Executive summary

Project Objectives

In recent years, piracy has been a growing business in the Gulf of Aden, Indian Ocean and other areas. Terrorism is another growing concern today. The objective of the project was to develop an integrated system for increasing the security of maritime infrastructures covering ports, passenger transport and energy supply against these threats.

Development strategy

Sectronic development was characterised by a close cooperation between R&D partners and end-users. Thirteen security scenarios have been established, based on end-users first-hand experience and formed the basis for assessing the effectiveness of candidate solutions. Suitable sensors and data feeds, communication and non-lethal response equipment have been thoroughly assessed, including field evaluation against real targets. Tactics and procedures have been developed and tested and safety and regulatory aspects have been addressed. Sectronic systems have been designed, developed and installed in ports and at sea for a 1-year operational evaluation period.

Project Outcomes

The combination of radar, sonar, infrared and visible cameras, AIS receivers and auxiliary sensors, anomaly detection algorithms, near real time sea state and security information and adequate non-lethal response equipment was found to be able to significantly decrease the risk of piracy or terrorism. A quantitative vulnerability reduction metric was developed and applied to single devices and to combinations of several devices in the SECTRONIC scenarios with analysis and discussion. The analysis provides some insight into the dynamics of vulnerability reduction.

Based on strong end-user recommendations, the Sectronic system on board does not require to be continuously manned. It runs in the background, automatically assessing risk level and raising an alarm when system or user-defined conditions are met.

A command and control terminal that integrates surface and sub-surface operational pictures and camera control has been developed. It is designed as a tactical decision aid, providing the operator with all relevant information available at the time an alarm is raised for instant decision making. It also controls the communication/response equipment for a quick reaction in case of attack.

An intuitive, user-friendly human interface has been developed, and most operators were "impressed by the command and control display and the possibilities of the system. The functionality and ease of use of the touch screen make it very intuitive and requires little training".

Following thorough, long-term evaluation by end-users including daily tests in some cases, it was found that the "Sectronic system performs well", the reference being the port of Rotterdam traffic image. Also "the system appears to be able to detect a diver with quite great certainty" and "diver alarm sensitivity settings are rather sophisticated and have been successfully tested. All the rules defined to trigger an alarm appear to work to satisfaction, both for surface and underwater activity".

The SECTRONIC consortium has been actively involved in a wide range of dissemination activities. Sectronic web site has been launched at an early stage of the project. Consortium members have presented SECTRONIC in 4 large international security conferences in Europe, North America and Middle East. They participated to 3 international workshops and 2 exhibitions on maritime security. The system has also been demonstrated to a large audience of international representatives of defence and maritime shipping industries.

1 Summary description of project context and objectives

1.1 The context

Over the past years serious incidents in the maritime world have occurred. All these incidents have lead to major losses, of crew and ships altogether. Piracy has flourished in the Gulf of Aden, in Indian Ocean and other areas. It still is a strong activity in more traditional areas like like the Malacca strait, where piracy has been a known threat for years.

Terrorism is also a growing concern today. This is not necessarily aiming at specific areas, but could hit for example a large cruise ship, which is a vulnerable target having thousands of people onboard. Should a ship like that be hit, the terror and threat would be dramatic (cf. attack against m/s Seaborne Spirit). Known acts of terror also include for example the bombing of the m/s Limburg.

One of the reasons behind initial success of pirates in the Indian Ocean and the developing business that followed is the lack of adequate detection and protection systems on board. The state of the art observation technologies currently available on board are not able to assess observation indicating a security treat sufficiently. For example, an object approaching cannot be automatically detected, characterized and tracked to determine if it is a potential intruder or a friendly small vessel. Nor can it be determined if a maritime infrastructure is approached by, for example, a diver. The state of the art is not able to exchange information of geophysical observations important for radar/sonar object extraction. It is not able to provide real-time object observations from a maritime infrastructure to onshore third parties, and it is not able to communicate security observations in real time to those parties. Moreover, the limited amount of information is not truly synthesized and presented in an intuitively way for end-users.

In short, the bridge has few reliable means to detect an imminent attack and, should they be able to observe it, they have very few means to prevent it from happening.
From these and other observations, it is obvious that Critical Maritime Infrastructures and utilities (sensitive buildings, vessels, piers, platforms, etc.) must be protected against damage, destruction or disruption by deliberate acts of terrorism, accidents, piracy or other forms of criminal activity.

1.2 Main Objective

The objective of the project is to develop an integrated system for the security of maritime infrastructures covering ports, passenger transport and energy supply against aforementioned risks.

With the Sectronic system, the crew is able to receive an early warning, to observe exactly what is happening, and to act before it is too late. Moreover, the system has an online and real-time communication channel to an onshore control centre allowing third parties to be informed about a critical situation. Those parties will be able to assist much more rapidly by having observations accessible in real-time.

For example, it is possible for a diver to place explosives under a vessel, swim away and have a large cruise ship capsize and sink within minutes. The crew has few means to notice, let alone to prevent this from happening. With the Sectronic system, the crew is able to detect, characterize and track the intruders, to signal and prevent them from closing in by means of non-lethal equipment.

1.3 The concept

The concept of the project is to combine short-range surface observations and sub-surface observations with long-range observations (e.g. Earth observation satellite data, coastal stations, etc.), and to implement this in a smart early warning system integrated on the ship bridge or port control room. This small area 24 hours surveillance system communicates with a local response system (e.g. alarms, sound waves) and with an onshore control centre, for early detection and prevention of attacks, malicious behaviour, accidents and damages, and to provide a response capability.

A security area is realised around a passenger ship, oil/gas production platform, floating production unit, oil/gas transport vessel or port infrastructure. The developed system has to provide 24h automatic surveillance, warn the sea master, port master, crew, operators and central controllers of potential risks at or under the sea surface and has the capability to launch responsive/ defensive measures.

Within the security area all objects (e.g. divers, small boats and vessels) are detected, characterized and tracked, enabling security related information to be processed and displayed in real-time to the end-users.

Observations can be communicated in real-time to an onshore control centre. This centre is the online hub for exchanging all security relevant information to/from infrastructures and third parties (i.e. coast guard, port authorities, etc.).

The project aimed at developing an integrated security system for the following applications:

- Intelligent intrusion detection above and below surface observing and protecting ships, energy production platforms and ports/harbours against terror and piracy attacks from divers and surface intruders. Additionally the system can assist in security related incidents like wreckage or man-over-board situations through observations that facilitate fast responding rescue missions.
- Security focused docking operation where the system provides all weather, night and day detection/ classification capability in narrow and shallow waters. Typically attacks on ships happen in the busy and complex docking process when security focus is lost due to the workload and complexity of information. The system helps selecting and presenting the most critical security related information in an intuitively understandable way.
- Security focused cruising by provision of above water forward looking sensors categorizing objects and alarming the officer of the watch of possible intruders or collisions as e.g. other (small) vessels, mines, floatsome, etc.
- At dock and in ports the system offers protection of the entire port area (under and above the surface) and may distribute observations in real-time to port authorities via the onshore control centre.
- Non-lethal reaction and response procedures that prevent an intruder to perform his mission. For example, the system may use non-lethal subsurface equipment that influences a diver’s respiration capability if the diver approaches too close to a production platform or vessel.

1.4 Scientific and Technical objectives

The main scientific and technical objectives of the system were to:

- Accurately and automatically observe, characterize and track any object of significance (i.e. divers equipped with open or closed breathing system, mines, dinghies, small vessels, etc.) 360 degrees around an infrastructure above and below the water surface 24 h a day in all weather conditions by means of short range equipment (sonars, radars, cameras, etc) and long range equipment (Earth Observation (EO) satellites, coastal stations, etc.)
- Automatically raise an alarm whenever a risk threshold is crossed. The difficulty is to detect all dangerous situations while minimising false positives
- Communicate the security-related information of significance to the infrastructure responsible (sea masters, operation control mangers, etc.) and selected authorised third parties of importance for the overall security situation (port authorities, coast guard, etc.) in real-time
- Aggregate, report, display and alarm the security information of significance in an intuitively understandable way (by means of images and numerical information)
- Enable response procedures and actions to be undertaken with no or very little delay. Time is critical in emergency situations and the system has to provide all necessary means to the operator to make instant decision and be able to deploy counter-measures at the same time.
- Undergo extensive testing, calibration, validation and demonstration phases in operational conditions

Two particular groups of technologies are considered to be able to significantly contribute to increase maritime security:

1. Online integration platform: Real-time observations and information exchange are operationally used in many industries today. An online information hub enabling security related observations to be exchanged between the maritime units and an onshore control and response unit needed to be implemented for the commercial maritime world.
2. Observation technologies: Modern radars, sonars and infrared cameras are now relatively inexpensive and can be applied to the protection of maritime infrastructures. Remote sensing observations from non-ship borne sensors are today very scarcely used for security related observations. However sea-state and weather conditions have a strong impact on the success rate of pirates in open ocean and thus accurate, up-to-date and detailed information is important for a safe voyage.

1.5 Work Packages

The Sectronic project started on 1 February 2008 for 36 months, followed by a 12-month extension period. The work was broken down in 5 work packages (Figure 1).
The objective of **WP1** was to assess sensors and metocean data, **WP2** was about implementation of communications, alerts, models and algorithms in the Onshore Control Center, **WP3** assessed nonlethal response equipment and developed tactics and procedures to counter intruders, **WP4** dealt with the safety assessment and regulatory framework, **WP5** was the bulk of the project and was about preparation and installation of the Sectronic system in end-users' maritime platforms and testing, calibration and validation in operational environment for a 12 month-period and WP6 dealt with project management, dissemination and exploitation activities.

2 Description of main S&T results/foreground

This section provides a summary of the activities and results from WPs 1 to 4 and a description of the results from work package WP5. The latter WP integrates the results and provides the conclusions of one year end-user experience in real operations.

2.1 Work package 1

Work package 1 forms the basis on which the whole Sectronic system was built. It reviews all aspects of security related scenarios, sensors, technology, data, counter-measures, algorithms and processors needed to design and develop an effective system.

2.1.1 Shipborne sensors and strategy

Shipborne sensors have been reviewed and assessed in security related scenarios. Thirteen high priority security scenarios have been defined with the active participation of Sectronic end-users. These scenarios include surface and underwater aspects, terrorism and piracy, small boats, rogue ship and divers, and ships in transit or in port or harbour. Simple threat classes with a limited number of options, and a limited number of environmental parameters have been defined in order to keep the project manageable and focus on high priority issues.

Technical requirements and parameters have been derived from the operational scenarios and form the basis for analyzing candidate sensors in security related applications. Commercially available sensors (at the time) and upcoming promising technologies have been reviewed and cover the following classes: Radar, Lidar, AIS, Sonar and complementary sensors.

The radar class includes four main branches, namely standard navigation radars, specialized radars for metocean measurement, general surveillance radars and novel multi-static distributed radar networks. The conclusion is that standard navigation radars can provide useful information but are lacking key detection and classification features against small targets, metocean measurement systems provide very useful components for surveillance but lack resolution and classification/anomaly detection features. These components (extractors) should be integrated in the security package. Two classes have been recommended for further investigation and system integration:

- specialised surveillance radars are new on the market but offer new technical capabilities which translate into improved detection and classification performance against targets identified in the scenarios
- distributed network radars which add static arrays, more advanced processing capabilities and better potential performance. However, this more modern solution has to meet two challenging requirements, cost reduction exercise and improved area coverage capability.

The Lidar system has been investigated with the view to complement both above and underwater sensors and achieve a high level of threat detection with a limited number of false positives. The conclusion is that the Lidar systems have a good potential to meet the security requirements and should be supported, but have to be limited to sector surveillance with current state-of-the-art equipment.
AIS equipment has been reviewed and was found to be a useful complementary sensor to radar.

The sonar systems have been reviewed with a focus on diver detection, as described in the Sectronic scenarios. Modern fishing sonars and specialised diver detection systems have been

reviewed. Although modern fishing sonars show advanced characteristics, they lack classification features, beam width is slightly too large and frequency is more optimised for longer range, less compact target. Based on trials conducted during the course of the project, the latter class was recommended but the results are somewhat sensitive to environmental conditions. Further development and/or use of complementary sensors was recommended.
The last series of sensors include devices that play a complementary role in the security package. Most will provide classification and identification clues and will help reduce false positives when combined with a primary, wide area intruder detection system. They include, inter alia, infrared and visible cameras. Existing shipborne sensors can provide metocean and auxiliary information for integration in the security package.

A strategy for exploiting shipborne sensors for security applications has been developed, based on the 13 Sectronic scenarios previously identified with end-users. An operational analysis has been conducted with the main objective of defining technical requirements for detection, classification and anomaly detection of all objects surrounding a vessel or a port infrastructure, underwater and above water. Detection and classification requirements have been analyzed and anomaly detection schemes have been derived from scenario analysis. A performance gap analysis has been conducted and technical requirements for primary (radar and sonar) and complementary (infrared cameras, AIS receivers, existing shipborne sensors, Lidar) sensors have been identified. Complementary between sensors has been assessed, e.g. detection and classification sensor characteristics, and multiple sensor solutions have been investigated.

The conclusion is that for surface threats, operational requirements can be met with a combination of primary (radar) and secondary (IR cameras) sensors. Only 3D solid state radar could provide the revisit time required to meet the most demanding requirements against a boat at high speed and close range. It also has a lot of advantages in terms of classification capabilities and installation requirements. Although this was the preferred option, it could not be recommended in this project as it was not compatible with the Sectronic budget. However, technology is evolving at a fast pace in this field and the cost of these systems should drop very significantly in the near future. This type of product should be re-assessed periodically. The Sectronic architecture was thus designed to accommodate upgraded technologies.

For the current Sectronic application, the traditional surveillance radar is meeting most of the requirements and fits within the budget. The major limitations come from the limited revisit time and range resolution. The former limits the capability of the radar to track boats at high speed and very close range and the latter limits the capability to discriminate 2 small boats very close to each other and greatly reduce any classification capability. These limitations were considered to be acceptable for the project as classification will mainly be achieved by infrared cameras.

As the traditional trade-off with all optical devices is between coverage (field of view) and resolution, the recommended solution was to use 1 or 2 directional cameras with a narrow field of view that will provide the resolution required for classifying gunmen at 500m. These devices have to be automatically controlled by the system and will focus on and follow the radar target that presents the highest risk level from a security point of view. Complementary fixed cameras could be used to provide a full 360° of the immediate surroundings of the vessel to cover any potential blind zone and take care of very short range intruders. Although this type of product was brand new on the commercial market, it was mature, commercially available from different sources, and was compatible with the Sectronic budget.

Diver detection sonars have been assessed and it was found they provide adequate detection performance in underwater scenarios. Furthermore some of the systems also provide a proven capability to discriminate between divers equipped with open circuit breathers, closed circuit breathers, animals or other dynamic object. Raising an alarm for underwater intrusion is thus limited to detecting the crossing of an underwater guard ring around the infrastructure by a diver.

The only important issue with diver detection sonar is mainly due to environmental effects, as the sonar may not perform as required in warm surface layers or similar conditions. The Lidar has been identified as a very good candidate for bridging this gap. Lidars can also be used to detect surface targets, have a good potential to meet the security requirements and should be supported, but have to be limited to sector surveillance with current state-of-the-art equipment in surface scenarios. For this reason, plus cost consideration and some limited lack of classification capability, the Lidar has not been recommended for the Sectronic package.

An algorithm for sensor exploitation has been developed and defines a sequence of information processing and actions that will take place when a target is detected in the vicinity of a vessel or a port infrastructure. It defines (1) what information is needed, (2) what sensor is collecting the data and how, (3) how the information is processed, (4) it defines 3 levels of risk and (5) the conditions for a target to trigger each of these levels. It also proposes a policy, tailored to the end-user requirements by means of system settings, that defines how the system will react to intruders, its sensitivity and impact on probability of detection and false alarms, and the level of operator involvement.

In conclusion, cost has been taken into account; a preferred technical solution has been identified but was not compatible with the budget available in this project. A more cost-effective solution that meets most of the technical and operational requirements has been identified and recommended for the project. An operating procedure has been defined, remaining gaps have been identified and recommendations for further improvement have been made.

2.1.2 Non-shipborne sensors and strategy

Options for using non-shipboard sensors for maritime security applications have been reviewed. The objective was to look at detection of hazards beyond the range of most shipboard sensors, i.e. detection, and understanding the intent, of ships at distances larger than 20nm, but limiting the area of interest to a region extending 270 nm out from the ship. Focus has been on use of the AIS system, coastal radars where available, as well as satellite-based AIS and radar sensors.

For monitoring ship traffic outside the range of shipboard sensors, it was found that AIS should be regarded as a valuable support tool. As in the case of shipborne AIS information, AIS data from shore stations and satellites are in themselves somewhat prone to errors, due to one or more of the following reasons:

1. Improper installation, resulting in system errors,
2. Accidental operator errors (mistyping etc),
3. Deliberate operator errors.

Undetected errors could potentially also occur due to transmission and decoding errors in coastal base stations or satellite receivers. However many errors can be detected and corrected for by cross-correlation with other sensors and external information sources.

Data from coastal radar stations should be used wherever available. Efforts should be spent on determining availability of coastal surveillance radars for vessel traffic monitoring.

Some satellite sensors are highly relevant for surveillance over longer distances. An algorithm for such activity has been developed and implemented by a Sectronic partner. It was also found that space based AIS data should become valuable in the future, both for long range tracking and for identifying anomalous behaviour of vessels at sea.

2.1.3 Assessment of available earth observation data

An assessment of earth observation data suitable for retrieval of sea state (wind, waves, current and sea surface temperature) and sea ice state (ice concentration and drift) has been made. The work has been focused on data generated by spaceborne and surface-based sensors, where the surface-based sensors include e.g. coastal radar, buoys, meteorological stations and observations from ships. In addition to earth observation data, relevant products from other service providers have also been included in the assessment.

Spaceborne altimeters and scatterometers allow for homogeneous, global and frequent coverage, which is an advantage for the retrieval of winds and sea state over open oceans. For coastal areas and large lakes it is instead recommended to use synthetic aperture radar (SAR) as this sensor type offers a higher spatial resolution than scatterometers and altimeters. For the Polar Regions, spaceborne microwave radiometers are the main sensors for retrieval of information about ice concentration over large areas. For areas with high traffic SAR data can be used to provide sea-ice maps with higher resolution. SAR is also the main sensor for estimation of ice drift.

Many of the products that are available online from various service providers are aggregated products where data from different space borne and surface based sensors and observations are combined and used as input for the product generation.

These products also include forecasts from models. Many of these products are only presented in a graphical format, usually as a map, which is difficult to integrate in the SECTRONIC service without a lot of manual interpretation. It was therefore a recommendation to focus on products that are available in the GRIB data format, which is an official WMO standard that is widely used by operational meteorological centres and data providers for storing and exchanging meteorological charts and other patterns of wind, sea state, temperature etc. There are a large number of spaceborne and surface-based sensors and systems from which it is possible to derive information about sea state and sea-ice state.

2.1.4 Recommendations for improved ship detection

Ship detection by offshore sensors (radar, sonar, lidar) are dependent on metocean conditions, notably waves, wind and sea surface temperature. Such metocean observations are available from a maritime infrastructure (MI) and also from external (to the MI) observational platforms (e.g. coastal stations, satellites, etc.). If a sensor’s operational performance envelope in respect to metocean conditions is known (or can be estimated), one can be able to estimate a sensor’s object/ship observation/detection capability at the location of the MI or ahead of a MI/ship (by using external observation platforms). A simple approach is to use lookup tables (indicating object detection capability in metocean conditions) for such estimations, which can be used by a sea/port master to understand the expected performance of a sensor under the prevailing or upcoming metocean conditions, which is of importance in a security context.

Ship detection in SAR imagery is highly dependent on wind conditions. Exploitation of knowledge about wind and sea state seems to be best utilised to plan which mode will give the best and most reliable detection result. The best polarisation strategy has been recommended for low and strong wind conditions and also in cases where one is forced to use steep incidence angles in order to obtain the required geographical coverage.

2.1.5 Selection of algorithms for metocean data

Available algorithms for wave height/speed/direction, current speed/direction, wind speed/direction and sea ice concentration/drift have been assessed. A first group of eight algorithms have been selected for implementation in the OnShore Conrol Center. For retrieval of wind information the CMOD5 is chosen. CMOD5 requires information about the wind direction, which can be obtained with the Local Gradient algorithm. Wave parameters can be obtained with the CWAVE program. For ocean current propagation the MCC algorithm for radiometer data and a method based on SAR Doppler shift have been selected. Sea-ice concentration can be retrieved with the NASA Team2 algorithm for radiometer data and an algorithm described by Dokken et al for SAR data. The primary recommendation for estimation of sea-ice drift is an algorithm called High Resolution Motion Characterization.

2.1.6 Anomaly detection specification and algorithms

It is possible to detect security related anomalies in a ship environment by processing data and information provided by local sensors, e.g. radar or sonar, by remote sensors only, e.g. AIS, and also by combining shipborne and non-shipborne information and tracks. Algorithms for detecting such anomalies have been specified, developed, tested and implemented.

Anomaly detection algorithms include a number of situations, either absolute or relative. In the former case, candidate threat units have behaviours which are suspicious by themselves whilst in the latter they have behaviours which are suspicious when put in relationship with the asset to protect or third party vessels.

As an example, for anomaly detection based on AIS data processing, the following situations have been considered:

1. change of static information,
2. route anomalies,
3. kinematic anomalies and
4. transponder anomalies.

For port installations, generic anomalies have been identified and relevant algorithm implemented. Anomalies identified in cooperation with the end users during the evaluation phase led to the development of a large number of additional situations.

For situations in open sea, six main classes of anomalies have been identified. For each of them, specific situations have been specified, an algorithm has been developed, tested and implemented.

More details are provided in the Sectronic specific reports.

2.2 Work Package 2

The main activities in work package 2 were the development and integration of the OnShore Control Center (OSCC) and specification and implementation of security related information in a Graphical User Interface. The objective of the OSCC was to enable exchange of security-related information between end-user’s maritime infrastructures (MI), onshore observation platforms and external data providers. To this end, all aspects of architecture, communications requirements and specifications, integration of algorithms, processing power, storage capability, hardware requirements have been defined in close cooperation with the partners.

Security related data to be exchanged between OSCC, MI and external data providers to OSCC have been defined in cooperation with the partners. Data products and data feeds to be used by metocean algorithms have been defined in the previous work package and integrated within WP2. Interfaces with external data providers have been developed, tested and integrated.

Metocean models and algorithms developed by partners in WP1 have been implemented, tested, optimised and upgraded on a regular basis.

The requirements for communicating relevant information between vessels and OSCC have been established. On the ship side, interfaces with local sensors, e.g. anemometers, ship radar tracks, ship heading and speed, etc. have been specified and developed. Given the cost and scarcity of communication bandwidth at sea, means to optimise bandwidth usage have been reviewed, tested and implemented. The result is that the 2-way communication worked flawlessly over the 13 months of test with the cruise vessel, apart from downtime due to maintenance periods or other exceptional situations.
A technical infrastructure has been developed in order to monitor and test the OSCC performance with real data and real algorithms. Tests included CPU usage, storage usage and network performance. Over the evaluation period, overall performance of the OSCC appeared to be more than adequate.

The principles of GUI design and initial mockups have been discussed with partners and professionals at an early stage of the project. Also a specific workshop was held on this topic with subject matter experts. The challenge was to integrate the security layer in a comprehensible and intuitively understandable way. Expertise and feedback collected during this phase has been integrated as much as possible in the GUI.
Control of response equipment, as defined in WP3, has also been integrated in the GUI. The solution that was implemented is the result of discussions with all end-users in terms of applicability, practicality, costs, perceived difficulty to install and safely operate the recommended solutions. Unfortunately, due to tight development constraints, the end-users have not had the possibility to use beta versions at an early stage.

In conclusion, the GUI was successfully developed and its user-friendliness was generally well perceived by the operators (ref. WP5 below). One of the strong points that was noted by the end-users was the limited amount of training time required to master most of the GUI functions. The GUI architectural flexibility allowed to include a large number of end-users' comments over the evaluation period. It also provides the very valuable capability to include a number of remote displays at will. This was a very useful feature for all installations as additional displays have been installed away, sometimes far away, from the main operator's station.
The OSCC has been successfully developed and, during the evaluation period, was able to: collect metocean data from external partners collect ship based sea state and security related data in near real time run algorithms to provide end-users with information described in WP1 send security related information to the maritime infrastructures successfully manage storage and security and keep a high level of performance.

2.3 Work package 3

The Sectronic system is designed for detection and classification of hostile surface and underwater intruders but also on ways and means to react and prevent an attack from happening. This paragraph presents a summary of the project in non-lethal response equipment, procedures and results. More detailed information is provided in Sectronic specific reports.

A top-down approach—from scenario, to mission (task), to relevant technologies—was used to reduce the plethora of nonlethal response technologies for law-enforcement, military, and personal protection to a manageable list of the most promising technologies for consideration in the SECTRONIC project. The scenarios driving the technology selection are those of the SECTRONIC project; namely, the protection of ports, cruise liners, and oil and gas platforms from terrorist and pirate attacks. The response missions follow accordingly: enforcing an underwater standoff, enforcing an above water standoff, and anti-boarding. The pool of technologies considered during the project is represented by an extensive bibliography. Only sixteen were considered to be plausible candidate technologies for SECTRONIC, and each of these was assessed qualitatively in terms of its effectiveness, maturity, and suitability for use on the platforms considered.

The filtering of non-lethal technology was based on first impressions of technology readiness and suitability for maritime scenarios. To that end, the technology must at least meet the following requirements: a) be commercially available, b) deter an attacker with a low probability of fatality and c) be suitable for deployment in a maritime scenario.

The following technologies were judged in the survey to meet the SECTRONIC scenarios and scope: Underwater loud hailer, Underwater Air Gun, Underwater Sparker, Long Range Acoustic Device (LRAD), High-pressure Water Canon, Fire Hose, Non-lethal projectiles, Irritant Spray, Tear Gas, Microwave Projectors, Laser Dazzlers, TASER Hand held, TASER Shockwave, Static Entanglement barriers, Deployable Entanglement barriers, Electric Fence.

The list of technologies was further reduced though detailed qualitative assessments and through a detailed readiness review. The methodology of technology readiness levels (TRLs) was applied to each of the technology groups in turn. Readiness, short comings, TRLs, and manufacturers have been reviewed and assessed. Inputs and first-hand experience from SECTRONIC user partners was critical in this assessment phase regarding technology suitability, limitations on what is demonstrable in fairly short order, and the inevitable resource constraints. Seven technologies have been considered for next-stage validation studies in WP3. All were considered to be of high technology readiness so far as mechanical functionality, availability, and support are concerned.

A validation plan was then developed for five of these technology classes, namely: 1) Underwater loud hailer, 2) Underwater Air Gun, 3) Long Range Acoustic Device (LRAD), 4) Laser Dazzlers, 5) Static Entanglement Barriers and Launched Entanglement Device. The validations were carried out and have been reported elsewhere. The goal was unbiased objective validation through first-hand experience and detailed analysis, going beyond demonstration to evaluation.

It was confirmed that all technologies perform to a large extent along the lines that manufacturers and others have claimed. As expected, however, there are limitations to performance or to the state of knowledge regarding overall effectiveness in real operation, apparently not addressed before, and, for some SECTRONIC applications and scenarios, these can be significant, perhaps even prohibitive against their use.

The eventual employment of SECTRONIC non-lethal response technologies occurs only in the last phase of more complete response approach, as a means of self-defence. As such, it is assumed to be bounded in all cases by a duty to 1) **warn**, 2) **prove hostile intent** and 3) **use proportional force**. The possible behavioural responses of the approaching threat were also categorised as follows: 1) **no change,** attacker is unaware of the activation of the device and continues his attack, 2) **warned-off** (show of vigilance), attacker is made aware that they have lost the element of surprise and chooses another target without experiencing any significant discomfort, 3) **voluntary compliance, a**ttacker chooses to comply having being exposed to a level of discomfort believing that a continued approach would be too painful or even fatal, 4) **involuntary compliance**, forced to comply due to severe pain and/or reflexive response, 5) **incapacitation, i**ncapacitated directly, either through physical restraint or physiological effect, rather than severe pain, 6) **aggravated approach,** the attacker is able to continue his approach while enduring significant discomforts serving only to aggravate him and increasing the risk of retribution, 7) **serious injury**, the attacker is halted due to serious injury.

This then allowed for the development of an effects-based parameter space onto which generic engagements could be plotted. By taking into account the limitation of various device types, an ideal engagement was proposed in terms of the effects required. This proportional layered response consisted of the following incremental phases: 1) **warning and determination of intent,** 2) **Voluntary compliance**, 3) **Incapacitation**

The warning and determination of intent phase allows an innocent contact to leave the area and avoid any interaction with a possibly painful nonlethal device. It also serves as a show of vigilance to deter a genuine threat preferring to maintain the element of surprise. In the case of a determined attacker approaching in a covert manner, his intent is revealed to the platform allowing the proportional response to continue.

The voluntary compliance phase serves as a shot across the bow of sorts in that the effect of the device is increased to portray a message of further retaliation to the threat. This gives the threat the option to comply before the more aggressive phase of incapacitation is brought to bear.

The incapacitation phase is the last line of defence and will be initiated if the threat continues to approach the platform following the voluntary compliance phase.

Having defined the ideal response in terms of generic effects, specific range requirements were developed here as a function of the various threats and scenarios considered within the SECTRONIC project. Suitable technologies were then determined taking into account both the range requirements and the platform on which they will be installed.

An action plan was developed in which the non-lethal response package was incorporated within the existing response measures currently recommended by public bodies. The action plan serves as a set of sequential instructions for the protected platform and will allow for proper preparation and training such that in the event of a genuine attack the crew can remain calm and professional in order to maximise the effectiveness of their response.

A paradigm of layered defence was applied to the SECTRONIC scenarios and above-water/underwater missions. SECTRONIC surveillance and response were combined in overlapping layers surveillance and response measures. Three layers were identified for the above water missions (countering small boats), and three for underwater missions (countering underwater intruders). The overall costs for the response technologies considered are roughly estimated to calibrate user expectations.

The three main layers of SECTRONIC above water defence identified for enforcing an above water security exclusion zones against small boats in the SECTRONIC Cruise Liner, Port, and Energy Platform scenarios are:

1. Outer Layer, radar surveillance, radio hailing,
2. Middle Layer, audible and visual warning to request cooperative standoff, while observing contact for compliance using cameras,
3. Inner Layer, intense audible and visual suppression, observing contact for compliance from cameras plus deck watch, alert authorities to non-compliance and activation of incapacitators

The three main layers of SECTRONIC underwater defence identified for enforcing an underwater security exclusion zone against underwater intruders are:

1. Outer Layer, sonar surveillance
2. Middle Layer, warning by loud hailing and close observation for diver at the surface with camera
3. Inner Layer, warning by loud hailer and activation of incapacitators

A quantitative vulnerability reduction metric was developed for assessing the benefit of using the non-lethal response technologies. The metric includes determining factors such as 1) Deterrence due to target shifting, 2) Timely intervention during the moments of attack by local authorities, 3) The impact that delay of an attack by non-lethal opposition may have, 4) The dissuasive impact that non-lethal opposition may have and 5) The incapacitation that non-lethal weapons may deliver.

The vulnerability reduction is then the difference of operation *with* and *without* the SECTRONIC system. The vulnerability reduction metric was applied to single devices and to combinations of several devices in the SECTRONIC scenarios with analysis and discussion. Unlike most treatments of vulnerability, the analysis provides some insight into the dynamics of vulnerability reduction, such as, in this case, into the division of labour between self-protective measures and reliance on authorities, which is of particular interest in SECTRONIC and elsewhere.

2.4 Work package 4

The Sectronic project aimed at introducing a range of novel technical solutions to ships and marine structures in an integrated system for the enhancement of maritime security. This section presents the regulatory issues linked to the introduction of new technologies in the Sectronic system and the integration with existing equipment. A range of requirements and regulations have been identified, and the main features of these have been reported and referenced elsewhere.

The first point was to provide the project partners with knowledge to avoid regulatory pitfalls in the development of systems in the course of the project. An attempt was made to identify challenges also beyond the timeline of the Sectronic project, extending the scope into the expected operational phase of any equipment or systems under evaluation in the Sectronic project.

A workshop with experts from relevant sections in DNV has been arranged in which regulatory issues related to the proposed equipment has been discussed. All systems to be introduced to a ship were considered to be add-ons, i.e. not intended to replace or substitute already installed, mandatory systems. If the new systems were to replace established systems, more rigorous investigations would be needed.

The investigation identified a number of issues which required attention from developers in the early phases of the project. Some of the challenges identified were of a serious nature, which could have limited the application of certain systems. However, no insurmountable challenges or showstoppers have been identified which would render the candidate systems inapplicable from a regulatory perspective.

A strategy for the fulfilment of rules and standards associated with the installation and use of the Sectronic system has been devised at an early stage in the project, prior to a final definition of the Sectronic system. The strategy was designed to accommodate different levels of problem complexity, relating to the level of ambition for the installation and use of the system, and the associated complexity of rules and standards. This involved the use of alternative risk based approach to approval, in order to fulfil rules and standards. During the course project, it became evident that it was possible to develop a standard for certification of Routing Decision Support Systems (RDSS), which included safety, security and efficiency considerations. The result of this development is a proposed draft type approval program which includes minimum requirements for the functions provided by RDSS.

The technologies and services anticipated in the Sectronic project (including all major sub-components) have been evaluated by DNV. No major show-stoppers have been identified among those. Preparatory work for filing an FSA (Formal Safety/Security Approval) to one of IMO's sub-committees has been conducted and a process and main content has been considered and identified.

2.5 Work package 5

2.5.1 Validation of models and algorithms

The main goal was to validate the considered sources of met-ocean data to be provided for the improvement of the performance of sensors included in the SECTRONIC system. Five different parameters have been considered: sea surface winds (speed and direction), surface currents (speed and direction), sea surface temperature, sea ice concentration and sea ice drift.

In order to achieve high spatial and temporal coverage and resolution, several data sources from each parameter have been considered. Although initial plan was to collect in-situ data sources from the commercial vessels that participated in the testing, calibration and validation of the SECTRONIC system, the approach finally adopted considered different data providers for the parameters of interest together with Chalmers algorithms. The parameter sources are limited to numerical weather prediction models and satellite retrievals. The latter include both processed parameters provided by different organizations and parameters derived by algorithms developed and/or implemented at Chalmers.

Considering different sources of parameters for wind, currents, sea ice concentration and sea ice drift and quality/availability risk analysis, the conclusion is that a first version of an operational implementation of the SECTRONIC system should include:

- Wind speed and direction from GFS Model Predictions from NCEP- NOAA. Since, although with low spatial resolution they are available in near-real time with global coverage.
- Wind speed and direction from ASCAT Measurements from OSI-SAF. Since, although with coverage limitations, they provide higher resolution than GFS model predictions in near real time.
- Geostrophic Currents from AVISO. Since they provide a daily updated estimation of ocean currents with global coverage.
- Sea ice concentration from the ready-to-use products from University of Bremen and EUMETSAT. These products complement each other in terms of spatial and temporal resolution and coverage.
- Sea ice concentration algorithms from passive microwave as well as SAR data. The SAR algorithm offers highest spatial resolution and the passive microwave algorithm is a back-up to other services.
- Sea ice drift from NCEP-NOAA and from SAR algorithm. The drift product from NCEP-NOAA is global and daily, with low spatial resolution. The SAR algorithm gives high resolution drift information for specific regions of interest.

The wind retrievals from SAR data can provide high resolution wind fields at coastal regions and can be considered for operational implementation.
Due to the limitation by cloud coverage the implemented algorithm to derive adjective surface velocities from infrared radiometer data presents a high risk of providing unreliable current

measurements without a careful pre-processing which imposes a severe restriction for an operational implementation in the SECTRONIC system.

According to constrains of every parameter it is possible to assign a risk for its operational implementation at the On-Shore Control Centre (OSCC) of SECTRONIC. At the end, all considered parameters have at least one risk-free (or low risk) source implemented at the OSCC, which in theory will guarantee the data provision to the SECTRONIC system.

2.5.2 System installation and introduction

The Sectronic system has been successfully installed on board a vessel and in ports. On average the installation and introduction process required a lot more effort than was originally anticipated. Some of the reasons to this situation are listed hereafter as they are a good basis for lessons learnt:

- introduction of new technology, e.g. diver detection sonar, in a commercial marine environment
- complexity and volume of equipment to be installed in maritime infrastructures, including cabling, metal work, interfaces…
- introduction of prototypes and products under development in a streamlined activity like a commercial shipyard, under very strict time constraints
- introduction of early versions of software in a very demanding environment such as ship bridge
- lack of regulatory legal framework for sonar operations in ports, especially in non EU ports
- increasing general public sensitivity to radiations, leading to issues with use of radars in ports
- difficulty to find locations in ports that combine operational interest and offer availability of power and network connections at a cost compatible with the project budget
- need to accommodate local requirements from end-users, leading to additional software development and integration efforts
- hardware failure, unavoidable given the volume and complexity of equipment
- …

However, all these difficulties have been overcome, thanks to an exceptionally active support from the end-users, their technical teams and the R&D partners. Some of the aforementioned issues are inherent to research activity and will be faced again in the future. Recommendations for the future should include the need to conduct a thorough assessment of environmental aspects at an early stage in the process and involve not only partners but also entities in the vicinity of the installation.

In conclusion, the following installations were successfully completed:

- diver detection sonar on a vertical rail, in fixed locations in ports
- sonar, deployable through a ship’s hull via an electric winch
- radar installed in temporary locations on top of laboratory containers for initial tests
- radar installed on fixed, dedicated tower on shore
- radar installed at a ship bow and retractable in case of heavy weather situations
- infrared cameras on fixed towers on shore
- infrared camera on top mast of a vessel
- all copper and fibre optic cabling on shore and on board between sensors and servers
- all interfaces with local sensors, e.g. AIS, and standard/satellite communication equipment
- all network interfaces with all end-users and external data providers

2.5.3 Energy supply system performance

The Energy Supply installation has suffered an important delayed for several reasons.

- Due to the peculiar situation where the platform is located, and the specific conditions for getting a working permit led to the decision of installing the Sectronic system after some feedback from the other end-users had been received
- To avoid unnecessary issues with early versions of the software, it has been decided to have an already close-to-operational system installed on the platform.
- The general situation has worsened over time, making it more important to come with a fully working solution
- The installation departs from the standard Sectronic and includes 2 cameras. This is very important from an operational point of view, but it required a lot of additional work for camera integration, which was not anticipated at all.

A plan has been coordinated with the partner involved who agreed to this delay providing that the work would be done as planned in the Description of Work, however after project closure. So the test period was mostly planned to happen in 2013. MARSS is committed to bring the Energy Supply test period to a successful conclusion after the end of the Sectronic project.

At the end of September 2013, when all was ready for installation and the travel details were being prepared, a new issue was raised with certificates for the radar installation technician. The level of certification that had been discussed so far was HUET and the technician was complying with this level. However the upper level BOSIET, standing for Basic Offshore Safety Induction and Emergency Training was required, according to Nigerian Department of Petroleum Resources. Significant additional cost was incurred by the certification process (3 day and a half training). An agreement was found in November and MARSS agreed to pay for additional cost. The first window of opportunity for training (end of January) could not be met, due to other commitments, and the technician will complete the training from the 31st of March to the 3rd of April 2014. He will then complete the installation.

2.5.4 Passenger transport system performance

The Sectronic system was tested on a cruise ship over a period of 12 months. This paragraph identifies the findings of the project in terms of both equipment and the human element. It does this by drawing on the research conducted whilst the vessel was both in port and at sea and the final feedback from the users on board and security management ashore. Due to the nature of the topic, more information is provided in Sectronic specific reports.

Evaluation tests involved high speed boats and divers approaching the vessel in various free or structured runs and also all kinds of target of opportunity. They include ship activity in port and at sea, in all weather conditions, covering areas from the Mediterranean Sea and the Canary Islands to northern Norway and Russia. In ports, very different situations were met, ranging from small, almost empty harbours with crystal clear waters to North European ports of Hamburg or Rotterdam, with high, sometimes extremely high levels of traffic, currents and water turbidity. The key findings of the evaluation period are presented hereafter.

2.5.4.1 Key Findings

Technical / Operational

- Detection/ False alarm rate against small boats in security applications is intrinsically higher than what is usual in standard navigation radar operations (small boats vs. ships), especially in busy ports

- Sonar performance depends on environmental conditions
- Underwater target localisation was not accurate enough with the current onboard installation. A solution has been devised but could not be implemented within the framework of the project.
- Good tracking performance against small, high speed boat at sea was achieved. Different types of manoeuvres have been tested during sea trials with the objective of assessing the capability of the tracker to follow the target. Changes of course and speed, including sharp turns and acceleration, complete stop in the water, etc. have been used. The tracker was working well in these difficult conditions while maintaining a very low level of false tracks.
- Important operational conclusions drawn from tests in favourable and adverse environments, both for surface and underwater applications
- Regular software upgrades via network are critical in the early stages of the test period
- Under operational conditions, a fully functioning Sectronic system should utilize the vessels own marine radar suite. However, it is noted that the current solution ensured that no critical navigation systems were interfered with during the project. This capability has been integrated during the course of the project and applied to the system installed in Rotterdam.
- High resolution infrared cameras are essential to track, focus and identify targets at appropriate range to allow sufficient time for the Officer Of the Watch to take action.
- The system architecture developed during the Sectronic project would comfortably be able to exploit and embrace more advanced technology as it comes to market. This includes radar and camera systems.

Human factors / Organisation / Legal

- Integration of the system in the ship organisation has to be well thought out. The Officer of the watch, in charge of the system, is too busy at times, especially in busy environments
- Location of the Graphical User Interface on the aft bulkhead of the bridge was in a sub optimal position. A better location of the operator's console at the bridge will enable it to be better integrated into the current bridge procedures
- Experience acquired by operators/officers difficult to hand over to new crew. Even with an intuitive, user-friendly Sectronic interface, officers, operators and support staff need regular training sessions
- Operators on an operational vessel are not fully prepared to the Research & Development aspects of this type of project, in particular with early software versions of a new system
- Usage of radars and sonars in ports requires prior authorisation and is currently uncommon. Legislation on security applications in port requires additional work
- The sonar was not frequently deployed with cooperating divers for safety reasons

Areas where the system has more benefits

- Dark 'finger' piers in certain ports
- Dark night operations
- An FPSO or a tanker vessel at anchor for prolonged periods could benefit from this technology. Under these circumstances, it is envisaged that the Sectronic system could play a very important role to alerting the ship's company of any small craft approaching and alerting the vessel to a potential attack. Even a couple of minutes warning onboard a vessel would be enough time to enable the crew to barricade themselves inside the accommodation block citadel of the ship.

- Many cargo vessels operate on long, slow passages with minimum manning in place. Their slow passages with few 'eyes' on the bridge reduces the possibility that something out of the ordinary will be detected. The passive Sectronic system may therefore provide a most needed early warning capability.
- The lack of a look behind radar / night vision capability makes any vessel vulnerable from being boarded at the rear. This is particularly the case with cruise ships where their Bridge is located at the forward end of the ship. Their main radar suite also has blind sectors in the rear of the vessel due to the position of the funnel.

Future work

- Although the false alarm rate has been continuously optimised over the evaluation period, some additional work is required on this point, especially in busy environments. This was a severe problem at an early stage as alarm overload is a source of concern to maritime officers due to the varied types of different equipment on a modern bridge. This highlighted the challenge of introducing and integrating new equipment into an operational environment.
- The system should be integrated with a full suite of appropriately scaled ECDIS charts. This would enable the Officer of the Watch to immediately cross reference the display on their navigational ECDIS with that on the Sectronic GUI. This would enhance the decision making capability of the Officer.
- When the Sectronic system tracks a vessel using AIS then the ability of the cue and slew camera to follow the target is always slightly delayed. This is due to the technological limitations of receiving real time AIS data (typically updated every 3-6 seconds). Some predictive capability of the Sectronic system in order to follow a vessel could be a useful enhancement. This feature has been implemented in Sectronic during the course of the project for radar tracks but should be extended to AIS tracks.
- The need for improved night vision capability was highlighted during the project. The capability to interrogate a target under night conditions from a distance that may provide enough time to prepare the vessel for attack would be useful. The technology tested during Sectronic was not capable of achieving this. However, improvements in infrared cameras since the start of the Sectronic project now make this possible.
- The system should be designed to tie in with a vessel's existing marine radar suite. This is of course technically possible but was outside of the scope of the project for safety reasons.

2.5.5 Port system performance

A Sectronic system comprised of radar, sonar, camera, processors and auxiliary equipment has been installed in the ports of Rotterdam and La Spezia with an objective to assess its performance and usability over a long period of time. The system has been evaluated in terms of operational performance, ease of use for the operator and usability for the ports against real and dummy targets in a somewhat challenging environment. More comprehensive information is provided in dedicated reports.

Over the evaluation period, it has been possible to:

- find an appropriate location to install the Sectronic systems including sensors;
- integrate the monitoring of the system into daily operations;
- find a way to generate underwater alarms of the systems;
- find out if the system is workable under the difficult circumstances in the port;
- find out if the system performs differently under different circumstances such as traffic and weather conditions

- give feedback on the GUI from an operational perspective
- get knowledge about the effectiveness of the Sectronic system in various conditions, influenced by seasons and the weather (wind, temperature), other sources of noise like from on shore industry and from vessels passing by or at greater distance
- find how many false alarms are raised and under which conditions
- find out what causes a false alarm and what settings be adjusted

For a number of reasons Port of Rotterdam preferred for the Sectronic project to develop a test set-up with a dummy diver over testing with real divers. The main points were that it was more difficult and less effective to work with a real diver as the number of runs would have been drastically limited, for safety and financial reasons. PoR preferred to run daily exercises with dummy divers for building statistics on operational performance. Actually tests conducted with a real diver always showed a positive detection by the Sectronic system, so this was not so much a concern for the tests.

The development of a test set-up and protocol using dummy targets proved to be far more complex and time-consuming than anticipated but was successfully achieved and gave the possibility to run daily exercises. Following numerous trials, a set-up has been defined in which a vessel tows a target that performs as a dummy diver. The set-up was as follows;

- As vessel a patrol vessel from the Port of Rotterdam was used.
- A dummy diver was defined within the Sectronic consortium and tested for daily operations. This dummy appeared to give the best results. When compared to a calibrated target, they appeared to perform almost identically
- The dummy first was dragged behind the patrol vessel whilst the vessel was sailing at very low speed (diver speed) and later pulled in with the ship standing still in the water.
- The distance between boat and dummy had to be quite significant

The Sectronic software has very sophisticated decision rules to recognize a diver and exclude most other objects not being a diver, such as a dummy. During the tests it was a point of discussion whether the findings were caused by the test setup or rather by the systems' performance.

The system was found to be stable, there were hardly ever break downs, even not when developing and adapting the systems' software or in situations of regular software upgrades. Based on daily tests, it is believed that the system is able to detect hostile divers with a high probability. False positive rate still needs to be improved although the alarm rules were found to be well defined and well working. Also if a definitive spot is chosen, fine tuning the equipment to the surrounding environment leads to a reduced number of false alarms and greatly increases usability.

Operators were impressed by the command and control display and the possibilities of the system. The functionality and ease of use of the touch screen make it very intuitive and requires little training to master most of the basic functions.

One finding was that the operators' interest tend to fade after a while as no real hostile intruder was detected during the test period. This was mainly due to;

- The fact that no 'real events' took place
- Getting used to the alarms that are triggered by above water activity
- It takes time to understand the nature of the false alarms from above water activity and draw conclusions from them

- The fact that around the test set-up -with the patrol vessel and dummy target- there was an amount of uncertainty which is in itself is inherent to a test program but requires a well defined program. So additional efforts were put in this direction
- The camera that was used in Rotterdam was not part of the standard Sectronic package and reacted slow and unpredictably. Notwithstanding great efforts to control the camera correctly, this was not very successful. For the operators however the camera functionality was an important feature of the system

However, following proper training, the operators were able to:

- Assess if the system can be used to detect objects under water, including the assessment of the sonar display quality, as well as the water quality/background noise in the port
- Assess whether the sonar was working properly
- Get an idea of the frequency of the false alarms that the system generates
- Building knowledge about the assessment of underwater objects detected by sonar
- Assess if the combination of radar and automatic IR camera has added value
- Make recommendations on improvements of the system and contribute to a final assessment
- see whether a group that is not necessarily trained to read a screen and do screen observations, would be able to work with the equipment
- make a number of recommendations to improve system effectiveness, some of which were taken into account and implemented immediately.

The use of a second screen next to the Sectronic screen that gives the Port of Rotterdam vessel traffic image proved very effective. It duplicates in fact the radar and AIS functionality of the Sectronic system but was nevertheless found useful in the test set-up. At the same time it served as a reference and showed that above water activity was captured by the Sectronic system in accordance with the PoR traffic image.

Key findings

Specific underwater port circumstances

The natural circumstances in the port may limit the monitoring range of the sonar system, but certainly have an influence on the test possibilities. If a definitive spot is chosen for the equipment, then the work starts to fine tune the equipment to the surrounding. This way a large number of false alarms can be excluded for that specific location and the usability greatly increases. Since this was a test location, this work has not been done to great detail but the fine tuning that has been done showed good improvements. It has thus been observed that fine tuning to a more tailor made system is useful for the best detection results with the least of false positive alarms.

Above water detection

- As the Sectronic radar and AIS detection could be easily compared with the vessel traffic image from the Port of Rotterdam, it appears that the Sectronic system performs well in this. Both traffic images were very similar
- The system performs well when a vessel enters the alarm zone; the alarm always goes off when the warning criteria are met, with very few errors. The vessels are displayed with the correct AIS data
- It was difficult to assess the number of (false) alarms, so a less scientific method of observing, discussing assessments and testing conclusions was used.

Under water detection
The system appears to be able to detect a diver with quite great certainty.
In an environment such as a port the screen shows a lot of less obvious activity, and it takes time to understand its nature and draw the correct conclusions
Diver alarm sensitivity settings are rather sophisticated and have been successfully tested
After initial calibration issues were solved, localisation appeared to be correct
Good understanding of the local environment is built over time and helps improving performance

All the rules defined to trigger an alarm appear to work to satisfaction, both for surface and underwater activity.

The use of a different camera than the one proposed by the Sectronic consortium has not been a success. The camera used in Rotterdam did not work in a satisfactory way, and hampered the overall system performance.

Assessment of the screen must be considered as a learning process, certainly in the beginning. Also in the choice of operators to man the system, those operators should be selected who have the natural curiosity to understand and appreciate the world that lies behind a mere screen. Although it improved over the evaluation period, the false positive rate still requires some work.

To test and trigger the system, two alternatives have been used: real divers hired by the project, and use of a dummy. The development of a test setup that uses a dummy diver has taken a lot of effort before starting the test period but is very important if one wants to train the operators in realistic conditions and conduct a thorough performance analysis.

Technical and operational knowledge to be able to judge upon system technical usability and financial consequences has been gained. The question about who to operate and how to react to a detection, would still have to be answered.

Recommendations

As currently defined, the system has to be installed in a fixed location. A mobile version that could be quickly deployed in a crisis situation would be greatly appreciated

When further developing and optimizing the Sectronic system, attention should be paid to further decrease the number of false positive alarms.

The system should be made more generic with respect to cameras and other equipment. If a client has reasons to opt for certain peripheral equipment, this should preferably be possible.

Attention should be paid to the department and people were the system will be operated within the organization. The Sectronic system is a good option in a situation in which a real threat is felt throughout the whole organisation that is in charge of protection of critical infrastructure or port facilities. It requires an interest of the operators and the capability for follow-up actions.

3 Potential impact and main dissemination activities and exploitation results

3.1 Potential impact

SECTRONIC’s targeted impact is a breakthrough in the security and protection of maritime infrastructure, passenger transport, offshore energy supply infrastructure and port infrastructure.
This statement is based on the gap between the level of risk posed by piracy and terrorism to the maritime industry and the current level of equipment of vessels and maritime infrastructures.

On one side, piracy has been a growing activity since the project started in 2008. It has moved from a small scale nuisance in limited areas to an organised business over, inter alia, most of the Gulf of Aden and the Indian Ocean. On the other side, ships undertaking a voyage in the Indian Ocean lack adequate detection and protection systems.

The Sectronic system, developed under this EC project, is designed to bridge the gap and provide sea farers with a most needed 24/7 automatic surveillance capability. Not only detection, but also automatic classification, based on multiple criteria, and the capability to delay and deter attackers by a combination of functions put together for the first time in such a system.

There are 1200 vessels sailing every single day in the Indian Ocean. Moreover, given the strategic importance of the area in the commercial world, a large number of vessels of the world fleet regularly cross the Ocean. In 2012, it is a safe statement to say that each of these vessels is under direct, far from negligible, threat of being hijacked. For these and other vessels, the Sectronic product can make a huge difference in the risk of being successfully attacked.

What is needed to transition Sectronic from a project to a product in high demand is a sound business plan and a thorough approach of the market. This is the subject of the next paragraphs.

3.2 Main dissemination activities

3.2.1 Introduction

The main dissemination activities include development of a targeted audience for the development and future of Sectronic, creation and population of a web site, design of a Sectronic logo, and production of a large number of project reports, development of leaflets and posters and organisation of Sectronic workshops.

3.2.2 Target audience

Contact details of the main authorities, companies and institutions that could be interested in the SECTRONIC products have been collected. The audience includes EC and national research programs, technical and scientific community, maritime interest groups and legislative bodies, maritime insurance companies, industrial stakeholders from crucial maritime infrastructures and general public.

3.2.3 Web site and logo

The project website has been set up for the general public and can be found at the web address: www.sectronic.eu. The public website provides general information on the project objectives and the work to be performed as well as details of the project partners, and contact details for the project coordinator. The web site has been updated throughout the project and contains a page with news items about the project.

A password-protected "members-only" area of the web site has been used to post non-public deliverables and other information internal to the project, for members of the consortium and the EC project officer only.

A logo was created in month one of the project to establish the project's identity. It is included in all presentations, reports, documents, etc., of the project.

3.2.4 Project Reports

Eighty two technical reports have been produced according to the delivery dates presented in the project's "Technical Annex" (Annex I – Description of Work). Those reports that are listed as "Public" ("Pu") in the Technical Annex are for dissemination activities and will be made available to the general public on the Sectronic Web Site.

3.2.5 SECTRONIC leaflet and poster

The SECTRONIC leaflet was developed in month six of the project and contains a brief overview of the project main goals, the technical approach, the expected achievements and a list of project participants. The leaflet serves as the project's *business card* and is being distributed as widely as possible in any appropriate occasion and was updated frequently.

3.2.6 SECTRONIC Workshops

In the project the SECTRONIC consortium organized workshops to increase general awareness about the significant maritime security improvements made possible by the project results:

- SECTRONIC Workshop on Maritime Security Systems and Project results at Midterm: The Midterm Workshop took place on September 24 2009 at DNV's office in Oslo, Norway. It was a one-day-event addressing the SECTRONIC system's composite of sub-systems, their functionality and how their functionality can best be shown in a Graphical User Interface (GUI). The need to further customize the GUI depending on the end-user's operational goals was discussed and how the already developed 3D rendering GUI software could be adapted to particular operational needs. Participants: MARSS, DNV, ACS, Chalmers, end user navigators/sea masters.
- Due to the inherent uncertainty with respect to the attackers' behaviour when encountering the SECTRONIC system and the crew's confidence when operating the equipment, a workshop comprising of maritime security experts was held at DNV (Oslo) in March 2011 in order to deal with this issue. Participants were maritime security experts, master mariners, risk analysts, naval architects, ISPS/ISM auditors from DNV, NURC, BW Offshore, Carnival Corporation and MARSS.
- SECTRONIC final review meeting and demonstration. The projects final review meeting was held March 27th 2012 at the Port of Rotterdam. The Netherlands, in this final review meeting a full demonstration of the SECTRONIC System was demonstrated at the Pistool Haven in Rotterdam harbour area. The EC officer, an external reviewer (PTA) and most of the project partners attended the review meeting. The system was demonstrated using a target ship and dummy diver. Detailed presentations on the main research developments and final discussion followed the demonstration.

3.3 Usage of Dissemination Channels

3.3.1 Publications

Publication of results in internationally renowned business and scientific journals such as the International Journal of Remote Sensing, IMO-reports, and provision of material to all types of public media;

- Psarros, G., Skjong, R., Eide, M.S., 2009, "The acceptability of maritime security risk", Journal of Transportation Security, Volume 2, Number 4, pp. 149-163.
- Psarros, G.A., Christiansen, A.F., Skjong, R., Gravir, G., 2011, "On the success rates of maritime piracy attacks", Journal of Transportation Security, Volume 4, number 4, pp. 309-335.

3.3.2 Knowledge transfer to other projects and networks

Dissemination activities are interfaced with activities at the European level in the relevant Technology Platforms related to Security and Surface Transport.

- Deliverable report D4.1.2a has been referenced in the EU project NAVTRONIC
- Deliverable report D6.2.1 – Strategy for fulfilment of rules and standards.

3.3.3 Participation to and/or Organization of Events

Workshop to prepare the Demonstration Project "European-wide Integrated Border Control System" (Phase 2).

SECTRONIC representatives took part in this workshop hosted by the European Commission, DG Enterprise and Industry in Brussels on March 12, 2009. The aim of the workshop was to provide input to the preparation of the next FP7 Security Research Work Program. In particular, the workshop was meant to stimulate the debate in order to define the structure and the content to be covered by Demonstration Program (phase 2) in the area of the European-wide Integrated Border Control System. More than 100 delegates participated in the work shop, consisting of a balanced representation of private and public sectors: experts from relevant research projects, national/European authorities, end users and Commission members.

US-EU Joint Workshop on Maritime Security-related R&D

On 27 - 28 April 2009, the Maritime Affairs Unit of the JRC Institute for the Protection and the Security of the Citizen (IPSC) hosted a workshop on research and development in the field of maritime security. The event brought together around 50 participants from the EU and the US, including from the Department of Homeland Security (DHS), Department of Defence, Coast Guard, and Navy. Delegates from SECTRONIC, several Commission services as well as from the EU Agencies EMSA (European Maritime Safety Agency) and Frontex (European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union) also attended the meeting. Representatives from industry involved in collaborative research projects were also participating. From the European side the various policies that impact on maritime security were introduced. In that connection SECTRONIC was presented as one of the five most relevant EU research projects in this field.

Research, Development & Innovation for a more Secure Europe Conference http://www.src10.be/

The annual Security Research Conference (SRC) is a meeting place for security research, technology development and innovation stakeholders in Europe. SRC'10 was organised under the Belgian Presidency by the Belgian Federal Science Policy Office (BELSPO) in cooperation with the European Commission through co-funding by the FP7 European Security Research

Programme on 22-24 September 2010. The conference showcased the importance of security research for citizens in view of the research agenda beyond FP7 and the 2020 perspective. The coordinator of SECTRONIC, Dr Patrick Grignan, was actively present at the conference. Dr. Grignan gave a presentation of the project and its results to date and took part in a panel discussion on "Maritime Security and needs for R&D". The audience included around 500 participants including research and innovation actors, policy makers and potential end-users.

Basics of defence against underwater intruders

SECTRONIC partners NURC and Port of La Spezia collaborated on hosting a 2-day course called "Basics of defence against underwater intruders", 1-2 Nov-2010, La Spezia. After 1.5 days of in-class seminars the last 0.5 day was dedicated to sea demonstrations using the Port of La Spezia's diver detection sonar installed by SECTRONIC in the Port of La Spezia. 17 students attended the course from many different nations. The objectives were to survey many aspects of defence against underwater intruders. It was intended for security planners, procurement, practitioners**.**

Defence Security and Equipment International (DSEI) http://www.dsei.co.uk/

MARSS presented SECTRONIC and gave live demonstrations of the system's capabilities at the Defence Security and Equipment International (DSEi) from 13-16 September 2011. Divers and speed boats attempted to approach the Royal Navy ship HMS Tyne undetected on multiple occasions, but each time the SECTRONIC system detected the approaching intruders, tracked their progress, raised alarms and eventually deterred the approaching threats. DSEI is the world's largest fully integrated international defence exhibition featuring land, sea and air products and technologies. The 2011 edition of the event brought together an audience of over 28,000 people from 121 countries, including top level international delegations at Service Chief and Defence Minister level, senior defence procurement and defence capability staff and international paramilitary security delegations and border control staff.

International Conference on Piracy at Sea (ICOPAS 2011) http://icopas2011.wmu.se/

On 17-19 October, 2011 the World Maritime University and the International Maritime Organization hosted the International Conference on Piracy at Sea (ICOPAS 2011) in Malmö, Sweden. The Conference goal was to enhance the exposure of the increased global threat of maritime piracy and discuss possible solutions in mitigating and eradicating this threat. In particular, the Conference highlighted the significant humanitarian impact of piracy and focused on "Save Our Seafarers" through humanitarian support initiatives. Representatives from DNV and NURC participated at the conference on behalf of SECTRONIC where they presented a paper on "Risk modelling of non-lethal response to maritime piracy and estimating its effect".

.

NATD 2011 North American Technology Demonstration 2011, 25-27 Oct 2011, Ottawa (www.2011natd.ca).

At NATD participants networked with numerous industry representatives involved in current and emerging Non-Lethal Capabilities. It was an international event, jointly organized and sponsored by NATO, CAN MoD and USA Joint Non-Lethal Weapons Directorate (JNLWD).

970 persons attended NATD from 30 nations: 62 % government / military / police, 38 % industry and others it was the largest international showcase of non-lethal technologies ever.

SECTRONIC partner NURC attended NATD, participating in meetings, demonstration, and exhibits. NURC's SECTRONIC work package on Non-Lethal Response Measures was particularly relevant to the event. NURC presented a poster about the SECTRONIC response activity.

NATO Emerging Security Challenges – Energy Security Scenario-Based Workshop on "Protection of Critical Energy Infrastructures against Terrorist Threats", Brussels, 29-30 Nov 2011

This was an initiative at NATO on counter-terrorism and energy security, in particular critical energy infrastructure protection against terrorist threats, including best practices to protect critical energy infrastructure (gas, oil, electricity), as well as harbour protection. The objective was to facilitate an exchange of information on procedures, experiences and best practices concerning critical energy infrastructure protection in the maritime domain between Allies and NATO's partners in a crisis scenario.
SECTRONIC partner NURC attended, participating as a panel member and expert on protection in ports and harbours. NURC also had an exhibit booth featuring (among other things) NURC's SECTRONIC work package on Non-Lethal Response Measures, which was particularly relevant to the event. NURC presented a poster about the SECTRONIC response activity... 100 persons attended from military, civilian, industry, and academics.

Maritime Security & Surveillance Conference

The Maritime Security & Surveillance Conference took place from 29 - 31 January 2012 in Abu Dhabi with the goal to discuss and develop strategies to maximise coastal security, combat piracy and other crimes at sea, enhance Maritime Domain Awareness (MDA), and improve port security, by driving multilateral cooperation and capability building based procurement. Several leading experts and professionals from regional and international naval forces, coastguards, border security forces, port operators and port security forces and other maritime agencies participated in this event which brought together over 200 delegates from UAE, Qatar, Kuwait, USA, UK, Europe, India and Sri Lanka. The coordinator of SECTRONIC, Dr. Patrick Grignan, took part in the conference and presented project results and solutions in a 30 minute presentation called "An EC-funded, cost-effective approach to surface and sub-surface protection of coastal and maritime infrastructure". Other speakers at the conference included senior level officials from the IMO; Combined Maritime Forces; US Coast Guard; Royal Air Force; NATO Maritime Interdiction Operations Training Centre; and others. SECTRONIC also had a stand at the conference from which leaflets and project information was distributed to the conference audience.

The NATO RTO Symposium on Port and Regional Maritime Security

The NATO RTO Symposium on Port and Regional Maritime Security will take place in La Spezia, Italy, from the 21-23 of May 2012. The symposium aims to showcase national and regional efforts in port and regional maritime security; advancements in persistent detection and tracking; automated identification of vessels of interest and non-cooperative vessels; and emerging data sources which support enhanced awareness. NURC and DNV will participate and disseminate SECTRONIC findings at the event. In particular, George Psarros .and Rolf Skjong's (DNV) paper on "Vulnerability influence on the success probability of a maritime piracy attack", will be presented at the conference.

3.3.4 Other publications

The partners are encouraged to publish research results and development results obtained from the project in accordance rules laid out in the consortium agreement. Addressees for dissemination of information includes the technical and scientific community, industrial stakeholders, port and public authorities, international legislative bodies (IMO), governmental organisations and the general public. It has been a goal to provide communication on both scientific and socio-economic topics, from basic general public information to high-level. The Port of Rotterdam has made one such high-level presentation in Havenmeester Nieuws to increase general awareness about the SECTRONIC project and the expected security benefits for the port, BW Gas has done another for the US Coast Guard & the US Navy, Chalmers has done one presentation for the EU Security Workshop hosted by the Swedish EC Council, etc.

3.4 Main exploitation results

3.4.1 Product description

The Sectronic system is an integrated system designed to increase security of maritime infrastructures covering ports, cruise vessels and energy production and transport. It comprises 2 main parts, an OnShore Control Center and an Offshore Integration Platform (OIP). The former is unique, fixed, on land while the latter has to be installed on each maritime infrastructure, e.g. vessel, to be protected.
The main functions of the OIP are:

- to work mostly autonomously, requiring human intervention only in case of alarm
- to collect short range radar and sonar information
- to track all surface and underwater objects in the vicinity of the maritime infrastructure, even high speed, highly manoeuvrable , low profile boats
- to collect visual and infrared information on each object
- to receive long range security related information sent by OSCC
- to combine short and long range information
- to make a technical assessment of the risk posed by each object
- to raise an alarm if the risk level meets some user-defined requirements
- to provide the operator with evidence gathered in the previous minutes for instant decision-making
- to provide the operator with the capability to trigger counter-measures if so needed
- to provide an intuitive and user-friendly interface with the operator
- to exchange security related information with the OSCC

The OIP comprises a radar or an interface to a high end X-band radar, a diver detection sonar, one or more infrared camera(s), multiple information processors, auxiliary equipment such as interface to AIS receiver, to ship communication system, etc.

The main functions of the OSCC are:

- to collect global security related information from different sources such as shore-based stations, AIS information providers, metocean data providers, etc.
- to process prepare and transmit all types of information requested by the OIP, such as wind speed, sea state, currents, etc
- to receive and forward to customers and allowed third parties all types of security related information sent by the OIP

By combining short and long range observations, a security area is built around the infrastructure and provides 24/7 surveillance with automatic alarm capability.

3.4.2 Market description

3.4.2.1 Commercial shipping

The shipping industry is responsible for the carriage of 90% of world trade and generates according to UNCTAD estimates annual freight rates of $380bn. As of 1st January 2008, the world trading fleet was made up of 50,525 ships, with capacity of 1.12 billion deadweight tons (dwt). The world fleet is registered in over 150 nations, and manned by over a million seafarers of virtually every nationality.
As with many other industrial sectors, however, shipping is susceptible to economic downturns. The global credit crunch have consequently dampened new building activities

significantly from the record levels observed in 2006 and 2007 to a more modest levels in 2008 and so far in 2009.

3.4.2.2 Ports

Worldwide there are now over 9,000 ports which fall under the International Ship and Port Facility Security (ISPS) Code. The boom in the world maritime trade has spurred these ports to expand their capacity, infrastructure and manpower and to reorganise their strategies to take advantage of the tremendous business prospects. At the forefront of this trend are the world’s four biggest port operating companies, namely Hong Kong-based Hutchison Port Holdings (HPH), Singapore’s PSA Corporation, Dubai Ports World (DPW) and P&O Ports managing ports worldwide. In recent years, these world-renowned port operators have embarked on an aggressive expansion drive to enlarge their global presence in container terminal operations and to increase their revenues. UNCTAD reported that combined, these terminal operators handled over a third of the global volume in 2006.

3.4.2.3 Offshore installations

According to a 2007 report by Douglas-Westwood offshore oil production has risen by over a third since 1991 and is forecast to continue to rise at about the same rate, reaching 35 million barrels per day in 2011. More and more of this exploration is taking place offshore and in increasingly deeper waters. As a result there were more than 6,500 offshore oil and gas installations worldwide at the beginning of 2007. About 4,000 of these are in the US Gulf of Mexico, 950 in Asia, 700 in the Middle East and 400 are in Europe. A large number of offshore fields are currently being developed in areas such as West Africa and Asia-Pacific. The growth in offshore gas production is even more significant with production forecasted to double by 2011 compared to end 2006 levels.

3.4.3 Target Market

The commercial shipping and maritime infrastructure market is acting proactively rather than reactively in their request for improved sensors and development of technology that can detect and prevent further terrorist or piracy attacks. The sector is as vulnerable as it is keen to find a solution. The many end users that are voicing their concerns and taking and active involvement in the development efforts of the SECTRONIC project is an indisputable evidence of this.

The high value and vulnerable vessel and maritime infrastructure market is the target market for the full SECTRONIC system. This segment has a combined fleet of over 38,000 assets. For these vessels and maritime infrastructure the SECTRONIC system would thus constitute a relatively small investment in relation to value of the protection it is offering.

3.4.3.1 Target market objectives

The first mover advantage of introducing new technology designed to fit the requirements of the major end-users in this segment will create a strong competitive advantage that the SECTRONIC consortium hopes to transfer into a 5% market share within five years of product launch.

3.4.3.2 Exploitation strategy

To bring the system into this significant and fast growing market, and to support a fast implementation decision, two main strategies will be followed;

1. Involvement of end-users in the development process and
2. Certification body assessment.

1. Involvement of the end-users in the development program

SECTRONIC's core strategy to ensure widespread usage of its results is to involve end-users from the target markets during the development process to establish trust and confidence in the proposed system.

By being involved in the testing program (i.e. WP 5), the Sectronic end-users and their operators/sea masters not only become familiar with and gain confidence in the system, they also get the possibility to influence the fine tuning of the system to fit the particular needs of their type of maritime infrastructure.

It has therefore been of uttermost importance to have active involvement, communication and feedback from end-users in order to understand their needs for a security system, involve them in the design and implementation of the system, improve the functionality of the system and to collect feedback for new and/or modified tools and functionality.

In the final part of the project the SECTRONIC end-users tested the system on their infrastructures. By a successful testing period of the system these major end users may be interested in installing the system on their total infrastructures and the proposed system will also display as a needed system for their markets in general. It is therefore expected that other companies will follow the decision done by these market dominators and also pursue installations of the proposed system.

2. Certification body assessment

The SECTRONIC equipment and infrastructure has the potential to set the agenda for next generation ship navigation, with elements affecting both security and safety. For a classification society, the importance of SECTRONIC lies in the fact that the equipment can potentially penetrate a huge market and can reduce security risks significantly in addition to improving performance.

Classification society also carry out risk analysis for operators, ports and states and therefore can reuse the knowledge about risk reducing effects of the new technology. The new infrastructure may also be used for various types of direct advice relating to ships and port security. The certification bodies thus play an important role in the exploitation of a system in the contest of market penetration.

At the International Maritime Organization's committee on Safety of Navigation there is an ongoing work on developing an e-navigation strategy. E-navigation is seen as a strategic framework for developing existing and future technological infrastructure onboard and ashore. As such the term E-navigation currently incorporates systems and services, but as an E-navigation user requirement is developed, it is envisaged that the term will also include an increased focus on more tangible elements. It should be noted that without e-navigation the multiplicity of systems and equipment would continue to evolve at varying degrees of effectiveness.

The development of e-navigation is an opportunity to optimize these developments, and ensure that the focus of future developments is on a holistic approach to safe navigation from berth to berth. The current IMO definition is:

"E-navigation is the harmonized creation, collection, integration, exchange and presentation of maritime information onboard and ashore by electronic means to enhance berth to berth navigation and related services, for safety and security at sea and protection of the marine environment"

The Correspondence Group submitted their report in NAV53/13 identified the core objectives of an integrated e-navigation system. These are as follows:
"Using electronic data capture, communication, processing and presentation, to:

1. Facilitate safe and secure navigation of vessels having regard to hydrographic and navigational information and risks (e.g. coastline, seabed topography, fixed and floating structures, meteorological conditions and vessel movements).
2. Facilitate vessel traffic observation and management from shore/coastal facilities where appropriate, for example in harbours and approaches.
3. Facilitate ship to ship, ship to shore, shore to ship and shore to shore communications, including data exchange as needed to achieve (i and ii).
4. Provide opportunities for improving the efficiency of transport and logistics.
5. Facilitate the effective operation of distress assistance, search and rescue services and the storage and later use of data for the purposes of traffic and risk analysis and accident investigation.
6. Integrate and present information onboard and ashore in a format which, when supported by appropriate training for users, maximizes navigational safety benefits and minimizes risks of confusion or misinterpretation.
7. Facilitate global coverage, consistent standards and mutual compatibility and interoperability of equipment, fitment, systems, operational procedures and symbology, so as to avoid potential conflicts between vessels or between vessels and navigation/traffic management agencies.
8. Facilitate (subject to a local risk assessment) a phased migration to e-navigation while maintaining physical aids to navigation and systems where required to ensure continued navigational safety, and having regard to legacy systems, the varying state of development of aids to navigation and systems in different parts of the world and the likely timescales for adoption.
9. Demonstrate levels of accuracy, integrity and continuity appropriate to a safety-critical system (under all operating conditions and having regard to risks of malicious or inadvertent interference).
10. Be viable as a safety-critical system on a stand-alone basis having regard to both the onboard and ashore applications of e-navigation
11. Integrate data and communications systems mandated for other purposes (e.g. security), as far as practicable, so as to minimize the number of 'stand-alone' systems onboard and ashore
12. Be scalable, to facilitate fitment and use, by smaller vessels (e.g. fishing, leisure vessels).
13. Be capable of development/adaptation to integrate other, value-added functionality, while avoiding any interference with or degradation of core safety-related functions.
14. Be capable of development/adaptation to facilitate low cost generational change as new capabilities and functionality are developed.
15. Facilitate effective waterway use for different classes of vessels.

It should be obvious from the above description of SECTRONIC that the project is in full compliance with this strategy, and will contribute on almost all aspects of the future E-navigation strategy. It is therefore important to contribute to this strategic development. For example, it is fairly clear that the infrastructure part of SECTRONIC goes beyond the technology envisioned in the E-navigation correspondence group. To this end, the documented work within WP4.3 describes the basis (information and assumptions) on which the certification scheme for Routing Decision Support Systems (RDSS) is developed. The result of this development is a proposed draft type approval program which includes minimum requirements for the functions provided by RDSS. The proposal for an RDSS certification scheme is also presented that should be further developed by adding relevant specifications on issues not yet fully covered by the current proposal and it can be updated after the consideration of input/experiences gained through testing/usage of the certification scheme on existing relevant systems.

There has thus been a lot of focus on not only the certification of SECTRONIC, but also on the systems role in future maritime regulations. The technologies and services anticipated in the project (including all major sub-components) have been evaluated by DNV. No major show-stoppers have been identified among those. Preparatory work for filing an FSA (Formal Safety/Security Approval) to one of IMO's sub-committees has been conducted and a process and main content has been considered and identified.

3.5 Conclusions

A plan for the exploitation of SECTRONIC results includes a final product description with a clear target market; the high value and vulnerable vessel and maritime infrastructure market with a combined fleet of over 38,000 assets of which a 5% market share is foreseen within five years of product launch. Two main strategies are followed to achieve the desired market penetration; first and most importantly the involvement of end-users with significant market power and influence in their respective segments and secondly, the active involvement of a major certification body in the high quality shipping segment.

4 Address of project public website and relevant contact details

SECTRONIC website:

http://www.sectronic.eu

SECTRONIC project technical coordinator:

Dr. Patrick GRIGNAN,
Marine And Remote Sensing Solutions Ltd

Tel: +44 207 871 2800
Fax: +44 207 657 3373
Email: pgrignan@marss.co.uk