AN APPROACH TO UNDERWATER CRITICAL INFRASTRUCTURES PROTECTION

Antonio Arnao, Antonio Sánchez, Manuel Pérez

Sociedad Anónima de Electrónica Submarina (SAES)

Carretera de la Algameca, s/n, 30205 Cartagena, Spain

Tlf. +34 968 508214 Fax: +34 968507713

a.arnao@electronica-submarina.com, a.sanchez@electronica-submarina.com,

m.perez@electronica-submarina.com

Abstract

After 9/11, a more complex environment and an unsafe world have faced us. All nations and communities are jointly pushed to reinforce their research and development resources, on the protection and security fields, to provide their citizens and critical infrastructures with a suitable degree of safety against potential terrorist actions.

Maritime transport represents a high percentage of global transport, therefore protection of approaches to harbours and internal harbour waters require of a special interest, even when these hostile actions are initiated and carried out from the sea.

In addition to well-known technologies, others are emerging to support the growth of necessities and capabilities required to allow more safety. This paper deals with different underwater threats and the platforms (e.g. unmanned vehicles), sensors and other means to be used, to detect, locate and counteract underwater threats as divers or small underwater vehicles.

Keywords: Harbour protection, Critical Infrastructure protection, underwater threats, unmanned vehicles, underwater sensors, diver detection.

1 INTRODUCTION

The European Commission in its main policy document on critical infrastructures '*Critical infrastructure protection in the fight against terrorism*' from 2004, offers the following broad description "*Critical infrastructures consist of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the member states. Critical infrastructures extend across many sectors of the economy, including banking* *and finance, transport and distribution, energy, utilities, health, food supply and communications, as well as key government services*."

In its Green Paper on Critical Infrastructures, published in November 2005, the European Commission identify the following key sectors to the national security and the essential functioning of industrialized economies:

- Energy
- Nuclear industry
- Information, communication technologies, ICT
- Water
- Food
- Health
- Financial
- Transport
- Chemical industry
- Space
- Research facilities.

Many of these sectors are related with harbour or marine environments through the facilities where the activities are developed, as is the case of oil refineries, nuclear power stations, electric power stations, vessels at pier side or anchored, etc. During the past few years the awareness of the necessity of protecting these critical infrastructures against terrorist threats has increased. Threats can generically operate from air, land and sea (above or below the surface). Figure 1 shows some of these critical infrastructures:

Figure 1. Some examples of critical infrastructures located in marine environments. Nuclear power station (left), oil refinery (middle) and oil platform (right).

Traditionally attention has been paid mainly on non-underwater threats, which have received the main part of the resources assigned to the protection of critical infrastructures. As a consequence, a high level technology against these threats has been developed, based on: access control, radars, thermal cameras, infrared cameras, etc.

However, the underwater threat has not been considered of high priority until terrorist attacks by divers have been planned or performed, as was the planned attack of Argentinean divers against British warships in Gibraltar during the Falkland war, the attacks of suicide divers from the Liberation Tigers of Tamil Eelanm (LTTE) to Sri Lanka navy vessels in 1995, causing the sinking of a number of them, or the attack from Hamas' divers to an Israeli beachfront guard post in 1994. As a consequence, the technical development to counteract underwater threats has been lower, but rapidly increasing in the last years.

The current trend is to provide an overall security environment for the protection of the critical infrastructures that encompasses all the foreseen threats by means of integrated system as this shown in Figure 2. These systems have to be, in turn, integrated in a higher layer with systems from the security forces, harbour authorities, etc., and coordinated by an unique authority.

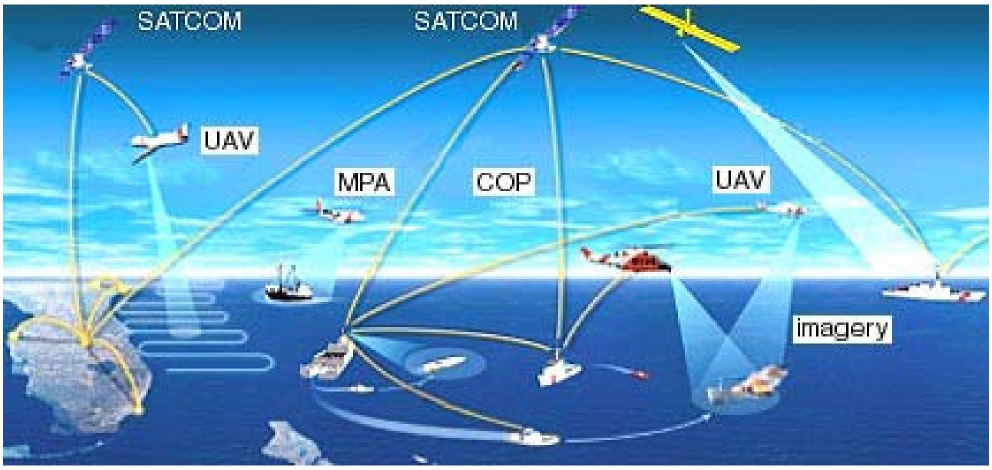


Figure 2. Integrated marine environment security system

Nowadays it is evident the lack of appropriate international laws regulating and encouraging the cooperation between nations in order to protect the critical infrastructures. In spite of this, international efforts have been performed in this field. Starting from 2002, the NATO Naval Armament Group (NNAG) launched the '*Defence Against Terrorism Programme of Work'*, focusing on Harbour and Port Protection. On this frame, Harbour Protection Trials (HPT) have been conducted, starting in 2004 in La Spezzia (Italy) with the aim of evaluating the harbour bottom mapping performance of AUV and followed by HPT-06 based also in La Spezia, devoted to test and verify the capability of modern technologies (AUV, integrated underwater surveillance systems) to counter the terrorism threat in harbour and to support MCM in confined waters, HPT-

07 held in Taranto (Italy) to test the capabilities of multiple sensors against surface intruders and HPT-08 held in Eckernforde (Germany) focused on three-dimensional system integration. Further additional HPT are programmed for 2009, centred on critical infrastructures protection, and 2010 focused on lethal and non-lethal responses.

2 POSSIBLE THREATS

The detection with a high level of confidence of underwater intruders is a very complex task due to the great complexity of the marine environment where the infrastructures to be protected are located. This environment is characterized by the presence of high noise and reverberation levels and by shallow waters with complex, varying with time thermal structures. These factors make significantly difficult the underwater acoustic propagation prediction. Furthermore, the aim is to provide simultaneous protection to a number of facilities along the coast and in the sea, preventing at the same time, as much as possible, the interference with the normal human activities in the area of operation.

The following underwater threats have to be taken into consideration:

- Submarines.
- Mini-submarines.
- Divers (closed and open circuits).
- Remotely operated vehicles (ROV).
- Underwater unmanned vehicles (UUV).
- Swimmer Delivery Vehicles (SDV).
- Sea scooters.
- Bottom-crawling vehicles.
- Mines
    - Bottom (Buried or not)
    - Moored
    - Limpet
- Underwater improvised explosive devices (IED).
- Non-explosive devices
- Decoys or non-identified objects.

Two of these threats are shown in Figure 3.

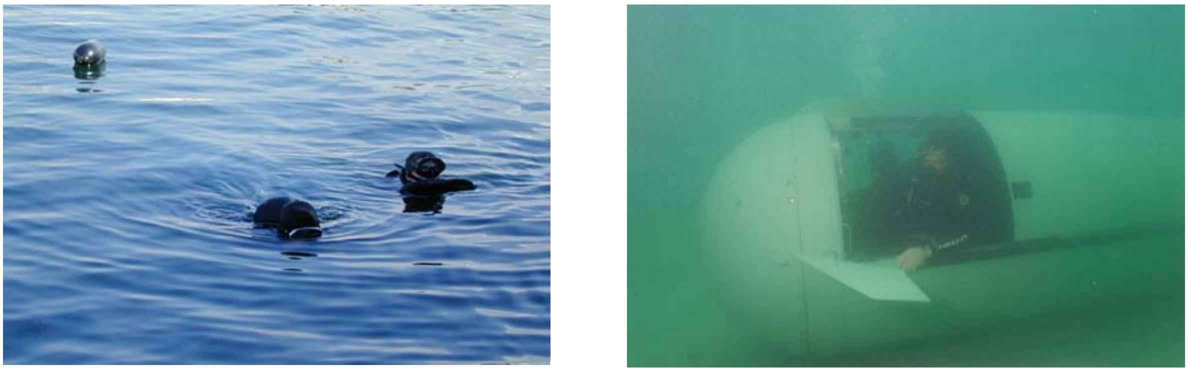


Figure 3. Examples of underwater threats

3 PLANNING, INTEGRATION AND DATA MANAGEMENT

The Communication, Command and Control (C3I) system will be in charge of all: the analysis of the data obtained from any of the available sources (internal or external) in order to plan the location of the surveillance sensors, the inspection and reconnaissance tasks to be performed by the vehicles (hull, pier, bottom) depending on the necessities and the established priorities, and the estimation of performances based on the characteristics of the operational medium, environmental conditions and kind of threat.

During the surveillance phase the C3I system will be in charge of monitoring the status of the sensors, compiling and integrating the data provided by theses sensors, monitoring the trajectory of the manned or unmanned vehicles, etc..

Finally, the C3I system will perform the classification of the contacts, as threat or not, the activation of the alerts/alarms and the coordination with other bodies responsible of acting in situations of crisis. It will provide also elaborated data to higher rank departments.

The first of these phases could have different degrees of complexity as a consequence that the complete system, or part of it, could be deployable as making part of a special scheme as opposite to a permanent system, and therefore has to be independently exploited or integrated with the rest of the already existing subsystems protecting the critical infrastructure.

4 THREAT DETECTION, IDENTIFICATION AND LOCALIZATION

A complete surveillance system against underwater threats has to incorporate the following capabilities:

- Detection of the threat.
- Tracking of the contact identified as threat.
- Identification or discrimination of the threat.
- Neutralization of the threat.

4.1 TYPES OF SENSORS

The sensors used to provide the capabilities listed above are the following:

a. Specific high-frequency active sonars.

b. Organic sonars of the warships.

c. Underwater physical barriers.

d. Underwater acoustic passive arrays.

e. Non-acoustic sensors (magnetic and electric-field)..

f. Optical sensors.

a. Chemical sensors.

Depending on the physical characteristics of the environment to be protected, the combination of a number of these sensors statically located with other ones installed on appropriate platforms will increase the effectiveness of the surveillance system. The effectiveness of these sensors will likewise depend on the kind of threat to be faced and on its distance.

Next the main characteristics of each of these sensors are described:

a. Specific high-frequency active sonars

The high-frequency active sonars specifically designed to detect small- and medium-size underwater objects, which are generically referred to as Diver Detection Sonars (DDS), has proven to be the most efficient way to detect the presence of divers and underwater vehicles. There is a wide range of this kind of sonars, already developed or in progress, which increasingly incorporate a higher number of capabilities and higher levels of performance. They are multi-beam sonars, with a typical range of frequencies between 70 kHz and 200 kHz (a higher frequency provides a more accuracy detection but reduces the detection distance) and a field-of-view depending on the particular system, providing the majority of them between 90º and 360º.

Current DDS incorporate algorithms for the detection, localization and tracking of the contact, and some of them allow also the classification of the contact based on its behaviour underwater (velocity, direction, trajectory, etc.). Typical detection distances for these sonars range between 300 and 800 m, which provide a time interval between 6 and 18 minutes to counter-act the threat. Two examples of currently available DDS are shown in Figure 4.

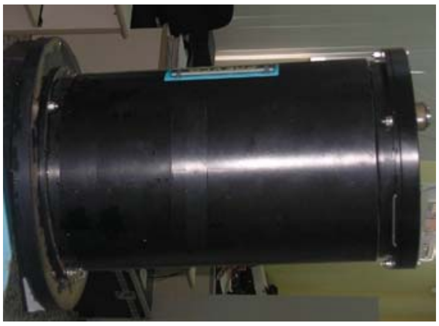
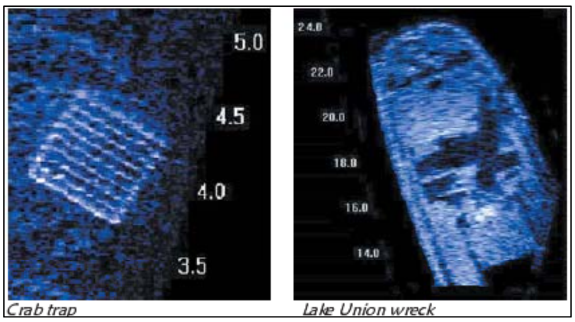


Figure 4. Subsurface units of the Diver Detection Sonars (DDS): Cerberus, manufactured by Qinetiq (left) and DAB_02, manufactured by SAES (right)

The inspection and reconnaissance vehicles incorporate very high frequency sonars (3D Acoustic Imagery) to inspect the bulls of the vessels and the docks. On the other hand, the bottom inspection is performed by means of side scan or synthetic aperture sonars. Some examples of the output of these sonars are presented in Figure 5.



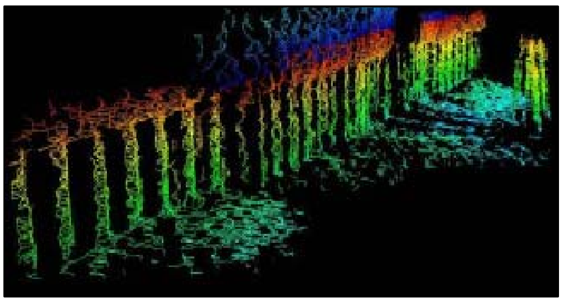


Figure 5. Examples of acoustic imagery

b. Organic sonars of the vessels

The organic passive and active medium-frequency sonars of vessels as Frigates or Corvettes allow the detection of submarines and mini-submarines in a typical range of distances between 3 Km and 10 Km., and of underwater vehicles of lower size, such as SDV, from lower distances. These kinds of sonars are not appropriate for the detection of small-size targets, as divers. Nevertheless, the high level of energy projected underwater becomes a weapon against any diver trying to operate in the area. Figure 6 shows the array of a hull-mounted cylindrical sonar.

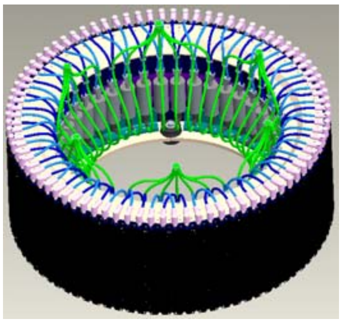


Figure 6.Array of a hull-mounted cylindrical sonar

The minehunter identification sonar is suitable for detecting small-size targets as divers, although, due to its high frequency of operation, detection distances are quite short. Figure 7 shows a simulation of the way of operation of this sonar.

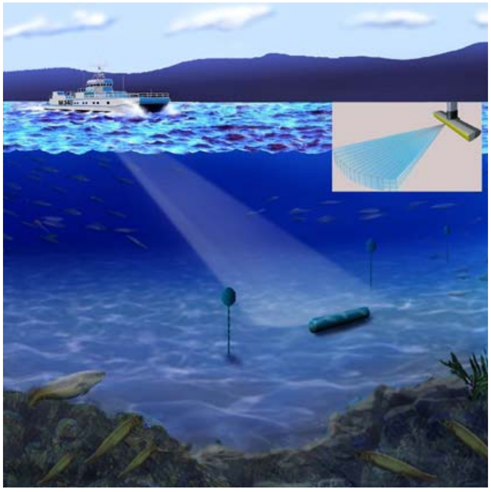


Figure 7. Example of way of operating of the minehunter identification sonar

c. Underwater physical barriers

Underwater physical barriers (see Figure 8) have constituted a traditional method of defence against non-desired underwater access to strategic harbours. Currently it is barely used due to the difficulty in deploying and maintaining these types of systems.

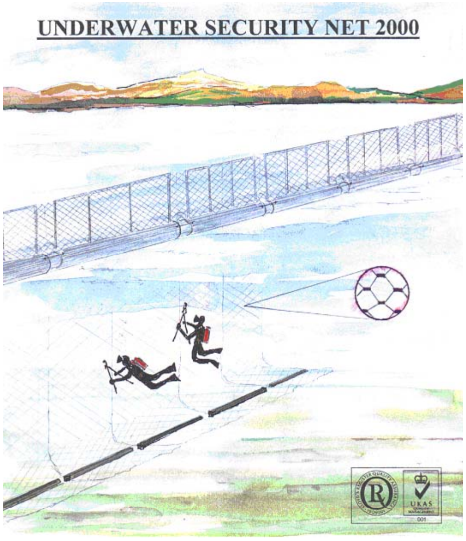


Figure 8. Underwater security net manufactured by A.R.S. Tech

d. Underwater acoustic passive arrays

The underwater linear arrays composed by a certain number of acoustic sensors and deployed on the sea bottom constitute an additional method to detect the presence of small vehicles and even divers. The array gain provided by the linked sensors permits to increase the detection capabilities of the system compared to individual sensors. The transient frequencies generated by the intruders when approaching to the target are increasingly more used by these kinds of systems to detect their presence. An example is shown in Figure 9.

Figure 9. Acoustic array Centurion manufactured by Northrop Grumman

e. Non-acoustic sensors (magnetic and electric field)

A complementary method to the acoustic sensors to detect the presence of threats is to use magnetic or electric field sensors. These non-acoustic sensors exploit the magnetic and electric fields generated by the underwater vehicles and by the metallic elements carried out by the divers to get their detection and tracking. The detection distance is very short in the case of divers. The number of sensors to be deployed depends on the size of the area to be protected and the type of threat to be counter-acted. An electric-field sensor is shown in Figure 10.

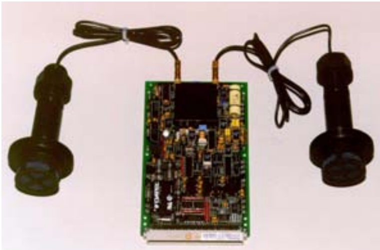


Figure 10. Electric field sensor SET-200/P manufactured by SAES

f. Optical sensors (LIDAR)

The use of optical sensors for underwater detection is currently being widely investigated. The LIDAR (Light Detection and Ranging) systems allow the detection of small underwater targets as divers and sea mines. The optical sensors are superior to the acoustic ones in terms of spatial resolution, compactness, deployment time and human interpretation of the output. Their drawback is the short detection range that extends up to a few tens of meters for divers and sea mines. An example of use of theses sensors is shown in Figure 11.

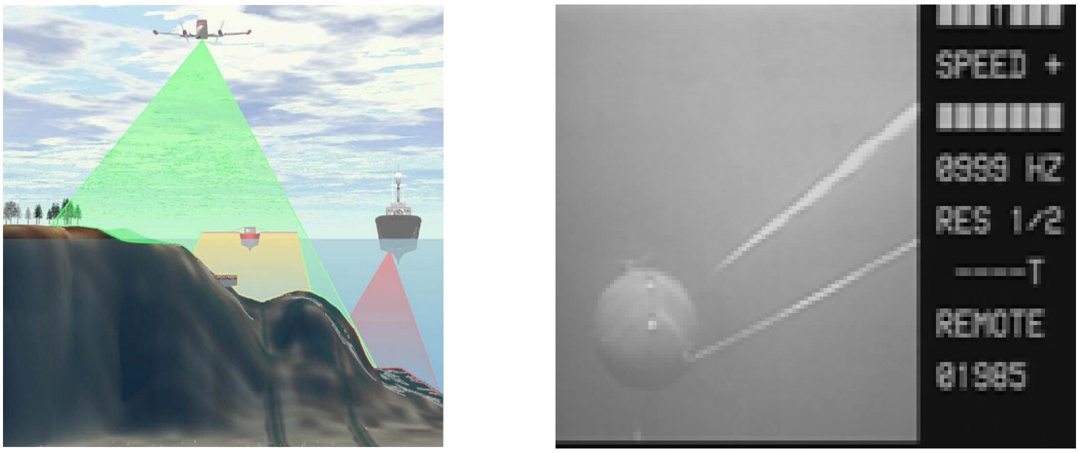


Figure 11. Examples of use of LIDAR sensors for surface and subsurface inspection.

g. Chemical sensors for detecting explosives

The detection of explosives by means of chemical sensors is currently being also widely investigated. Among the techniques applied to detect explosives it is found the use of substances capable of detecting molecules such as DNT (dinitrotoluene, close similar to TNT), which is used in practically all the explosives, from the detection of the vapours emanated from these molecules, and the analysis of samples of water in order to isolate molecules characteristics of the explosive materials. Figure 12 shows the simulation of the laying of a mine on the hull of a vessel.

Figure 12. Simulation of the laying of a limpet mine on the hull of a vessel

4.2 COMPLEMENTARY TASKS

Apart from the individual sensors or arrays of sensors used to prevent the access of hostile divers and vehicles up to the protected infrastructures, there exist complementary tasks of inspections of these infrastructures in order to detect the possible presence of mines and explosives as a result of a previous action. Divers through visual inspection have traditionally performed these tasks. At present, apart from divers, unmanned autonomous vehicles (ROV, ASV, AUV and UUV) are used to undertake this task. These vehicles carry video cameras and multi-beam or side scan sonars to detect and identify the explosive devices and in some cases they are equipped to perform the neutralization task. Portable video and sonar systems to be held by divers have been also manufactured, but the general trend is to use unmanned vehicles to perform these actions in order to avoid the risk assumed by the divers. In occasions, marine mammals have been specially trained to detect the presence of small size objects in harbour environments. Particularly, dolphins characterize by their exceptional biological sonar that permit them to detect objects in the column of water and in the sea bottom, and the sea lions are very adequate for detecting small objects due to their high capacity of vision with low levels of light and in turbulent waters.

Figure 13 shows some examples of unmanned autonomous vehicles.

Figure 13. Unmanned autonomous vehicles. REMUS (UUV) manufactured by Hydroid (left) and PLUTO PLUS (ROV) manufactured by Gaymarine (right).

5 WAYS OF COUNTERACTING THE THREAT

Once identified and localized the threat adequate measures to neutralize it have to be undertaken. Normally, it will imply the displacement of the security personnel on board of boats towards the zone in which the intruder has been localized, or the sending of unmanned surface vehicle (USV). The sent platform has to be able of confirming, intercepting and stopping the threat. The confirmation of the threat is produced thorough the sensors on board of the platform such as cameras and high-resolution sonars. The interception and neutralization of the threat is normally performed by means of the use of sound acoustic sources, in which the level of the emitted acoustic energy can vary from the emission of warning signals using a projector to the emission of high levels of acoustic energy that can stun or in extreme cases cause the death of the intruder. Other alternative mean is the use of laser emissions with different levels of energy. Figure 14 presents an unmanned surface vehicle used to counteract the threat.

Figure 14. Unmanned surface vehicle (USV) PROTECTOR for the neutralization of underwater threats manufactured by Rafael

6 CONCLUSIONS

The interest in the protection of critical infrastructures in marine environments against underwater threats has increased significantly during the last years. The main objective is to configure a complete security frame jointly with the protection against threats coming from land, air and sea surface, based on systems integrating different kind of sensors, each of them optimally fitted to the particular threat to be addressed. These systems have to be, in turn, integrated in a higher layer with systems from the security forces, harbour authorities, etc., and coordinated by an unique authority.

The technical complexity and the capabilities provided by the systems designed to counteract the underwater threat are progressively of a higher level, existing already some of them that allow to detect, localize, track and classify the threat contacts with a high degree of accuracy.

Unmanned vehicles with sensors integrated into their platforms are progressively more used in tasks of detection, identification and neutralization of the threat.

REFERENCES

[1] Annati M, Harbour protection and defence of the coast. Naval Forces 2008; 29(III):24-37

[2]. Vego M. Harbour protection, Naval Forces 2007; 28(III):9-20.

[3]. Bovio, E., Rothenbach M., Petillot Y.and Reed S. Autonomous underwater vehicles for port protection Annual Reviews in Control. Volume 30, Issue 2, 2006