COURSE HANDOUT

Security Training for Seafarers with Designated Security Duties

As per Section A – VI/6 (Para 4,5 & 6) of STCW 2010

NAVIGATOR MARITIME ACADEMY

(Approved by DG Shipping, Ministry of Shipping, Govt. of India)
(MTI No. : 108025 & Approval No.: TR/A/58/2019)
Plot No – 342, Fathepur Sikri Road, Patholi, Agra, Uttar Pradesh
Tel No: +91-8006891234
E-mail: training@navigatormaritime.ac.in
Web: www.navigatormaritime.ac.in

Navigator Maritime Academy

342, FATHEPUR SIKARI ROAD, PATHOLI, AGRA, UTTAR PRADESH 282010

Course Outline for

Security Training for Seafarers with Designated Security Duties (STSDSD)

Subject Area	Methods of teaching	Hours	
		Lecture	Exercise
1. Introduction 1.1 Course overview 1.2 Competences to be achieved 1.3 Current security threats and patterns 1.4 Ship and port operations and conditions	Lecture / Presentation	1.0	
2. Maritime Security Policy 2.1 Familiarity with relevant international conventions, codes, and recommendations 2.2 Familiarity with relevant government legislation and regulations 2.3 Definitions 2.4 Handling sensitive security-related information and communications	Lecture / Presentation	0.75	
3. Security Responsibilities 3.1 Contracting governments 3.2 Recognized Security Organizations 3.3 The company 3.4 The Ship 3.5 The port facility 3.6 Ship Security Officer 3.7 Company Security Officer 3.8 Port Facility Security Officer 3.9 Seafarers with designated security duties 3.10 Port Facility personnel with designated security duties 3.11 Other personnel	Lecture / Presentation	1.25	
4. Ship Security Assessment 4.1 Assessment tools 4.2 On-scene security surveys	Lecture / Presentation	1.0	
5. Security Equipment 5.1 Security equipment and systems 5.2 Operational limitations of security equipment and systems 5.3 Testing, calibration and maintenance of security equipment and systems	Lecture / Demonstration of Equipments	1.0	0.25
6. Threat Identification, Recognition, and Response 6.1 Recognition and detection of weapons, dangerous substances and devices 6.2 Methods of physical searches and non-intrusive inspections 6.3 Execution and coordination of searches	Lecture / Demonstration of Equipment's	1.0	0.5

6.4 Recognition, on a non-discriminatory basis, of persons posing potential security risks 6.5 Techniques used to circumvent security measures 6.6 Crowd management and control techniques			
7. Ship Security Actions 7.1 Actions required by different security levels 7.2 Maintaining security of the vessel/port interface 7.3 Familiarity with the Declaration of Security 7.4 Execution of security procedures	Lecture / Demonstration of Equipments	0.5	0.25
8. Emergency Preparedness, Drills, and Exercises 8.1 Execution of contingency plans 8.2 Security drills and exercises 8.3 Use of Citadel where provided onboard.	Lecture / Presentation	1.0	
9. Security Administration 9.1 Documentation and records	Lecture / Presentation	0.5	
10. Anti-Piracy Piracy Awareness – Prior to Entering Areas of Risk 10.1 Appraise the strengths and vulnerabilities of Crews and ships. 10.2 Know the Anti – piracy measures (civilian and Military) 10.3 Understand the contents of the Best Management Practices (BMP) 10.4 Pirates Business Model	Lecture / Presentation	1.3	
11.Pirate Attack 11.1 Examine the implications of a piracy Attack 11.2 Assess how to defend the crew and the Ship 11.3 Coping In a Hostage Situation	Lecture / Presentation	2.0	
12.The Release Process 12.1 Discuss the additional dangers associated With the release process	Lecture / Presentation	0.5	
13.Seafarers Family 13.1 Enable seafarers to consider what they May wish to share with their family Concerning the risks of piracy 13.2 Discussion with participants and closing session	Lecture / Presentation	0.7	
Assessment and Feedback		0.5	
GRAND TOTAL		13.0	1.0
TOTAL		14.0	

1. Introduction

1.1 Course overview

This course covers Security Training for Seafarers with designated Security Duties as per Section A – VI/6 (para 4, 5,& 6) of STCW 2010.

1.2 Competences to be achieved

On completion of this course the trainee would be able to understand the importance of security aspects involved in maritime industry viz. Ships, ports, cargo, ship personnel, passengers etc. and to understand the framework involving co-operation between contracting Governments, Government agencies, local administrations to detect security threats if any and take suitable preventive measures against any incident affecting ships or port facilities affecting international trade.

1.3 Current security threats and patterns

Sea piracy:

Sea piracy has existed since ancient times. However, over the last 20 years the menace of piracy has had a very real impact on international shipping, with horrifying incidents of hostage-taking and assault, of crew members traumatized, left adrift or even killed.

There are political, economic, social, legal and security reasons for the recent spurt in piracy, which include political instability resulting in lack of governance of the littorals, the absence of political will on the part of states to fight piracy, poor socio-economic conditions pressurizing local populations to commit piracy for survival, inadequate military capability to respond.

Pirates have been active in Asia (South China Sea, South-East Asia and South Asia), the Persian Gulf, Africa (the Horn of Africa and the west coast), the Caribbean and Latin America. In recent times South-East Asian waters, particularly the Straits of Malacca, and the Gulf of Aden in East Africa have been the hot spots of sea piracy and attracted international attention.

Terrorism at sea and from the sea:

During the last few decades, several terrorist groups have mushroomed across the globe. Notwithstanding the fact that the sea is a complex medium, and requires great mastery to conduct attacks, these groups have developed significant capability to conduct attacks at sea, under the sea and more recently from the sea.

There are a number of other areas where the maritime industry is vulnerable. Many of the measures applied to meet the requirements of the ISOS Code will have positive benefits in countering these other threats. These threats include:

- Pilferage and theft
- IIIicit drugs smuggling
- IIIegal migrants and stowaways

1.4 Vessel and port operations and conditions

In considering the nature and experience of global terrorism it is recognized that maritime industry may be at risk from:

1 Attempts to use ships as a means of delivery of weapons of mass destruction or major explosive devices to target States:

2 Attempts to hijack ships taking passengers and crew hostage in order to gain leverage:

3 Direct attacks on personnel and passengers within ports:

4 Direct attacks on ships where the State of Registry or the operating company is deemed to be representative of a target State:

5 Direct attacks on the port infrastructure-given the potentially disastrous consequences of an attack on ports due to the nature of dangerous, hazardous and noxious substances carried as cargo in substantial quantities or stored/transiting and distributed or processed at/or near ports:

6 Direct attack on industrial processes in ports and surrounding areas such as nuclear power plants and hazardous/noxious chemical and other works:9

7 The release of hazardous or noxious cargo , from ships or within port, to cause widespread danger to life or to the marine environment:

8 Sabotage of navigational facilities and other areas vital to the operation of the port: Criminal Activities

Criminal activities at ports represent major lass of revenue for shippers: handling agents, ship operators and governments. They also detract from the reputation of the port, thus adversely affecting future business (and national prestige). Such activities may include but are not limited to:

1. Theft of cargoes with implications for compensation claims, insurance charges, government revenues, etc:
2. Commercial smuggling:
3. Smuggling of contraband including narcotics, endangered species and nuclear material:
4. Illegal migration of persons.

2. Maritime Security Policy

2.1 Relevant international conventions, codes, and recommendations

The Diplomatic conference on Maritime Security held in London in December 2002 adopted new provisions in the International Convention for the safety of Life at Sea, 1974 and the code (the complete name of the code is the International Code for the Security of Ships and of Port Facilities). As referred to in regulation XI-2/1 of SOLAS 74 as amended, is the International Ship and Port Facility Security (ISPS) code.

The tragic events of 11th September 2001, International Maritime Organization in November 2001, unanimously agreed to the development of new measures relating to the security of ships and of port facilities for adoption by a conference of contracting Governments to the Internal convention for the safety of Life at Sea (known as the Diplomatic Conference on Maritime Security) in December 2002.

The Diplomatic Conference (9 to 13 December 2002) adopted amendments to the existing provisions of the International convention for the Safety of Life at Sea, 1974 (SOLAS 74) accelerating the implementation of the requirements to fit Automatic Identification Systems and adopted new regulations in Chapter XI-I of SOLAS 74. The Diplomatic Conference also adopted a number of conference resolutions, including those covering implementation and revision of this code.

2.2 Relevant government legislation and regulations

Parts A and B of the Code are the mandatory requirements regarding the provisions of Chapter XI-2 of SOLAS, 1974 as amended and guidance regarding the provisions of Chapter XI-2 of SOLAS 1974 as amended and Part A of the Code. It is cognized that the extent to which the guidance applies may vary depending on the nature of the port facility and of the ship, its trade and its cargo.

OBJECTIVES

1. To establish an international framework involving co-operation between contracting Governments, Government agencies, local administrations and the shipping and port industries to detect security threats and take preventive measure against security incidents affecting ships or port facilities using international trade

2. To establish the respective roles and responsibilities of the contracting Governments, Government agencies, local administrations and the shipping and port industries, at the national and international level, for ensuring maritime security;

3. To ensure the early and efficient collection and exchange of security related information.

4. To provide a methodology for security assessments so as to have in place plans and procedures to react to changing security levels.

5. To ensure confidence that adequate and proportionate maritime security measures are in place.

2.3 Definitions

1. Ship security plans means 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 ship from the risks of the security incident.

2. Port facility plan means a plan developed to ensure the application of measures designed to protect the port facility and ships, persons, cargo, cargo transport units and ship's stores within the port facility from the risks of a security incident;

3. Ship security officer means the person on board the ship, accountable to the master, designated by the company as responsible for the security of the ship, including implementation and maintenance of the ship security plan and for liaison with the company security officer and port facility security officers.

4. Company security officer means the person designated by the company for ensuring that a ship security assessment is carried out; that a ship security plan is developed, submitted for approval and facility security officers and the ship security officer.

5. Port facility security officer means the person designated as responsible for the development, implementation, revision and maintenance of the port facility security plan and for liaison with the ship security officers and company security officers.

6. Security level 1 means the level for which minimum appropriate protective security measures shall be maintained at all times.

7. Security level 2 means the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident.

8. Security level 3 means the level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target.

9. Safety means measures to prevent an incident that happens accidentally.

10. Security means measures to prevent an incident that happens intentionally.

2.4 Handling sensitive security-related information and communications

FUNCTIONAL REQUIREMENTS

1. Gathering and assessing information with respect to security threats and exchanging such information with appropriate contracting Governments.

2. Requiring the maintenance of communication protocols for ships and port facilities.

3. Preventing unauthorized access to ships; port facilities and their restricted areas.

4. Preventing the introduction of unauthorized weapons, incendiary devices or explosive to ships or port facilities.

5. Providing means for raising the alarm in reaction to security threats or security incidents.

6. Requiring ships and port facility security plans based upon security assessments.

7. Requiring training drills and exercises to ensure familiarity with security plans and procedures.

3. Security Responsibilities

3.1 Contracting governments

1. Subject to the provisions of regulation XI-2/3 and XI-2/7, Contracting Governments shall set security levels and provide
Guidance for protection from security incidents. Higher security levels indicate greater likelihood of occurrence of a security incidence. Factors to be considered in setting the appropriate security level include:

   (i) the degree that the threat information is credible

(ii) the degree that the threat information is corroborated

(iii) The degree that the threat information is specific or imminent.

(iv) The potential consequences of such a security incident.

2. Contracting Governments, when they set security level 3, shall issue as necessary, appropriate instructions and shall provide security-related information to the ships and port facilities that may be affected.

3. Contracting Governments may delegate to a recognized security organization certain of their security-related duties under chapter XI-2 and this part of the code with the exception of :

(i) setting of the applicable security level

(ii) approving a port facility security assessment and subsequent amendments to an approved assessment

(iii) determining the port facilities which will be required to designate a port facility security officer.

(iv) approving a port facility security plan and subsequent amendments to an approved plan

(v) Exercising control and compliance measures pursuant to regulation X102/9.

(vi) Establishing the requirements for a Declaration of Security.

4. Contracting Governments shall, to the extent they consider appropriate, test the effectiveness of the ship security plans or the port facility plans, or of amendments to such plans, they have approved, or in the case of ships of plan which have been approved on their behalf.

3.2 Recognized Security Organizations

- Each ship shall carry on board a ship security plan approved by the administration the plan shall make provision for the three security levels as defined in this part of the code.

1. Recognized security organization may prepare the ship security plan for a specific ship.

- The administration may entrust the review and approval of ship security plans or of amendments to a previously approved plan, to recognized security organizations.
  1. In such cases, the recognized security organization undertaking the review and approval of a ship security plan, or its amendments, for specific ship shall not have been involved in either the preparation of the ship security assessment or of the ship security plan, or of the amendments, under review.

3.3 The company

- The company shall ensure that the ship security plan contains a clear statement emphasizing the master's authority. The company shall establish in the ship security plan that the master has the overriding authority and responsibility to make decision with respect to the safety and security of the ship and to request the assistance of the company or of any contracting Government as may be necessary.

- The company shall ensure that the company security officer, the master and the ship security officer are given the necessary support to fulfill their duties and responsibilities in accordance with chapter XI-2 and this part of the code.

3.4 The vessel

The ship to which the requirements of chapter XI-2 and part A of this Code apply are required to have and operated in accordance with, a Ship Security Plan approved by or on behalf of the Administration, The Company and Ship Security Officer should monitor the continuing relevance and effectiveness of the plan, including the undertaking of internal audits. Amendments to any of the elements of an approved plan, for which the administration has determined that approval is required, have to be submitted for review and

approval before their incorporation in the approved plan and their implementation by the ship.

The ship has to carry an International Ship Security Certificate indicating that it complies with the requirements of chapter XI-2 and part A of this Code includes provisions relating to the verification and certification of the ship's compliance with the requirements on an initial, renewal and intermediate verification basis.

- Such plan shall be developed, taking into account the guidance given in part of this code and shall be written in the working language or languages of the ship. If the language or languages used is not English, French or Spanish, a translation into one of these languages shall be included. The plan shall address, at least the following :

  1. Measures designed to prevent weapons, dangerous substances and devices intended for use against persons, ships or ports and the carriage of which is not authorized from being taken on board the ship.
  2. Identification of the restricted areas and measures for the prevention of unauthorized access to them.
  3. Measures for the prevention of unauthorized access to the ship.
  4. Procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the ship or ship/port interface.
  5. Procedures for responding to any security instructions contracting governments may give at security level 3.
  6. Procedures for evacuation in case of security threats or breaches of security.
  7. Duties of shipboard personnel assigned security responsibilities and of other shipboard personnel on security aspects.
  8. Procedures for auditing the security activities.
  9. procedures for training, drills and exercises associated with the plan

10. procedures for interfacing with port facility security activities

11. procedures for the periodic review of the plan and for updating

12. Procedures reporting security incidents.

13. Identification of the ship security officer.

14. identification of the company security officer, including 24 hour contact details

15. Procedures to ensure the inspection, testing, calibration and maintenance of any security equipment provided on board.

16. Frequency for testing or calibration of any security equipment provided on board.

17. Identification of the locations where the ship security alert system activation points are provided.

18. Procedures, instructions and guidance on the use of the ship security alert system, including the testing, activation, deactivation and resetting and to limit false alerts.

3.5 The port facility

The port Facility security Plan should indicate the operational and physical security measures the port facility should take to ensure that it always operates at security level 1. The plan should also indicate the additional or intensified security measures the port facility can take to move to and operate at security level 2 when instructed to do so. Furthermore, the plan should indicate the possible preparatory actions the port facility could take to allow prompt response to the instructions that may he issued by those responding at security level 3 to a security incident or threat thereof.

3.6 Vessel Security Officer

A ship security officer shall be designated on each ship
In addition to those specified elsewhere in this part of the code, the duties and responsibilities of the ship security officer shall include, but are not limited to:

1. undertaking regular security inspections of the ship to ensure that appropriate security measures are maintained.
2. maintaining and supervising the implementation of the ship security plan, including any amendments to the plan.
3. co-ordinating the security aspects of the handling of cargo and ship's stores with other shipboard personnel and with the relevant port facility security officers.
4. proposing modifications to the ship security plan.
5. reporting to the company security officer any deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance and implementing any corrective actions.
6. enhancing security awareness and vigilance on board
7. ensuring that adequate training has been provided to shipboard personnel, as appropriate.
8. reporting all security incidents.
9. co-ordinating implementation of the ship security plan with the company security officer and the relevant port facility security officer
10. ensuring that security equipments is properly operated, tested, calibrated and maintained.

3.7 Company Security Officer

The company shall designate a company security officer. A person designated as the company security officer may act as the company security officer for one or more ships, depending on the number or types of ships the company operates, provided it is clearly identified for which ships this persons is responsible. A company may, depending on the number or types of ships they operate, designate several persons as company security officers provided it is clearly identified for which ships each person is responsible.

In addition to those specified elsewhere in this part of the code, the duties and responsibilities of the company security officer shall include, but are not limited to :

1. advising the level of threats likely to be encountered by the ships using appropriate security assessments and other relevant information.
2. ensuring that ship security assessments are carried out
3. ensuring the development, the submission for approval, and thereafter the implementation and maintenance of the ship security plan.
4. ensuring that the ship security plan is modified, as appropriate, to correct deficiencies and satisfy the security requirements of the individual ship.
5. arranging for internal audits and reviews of security activities.
6. arranging for the initial and subsequent verification of the ship by the administration or the recognized security organization.
7. ensuring that deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance are promptly addressed and dealt with.
8. enhancing security awareness and vigilance.
9. ensuring adequate training for personnel responsible for the security of the ship.
10. ensuring effective communication and co-operation between the ship security officer and the relevant port facility security officers .
11. ensuring consistency between security requirements and safety requirements.
12. ensuring that, if sister-ship or fleet security plans are used, the plan for each ship reflects the ship-specific information accurately.

13. ensuring that any alternative or equivalent arrangements approved for a particular ship or group of ship are implemented and maintained.

3.8 Facility Security Officer

The port facilities which have to comply with the requirement of chapter XI-2 and part A of this Code are required to designate a port Facility Security Officer. The duties, responsibilities and training requirements of these officers and requirements for drills and exercises are defined in part A of this Code.

3.9 Vessel personnel with specific security duties

Shipboard personnel having specific security duties and responsibilities shall understand their responsibilities for ship security as described in the ship security plan and shall have sufficient knowledge and ability to perform their assigned duties, including , as appropriate:

- knowledge of current security threats and patterns.
- recognition and detection of weapon, dangerous substances or device.
- recognition of characteristics and behavioral pattern of persons who are likely to threaten security.
- techniques used to circumvent security measures.
- crowd management and control techniques.
- security related communications.
- knowledge of emergency procedures and contingency plan.
- operations of security equipment and systems.
- inspection, control and monitoring techniques.
- Methods of physical searches of persons, personal effects, baggage, cargo and ship's stores.

3.10 Facility personnel with specific security duties

Port Facility personnel having specific security duties and responsibilities shall understand their responsibilities for ship and port facility security as described in the Port Facility security plan and shall have sufficient knowledge and ability to perform their assigned duties.

3.11 Other personnel

All other shipboard personnel should have sufficient knowledge of and be familiar with the relevant provisions of the ship security plan.

4. Vessel Security Assessment

The ship security assessment is an essential and integral part of the process of developing and updating the ship security plan.

4.1 Assessment tools

The company security officer shall ensure that the ship security assessment is carried out by person with appropriate skills to evaluate the security of a ship, in accordance with this section, taking into account the guidance given in part B of this code.

Subject to the provision of Ship security plan a recognized security organization may carry out the ship security assessment of a specific ship.

4.2 On-scene security surveys

The ship security assessment shall include an on-scene security survey and at least, the following elements :

(i) identification of existing security measures, procedures and operations.

(ii) identification and evaluation of key shipboard operations that it is important to protect.

(iii) identification of possible threats to the key shipboard operations and the likelihood of their occurrence, in order to establish and prioritize security measures.

(iv) identification of weaknesses, including human factors, in the infrastructure, policies and procedures.

4.3 Security assessment documentation

The ship security assessment shall be documented, reviewed, accepted and retained by the company.

5. Security Equipment

5.1 Security equipment and systems

screening by metal detector;
intruder detection alarm systems;
security patrols and inspections;
Ship Security alert systems.

closed circuit television cameras; and

Night vision binoculars, flash lights, whistles, fire hoses, razor/ barbed wires, walkee talkees, anti-shatter strings etc are also included in the security equipment.

5.2 Operational limitations of security equipment and systems

Possible Vulnerability may include :-

- Conflicts between safety and security measures
- Conflicts between shipboard duties and security assignments
- Watch keeping duties, ship's personnel size, particularly with implications on Crew fatigue, alertness and performances.
- Training deficiencies
- Insufficient, poorly maintained or poor quality security equipment.
- Poor quality or unsuitable security equipment and system.
- Poor communications systems.

5.3 Testing, calibration and maintenance of security equipment and systems

Proper maintenance, routine testing and calibration of security equipment must be conducted as the maker's instructions or Planned Maintenance System. A proper record is maintained of all such tests and calibration.

6. Threat Identification, Recognition, and Response

6.1 Recognition and detection of weapons, dangerous substances and devices

Ship Security Assessment to Port facility security assessment are basically a Risk Analysis to determine which part(s) are more susceptible and/or more likely, to be the area of attack.

Risk is defined as a father of threat of an attack coupled with the vulnerability of the larger consequences of an attack.

But standard definitions is

Risk = Likeliness consequences

Here : Threat x Vulnerability = Likelihood

In fact vulnerability means by protective measures procedures and operations.

Possible threat to key vessel operation may include :-

- Bombing
- Sabotage
- Hijacking
- Unauthorized use
- Smuggling
- Cargo tempering
- Stowaways, piracy
- Hostage taking
- Vandalism
- Transporting weapons of mass destruction
- Use of vessel to carry perpetrators and their equipments.
- Use of the ship itself as a weapons or as means to cause damage or destruction.

6.2 Methods of physical searches and non-intrusive inspections

SEARCH TECHNIQUES

THE THREE C'S

CARRIER

MANNER – APPEARANCE – REASON

CONTAINER

TYPE – WEIGHT – TARGET

CONTENTS

RELEVANT – COMPONENTS – CONCEALED

A SECURITY INFORMATION NOTICE

- All person boarding are required to show a Boarding Pass.
- All persons and baggage are liable to be searched.
- No drugs are allowed on board. No weapons are allowed on board.
- Only authorized visitors are allowed.

SEARCH QUESTIONS

- WHY AM I DOING THIS ?
- WHAT AM I LOOKING FOR ?
- WHERE WOULD I CHOOSE TO HIDE SOMETHING ?

6.3 Execution and coordination of searches

To ensure that a thorough and efficient search is completed in the shortest possible time, search plans should be prepared in advance. This should normally be done by management in conjunction with the master and can be reviewed and modified in the light of experience.

The search plan should be comprehensive, and should detail the routs searchers should follow and all the places on the route where a package might be hidden.

The plan should be developed in a systematic manner to cover all options and to ensure overlap or omission.

SECURITY SEARCH AND PATROL CHECKLIST

SHIP IN PORT OR AT ANCHOR

1	In port or at designated anchorage, provide full lighting on deck and over side particularly at the bow and stern	
2	Maintain a constant supply of water to the hawse pipes, and same to be kept closed by their covers	
3	Keep fire line always under pressure and some fire hoses duly connected ready to be used.	
4	In port restrict access to the ship to one point	
5	Ensure the gangway is linked by walkie-talkie to the other watch keepers.	
6	After arrival organize a system of immediate notification to the authorities/Coast Guard.	
7	Complete	

WHEN AT SEA

1	Increase surveillance and vigilance during hours of darkness	
2	Maintain constant visual and radar watch.	

3	Seal off all means of access to the ship.	
4	Maintain fire line under pressure and have water hoses duly rigged.	
5	Illuminate the deck, particularly at the stern in sensitive waters	
6	Brief the Engine Room and crew about precautions to be taken and agreed signals on security breach.	
7	Establish and maintain communication with CSO.	

WHEN SECURITY BREACH IS SUSPECTED

1	Sound the general alarm and ship's whistle.	
2	Alert CSO and all other concerned parties	
3	Switch on all decks and over side lightings and use searchlight to illuminate and dazzle.	
4	Alert shore authorities and other vessels in the vicinity. If possible also alert the INMARSAT Rescue Co-ordination Centres.	
5	Fire warning flares, rockets if safely gas free and/or operate water hoses.	
6	Consider stopping cargo operations if applicable.	

SEARCH CHECKLIST

AREA 1 - ACCOMMODATION

1	Bridge/Radio Room/battery locker/toiler	
2	Cabins/shower room	
3	Linen lockers	
4	Recreation rooms	
5	Galley/galley stores/fridge	
6	Changing rooms	

7	Accesses to engine room	
8	Lifeboats	
9	Safety/emergency locker	
10	General store rooms	
11	Laundry	
12	Hospital	
13	CO_2 Room/Foam fixed fire extinguishing system room	
14	Emergency generator room	
15	Ship's office	
16	Air conditioning rooms	
17	Monkey island	
18	Swimming pools	
19	Mess room/saloon	

AREA 2 - ENGINE ROOM

1	Engine room space	
2	Control room	
3	Purifier room	
4	Store room	
5	Steering gear	
6	Engine room bilges/bottom plates	
7	Shaft tunnel	
8	Changing rooms	
9	Funnel casings/funnel top	

AREA 3 – CARGO SPACES

1	Cargo holds	
2	Hatch coaming	
3	Vents	
4	Deck cargo	
5	Hatch-cover recesses	
6	Car decks	
7	Garages	

AREA 4 – MAIN DECK SPACES

1	Hold accesses	
2	Mast houses/mast heals	
3	Pump room winch rooms	
4	Crane cabs	
5	Forecastle	
6	Paint lockers	
7	Rope lockers	
8	Chain lockers	
9	Hawse pipes	
10	Fan rooms	
11	Bow/stern thruster spaces	

6.4 Recognition, on a non-discriminatory basis, of persons posing potential security risks

Those unwilling or unable to establish their identitiy and/or purpose of theis visit when requested to do so should be denied access to the ship and their attempt to obtain access should be reported, as appropriate, to the SSO, the CSO, the PFSO and to the national or local authorities with security responsibilities.

6.5 Techniques used to circumvent security measures

- False identity to obtain access to the ship.
- Creating diversion or confusion.
- Making use of lapses in the vigilance and security measures.
- Using blind spots i.e. the areas not covers in CCTV or any other monitoring systems.
- Tempering with the security devices.

6.6 Crowd management and control techniques

Crowd Management is not only about controlling the crowd, but also managing the crowd with confidence, knowledge, effective communication and leadership. While all crew need to become familiar with crowd management, it is mandated by STCW for masters, officers and other personnel who are designated on Muster Lists to assist passengers in emergency situations on passenger vessels.

Crowd Management is a comprehensive course incorporating

•Life-saving appliances and control plans: Muster lists and muster stations, emergency alarms (general emergency, man overboard, abandon ship), launching of survival crafts and the proper donning of life jackets.

•Mustering procedures: Preparation and launching of equipment, staff assignments, custody and use of communication equipment, manning of fire teams, etc.

•Operational limits: Ship's layout (exits, stairwells, elevators, etc.), power failures, emergency lighting

•Emergency procedures: Guidelines for assembling passengers, conducting a vessel search, keeping order and discipline, leadership skills

•Communications: Alarms, language barriers, clear and reassuring orders, rumor control, anxiety, special assistance for the disabled, communicating with the bridge. Although designed primarily for the commercial sector, this course is directly relevant to yachts.

7. Vessel Security Actions

7.1 Actions required by different security levels

- A ship is required to act upon the security levels set by contracting Governments as set out below.

- At security level I, the following activities shall be carried out through appropriate measures, on all ships taking into account the guidance given in Part B of this Code, in order to identify and take preventive measures against security incidents;

  (i) ensuring the performance of all ships security duties;

  (ii) controlling access to the ship

  (iii) controlling the embarkation of persons and their effects

  (iv) monitoring restricted areas to ensure that only authorized persons have access

  (v) monitoring of deck areas and areas surrounding the ship

  (vi) supervision the handling of cargo and ship's stores and

(vii) ensuring that security communication is readily available.

- At security level 2, additional protective measures, specified in the ship security plan, shall be implemented for each activity detailed above in the security level 1, taking into account the guidance given in the part B of this code.

- At security level 3, further specific protective measures specified in the ship security plan, shall be implemented for each activity detailed above in the security level 1, taking into account the guidance given in part of this code.

- Whenever security level 2 or 3 is set by the Administration , the ship shall acknowledge receipt of the instructions on change of the security level.

7.2 Maintaining security of the vessel/port interface

- Prior to entering a port or whilst in a port within the territory of a Contracting Government that has a set security level 2 or 3, the ship shall acknowledge receipt of this instruction and shall confirm to the port facility security officer the initiation of the implementation of the appropriate measures and procedures as detailed in the ship security plan, and in the case of security level 3, in instructions issued by the contracting government which has set security level 3. The ship shall report any difficulties in implementation. In such cases, the port facility security officer and ship security officer shall liaise and co-ordinate the appropriate actions.

- If a ship is required by the Administration to set, or is already at a higher security level than that set for the port it intends to enter or in which it is already located, then the ship shall advise, without delay, the competent authority of the Contracting Government within whose territory the port facility is located and the port facility security officer of the situation.

(i) In such cases, the ship security officer shall liaise with the port facility security officer and co-ordinate appropriate actions, if necessary.

- An administration requiring ships entitled to fly its flag to set security level 2 or 3 in a port of another contracting Government shall inform that Contracting Government without delay.

- When advising such ships of the applicable security level, a Contracting Government shall, taking into account the guidance given in part B of this Code, also advise those ships of any security measure that they should take and, if appropriate, of measures that have been taken by the Contracting Government to provide protection against the threat.

7.3 Familiarity with the Declaration of Security

Contracting Governments shall determine when a Declaration of Security is required by assessing the risk the ship/port interface or ship-to-ship activity poses to persons, property or the environment.

A ship can request completion of Declaration of security when :

1. the ship is operating at a higher security level than the port facility or another ship it is interfacing with.
2. there is an agreement on a Declaration of Security between Contracting Governments covering certain international voyages or specific ships on those voyages.
3. there has been a security threat or a security incident involving the ship or involving the port facility as applicable.
4. the ship is at a port which is not required to implement an approved port facility security plan or
5. the ship is conducting ship-to-ship activities with another ship not required to have an implement an approved ship security plan.

Request for the completion of a Declaration of Security, under this section, shall be acknowledged by the applicable port facility or ship.

The Declaration of Security shall be completed by :

1. the master or the ship security officer on behalf of the ship(s) and if appropriate.
2. the port facility security officer or if the Contracting Government determines other wise, by any other body responsible for shore-side security on behalf of the port facility.

The Declaration of Security shall address the security requirements that could be shared between a port facility and a ship and shall state the responsibility for each.

Contracting Governments shall specify, bearing in mind the provisions of regulation XI-2/9.2.3, the minimum period for which Declarations of Security shall be kept by the port facilities located within their territory.

Administration shall specify, bearing in mind the provisions of regulation XI-2/9.2.3, the minimum period for which Declarations of Security shall be kept by ships entitled to fly their flag.

7.4 Execution of security procedures

In this context, the following procedures are recommended for ship operators:

- Conduct stowaway awareness training for all ships twice annually.
- Review port security provided to their ships and insist that it be adequate.
- Develop a stowaway- handling manual for use aboard each ship.
- Prepare stock media responses and place them in each stowaway manual for use in dealing with the media.
- Place equipment and supplies onboard each ship to be deployed in the event of a stowaway incident.

- Conduct and document thorough ship searches following each port of call.
- Maintain an effective gangway watch, 24 Hours per day and 7 days a week.
- Supervise longshoremen and ensure all stevedores disembark.
- Be alert to problem ports and share in information within the fleet.

8. Emergency Preparedness, Drills, and Exercises

8.1 Execution of contingency plans

- The company security officer and appropriate shore-based personnel shall have knowledge and have received training, taking into account the guidance given in part B of this code.

- The ship security officer shall have knowledge and have received training, taking into account the guidance given in part B of this code.

8.2 Security drills and exercises

- To ensure the effective implementation of the ship security plan, drills shall be carried out at appropriate intervals taking into account the ship type, ship personnel changes, port facilities to be visited and other relevant circumstance, taking into account the guidance given in part B of this code.

- The company security officer shall ensure the effective co-ordination and implementation of ship security plans by participating in exercises at appropriate intervals, taking into account the guidance given in part B of this code.

8.3 CITADEL-

A citadel is a designated pre-planned area specifically built into the ship where – In the event of imminent boarding by pirates – all crew can seek refuge with the objective of preventing the pirates from gaining control of the vessel. The Citadel should have control capability of the vessel, emergency rations, safe air supply, CCTV control and good external communications.

Is a citadel a safe solution? Well, several incidents have proven that it can thwart pirates' efforts to take over a ship. In several

cases now, the crew made it safety to the Citadel, sat tight and the pirates were apprehended by naval forces or just gave up.

Citadels can also improve the effectiveness of naval forces. If the crew is safety ensconced in the Citadel, it can then allow naval forces, who in the past have been hesitant to intervene on a vessel once the pirates are on board for fear of harming the crew, to engage the pirates knowing the crew is safe.

There are risks. Pirates have proven they adapt and it won't be long before we'll be hearing of incidents where more effective explosives then rebounding RPGs are being used to gain access to these safe rooms. One can only imagine how the pirates will respond to the crew after gaining access, not to mention potential casualties from the explosives. But many Citadels are being built in areas within the vessel that can withstand explosives (double bulkhead protection) and are being equipped with safeguards to protect the crews from attempted forced entry.

There is also a risk of vandalism as pirates become frustrated if they cannot gain access but repairing vandalism damage is certainly preferable to a crew of hostages and ransom fees.

So is this the solution …..no. until we see "stability" and "Somalia" in the same headline, pirates will continue to threaten vessels in the region. Vessels should continue to follow the guidelines established in the BMP4 and keep up-to-date with latest reports on pirate activity.

Citadels won't stop the pirates from attempting to board. But what they can do, when the situation warrants, is help address many of the issues impacting the industry once pirates have boarded : giving the crew a chance to remain safe; preventing the pirates from gaining control of the vessel; and offering naval forces time to reach the vessel and engage the hijackers. Not to mention it's more cost-effective then armed security or escorts.

9. Security Administration

9.1 Documentation and records

The appendix to this guidance provides the standard data set of security- related information a ship might be expected to submit prior to entry into port.

STANDARD DATA SET OF SECURITY RELATED INFORMATION

1 Particulars of the ship and contact details

1.1 IMO Number
1.2 Name of ship
1.3 Port of registry
1.4 Flag State
1.5 Type of ship
1.6 Call Sign
1.7 Inmarsat call numbers
1.8 Gross Tonnage
1.9 Name of Company
1.10 Name and 24-hour contact details of the Company Security Officer

2 Port and port facility information

2.1 Port of arrival and port facility where the ship is to berth, if known

2.2 Expected date and time of arrival of the ship in port (paragraph B/4.39.3 of the ISPS code)

2.3 Primary purpose of call

3 Information required by SOLAS regulation XI-2/9.2:1 3.1 The ship is provided (SOLAS regulation 9.2.11) with a valid:

International Ship Security Certificate Yes No

Interim International Ship Security Certificate Yes No

3.1.1 The certificate indicated in 3.1 has been issued by < enter name of the Contracting Government or the Recognized Security Organization>and which expires on <enter date of expiry>

3.1.2 If the ship is not provided with a valid International Ship Security Certificate or a valid Interim International Ship Security Certificate explain why?

3.1.2.1 Does the ship have an approved ship security plan on board? [ ] Yes [ ] No

3.2 Current security level (SOLAS regulation XI-2/9.2.12): [ ]

3.2.2 Location of the ship at the report is made (paragraph B/4.39.2 of the ISPS Code)

3.3 List the last ten calls, in chronological order with the most recent call first, at port facilities at which the ship conducted ship/port inteface5 together with the security level at which ship operated (SOLAS regulation XI-2/9.2.1.3):

Date

No From6 To6 Port. Country, Port Facility and UNLOCODE3 Security Level

3.3.1 Did the ship, during the period specified 3.3, take any special or additional security measures, beyond those specified in the approved ship security plan? [ ] Yes [ ] No

3.3.2 If the answer to 3.3.1 is YES, for each of such occasions please indicate the special or additional security measures were taken by the ship (SOLAS regulation XI-2/9.2.1.4):

Date

No From6 To6 Port. Country, Port Facility and UNLOCODE3 Ship-to-Ship additional security measures

3.4 List the ship-to-ship activities7 in chronological order with the most recent ship-to-ship activity first, which have been carried out during the period specified in 3.3

[ ] Not applicable

Date

No From6 To6 Location or Latitude and Longitude Ship-to-Ship activity

3.4.1 Have the ship security procedures. Specified in the approved ship plan, been maint[]ned d[]ing each of the ship-to-ship activities specified in 3.4(SOLAS regulation XI-2/9.21.5)? Yes No

3.4.2 If the answer to 3.4.1 is NO identify the ship-to-ship activities for which the ship security procedures were not maintained and indicate, foe the security measures which were applied in lieu:

Date

No From6 To6 Security measures applied Ship-to-Ship activity

3.5 Provide a general description of cargo aboard the ship (SOLAS regulation XI-2/9.2.1.6 and paragraph B/4.39.5 of ISPS Code):

3.5.1 Is the ship carrying any dangerous substances8 as cargo? Yes[] No[]

(50)

3.5.2 If the answer to 3.5.1 to 3.5.1 is YES, provide details or attach a copy of the Dangerous Goods Manifest (IMO FAL Form 7)

3.6 A copy of the ships Crew List (IMO FAL Form 5) is attached []

(SOLAS regulation XI-2/9.2.1.6 and paragraph B/4.39.4 of the ISPS Code)

3.7 A copy of the ship's Passenger List (IMO FAL Form 6) is attached []

(SOLAS regulation XI-2/9.2.1.6 and paragraph B/4.39.4 of the ISPS Code)

4 Other security-related information

4.1 Is there any security-related matter you wish to report? [] Yes [] No

4.1.1 If the answer to 4.1 is YES, provide details9

5 Agent of the ship at intended port of arrival

5.1 Name mid contact details (telephone number) of the agent of the ship at the intended port of arrival:

6 Identification of the person providing the information

6.1 Name:

6.2 Title or position10:

6.3 Signature:

This report is dated at<enter place>on<enter time and date>.

AMENDMENTS TO SOLAS 74

THE FOLLOWING CHANGES HAVE TAKEN PLACE IN SOLAS-74 IN COMPLIANCE WITH THE LATEST SECURITY REQUIREMENTS

A) SOLAS chapter V, regulation 19 has been amended to make the first safety equipment survey after 1st July, 2004 but not later than 31st December, 2004 as the cutout date for implementation of AIS on ships other than passenger vessels and tankers of 300 gross tonnage and above but less than 50,000 gross tonnage.

Ships fitted with AIS shall maintain AIS in operation at all times except where international agreements, rules or standards provide for the protection of navigational information.

B) The existing chapter XI is renumbered as Chapter XI-1

1. Regulation 3 in XI-1 has been amended detailing ship's identification number.

2. New Regulation 5 has been added in XI-1 detailing the requirements and procedures for maintaining a "Continuous Synopsis Record" (CSR) on board vessels.

C) Complete new Chapter numbered as XI-2 has been included.

CHAPTER XI-2

SPECIAL MEASURES TO ENHANCE MARITIME SECURITY

Regulation 1	Definitions
Regulation 2	Application
Regulation 3	Obligations of contracting Governments with respect to security.
Regulation 4	Requirements for companies and ships
Regulation 5	Specific responsibility of companies
Regulation 6	Ship security alert system
Regulation 7	Threats to ships
Regulation 8	Master discretion for ship safety and Security.
Regulation 9	Control and compliance measures
Regulation 10	Requirements for port facilities
Regulation 11	Alternative security agreements
Regulation 12	Equivalent security arrangements
Regulation 13	Communication of information

Appendix to Part A

Appendix 1 : INTERNATIONAL SHIP SECURITY CERTIFICATE

Appendix 2 : INTERIM INTERNATIONAL SHIP SECURITY CERTIFICATE

Appendix to Part B

Appendix 1 : FORM OF A DECLARATION OF SECURITY BETWEEN A SHIP AND A PORT FACILITY

Appendix 2 : STATEMENT OF COMPLIANCE OF A PORT FACILITY

RESOLUTIONS :

Total 11 Resolutions were adopted in Diplomatic Conference in Dec. 02

RESOLUTION 1 : Adoption of amendments to the annex to the International convention for the safety of Life at Sea, 1974, as amended.

RESOLUTION 2 : Adoption of the International Ship and Port Facility Security Code.

RESOLUTION 3 : Further work by the International Maritime Organization (IMO) to the enhancement of Maritime Security.

Bearing in mind the provisions of chapter XI-2 of convention and the International Ship and Port Facility security (ISPS) Code, to :

(a) develop training guidance such as model courses for ship security officers, company security officers, port facility security officers and company, ship and port security personnel.

(b) review the IMO's assembly resolution A.787(19) as amended by resolution A.882(21) on procedures for port state control and, if found necessary develop appropriate amendments thereto.

(c) consider the need and, if necessary, develop further guidance on control and compliance measures on aspects other than those already addressed in part B of the ISPS code.

(d) consider the need and, if necessary, develop guidelines on recognized security organizations.

(e) review the IMO assembly resolution A.890(21) on principles of safe manning and, if found necessary, develop appropriate amendments thereto.

(f) review the aspect of security of ships to which chapter XI-2 of the convention applies when interfacing with floating production storage units and floating storage units and take action as appropriate.

(g) consider, in the context of security, relevant aspects of facilitation of maritime traffic such as, for example, port arrivals and departures, standardized forms of reporting and electronic data interchange and take action as appropriate.

(h) review the IMO's Assembly resolution A.872(20) on guidelines for the prevention and suppression of the smuggling of drugs, psychotropic substances and precursor chemicals on ships engaged in international maritime traffic and, if necessary, develop appropriate amendments thereto.

(i) consider the need and, if necessary, develop any other guidance or guidelines to ensure the global, uniform and consistent implementation of the provisions of chapter XI-2 of the convention or part A of the ISPS Code.

And to adopt them in time before the entry into force of the amendments to the convention adopted by the conference or as and when the IMO considers appropriate.

RESOLUTION 4 : Future amendments to chapters XI-1 and XI-2 of the 1974 SOLAS convention on special measures to enhance maritime safety and security.

RESOLUTION 5 : promotion of technical co-operation and assistance.

There is a proposal to set up a Maritime Security Trust Fund apart from co-operation offered by richer nations.

Contracting Governments to the convention and member states of the IMO to :

a) provide, in co-operation with the IMO, assistance to those states which have difficulty in implementing or meeting the requirements of the adopted amendments or the ISPS code, and

b) use the Integrated Technical Co-operation Program of the IMO as one of the main instruments to obtain assistance in advancing effecting implementation of, and compliance with, the adopted amendments and the ISPS code.

RESOLUTION 6: Early implementation of the special measures to enhance maritime security.

Contracting Government and Administrations concerned designate dates, in advance of the application date of 1st July 2004 by which requests for :

1. review and approval of ship security plans
2. verification and certification of ships
3. review and approval of port facility security assessment and of port facility plans

RESOLUTION 7 : Establishment of appropriate measures to enhance the security of ships, port facilities, mobile offshore drilling units on location and fixed and floating platforms not covered by chapter XI-2 of the 1974 SOLAS Convention.

Chapter XI-2 of the convention applies only to :

a) the following types of ships engaged on international voyages:

   i) passenger ships, including passenger high-speed craft

   ii) cargo ships, including cargo high speed craft of 500 gross tonnage and upwards.

   iii) mobile offshore drilling units.

b) port facilities serving such ships engaged on international voyages.

RESOLUTION 8 : Enhancement of Security in Co-operation with the International Labour Organization (ILO)

Seafarers Identity Documents and work on the wider issues of port security.

RESOLUTION 9 : Enhancement of security in co-operation with the World Customs Organization.

Invites WCO to consider urgently measures to enhance security throughout international closed cargo transport units (CTU) movement.

RESOLUTION 10 : Early implementation of long-range ship's identification and tracking.

Inmersat polling is currently appropriate system for the issue underlined. The above ships should be prepared to respond automatically to inmersat polling or to other available system.

RESOLUTION 11 : Human element related aspects and shore leave for seafarers.

SECURITY GUIDELINES FOR VESSELS

Navigation and vessel inspection circular No. 1002 of USCG,

- Performing Security Assessments
- Demonstrating Security Plans
- Implementing Security i.e. Protective measures
- Procedure and Operations.

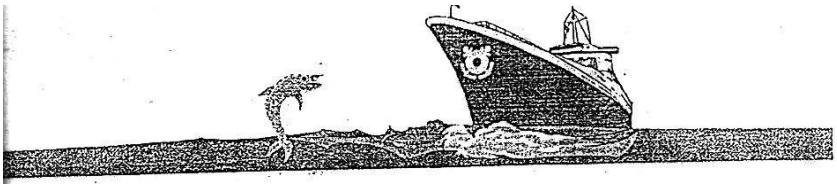
TRAINING COURSES — ABBREVIATIONS

CG	=	CONTRACTING GOVERNMENT
DA	=	DESIGNATED AUTHORITY
RSO	=	RECOGNISED SECURITY ORGANISATION
CSO	=	COMPANY SECURITY OFFICER
DOS	=	DECLARATION OF SECURITY
SSO	=	SHIP SECURITY OFFICER
SSA	=	SHIP SECURITY ASSESSMENT
SSP	=	SHIP SECURITY PLAN
PFSA	=	PORT FACILITY SECURITY ASSESSMENT
PFSP	=	PORT FACILITY SECURITY PLAN
ISPS CODE	=	INTERNATIONAL SHIP AND PORT FACILITY SECURITY CODE
ISSC	=	INTERNATIONAL SHIP SECURITY CERTIFICATE
NAVIC	=	NAVIGATION AND VESSEL INSPECTION CIRCULAR

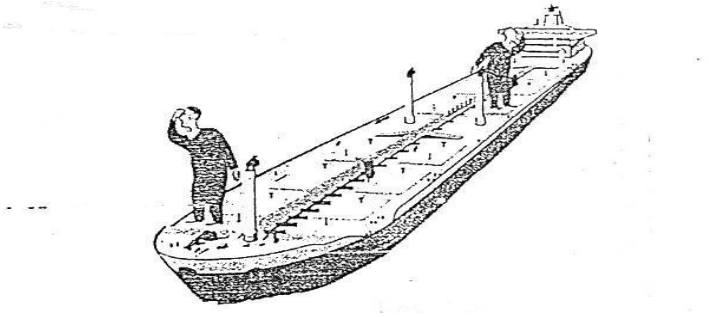
SECURITY LEVELS 1, 2, 3

The Security levels 1, 2, 3 correspond to normal, medium and high threat situations respectively.

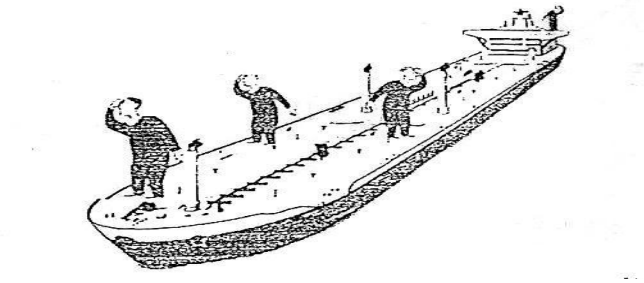
Level 1
the ship operates as usual.



Level 2
provides for additional measures in case of increased risk of a security incident.



Level 3
is the highest level and applies for the period of time when there is an imminent risk of a security incident.



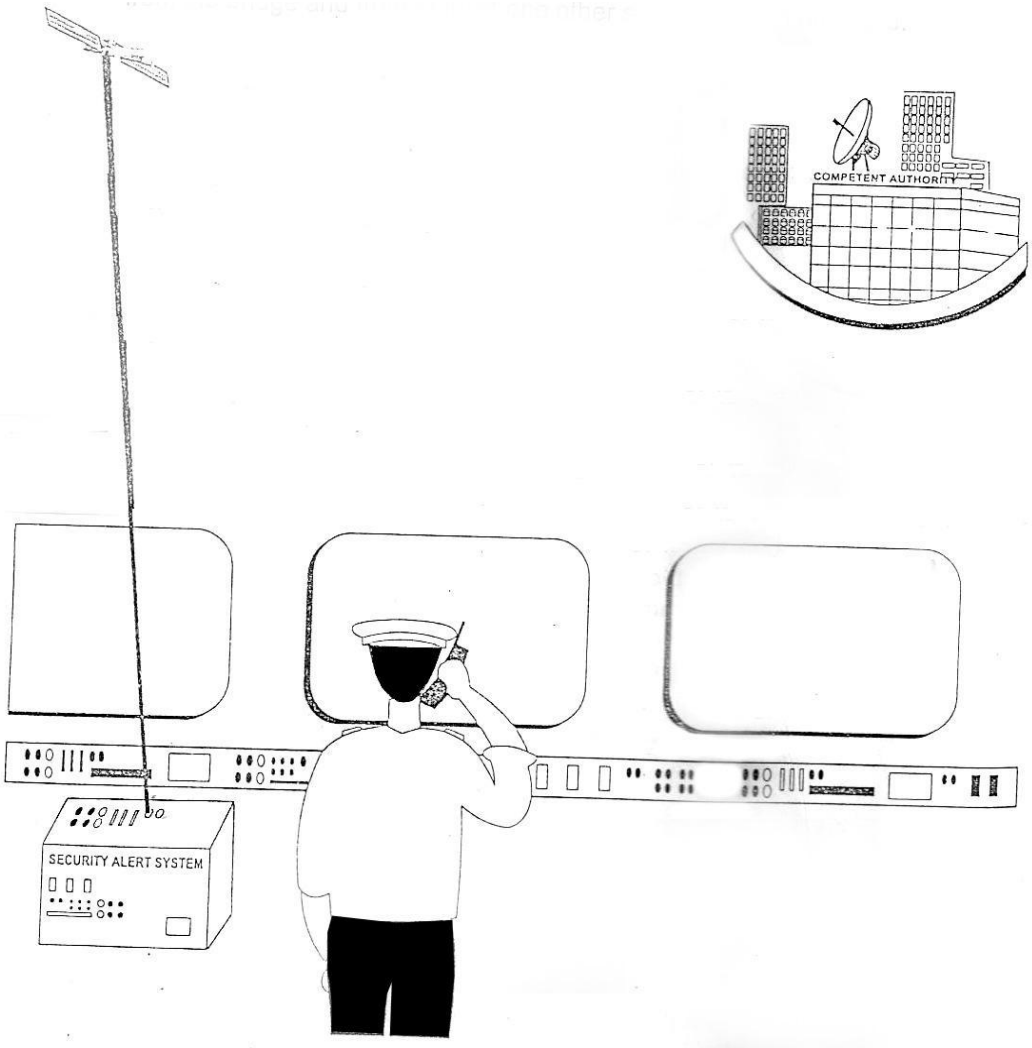
The SSO will inform you of the current security level on board and any .....

SHIP SECURITY ALERT SYSTEM

Ships are required to have a Security Alert System which, when activated, will transmit a ship-to-shore security alert to a competent authority designated by the Flag Administration. The Security Alert will identify the ship, its location and that the security of the ship is under threat or has been compromised.

The Ship Security Alert will not sound any alarm on board nor to any other vessel or authority in the immediate vicinity.

The Ship Security Alert System must be capable of being activated from the bridge and from at least one other secret location on board.



10. Anti Piracy

Difference between piracy and armed Robbery:
The legal difference between piracy and armed Robbery is that piracy is conducted outside of a nations territorial waters, whereas armed robbery , (which may for all practical purposes amount to the same thing as piracy), is conducted inside territorial waters

Piracy attack – DEEFINITION:
A Piracy attack may include (but is not limited to) actions such as the following

- Use of violence against the ship or its personnel or any attempt to use violence.
- Attempts to board the vessel where the master suspects the persons are pirates.
- Attempts to overcome the ship protective measures by the use of ladders, grappling hooks and weapons.

10. Piracy awareness – prior entering areas of risk

What will be the risk during sailing?

Statistically the risk of being captured is very small.

In 2011 situation: 648 seafarers were taken in Somalia. There were approximately 42,450 vessels transiting the Goa in 2011 (One Earth future Foundation document

Economic cost of piracy 2011. Based on an average vessel crew of 15 this gives a percentage of 0.001% seafarer's being taken hostage

Maritime piracy is a reality for a small number of seafarer and their families concern about maritime piracy is a reality for many seafarers and their families

The risk is small, but the concerns are large.

PIRATES PRONE AREA AT SEA:

SOUTH EAST ASIA AND INDIAN SUB CONTINENT

Bangladesh sea coast

Indonesia: Tanjung Priok – Jakarta / Dumai, Belawan , Balipapan, Taboneo, Muara jawa, Samarinda, Nipah Anchorage waters. Pirates normally armed with guns / knives and / or machetes. Generally be vigilant in other areas. Many attacks may have gone unreported. Pirates / robbers normally attack vessel during the night when spotted and alarm sounded, pirates/robbers usually abort the attempted attacks.

Malacca Straits: Although the number of attacks has dropped substantially due to the increase and aggressive patrols by the littoral states authorities since JULY 2005, ships are advised to continue maintaining strict anti piracy watches when transiting the straits. Currently, there are no indications as to how long these patrols will continue or reduce.

Singapore Straits: Vessel are advised to remain vigilant and to continue maintaining adequate anti piracy watch and measures. Pirates /robbers attack ships while underway or while anchored at the straits.

South China Sea: Although, no attacks reported recently in the vicinity off Anambas / Natuna / Mangkai islands / Subi Besar / Merundung area, vessel are advised to remain vigilant.

AFRICA AND RED SEA.

Lagos (Nigeria)

Cotonou (Benin):

Lome

Abidjan (Ivory Coast):

Gulf of Aden/ Red Sea:

Somalia.

10.1 The strengths and vulnerabilities of crews and ships

10.1.1 Ships to be like a fortress – the available strengths of the ship to defend a pirate attack

10.1.2 Being slow moving, ship is a vulnerable target with limited deterrent in terms of returning an attack

10.1.3 Other Factory which determine the vulnerability of attack are

- Ship size
- Speed
- Freeboard
- Sea state
- Visibility
- Day night condition affecting the vulnerability to an attack

10.2 The anti – piracy measures (civilian and military)

- Private armed forces and security services and military of various countries provided the support

Measures to prevent piracy at sea

- The Government has initiated various preventive/ mitigating security measures to deal with piracy at sea. These are as follows:

(i) An inter – Ministerial Group of officers (IMGO) has been set up to deal with hostage situation arising out of the hijacking of merchant vessel with Indian crew on board.

(ii) Issuance of notices by Director General of Shipping detailing elaborate anti – piracy measures (Best Management Practices) including safe house/citadel.

(iii) Banning of sailing vessel to ply in waters south or west of the line joining Salalah and male.

(iv) Naval escort provided by Indian naval ships in Gulf of Aden.

(v) Enhanced vigil by Indian navy in Indian Exclusive Economic Zone (EEZ) and westward up to 65 degree east longitude.

Besides India is participating in the contact Group of piracy off the coast of Somalia (CGPCS) meetings, which is a United Nation (UN) initiative, to address the piracy related concerns. Since its inception the Government have actively participated in all efforts of the CGPCS to share information, coordinate actions of its navies, raise public and merchant marine awareness of the risks of apprehended pirates. India has successfully brought to the attention of the CGPCS the welfare of the hostages and their families and the responsibilities of the ship owners, both during a piracy situation as well as after the hostages have been released.

10.2.1 The anti – piracy measures that can be adopted make the ship less vulnerable to prates boarding it

Since 1 February 2009, MSCHODA (www. mschoa.org) has established the internationally recommended transit corridor (IRTC) within the Gulf of Aden. Military assets (Naval and Air) are strategically deployed within the area to best provide protection and support to merchant ships.

Ships/owner are advised to register their details on the MSCHOA website and obtain further information regarding the close support protection details for ships transiting the Gulf of Aden.
Masters using the IRTC are not relieved of their obligation and should continue to maintain a strict 24 hour lookout using all available means to get an early warning of an approaching threat. Vessels have been attacked / hijacked in the corridor.

Masters are also advised to maintain a listening watch on recommended VHF Channels in order to hear the Maritime Advisory Calls from the warships in the area who will make general security broadcasts and in turn also listen to merchant ships calling them.
Masters are also advised to monitor the IMB piracy Reporting Center (PRC) broadcast and warning via Inmarsat C EGC safety net. All attempted and actual attacks and suspicious sightings reported to warships should also be reported to the IMB PRC.

10.2.2 Adopting self – protecting measures to detract deter or delay a piracy attack
The SPMS are the most basic level which will likely be effective. The advice rests on the premise that
"If pirates are unable to board a ship they cannot hijack it"

- Watch keeping & Enhanced Vigilance

There is advice that vessels should consider a shorter rotation of the Watch period in order to maximize alertness of the lookouts. The use of anti-glare binocular s is encouraged. The use of "well constructed dummies" remains – however the unequivocal view is that, "A proper lookout is the single most Effective methods of self protection where early warning of a suspicious approach or attack is assured, and where defenses can be readily deployed."

- Enhanced Bridge Protection

The bridge is usually the focus for any pirate attack. BMP4 states that Kevlar jackets and helmets (preferably in non-military colours) should be available for

The bridge team. Flying glass is a major issue when the bridge is attacked – as such the use of security glass film often called Blast Resistant Film is encouraged.
Metal (steel/aluminum) plates may be used for the side and rear bridge windows and the bridge wing door windows. The use of sand bags on bridge wings is also encouraged. In order to protect from RPG shells the guidance states that "the sides and rear of the bridge, and the bridge wings, may be protected with a double layer of Chain Link Fence
Which has been shown to reduce the effect of an RPG round. Proprietary

Razor wire
Should be secured so pirates cannot pull off the razor wire with, for instance, the hook of their boarding ladder.

FIT SENSORS

USE DECK WATER

Control of Access to Bridge, Accommodation & Machinery Spaces
It is very important to control access routes to deter or delay pirates who have managed to board a vessel. If pirates do again access to the upper deck of a vessel they will be tenacious in their efforts to access the accommodation section and in particular the bridge. It is strongly recommended that significant effort is expended prior to entry to the High Risk Area to deny the pirates access to the accommodation and the bridge, should they overcome the vessel's ship protection measures and be able to board the vessel. All doors and hatches providing access should be secured. Afford the ship the maximum protection possible

10.2.3 Transiting the high risk area in the recommended zone and preferably in a convoy

Best Management Practices (BMP4), provides Suggested Planning and Operational Practices for Ship Operators, and Masters of Ships Transiting the High Risk Area

- Great emphasis places on the briefing of crew and of the conducting of drills.
- Master's should also consider Testing SPMs, testing of the security of all access points and a thorough review of the SSP
- Master's are advised to prepare an Emergency Communication Plan, this will include all emergency contact numbers and prepared messages.

Reporting of Somali incidents only-

The UK Maritime Trade Operations (UKMTO)
The Maritime Security Centre – Horn of Africa (MSCHOA) which is the planning and coordinate centre for EU Naval forces (EUNAVFOR)

UKMTO: Tel: +971 50 552 3215, Fax: +971 4 306 5710, Email: UKMTO@eim.ae

MSCHOA: Tel: +44 (0) 1923 958545, Fax: +44 (0) 1923 958520, Email: postmaster@mschoa.org

NATO: Tel: +44 (0) 1923 956574, Fax: +44 (0) 1923 956575. Email: info@shipping.nato.int

IMB PRC: Tel: +60 3 2031 0014, Fax: +60 3 2078 5769, Email: piracy@iccccs.org/ imbkl@icc-ccs.org

- The ships AIS policy is reviewed. The recommendation is now to keep AIS on-though this is left to the Master's discretion. This section once again stresses the importance of reporting to MSCHOA and UKMTO. During transit through the High Risk Area:
- No maintenance should be performed on essential equipment in the Engine Room.
- There is an enhanced policy for daily reporting to UKMTO via email at 0800 GMT.
- Masters are encouraged to carefully review all warnings

10.2.4
Communication with the flag state, costal authority and task force to update ship position frequently is very vital

10.3 Understand the contents of the best Management practices (BMP) guide as issued by Industries bodies and updated from time to time

The three Fundamental Requirements of BMP"

In essence these consist of:

Register at MSCHOA – In addition to the usual bounding areas, the Straits of Hormuz are now included

Report to UKMTO
- UKMTO acts as the primary points of contact for merchant vessels and liaison with military forces in the region and it is the primary point of contact during an attack. For this reason UKMTO should be made aware that the vessel is transiting the High Risk Area.

Implement Ship Protection Measures (SPMs)
- These are the most basic measures likely to be effective at reducing the risk of piracy attack. If pirates are unable to board a ship they cannot

BMP4 stresses some basics on how to avoid being a victim of piracy:

- Do not be alone
  - Report, use IRTC, and keep AIS On
- Do not be detected
  - Use Nav. Lights only, Follows NAVWARNS
- Do not be surprised
  - be vigilant
- Do not be vulnerable
  - SPMs
- Do not be boarded
  - Speed and manoeuvers
- Do not be controlled
  - Drills, Citadels, access control

- If armed Private Maritime Security Contractors are present on board a merchant vessel, this fact
  Should be included in reports to UKMTO and MSCHOA.

The international Maritime Organization (IMO) have produced guidance in the form of an IMO Circular for ship operators and Masters and for Flag

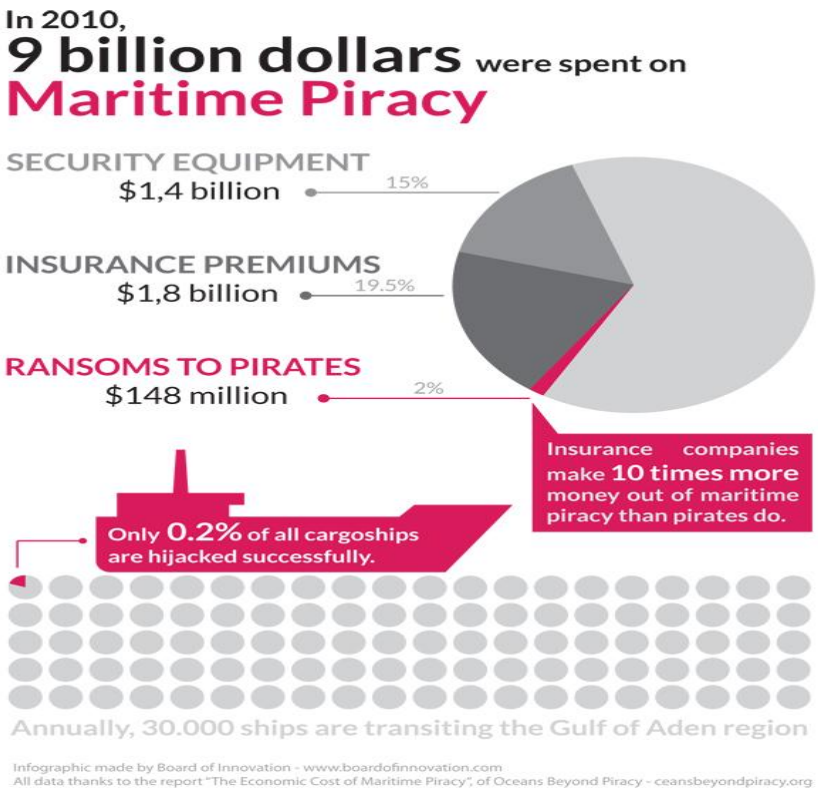
- States on the use of Private Maritime Security Contractors in the High Risk Area.

- The current IMO guidance on the use of armed Private Maritime Security Contractors is included on the MSCHOA website (www.mschoa.org).

- Armed Private Maritime Security Contractors there is an additional examination on the use of armed Private Maritime Security Contractors.
  The use, or not, of armed Private Maritime Security Contractors onboard merchant vessels is a Matter for individual ship operators to decide following their own voyage risk assessment and approval of respective Flag States.

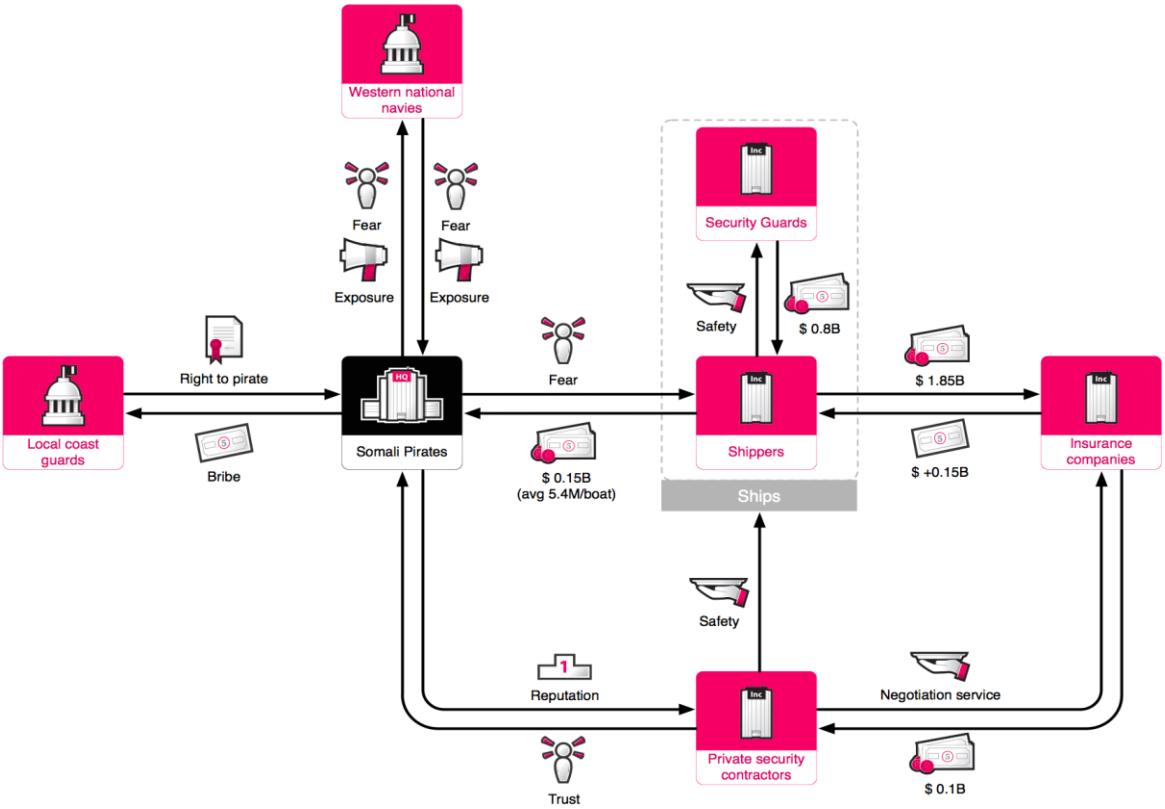
Subject to risk analysis, careful planning and agreements, the provision of Military Vessel Protection Detachments (VPDs) deployed to protect vulnerable shipping is the recommended option when considering
armed guards. This advice does not constitute a recommendation nor endorsement of the general use of armed Private Maritime Security Contractors.

10.4 Pirates Business model



In a report about "The Economic Cost of Maritime piracy", the annual cost of Piracy, is estimated between $7 to $12 billion dollars. The most remarkable fact is that only iess than 2% of the annual estimated cost actually goes to the pirates. So where is all the other money going to? The business model involves more parties then only Somali fisherman and shippers. As we have visualized below; insurance companies, security contractors and national navies are winning in this model too.

The piracy model is a great example of the **"Fear Economy"**. Nowadays many (legal) companies use "fear "to boost their business. unnecessary insurances.



In 2010, $148 million of ransoms were paid to pirates. On the other hand, **$1.85 billion dollars were spent on insurances to cover piracy**, that's 10 times more than the actual ransoms that are given to pirates. In reaction to the growing threat and cost of ransoms, the whole model came in a loop and the maritime insurance industry has responded by increasing its shipping rates and premiums. As national navies declared the Gulf of Aden as a war zone, premiums increased even more.

Another winning party are the private security contractors. Their job is not to prevent piracy but to free the ship and crew by negotiating and delivering the ransom. Of course it is in the interest of the insurance companies that those ransoms stay as low as possible; that's why a good collaboration between those two parties has been established. Security contractors enter into a sort of partnership with the attackers, building up reputation for fair play. "Successful negotiation funnels cash to criminal gangs, fueling further hijacking – and further opportunities for security companies."

If you know that only 0,2% of all cargo ships in the northeast Gulf of Aden is hijacked, the average cost of an armed transit through Somali waters is in the order of $34.000, war risk insurance can go up to $150.000 per ship, per voyage; **it's may be better to take the risk!**

Somali Piracy Declines While West African Piracy Spreads

U.S. Navy sailors and Nigerian Special Forces fighters train to combat piracy off the coast of West Africa.

Piracy off the coast of Somalia has fallen steeply since 2011 as a result of a U.S.-led international campaign, but it is flourishing along the coast of West Africa

Somali pirates captured 10 vessels in 2012, compared to 34 in 2011 and 68 in 2010. The last successful Somali pirate attack on a large commercial vessel occurred nearly one year ago on May 10, 2012.

"The trend is clear," "The progress that has been made is real and remarkable."

International campaign against Somali piracy has disrupted the pirates' "business model."

"Pirates today can no longer find helpless victims like they could in the past, and pirates operating at sea now often operate at a loss.

This Factors that decline piracy in Somalia.

- An international campaign coordinated by more than 80 countries and international organization.
- Placing armed security teams aboard merchant ships and
- Using security measures such as razor wire and
- Passing through pirate-infested waters at maximum speed
- Tracking the financial flows from piracy operations, leading to the capture and jailing of pirate kingpins; and
- Supporting the formation of a responsible government in Somalia capable of controlling its territorial waters.

"Once Somalia is capable of policing its own territory and its own waters, piracy will fade away. To that end, the United States continues to support the newly established government in Mogadishu.

11. Pirate Attack

11.2 Assessing to defend the crew and the ship

There is a detailed examination of the criteria that any Naval/Military forces will apply before
considering a boarding operation to release the crew from a Citadel.
The criteria include:
100% of the crew must be secured in the Citadel.
The crew of the ship must have self contained, independent reliable 2-way communications
(sole reliance on VHF communication is not sufficient)

The pirates must be denied access to ship population
Closed Circuit Television (CCTV)
& Upper Deck Lighting BMP4 goes into some detail about the use of Closed Circuit Television (CCTV)
and the use of Upper Deck Lighting.
However it is stressed that navigation lights should not be switched off at night.
Ship's Tools & Equipment There is a section on the importance of denying pirates the use of ship's tools or equipment. The BMPs also stress the importance of protecting ship's equipment such as gas bottles or flammable liquids/materials-using sand bags or Kevlar blankets.

Safe Muster Points/Citadels

Safe Muster Point is a short-term safe haven, which will provide ballistic protection should the pirates commence firing with small arms weaponry or RPGs. Citadels get a lot of coverage in BMP4-If citadels are to be employed, they should be complementary to, rather than a replacement for, all other ship Protection Measures set out in BMP4. It is stressed that establishing a Citadel maybe beyond the capability of a ship's staff alone, and requires external technical advice and support. The details of the construction and operation of Citadels are beyond the scope of this booklet. A detailed document containing guidance and advice is included on the MSCHOA website. BMP4 perhaps reflecting this fact has deleted a series of measures to enhance a safe-haven. It is important to remember that the use of a Citadel, even where the criteria are applied, cannot guarantee a Naval/Military response. This is now explicit within the BMPs.

Private Maritime Security Contractors use of private maritime security contractors – both armed and unarmed Private Maritime Security Contractors is a matter for individual Ship Operators following their own voyage risk management. The deployment onboard is subject to the national laws of the Flag State. If armed Private Maritime Security Contractors are to be used they must be as an additional layer of protection and not as an alternative to BMP.

11.2.2 The step by step actions to be taken during an attack

If a vessel suspects that it is coming under a pirate attack, there are specific actions that are recommended to be taken during the approach stage, and the attack stage. It should be noted that the pirates generally do not use weapons until they are within two cables of a vessel. Therefore any period up to this stage can be considered as "approach" and gives a vessel valuable time in which to activate her defences, and make it clear to pirates that they have been spotted and the vessel is prepared and will resist.

Approach Stage

When being approached, if not already at full speed, increase to maximum. Steer a straight course to maintain a maximum speed.

The communication plan at this time is vital, and in addition to previous advice BMP4 also states that once established, the vessel should maintain communication with UKMTO. The advice also states that attacks should reported with UKMTO even if the vessel is part of a national convoy so other merchant ships can be warned.

The issue of ballistic protection is a key element of the new guidance, and when under attack it is stressed that all crew except those required on the bridge to muster at the Safe Muster Point or Citadel if constructed, so that the crew are given as much ballistic protection as possible should the pirates get close enough to use weapons.

When discussing the man oeuvres used to keep clear of pirates, the latest advice no longer Contains explicit mention of the use of bow and stern wash to restrict incoming pirates.

When the attack comes in, the advice is to ensure that all external doors and, where possible, internal public rooms and cabins, are fully secured

In addition to the emergency alarms and announcement for the benefit of the vessel's crew, sound the ships whistle/foghorn continuously to demonstrate to any potential attacker that the ship is aware of the attack and is reacting to it.

During Attack Stage:

It is important to reconfirm that all ship's personnel are in a position of safety. As the pirates close on the vessel, Masters should commence small alterations of helm whilst maintaining a speed to deter skiffs from lying alongside the vessel in preparation for a boarding attempt. These maneuvers will create additional wash to impede the operation of the skiffs. It is stressed that substantial amounts of helm are not recommended, as these are likely to significantly reduce a vessel's speed.

11.2.3 Retreat the citadel in the event pirates board the ship

11.2.4 Communication channels must be kept open with task forces and local co-ordination authorities to update situation periodically.

If the Pirates take Control

'If the Pirates take Control"- "try to remain calm" Before the pirates gain access to the bridge inform to UKMTO. Ensure that the SSAS has been activated and the AIS is switched on.

As with earlier BMPs it is stressed that no resistance should be offered to the pirates once they reach the bridge. BMP4 now expressly states that pirates are likely to be aggressive, highly agitated and possibly under the influence of drugs (khat).

If the bridge/engine room is to be evacuated the main engine should be stopped and all Way taken off the vessel if possible, (and if navigationally safe to do so). All remaining crew members should proceed to the designated Safe Muster Point.

BMP4 also stresses that any CCTV should be kept running.

11.3 Coping in a hostage situation

Remember it is the situation which is abnormal not you
Think positively, Stay calm, focused compliant and confident.
Maintain hygiene and good physical health.
Keeping busy and maintaining routine lessens anxiety.

11.3.1 Examine possible personal reactions to activities of pirates during a hostage situation

11.3.2 Reiterate the importance of obedience to the pirates orders there are no dead heroes.

11.3.3 Understand possible personal reactions in immediate crisis situation, post crises situation, short term after situation

11.3.4 Understand provocations from pirates and possible techniques to cope with the ensuring hostage situation.

11.3.5 Coping in the long term in the captive situation

12 The Release process

12.1 Understand what happens prior to the release

After the negotiation between the pirates and concerned authorized get materialized hostage will be released

The means and mode of transfer of money will be agreed the position of vessel may be altered according to the demand.

12.2 The additional dangers associated with the release process

If the agreed amount to pay is being delayed due to some reason this may affect the hostage. Crew can give an assurance that will stay together with pirates until the money is handed over to them.

12.3 The safeguards to adopt during the release process follow blindly the instruction given do not show heroic acts at last be cool, Hold your patience, ----------only aim is to return home.

12.4 The practical needs of the crew after release

- Good food
- Medical Check up
- Psychological support and training.
- Set of clothes.
- Direct communication with their family members
- Complete ship should be provided with disinfectant, cleaning, material and toiletries.

12.5 Various parties Involved in the post release

- Shipping company / owner
- Flag state.
- 3rd party negotiator
- Consulate

13 Seafarer's family:

13.1 Advantage of seeking employment with reputed ship owner/manager

Involvement

- Need for credible information
- Company Liaison person
- Support during & after incident
- Support organizations

13.2 Sharing with family regarding risk of piracy

A seafarer should take the lead in and is responsible for informing his family members about piracy and company-procedures.

Ask this questions regarding piracy?

- What could be the greatest worries or concerns in your family about Piracy?
- What is your own specific responsibility towards your family?

13.3 Possible reaction and worries of family during a piracy crisis:-

- Confusion, Uncertainty, Worry, Fear, Anxiety, Shock, Anger, Distrust
- Concerns regarding financial situation
- Family strife
- Loss of trust with the comapny

13.4 Seafarer's own specific responsibility

Seafarers should be able to communicate with their families the procedure the company has in place to protect the vessel and crew from pirates and what would happen in the unlikely event of the vessel hijacked.

- Ensure that the family has the correct contact details of the company in the event of a piracy attack
- Ensure that the company has the up-to-date family contact details and family liaison representative details
- Seafarers should know their legal rights and contractual entitlements after a period of piracy

13.5 Be aware of the reactions of the family members when informed about the seafarer being taken hostage.

Reaction of the family following an attack will be similar to those of the seafarer

There will be confusion of information as for the first few days there may me little or no communication from the ship. This will lead to

- Confusion
- Uncertainty,
- Worry, Fear, Anxiety, Shock, Anger, Distrust.
- Loss of faith with the company.