Masters, crew, naval architects and shipyards, so everyone has the tools they need to make an informed decision about security measures for their fleet. The paper does not include guidance on general navigation practices or on implementation of the International Ship and Port Facility Security (ISPS) Code.

Different vessel types and sizes may need different security procedures, and some in specific trades or trading patterns may need additional measures not covered here. It is recommended all companies complete a thorough security threat and risk assessment, identify and implement mitigation measures.

Vessel hardening is the physical measures taken to improve a vessel's security integrity. Any vessel hardening measures adopted should not compromise the vessel's compliance with the International Convention for the Safety of Life at Sea (SOLAS) regulations. Escape routes should be kept clear and nothing should interfere with the crew's ability to respond to non-security related emergencies.

This paper complements the OCIMF information paper *Ship Security – Bridge Vulnerability Study* and should be read alongside it.

1.2 Scope

Based on lessons learnt from developing best management practice, this paper recommends a layered defence methodology to aid in the mitigation of the risks posed by identified threats. Although the focus is on vessels when underway, measures are examined for vessels at anchor and alongside.

1.3 Layers of defence

The layers of defence are suggested and these are described in detail, with information on additional hardening measures, training and planning, in the appendices.

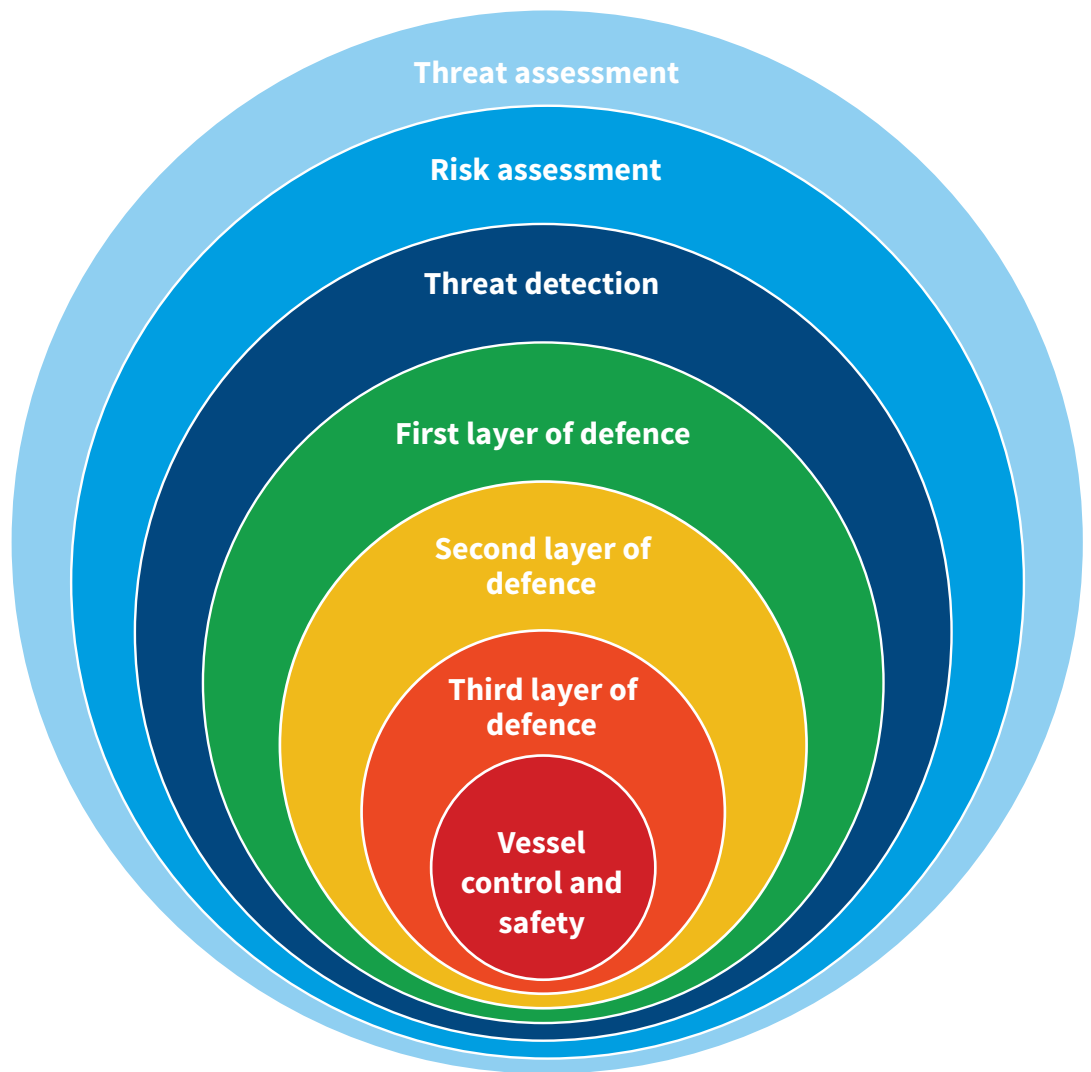


Figure 1.1: *Layers of defence*

2 Threat assessment

Threat assessment is the identification and evaluation of external factors that could intend to cause damage or injury, thereby adversely affecting the safe operation of a vessel. The threat assessment must include all security threats. These can be broadly divided into two categories: physical and virtual.

Physical security threats may come from the air, land or sea. They are more easily identified than virtual security threats.

Virtual security threats may take the form of cyber-attacks on electronic hardware and software (computer and control systems) and can disable vessel operating systems. They are harder to identify than physical security threats. It is recommended that vessels and companies have procedures covering all aspects of cyber security. Cyber security awareness should be an integral part of any training programme.



Figure 2.1: *The threat triangle*

Figure 2.1 illustrates the threat triangle. Capability means attackers have the physical means to conduct an attack. Intent is demonstrated by continued attacks. Opportunity is what is mitigated by the company, ship and crew through application of the measures described.

If one side of the triangle is removed, then risk is minimised. The company/Master cannot influence either capability or intent, therefore mitigation measures focus on minimising opportunity.

3 Risk assessment

Risk assessment is a systematic procedure for measuring and managing the likelihood that the harm from a particular threat will occur. It is an integral part of voyage planning within a safety management system. The risk assessment should identify measures for prevention, mitigation and recovery, which will mean combining adherence to statutory regulations with supplementary measures.

It is recommended that the completed company risk assessment is subject to regular review. The review would question whether:

- New risks are identified and existing risks confirmed or removed.
- It is practical and realistic.
- The adopted self-protection measures reduce the identified risks.

It is recommended that the company's risk assessment is also updated when additional self-protection measures are introduced. The updated risk assessment would identify residual risk which would need to be understood and accepted by senior management.

It is recommended a Vessel Hardening Plan (VHP) is created, based on the company risk assessment. The VHP should outline what mitigation measures are needed to reduce the risk to As Low as Reasonably Practicable (ALARP). It could be a stand-alone document, be incorporated into company procedures or be contained within the Ship Security Plan (SSP). An example of a VHP is given in appendix C.

3.1 Regional specific risks and advice

A number of regional coordination centres offer guidance for their geographical areas. Regional guidance gives area-specific advice and should be consulted at the start of any risk assessment or voyage preparation. National and industry guidance, together with the security charts produced by UKHO, contain the contact details of authorities.

4 Threat detection

The detection of any threat may be intelligence led. There are several commercially available intelligence services offering near real time analysis of maritime security threats. Vessel operators can use this information to update their fleet immediately about threats in the areas where they are operating. The following are recommended to aid continuous improvement:

- Regular security drills and training.
- Lessons learnt are captured and communicated.

4.1 Tracking/monitoring and reporting

If intruders board a vessel they may target vessel systems and, in particular, communications antennae. Technically capable intruders have been known to disable aerials including Automatic Identification System (AIS) and Long Range Identification and Tracking (LRIT). Companies may consider an independent fleet tracking system; several are available. It is important that vessels regularly report their position to regional authorities. Factors to consider include:

- How much redundancy the system has.
- Whether it is stand-alone or relies on the power and antennae of existing on-board communication systems.

4.2 Radar

Consider positioning the radar antenna in a way that reduces or eliminates blind sectors caused by the superstructure. Where it is not possible to eliminate blind sectors, extra radars, such as stern facing radars, could be fitted to give all-round coverage. Specialist software can help analyse sea clutter to identify small objects. Standard X-Band radar sets are sometimes unable to pick up small craft especially if their hulls are made of Glass Reinforced Plastic (GRP) or wood. As technologies improve, companies may want to install new equipment or upgrade what they already have. For example, fused radar pictures can provide a single overview of all available data feeds.

4.3 Automatic Identification System

Consider the position of the AIS aerial to give all-round coverage maximising situational awareness.

4.4 Searchlights/lighting

Consider fitting searchlights in places which offer all-round visibility. A single searchlight will not be able to give 360-degree coverage. As well as offering enhanced detection capabilities, searchlights can also deter potential intruders.

When offshore or at port a vessel's lighting capabilities should enable the crew to detect approaches and possible security breaches on both the shore and seaward sides. Gangways and access points should be adequately lit so approaching personnel can be identified before they reach the point of embarking. When considering the positioning of lights on a vessel it is important to make sure the lighting does not create areas of dead light (excessive shadow areas) that can conceal small craft and intruders. Passive Infrared (PIR) activated floodlights on the periphery of the vessel make sure the lights come on even if attackers are not spotted in advance. These should be placed to avoid interference with other sensors.

When underway, vessels should minimise external lighting, except for mandatory navigation lights. This can stop attackers establishing points of reference when approaching a vessel. Turning on the vessel's lights as attackers approach could also alert them that they have been seen and may encourage them to call off the attack. Searchlights can be used systematically to probe for suspect craft, illuminating radar contacts when possible. With the highest-power

xenon light sources, the suspect craft can be fully illuminated and identified quickly, so any necessary evasive action can be taken. High-power searchlight beams acting as a non-lethal deterrence can also disorientate attackers by leaving them temporarily unable to see.

4.5 Closed Circuit Television

The installation of Closed Circuit Television (CCTV) on board offers all-round visibility. To make it even more effective, consideration should be given to:

- Including thermal imaging.
- Having the ability to record and play back, with an extended memory function.
- Having monitors in a central location with repeaters in the cargo control room and, where applicable, a citadel or safe muster point. To monitor any potential intrusion, also consider CCTV in the accommodation block.
- Making camera units discreet or disguised, so they are less likely to be spotted and immobilised if attackers breach on-board security.
- Installing dummy cameras to distract attackers from genuine camera units.
- Making it possible for the CCTV to be monitored remotely, for example by headquarters (HQ)/charterer. This should be balanced against any perceived cyber threat or crew concerns about being 'spied-on' during normal operations.
- Installing software to make sure the last CCTV image is sent to company HQ if the system is disconnected.
- Linking the activation of the Ship Security Alert System (SSAS) to the CCTV to allow remote monitoring from company HQ.
- Building in capacity for upgrades and expansion.

While many vessels have CCTV systems, they are predominantly used for monitoring cargo manifold areas, with some also covering both the bow and stern areas to monitor mooring operations. Consider expanding any existing CCTV coverage to permit the monitoring of key access points or other vulnerable areas. Where there is no existing CCTV coverage at all, it may be possible to install a CCTV system with the required coverage. Some intruders may be knowledgeable about CCTV systems and try to disable cameras.

Consideration may be given to the ability to control and monitor any CCTV system from several different locations, such as the company HQ, the bridge, the engine control room, the cargo control room and the citadel. Recording CCTV footage may help law enforcement agencies to identify and prosecute any intruders. If there is a hijacking, intruders could be in control of the vessel for some time, so recording facilities should be able to cover several days.

CCTV systems can be supplemented by audio devices. These may help alert the Officer of Watch (OOV) to covert attempts to either board the vessel or enter a restricted space. Audio devices might be built in to CCTV cameras or separate. Again, it would be an advantage if there was a way of recording any audio material picked up.

4.6 Motion sensors

Motion sensors, used either vessel-wide or in compartments as part of an integrated intruder detection and alert system, can warn crews of an attempted or actual intrusion/boarding. They should only be used as an extra layer of hardening, and not a primary layer of defence.

Motion sensors detect changes in the local environment; they can be active or passive. Professional advice should be sought on which is best for each vessel.

When designing or retrofitting an integrated intruder detection and alert system on board a vessel, or installing stand-alone motion sensors, think about the location (hazardous areas), type, area covered and alarm outputs along with the other physical hardening measures being deployed as part of the vessel's layered defence. The marine environment should also be considered.

4.7 Mirrors

Carefully placed mirrors can provide an efficient and cost effective way of enhancing security, as well as making navigation safer. Mirrors can eliminate blind spots created by the vessel's crane, for example. Correctly positioned mirrors allow the watchkeeper to have a clear view from the bridge of the vessel's quarters areas, the whole of the stern sector (with overlap) and the propeller wake.

The angle of the mirrors should be adjustable both horizontally and vertically as required for best effect. The housing and construction should be robust enough to withstand all environmental conditions.

4.8 Watchkeepers

Watchkeepers should be alert to all potential threats and the risks they pose. If required, extra lookouts should be placed in areas where full visibility from the bridge is not available. It is important to consider crew fatigue when preparing to transit areas of increased threat.

4.9 Pattern of life

An understanding of usual maritime behaviour in a given area (pattern of life) enables early detection of potential threats. This should be a feature of both the threat and risk assessments.

5 First layer of defence

The first layer of defence is about controlling access to a vessel, whether it is at sea, waiting offshore, at anchor or berthed in a port. Access control falls into two main categories:

- Managing access by legitimate visitors during normal operations.
- Preventing unauthorised access by people who might want to board the vessel for criminal activity, e.g. theft, kidnap, hijack, terrorism, stowing away, etc.

ISPS Code procedures for managing access to a vessel should be followed.

Choose access control measures based on a thorough assessment of the vessel. Several types of equipment are available to help control access. Some can be retrofitted. Others may only be suitable for new-build vessels; these are outlined in appendix A.

Security measures to control access must not compromise the crew's ability to abandon the vessel or manage other emergencies.

Controlling access to a vessel can be divided into:

- Preventing access while at sea or offshore (section 5.1).
- Managing access while in port or at anchor (section 5.2).

While preventing access at sea is mainly about installing physical barriers, managing access in port or at anchor is about combining stringently implemented on-board procedures with physical barriers.

5.1 Preventing access to the vessel while at sea or offshore

Physical barriers for preventing boarding by ladders and grappling hooks include razor wire, GRP spikes and chain link fence (see 5.1.4) around the outside perimeter of the vessel.

When considering which to use, assess the vessel's most vulnerable points. Intruders typically attempt to get access from the lowest point above sea level, which is generally the vessel's stern. The vessel's design might offer other access points. Other vulnerable areas may include:

- Panama and roller lead openings.
- Lifeboat/life raft embarkation areas.
- Hawse pipes.
- Accommodation ladders, pilot ladders and gangway access points.

Physical barriers should be appropriate to the type of vessel. For example, it is not appropriate to install electrified barriers on a tanker.

Vessels designed with a sunken poop deck might need extra protection.

5.1.1 Razor wire

Razor wire is probably the most common barrier. It is relatively cost effective and does not require a lot of space for storage when not in use. It can be used in single or multiple layers and is highly visible. The disadvantages of razor wire are the time taken to rig and de-rig and the risk of minor injury if the correct Personal Protective Equipment (PPE) is not used.

When used it is important to secure razor wire to the vessel properly to stop it being breached.

5.1.2 Spikes

Spikes are another common way of protecting a vessel's perimeter. They usually consist of a number of sharp points, about one metre long, attached to a bar, also about one metre long, mounted outside the vessel's handrails with the points facing outboard. Any intruders risk serious injury if they try to climb over or through them. Spikes can be made of either steel or GRP. The main disadvantage of spikes is the storage space they need when not in use and the time it takes to rig and de-rig them. Permanently fitted spikes could resolve this and it is common to have them hinged so they can be changed from pointing outboard to pointing vertically.

5.1.3 Plastic barriers

Plastic or GRP barriers are designed to fit over the vessel's rails around part or all of the vessel's perimeter and make it difficult for ladders or grapples to hook on. They are rigid and usually 'P' shaped in profile. They are also readily available.

While devices like this are reportedly effective, the disadvantages include:

- Barriers need a considerable amount of storage space when not in use.
- If permanently fitted, they can be damaged in heavy weather, particularly when the vessel is laden.
- If a vessel has 'green water' on deck, its force on the barriers could damage the vessel's rails.
- Barriers may need to be removed during mooring and cargo operations.

Tanker operators should assess how flammable large quantities of plastic or GRP are.

5.1.4 Chain link fencing

A double layer of chain link fencing has been effective where intruders use more aggressive tactics, e.g. Rocket Propelled Grenades (RPG) to either intimidate the crew or disable the vessel for boarding. It is usual to fit chain link fencing around the outer perimeter of the bridge deck using scaffolding poles and clamps. To be most effective, fencing needs to be fitted as far away as possible, horizontally, from the wheelhouse.

While chain link fencing is reportedly effective:

- It is time-consuming to rig and de-rig.
- Clamps can damage the paintwork on the railings, causing corrosion.

5.1.5 Water and foam cannon systems

Water hoses, foam monitors or water cannons may deter or delay intruders trying to board the vessel. It is recommended they are rigged in a fixed position before a vessel enters areas of risk, as adjusting them once a vessel is under threat would leave an operator exposed.

A wide variety of systems is available, including high-pressure water jet systems which can provide any coverage that the company risk assessment says is necessary. Installing a fixed baffle plate at the front of the water jet nozzle can increase coverage.

Other systems include water cannons that deliver water in a sweeping arc, or spray rails that create a curtain of water over the vessel's side. Both can be operated remotely.

Foam can be used but must be in addition to a ship's standard firefighting equipment stock. Foam can be disorientating for perpetrators and makes the deck difficult to walk on. For the same reasons, ships' staff need to be cautious when using foam for security purposes.

5.1.6 Ballast overflow

Ballast overflow is the intentional over-flowing of ballast tanks to create a large volume of water across the deck and vessel's side to hamper intruders attempting to board. Care should be taken to stop too much pressure building up in any compartment.

5.1.7 Propeller arresters

Propeller arresters are designed to foul the propeller and stop the engine of a small boat/speedboat closing on the vessel, preventing the boat from coming alongside and boarding. Evaluate the position of the propeller arresters carefully to avoid any adverse impact on the vessel.

Environmental factors like wind speed and wave height can make propeller arresters less effective.

5.1.8 Protection of rudder trunk

Sterns with open rudder trunks are traditional and still exist on many vessels. Authorities have discovered drugs and stowaways in this void space leading to vessels being detained in port. Authorities found the void space had been accessed from sea level.

A vessel with an open rudder trunk should have ways of preventing unauthorised access. Steel bars or grills covering larger openings are an option. The inspection hatch in the steering gear room can be used to look down into the rudder trunk. If the rudder trunk cannot be protected, consider a stowaway search of the rudder trunk before departure.

5.1.9 Other physical barriers

Sand bags, water barrels, plastic lining for glass to prevent fragmentation and steel plating around vulnerable areas, especially the bridge, can also be considered. For more details, see OCIMF's *Ship Security – Bridge Vulnerability Study* and *Ship Security – Hull Vulnerability Study*.

5.1.10 Guards

5.1.10.1 Unarmed guards

In some parts of the world it may be possible to deploy Private Maritime Security Companies (PMSCs) to protect vessels from piracy. PMSCs should only be deployed after a detailed risk assessment covering all aspects of having them on board. Unarmed guards or security advisors have been used to provide advice to Masters faced with challenging security situations and will ensure the Master is provided with the best advice to harden the vessel. Their presence can also instil confidence in the crew.

5.1.10.2 Armed guards

When considering PMSCs, carry out a risk assessment and crew briefing covering issues such as Flag State requirements for deploying these teams, along with embarking, handling, cleaning and test-firing their weapons. Also check whether:

- There are any Coastal State restrictions for the waters a vessel will enter with an armed PMSC on board.
- The prospective PMSC has had a due diligence audit, with any deficiencies noted and action taken to correct them.
- The PMSC 'Rules for the Use of Force' are fit for purpose and have had a legal review.
- The Standard Operating Procedures (SOPs) of the PMSC have been reviewed to make sure they are in line with the company's own management system.
- The company management system reinforces the Master's overriding authority.
- Local regulation requires military or police forces to embark prior to entering harbour.
- Bonding and stowage of arms and ammunition is required. A bonded stowage is a secure container, locker or compartment where weapons and ammunition are stored as directed by local regulations.

For more information see OCIMF's *Guidance for the Employment of Private Maritime Security Companies*.

5.2 Managing access to the vessel while in port or at anchor

Access control while the vessel is in port or at anchor falls into two main categories:

- Managing legitimate visitors during normal operations.
- Preventing unauthorised people getting access to the vessel for theft, kidnap, hijack or terrorism, or as stowaways.

There are considerable time and resource restraints on the vessel while in port, but the security of the vessel must not be compromised by inadequate application of security procedures.

Managing the access of legitimate visitors, whether under way, at anchor or alongside in port, relies fundamentally on following ISPS procedures. Other measures to consider are outlined in this section.

5.2.1 Point of access

Restrict access to a single point and monitor it at all times. Make sure you have the crew numbers to do this and stay within labour regulations and work/rest hours.

Make sure the point of access is adequately lit and personnel monitoring it are protected from the elements.

5.2.2 Monitoring

5.2.2.1 Point of access

CCTV monitoring of the point of access can let onboard personnel control access remotely, e.g. from inside the accommodation block.

5.2.2.2 Moorings

When a vessel is moored in a fairway or away from berth, the fitting of the following should be considered:

- Access alarms/motion detectors at points of possible access.
- Anti-climb devices on moorings and along ship-side rails.
- CCTV to cover mooring stations and areas of possible access.

5.2.2.3 Restricted areas

Restricted areas are covered in the vessel's SSP and should be monitored. The control of access to restricted areas may be enhanced by using key or combination locks, padlocks, key code pads or door sensor locks. While it may be possible to breach locked doors and get access, this may alert vessel staff and raise the alarm.

In an emergency, shipboard personnel should be able to access and exit the accommodation block and machinery spaces. When berthed alongside, contingency plans should consider how access is granted to firefighting crews and emergency services. This may include identifying key access doors and staff responsible for ensuring they are unlocked.

5.2.3 Visitor control

When berthed, access to the vessel requires careful management. The port authority should be given prior notice of expected visitors/contractors to the vessel. When embarking all visitors should be escorted or given access cards that restrict movement to areas of their business.

5.2.4 Security staff and boats

Local security guards can be employed to supplement the crew. This can be particularly useful in ports where stowaways are known to be a risk. Local guards can monitor the immediate access to the vessel, the jetty and the vessel's offshore side. Where armed guards are available, get legal advice before using them to understand any implications for the Master and the company. On tankers, consider the safety situation should weapons be discharged.

While at anchor, security boats from the vessel or provided by a third party can protect the vessel at locations where hostile boarding is a known risk.

5.3 Emerging technologies

New technologies are available for maritime use. Remote controlled drones, hull-mounted sonars and autonomous underwater vehicles have been proven to be of security value and can help prevent access to a vessel.

6 Second layer of defence

This section gives guidance on measures to prevent or delay access to the accommodation block, vessel's stores and machinery spaces. This may be to stop petty theft, to stop intruders intent on taking control of the vessel and/or taking the crew hostage, or both. This section assumes that, for whatever reason, it has not been possible to stop unauthorised access to the vessel's deck, i.e. the first layer of defence has been breached. When considering new equipment or measures, remember that educating everyone involved in its use is an important part of mitigating risk.

This section covers existing vessels. Guidance for new-build vessels is contained in the appendices.

6.1 Secondary doors

Consider fitting secondary doors to outside or inside access points to the accommodation block and engine room. Existing doors are not routinely secured beyond fitting a padlock, or similar, which is easily breached with a crowbar or hammer. A secondary door, whether it is a single-piece or multiple panel design, confronts an intruder with a barrier they cannot overcome without sophisticated tools or cutting equipment. Doors like this should present a smooth surface to intruders, without handles or locks, and the crew should be able to secure them from the inside. They should also be strong enough to withstand a sustained physical assault with hand-held tools.

If secondary doors are not fitted to the accommodation block, it is recommended that they are fitted to the citadel or safe muster point as part of the third layer of defence. The accommodation doors should then have some way of slowing down access to give the crew time to retreat to the citadel or safe muster point and secure the doors. If the machinery spaces are identified as the citadel, it is important that all access points have secondary doors, including funnel doors and upper deck access doors.

6.2 Monitoring

Vessel operators could consider installing a monitoring system with alarms on all doors or hatches with access to store rooms, CO2 room, accommodation block and engine casing, etc.

6.3 Door and door jambs

Doors and door frames should be hardened and extra locks should be fitted. It is always preferable to make securing and hardening arrangements integral to a vessel's structure rather than using a temporary arrangement. Door jambs, wedge braces and other improvised arrangements can help secure doorways and access points in the absence of other measures. For example:

- Door jambs placed at various points on a door can stop it opening.
- Fabricated door wedge braces can secure doors and strengthen the weakest parts against attack. Wedge braces fit over the door handle and brace against it and the door, preventing the door from being opened. Braces can be as simple as lengths of timber but are generally made from steel tubing and plating.
- Door locking bars can secure doors if there is enough room to install strong enough supports either side of the door frame. Placed properly, these bars protect the door across its whole width on both the lock and hinge side. This gives the best protection against break-in attempts using brute force against the door.
- Scaffold support/shoring props can work where the door is facing a suitable bulkhead or strong point.
- Pallets can in some cases block doors closed and stop them being opened easily.
- Wire strops and turnbuckles can secure hatches and skylights.

6.4 Windows

There is little point in preventing or slowing access to the accommodation block through the doors if intruders can get in by simply breaking a window or porthole. Consider fitting windows or portholes with deadlights or blank covers of the sort usually fitted on upper decks for use in heavy weather.

Windows and portholes can also be fitted with security bars. If fitted to the outside, they need to be welded in place. On some vessels it may be possible to bolt metal grills or bars to the inside of windows or portholes. Whether fitted inside or outside they should be close enough together to stop even the smallest person getting through. When deciding whether or not to fit permanent bars to windows or portholes, consider what effect they could have on crew morale when not in a piracy risk area.

6.5 High strength glue

State-of-the-art bonding material able to withstand over 1.5 tonnes of pull is available for securing metal portholes and grills, and it is specifically designed to attach to any surface on the inside of the vessel superstructure. In an emergency, or when the vessel is out of high-risk areas, the crew can remove the cover from the bonded frame.

6.6 Staircases, hatches, vents and ladders

Outside staircases and ladders can be made difficult to climb by fitting hinged metal plates, which obstruct the stairs and ladders where they pass through each deck. This is only recommended if it does not affect the crew's safety under normal conditions or their ability to deal with non-security emergencies, e.g. accommodation fire.

6.7 Pipework

The vessel's scupper pipes and other external pipework, e.g. fire main or external cable runs, can be used by intruders to scale an accommodation block and gain access to the higher decks and wheelhouse. Two measures to prevent this are:

1. Fitting spikes to pipework or cable runs so they cannot be climbed. These spikes are usually made of galvanised steel and come in various lengths.
2. Installing angled baffle plates at strategic locations.

7 Third layer of defence

If intruders breach the second layer of defence, the measures in this section may deter, disorientate, or slow their progress. They have been developed based on crews' experience of attacks in the Indian Ocean.

7.1 Internal smoke cannon, strobe lights and noise makers

As a final barrier should intruders manage to enter the accommodation block, consider fitting distraction devices, such as internal smoke cannons, strobe lights and noise makers. These can be fitted in either a compartment or alleyway, and activated either remotely or automatically. Once activated, smoke cannons quickly fill the space with non-toxic smoke which, while safe to breath, disorientates everyone in the space. They can be supplemented with strobe lights and/or a loud horn that will increase disorientation.

7.2 Lift shafts

If the vessel has a lift, consider preventing the lift trunking being used to access the engine room. Usually this can only be done by making sure the lift car is stopped and isolated, i.e. deactivated at the vessel's upper deck level, preventing intruders from forcing the lift doors open and using the shaft to access the engine room from above.

Emergency escapes from any lift trunking must allow personnel to get out but stop intruders getting in.

7.3 Safe muster points and/or citadels

A safe muster point is a designated area chosen to provide maximum physical protection to the crew and will be identified during the planning process. If the threat assessment identifies risks that may result in a breach of the hull on or below the waterline, a safe muster point must be identified above the waterline. In many ships, the central stairway may be a safe location as it is protected by the accommodation block and is above the waterline.

Where explosion is a risk, for example the use of Water-borne Improvised Explosive Devices (WBIED) in regions of instability, consideration should be given to the likely path of the blast. The safe muster point should be selected with this in mind.

A citadel is a safe location the vessel's crew can retreat to if other defence layers fail to stop intruders boarding the vessel to take control of it or take the crew hostage.

A citadel offers the most protection for a crew, and getting to it quickly and safely needs to be an important part of any company training plan.

Citadels can range from a single location or room to a larger space, like the accommodation block or machinery space. Whichever option is chosen, it should be big enough for the whole crew plus any extra staff onboard (e.g. a PMSC) to be able to survive there for a reasonable time, e.g. three to five days. Experience from the Indian Ocean suggests the amount of time the crew might have to stay in a citadel varies considerably depending on the vessel's location and the attackers' methods.

A fully functioning citadel must have equipment for two-way communications with company HQ and any nearby naval/law enforcement forces. Communications should include Very High Frequency (VHF) for local area communications and Satellite Communications (SATCOM) for worldwide communications. Ideally, both VHF and SATCOM should have their own power supplies or battery back-up so the crew can use the equipment without using the vessel's main power supply. Also, consider giving the crew the ability to activate smoke and other security systems from the citadel.

Threat awareness and the risk assessment are critical to aid the decision to use a safe muster point or citadel. Emerging threats, such as aerial drone attacks against tankers in 2021, have been shown to be more likely to impact the superstructure.

7.3.1 External water pipes and air conditioning

Crews have been known to stay in the citadel for over 36 hours while intruders attempt to breach it by making it uninhabitable. To make them sustainable, citadels should have bottled water available and air conditioning systems should be shut down. Location should be considered when deciding how much bottled water to make available in the citadel (i.e. more water will be needed in hot climates).

8 Vessel control and safety

Restricting vessel functions (propulsion, lighting, air conditioning, etc.) is a way to impede intruders once they are on board. This section describes how shipboard systems can protect crews against intruders. Given that many vessel control systems can be operated remotely, they may be susceptible to cyber-attack.

8.1 Control of services

A general blackout will bring the whole vessel to a standstill and is an excellent way to disorientate people. On-board electrical switchboards can be rigged to create a blackout safely throughout the vessel without affecting the citadel/safe area.

8.2 Security of fixed fire suppression systems

Consider protecting the remote activation of fixed fire suppression systems to stop intruders being able to use them as a weapon or threat.

8.3 Navigation and engine control from the citadel – duplicate system

When the crew have withdrawn to the citadel they may not be able to navigate by sight or manoeuvre the vessel. To keep command and control of the vessel, and to navigate it safely, they must maintain situational awareness. From the citadel, this is only possible with satellite navigation. A secondary or duplicate navigation system can be installed in the citadel (sometimes referred to as a slave system). Consider:

- Computer systems with navigational programmes connected to a Global Positioning System (GPS) antenna.
- Slave radar display.
- Secondary Electronic Chart Display and Information System (ECDIS).
- Secondary Engine Control Room (ECR) controls.

Appendix A Designing security into new-build vessels

A1 Introduction

Lessons observed from experience in the Gulf of Guinea and Indian Ocean suggest it is possible to be more innovative with security measures when they are incorporated into the design of a new build vessel. When designing and building new vessels, naval architects might consider design and equipment features such as the hull form, the placement of access points, the design of the accommodation block and protection of critical systems.

A2 Core design

A2.1 Hull form

Designs with sunken poop decks present a security weak point.

A2.2 Accommodation block and engine casing

The design of the accommodation block and engine casing can form a primary citadel preventing intruders from getting in. Consider:

- A smooth accommodation block and engine casing, i.e. no staircases, ladders or platforms outside the shell of the accommodation block. Secondary security doors would need to supplement the watertight doors at the upper deck access to the staircases/ladders and other access points to the accommodation block or engine casing.
- Eliminating cable runs, scupper down pipes or other external pipework attached to or near to the outer casing of the accommodation block or engine casing that intruders could use as access points.
- Running staircases, ladders, cable runs or pipework through the internal stairwells. This allows inspection and maintenance and also minimises any damage to living spaces should there be a failure of any kind.

As well as deadlights fitted to the upper deck windows or portholes, security grills or roller-type shutters could be fitted to all other accommodation block windows or portholes. These shutters are fitted to the inside of the window or porthole and retract into the bulkhead lining when not in use. When in use, they can be pulled across the window or porthole and secured in place.

Accommodation blocks designed with these measures in mind, along with the measures outlined in appendix C are well-suited as citadels. The machinery space can act as a secondary citadel, if the accommodation block is breached.

A2.3 Upper deck

Permanent mounts to support anti-RPG chain link fencing have also proved to be useful. These mounts can be integrated into the handrails surrounding the wheelhouse, allowing much quicker rigging and de-rigging of this fencing. During construction, it should be possible to fix mounts to the front of the wheelhouse, providing all-round protection from RPGs. To be effective the mounted fencing should be as far as possible from the wheelhouse. Where mounts are fitted to the front of the wheelhouse, allow for access to these points to rig and de-rig the fencing.

Physical security measures are more easily incorporated into the design and construction of new vessels. Areas where security features have emerged in recent design are:

- The accommodation block. In some cases, the accommodation block becomes the primary citadel.
- No external stairs.
- Deadlights on lower levels – shutters above.
- No external scuppers, pipes or cable runs.
- Internal emergency escape trunking and self-contained ventilation.
- Built in noise generators/fog cannons, CCTV in each alleyway/light and sound alarms.

- Internal doors strengthened from stairways.
- Emergency routes/escape exits/funnel casing doors all strengthened.
- No bridge wing doors to reduce access from the upper deck to the primary conning position.
- Fixed mounting points for chain fences, etc.
- Use of armoured plated glass and blast shields on bridge windows.
- Provision of a secondary conning position within the primary citadel.
- A permanent citadel with independent communications and sensors.
- Secure/hidden antennae built into the superstructure.
- Built-in satellite tracking to enhance company monitoring.
- The use of keypad access or door proximity sensors on internal doors.
- Secondary steel plate doors inside watertight doors.
- Hidden information security and communications systems.

A3 System design

A3.1 Communications and control systems

Intruders are becoming more aware of, and familiar with, vessel communications systems and may try to disable it. It is important the citadel is fitted with an independent communication systems using its own antennae and power supply. Hijackers are likely to destroy satellite aerials at the first opportunity to disrupt communication from/to the vessel. To avoid this, the antennae should be concealed. Consider positioning a secondary aerial system inside the citadel, in case the main aerial system is destroyed.

A3.2 Ship Security Alert System

The Ship Security Alert System (SSAS) is an ISPS requirement. SSAS alerts can be sent to any destination via SATCOM including regional coordination centres, a national security organisation, the vessel owner or any other third party organisation. Any or all of these can then take action in line with set procedures.

The procedure for SSAS ought to include a duress word. Automated camera systems can be activated when the SSAS alert is sent. Any modification to an SSAS unit needs Class approval. The installation of a second set of activation buttons close to the SSAS unit's activation point might be considered to avoid any modification to the existing SSAS unit.

A3.3 Geo-fencing

A geo-fence is a virtual perimeter for a real-world geographic area. A geo-fence can be generated dynamically (i.e. a radius around a fixed point) or be a pre-defined set of boundaries (for example a nation's territorial waters).

When the location-aware device enters or exits an area that has been bounded by a geo-fence, a notification is generated that contains information about the location of the device. This notification can be sent to another device, e.g. an email account, mobile phone or electronic map. Once this information is received, action can be taken. For example, if a vessel deviates from its intended route by more than five nautical miles, the action might be to contact the vessel to make sure operations are normal.

Any security measures fitted to a new or existing vessel should be tested regularly so that they are available on entering or crossing areas with a defined or emerging security threat. It is recommended to include and record testing in the vessel's maintenance system.

Appendix B Training

B1 Training

Security training for crew and shore based personnel is core if security measures are to be effective. The training recommendations given here are in addition to the base requirements contained within the ISPS Code and International convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW). The correct and thorough implementation of the ISPS Code's training and drill requirements form the foundation of an operator's security training programme and should be developed in to a training strategy for both fleet and shore based personnel.

Many companies have introduced behaviour based safety systems that address unsafe or questionable behaviours before they lead to a near misses or actual unwanted events. Security is often omitted or overshadowed in these programmes as the spotlight is solely shone on safety related behaviours. Including security behaviours within these programmes is vital in influencing crew members' thinking and behaviours regarding security of their own vessel and the awareness of potential security weaknesses. Crew members should be equipped with the tools to help them identify any security related deficiencies which need to be addressed. Hardening of a vessel against intruders begins with a knowable well trained crew who understand the current security situation and can take proactive measures to counteract these threats. Operators are encouraged to reassess their behaviour based safety systems with the aim of including security related behaviours.

Training is an essential part of maritime operations and, if conducted regularly with agreed objectives, will ensure management and crews are best prepared.

Effective training will ensure vessel crews are adequately prepared for any possible security threat scenario and understand the prevailing threats in their regions of operation. Operators should ensure all their shore based personnel have a basic understanding of the security threats that face the vessels in their fleet.

All training development must align with company policy.

When developing a security training plan the following topics should be considered.

B1.1 Company

- Briefing the sequence of events and expected tactics employed in a typical piracy attack for the region of operation. This should include examples of recent incidents and lessons identified.
- Ensure shore based personnel complete training in crisis management, including family liaison, trauma support, kidnap and ransom procedures. Consider integrating specialist hostage negotiators and trained welfare support staff into company exercises.
- Brief crews on how the company would react to a piracy event including the support mechanisms available for crew member's families.
- Brief on how to behave in the event of being taken hostage by maritime criminals and the psychological effects this is likely to have on crew members.
- Implement data security awareness for fleet and shore based staff.

B1.2 Company Security Officer

- Creating region specific briefings on the current security threats to the vessel in port and underway.
- Understand and recognise normal patterns of life in the region of operation this should include recognition of typical local fishing vessels and the methods they employ. Areas of high density fishing should be identified.
- Train on the correct deployment of vessel hardening measures including specific safety precautions to be taken by vessel crews.
- Train the vessel management team on how to interpret security related reports from differing information sources.
- Conduct security drills with realistic scenarios and periodically involving shore based participation. All drills should have a debrief session where areas for improvement can be identified and corrective actions taken.
- Brief how security/anti-piracy measures should be incorporated into a vessels passage plan including route planning and watch setting.
- Brief on regional reporting requirements for the vessel and on what support a vessel can expect from regional agencies.

B1.3 Vessel

- Understand the attack methodologies of pirates and how to identify illicit behaviour.
- Specific training on how to react in the event that the vessel is boarded.

Appendix C Vessel Hardening Plan
















A Vessel Hardening Plan (VHP) can ensure vessels are prepared for operations in areas of increased security. A VHP ought to be considered as part of any voyage preparation and more so when the vessel will cross known areas of maritime crime or piracy. The requirement for a VHP should be defined within the company management procedures for security.

The Company Security Officer should be responsible for the VHP ensuring process is in place for hardening the vessel. The Master and the Ship's Security Officer are responsible for reviewing the VHP before transit or operation within known security risk areas.

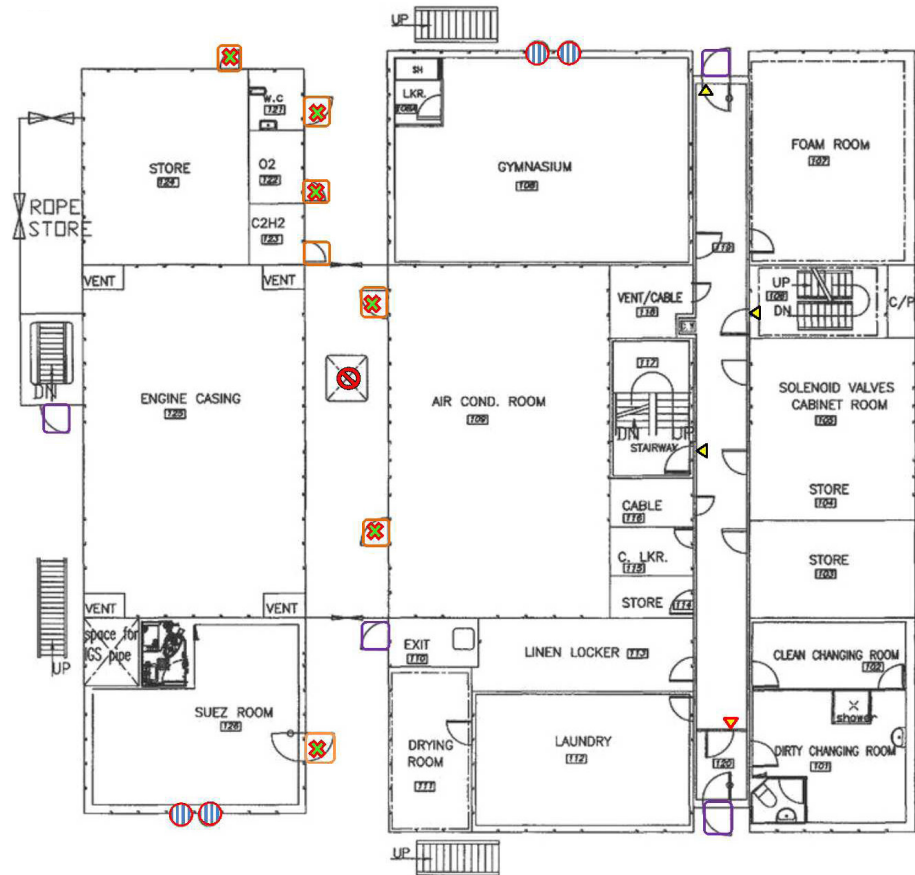
It is recommended that vessel owners and managers should develop and use a VHP.

Example checklist		Authorised by:
		Reviewed by:
		Prepared by:
Vessel name		
IMO number		
Number	Item	On board
01	Hidden communications	No of Sets
02	SSAS programmed to regional centres (UKMTO)	Yes/no
03	90cm razor wire on board	How much?
04	50cm razor wire on board	How much?
05	Number of windows in accommodation barricaded	How many?
06	Number of doors barricaded	How many?
07	Number of round port holes on doors barricaded	How many?
08	Number of outside stairs barricaded (by what system)	How many?
09	Barricading of piping systems around the accommodation area to ensure they cannot be used as access to the bridge area	
10	Number of traffic mirrors on board	How many, where?
11	Piracy radar fitted and aft scanner in place	Yes/no
12	Night vision binoculars available	Yes/no
13	Blast resistant film fitted in bridge windows	Yes/no
14	Bullet proof vest for bridge team	How many/where stowed?
15	Bullet proof helmet for bridge team	How many/where stowed?
16	Goggles for bridge team	How many/where stowed?
17	Outside protection for armed guards – covering bridge wing guard rails with 6mm steel; plate and sand bags for protection	
18	Medical pack for emergency	Yes/no
19	Vessel specific procedures for darkening the vessel if under attack	Yes/no
20	Bridge guidance for manoeuvring if under attack	Yes/no
21	Weapon locker installed	Yes/no
22	Evidence collection equipment in place, e.g. CCTV/hidden cameras Describe:	Yes/no
23	Other means in used for hardening the vessel when entering a high risk area? Describe:	Yes/no

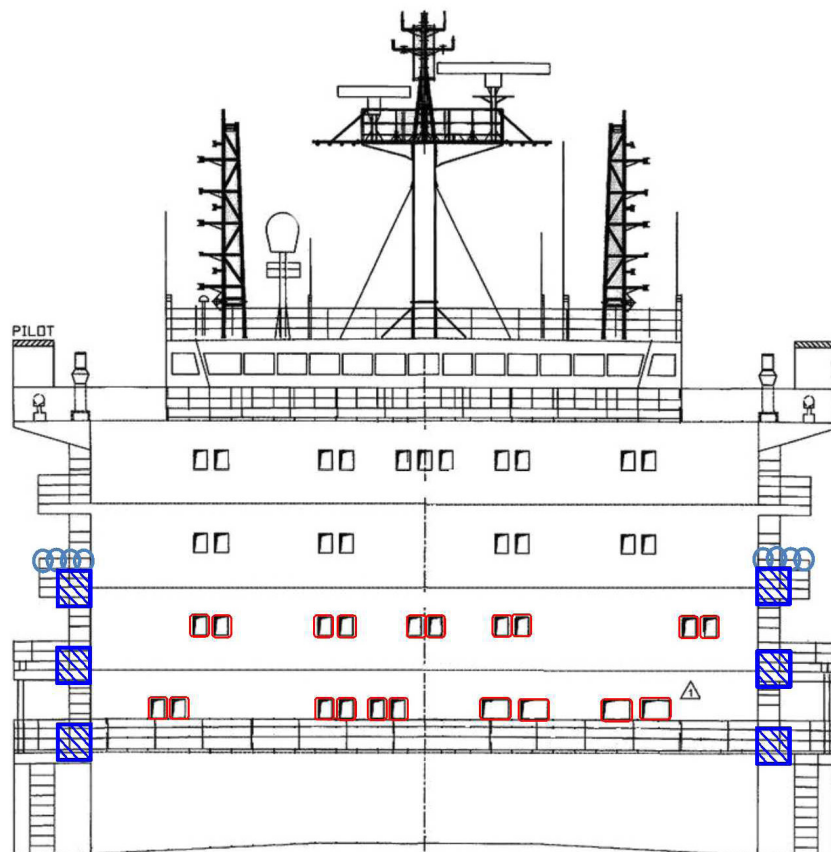
A drawing of all hardening measures as shown above should be marked on the vessel's general arrangement plan and attached to this table. A standard convention for labelling should be used.

Symbol	Description	Actions
	Porthole – easily accessed from landing, deck or reached via a climbing aid	Installation of internal grills denies access
	Porthole fitted with dead light cover or retro-fitted welded bars	Confirm that the distance between bars does not exceed 100mm
	Emergency exit door – watertight design, steel plate with porthole vision panel	Installation of internal porthole protection plate, to deny access by breaching porthole
	Watertight door – external storage areas	Fitting of a padlock protection box to deny access to padlock
	Watertight door – internal access	Requires one of the approved methods of securing the door internally
	Access hatch – providing direct access into engine room	Requires one of the approved methods of securing the hatch internally
	Internal access door chock – identified as part of the safe corridor route from bridge to citadel	Fitting of one door securing devise, point of the symbol identifies which side of the door it should be fitted
	Internal access door bar	Fitting of one or two drop down door bar securing devices
	Razor wire	Two rolls of razor wire to be installed one on top of the other with steel retaining wire running through the middle
	Fire position	Consider good arcs of view, multiple fire positions and ballistic protection
	Stairwell grille	Restrict access via external stairwells
	Fire hoses	Consideration to location to ensure overlap of water jets
	Weapons locker	
	Padlock protector	Fitting of a padlock protection box to deny access to padlock
	Anti-climb barrier	To prevent access to higher decks via pipes

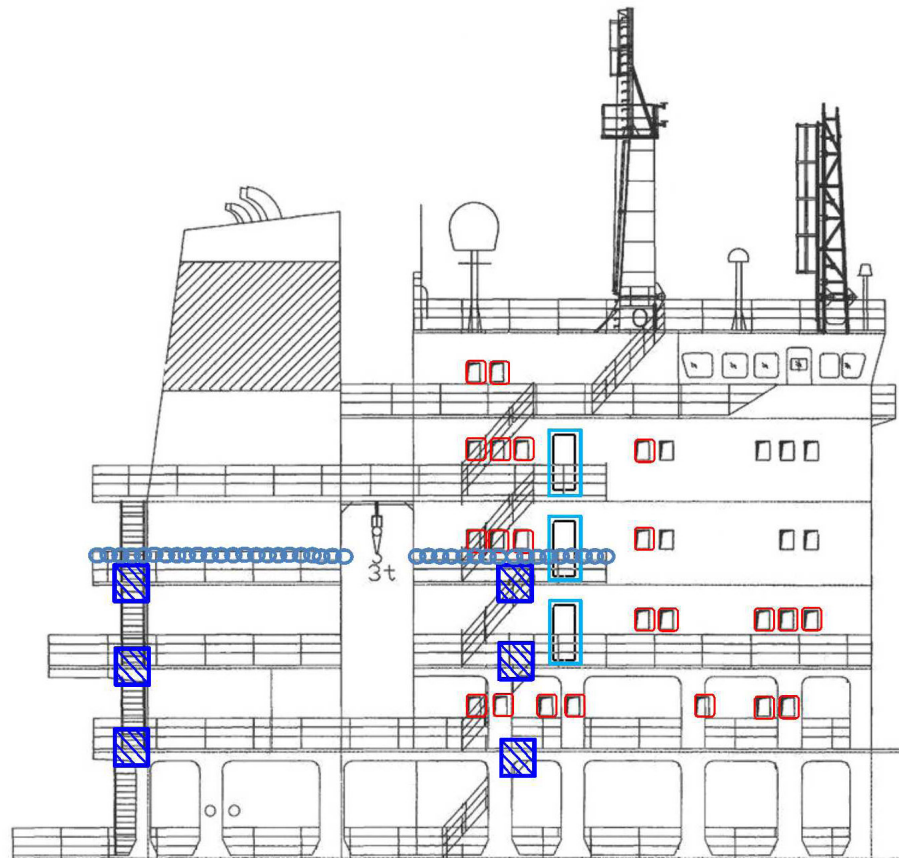
Upper deck



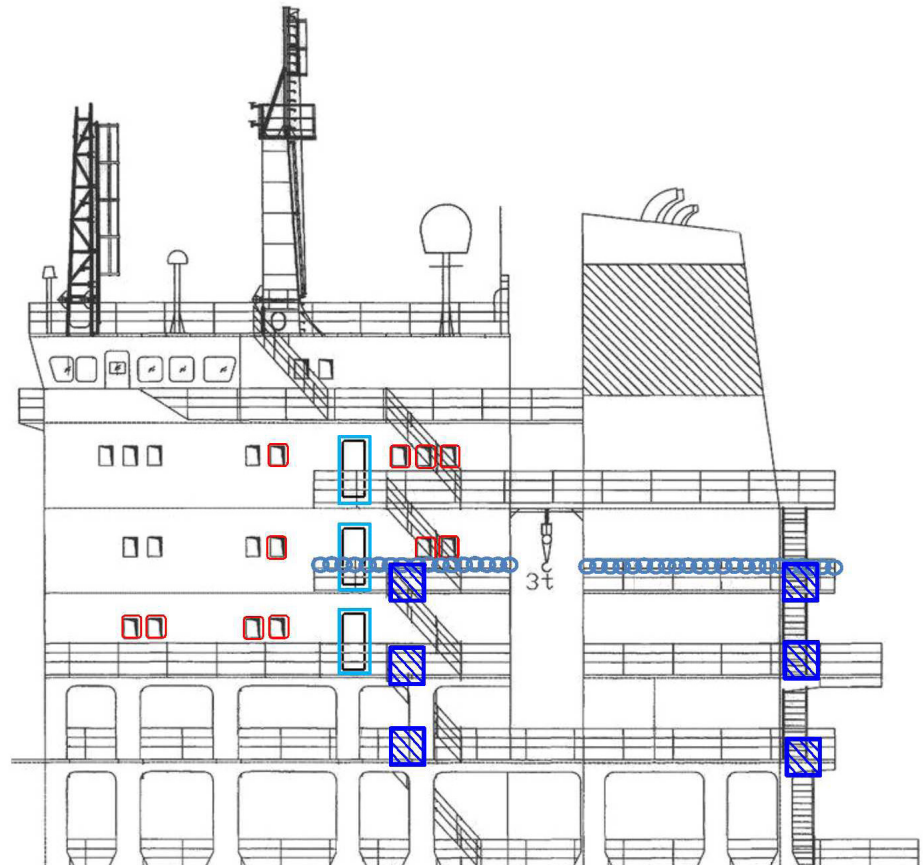
Front view



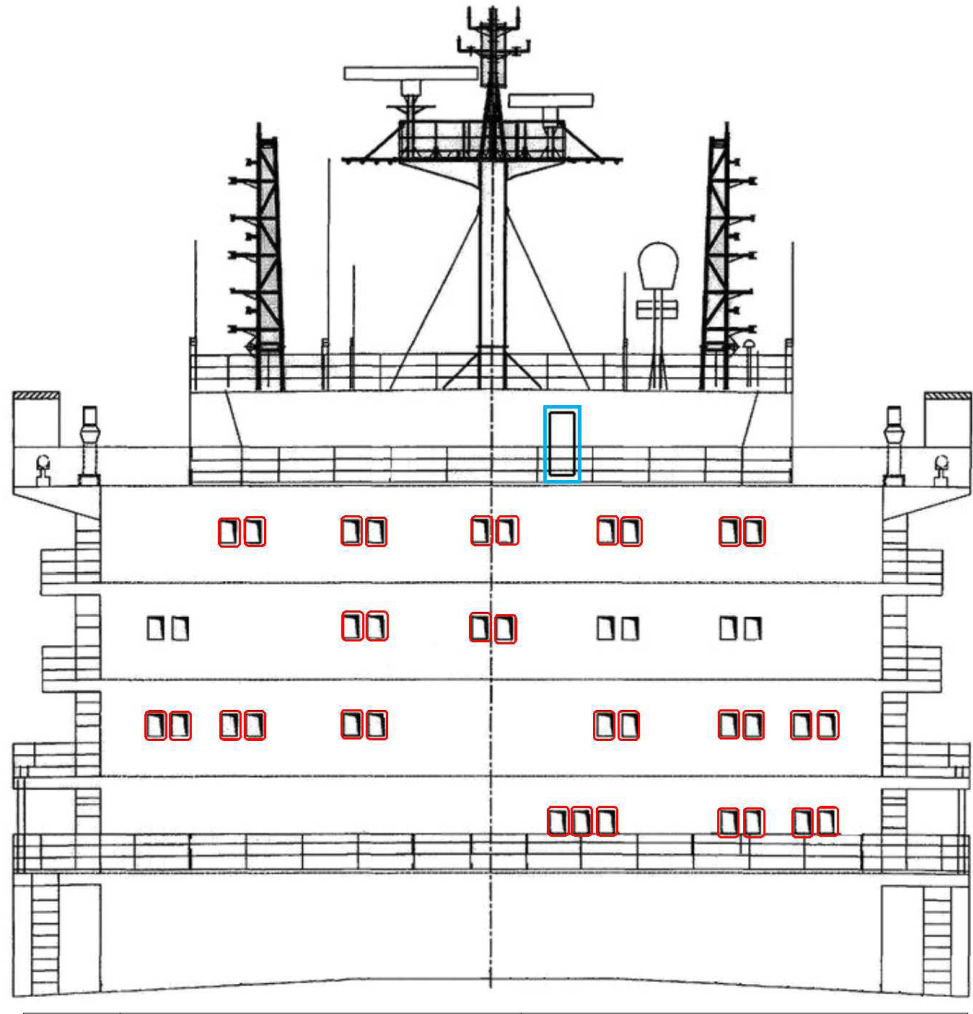
Starboard view



Port view



Aft view





Our vision

A global marine industry that causes no harm to people or the environment

**Oil Companies
International Marine Forum**
29 Queen Anne's Gate
London SW1H 9BU
United Kingdom

T +44 (0)20 7654 1200
E enquiries@ocimf.org

ocimf.org