

ANTI-PIRACY SYSTEM FOR THE MARITIME NAVIGATION IN  
CRITICAL AREAS, AND DEVICE FOR DATA EXTRACTION FROM ON  
BOARD SENSORS

5           The present invention concerns an anti-piracy system for the  
maritime navigation in critical areas, and device for data extraction from on  
board sensors.

10           More in detail, the present invention concerns an anti-piracy  
maritime system based on the analysis and tracking of targets. Such a  
system takes into account different information sources, to provide to the  
final user a secure navigation channel within a critical area and more in  
general in the Economic Exclusive Zone (EEZ), managed by costal  
centres or VTS (Vessel Traffic Services) systems. The invention further  
concerns a device for data extraction from sensors on board of ship that is  
15           utilized in the system of the invention.

20           In the last 10 years, the Applicant has developed, among others,  
the following products: the Vessel Traffic Service (VTS) and the Vessel  
Traffic Management Service (VTMS), exploiting the research and know-  
how patrimony gained in the defence of critical missions and in the Air  
Traffic Control" (ATC) fields, wherein the society is committed in the  
delivery of all-in-one systems, with respect to a large ensemble of  
consumers all over the world. The VTS and maritime traffic control  
systems have been installed all over Italy, including a particular system for  
the management of the traffic in the lagoon of Venice and in various  
25           countries of the world, including Russia, China, Poland, Yemen and  
recently Turkey and Panama. Moreover, the river version of the same  
systems, for the control of river traffic, is being installed in Serbia on the  
Danube river.

30           When an electronic system based on sensors coupled with  
extensive database processing capabilities, the product of the Applicant is  
called Vessel Traffic Management and Information System (VTMIS).

          The Applicant is being currently implementing the Italian national  
VTS system which comprises:

- 35           - 73 radar sites;  
          - 3 mobile radar units;  
          - 39 local control centres;  
          - 14 regional centres;  
          - 1 national centre;

From: Barzanò &amp; Zanardo

To: 00498923994465

Page: 9/40

Date: 15/05/2012 16:17:45

PCT/IT 2011/000 286 - 15-05-2012

2

- 1 training centre.

The system has a control and command organization at multiple levels, a redundant coverage of critical areas, the possibility of integrating data/services or Exchange them with a certain number of external (both

5 civil and military) organizations: an important example of this integration ability is given by the interconnection and exchange of data between the National Vessel Travel Service (NVTs) and the National Coastal Surveillance System (NCSS), entirely managed by the Italian Military Navy.

10 From 1990 the Applicant is actively present in the main International commission (IMO - International Maritime Organization, IALA - AISM International Association of Marine Aids to Navigation and Lighthouse Authorities, European projects, etc.), its maritime business has naturally evolved to satisfy the recent market needs, including improvements to the

15 Vessel Traffic Management (VTM), e-Navigation, LRIT (Long Range Identification and Tracking), coastal surveillance, river navigation surveillance and management and portal security systems.

The marine piracy has doubled in 2009 as indicated by the International Maritime Bureau (IMB). The IMB believes that the escalation

20 of the piracy will have significant economical consequences for the emerging economies countries. As a consequence, these Countries should adopt a system to secure certain commercial routes to avoid threats and establish an IMB Piracy Reporting Centre (PRC) in Kuala Lumpur, Malaysia. Most part of the reports is relevant to the increase of

25 the activity in the Aden gulf and in the Somalian coastal waters, wherein more than 150 accidents occurred in the past year.

The patent document US2009045983 describes a sea friend/foe recognition system is described (WFSS) which utilizes a SIM ("Subscriber Identity Module") card with a SIM reader on board of a watercraft. A

30 transmitter, which is coupled with the SIM reader, transmits information from the SIM card, as well as positioning information, to a tracking station of the system. The advantage of this system would be that of prevent non-authorised modifications of the watercraft information when utilised together with the AIS standard, as well as the auto-identification of a large

35 number of watercrafts without remaking the global AIS & GMDSS standards. However, the transmission of the ID but not of all the authentication of all the AIS messages by the key relevant to the ID is

described. In particular, one an RFID is utilized, for the ID information and such an information is transferred unencrypted through the AIS. All this presupposes a network infrastructure (GSM o equivalent) currently present only near the coasts.

5           The patent US 2003233176 describes a maritime data collection and distribution system comprising a ship configured to transmit a signal (by satellite) corresponding to the current position of the ship, or to the foreseen position of the ship, a computer network including one or more databases, each one comprising one or more interest zones, wherein the  
10 interest data zone corresponds to a controller zone, and a services provider configured to receive the signal, recuperate one or more data of interest zones from the computer network on the basis of the signal and transmit to the ship one or more zone of interest data for the ship. The zone of interest data is constituted by maritime that are favourable to a  
15 secure and economical utilization of the ship. The interested zone is a three-dimensional area surrounding the ship or a time-limited zone surrounding the ship.

          The patent document US 2008079608 describes a method for the optimization of the programming of the ships entering and editing into/out  
20 of the port, the method comprising the steps of:

- a. combining the information from an automated identification system on each ship with the planning of information on each ship from a sending system to produce a combined programming/ID for each ship;
- 25 b. tracking the latitude and longitude of each ship by GPS for the production of latitude and longitude tracked for each ship;
- c. comparing tracked latitude and longitude of each ship with the existing port maps;
- d. continuously comparing the programming/ID for each ship with the  
30 tracked latitude and longitude of each ship.

          The signalling are sent each time that the tracked latitude and longitude do not correspond to the expected latitude and longitude of each ship in a given instant. The method tracks and records each time a pilot embark or disembark from a ship.

35           Embodiments of the present invention seek to provide an advanced anti-piracy system that adapts perfectly to the functional VTMS architectures and constitutes a complementary function for the defence of extended areas that are

threatened by pirates or terrorists. The system object of the invention can also be utilized in all the control systems for boundary, national security/protection and Exclusive Economic Zone (EEZ).

According to a first aspect of the present invention, there is provided a maritime anti-piracy system, for the recognition of suspect watercrafts around one or more co-operating ships to be protected, comprising:

- a shore-based control system, comprising:
  - one or more centres, geographically distributed, comprising shore sensors for detecting watercrafts surveillance data;
  - a central station for collecting and elaborating watercrafts surveillance data;

the shore-based control system comprising a bi-directional communication network between said one or more centres and said central station, in such a way that the central station be able to send commands to said shore-based sensors;

- a communication system between said one or more centres and said one or more co-operating ships to be protected,

The anti-piracy system being characterised in that it comprises:

- one or more devices, mounted on board of corresponding said one or more co-operating ships to be protected, for maritime surveillance data extraction from maritime surveillance sensors, which are mounted on board of corresponding said one or more co-operating ships to be protected and are suitable to watch over the space around said one or more co-operating ships, said one or more devices for data extraction being suitable to send said maritime surveillance data to at least one of said one or more centres through said communication system;
- an identification and authentication system of said one or more co-operating ships to be protected, which functions through said communication system and is shared among said one or more centres and each of said one or more co-operating ships to be protected,

Said central station for collecting and elaborating data elaborating the data coming from said one or more centres, and therefore also from said one or more co-operating ships to be protected, and launching the relevant alarms in the case of recognition of suspected watercrafts.

Here by "maritime surveillance" is meant the watching over the

watercrafts in a maritime zone.

The elaboration performer by the central station can comprise the crossing of all the data in order to individuate the suspected watercraft or recognize watercrafts silhouettes that are not among the forms of the co-operating ships, with particular reference to the processing of the kinematics of all the watercrafts to the end of assigning to each one of them a threat level that can be simplistically be friend, foe, neutral, based on heuristics and intelligent systems that learn and improve by experience the reliability of the proposed result.

Preferably according to embodiments of the invention, said maritime surveillance sensors comprise the radar mounted on board of said one or more co-operating ships to be protected.

In such a way, by enlarging, by means of the on-board radar and optionally also the camera(s), the coverage of the shore systems, one may drastically decrease the reaction times for the possible counter-measures (time factor is fundamental as above mentioned).

Preferably according to embodiments of the invention, said identification and authentication system comprises one or more AIS transmission devices mounted on corresponding said one or more co-operating ships, and at least a shore AIS receiving device, said one or more AIS transmission devices being suitable to transmit information of authentication of the identity of said corresponding said one or more co-operating ships to said at least a shore AIS receiving device.

Preferably according to embodiments of the invention, to each of said one or more AIS transmission devices and said at least a shore AIS receiving device an encryption unit is associated, which generates a key for the authentication of the AIS messages, without changing the structure of the exchanges messages, i.e. within the AIS systems standards.

Preferably according to embodiments of the invention, said identification and authentication system comprises or is constituted by a VHF communication with encrypted signature.

Preferably according to embodiments of the invention, said shore-based sensors comprise at least a shore camera and said maritime surveillance sensors comprise at least a camera, said central station elaborating the video data coming from said shore-based sensors and said maritime surveillance sensors to obtain watercrafts video tracks, including said suspected watercrafts and said one or more co-operating ships, which are elaborated

together with at least a track coming from said at least a shore AIS receiving device and said radar relevant to the same watercrafts, and may improve the recognition of the same watercrafts.

5 This may be a novelty in the field, because till now the electro-optic information have not been integrated with the radar ones. One can integrate the data from shore cameras and/or on-board cameras. In particular, one integrates information coming from the optical analysis of the video fluxes of the (high-sensibility, daily and infrared) cameras with the information obtained from the processing of the electro-magnetic  
10 signals provided by radars and the AIS radar signals.

Preferably according to embodiments of the invention, said central station elaborates video data from camera to additionally obtain the watercrafts silhouettes and compares them with a series of pre-defined silhouettes relevant to known ships.

15 This may increase the confidence of the recognition and adds silhouette information of the watercraft under examination. This may be a novelty as well, since as yet the recognition of the watercraft silhouette has been committed to analysis of satellite data of difficult (and expensive) realization and certainly not in quasi-real-time. Typically one collects  
20 satellite data for a long time period and then elaborates them off-line, obtaining the silhouettes of the watercrafts under examination.

One integrates thus information from the optical analysis of the video streams of the (high-sensibility, daily and infrared) cameras with the information obtained from the elaboration of the electro-magnetic signals  
25 provided by the radars and the AIS radar signals.

According to a second aspect of the present invention, there is provided a device for maritime surveillance data extraction from maritime surveillance sensors including radar sensors, disposed within a ship to be protected against suspect watercrafts in said space and configured to  
30 watch over the space around the ship, said ship including a data transmission device for sending data to a shore centre through an associated communication system, the device being characterised in that it comprises:

- 35 - a connection module for connecting to said maritime surveillance sensors, comprising:
  - a direct connection module, which extracts the data and calculates tracks; and

- a bus indirect connection module (ETH), which is a sniffer for tracks data extraction;

Which produce elaborated tracks by representing tracks in pre-defined formats;

- 5 - a gateway module connected to both said module for connecting to said maritime surveillance sensors and configured to be connected to said data transmission module;

-

10 , in such a way that, in use, said elaborated tracks are transmitted to shore through said gateway module.

Preferably according to embodiments of the invention, each of said one or more devices for data extraction comprises:

- a module for connecting to said maritime surveillance sensors, by means of data bus or by direct connection;
- 15 - a gateway module for connecting to a data transmission module mounted on board of said one or more co-operating ships for the sending of the extracted data to shore through said communication system.

20 Without the direct connection module (tracker), one loses the great many cases wherein there are watercrafts that works with a format which is not standard and cannot therefore transmit to shore the data obtained from the on board sensors (the human operator in such a case

communicates the recognition, for example by phone).

Thanks to the device according to embodiments of the invention, one may enlarge the action range of the maritime localization (watching), since the on board sensors extend and detail the localization beyond the range of the shore sensors.

Preferably according to embodiments of the invention, each of said one or more devices for data extraction comprises an extracted data elaboration module, which is suitable to prepare elaborated data to be transmitted through said gateway module.

Preferably according to embodiments of the invention, extracted data elaboration module functions also as on board tracker, in particular in the case of data extracted from on board radar sensors.

Indeed many ships work with a non-standard format, failing said tracking module, and therefore they cannot transmit the data obtained from on board sensors (the human operator, in such a case, has to communicate the recognition, for example by phone).

Thanks to the device according to embodiments of the invention, one may enlarge the action range of the maritime localization (watching), since the on board sensors extend and detail the localization beyond the range of the shore sensors.

Preferably according to embodiments of the invention, said gateway module is suitable to operate towards a VHF radio data transmission module mounted on board of said one or more co-operating ships.

Preferably according to embodiments of the invention, said gateway module is suitable to operate towards a satellite and/or U/VHF radio transmission module, mounted on board of each of said one or more co-operating ships for sending of data to shore control system.

Preferably according to embodiments of the invention, said gateway module comprises a sub-module for the management of commands and parameters relevant to the radio communication, such as for example the hand-over in the selection of the frequencies and radio channels to be utilised in said communication system.

Preferably according to embodiments of the invention, each of said one or more devices comprises two modules of connection to said maritime surveillance sensors:

- a direct connection module, which extracts the data and represents them in a pre-defined format;

- a bus indirect connection module (ETH), which is a sniffer for data extraction and data representation in a standard protocol.

5 Preferably according to embodiments of the invention, said identification and authentication system utilises indifferently either message No. 8 or 6 of the AIS standard, being provided electronic elaboration means which append a secret information to the string of the 24 AIS messages and calculate a hash of the whole string so obtained, said a hash being inserted in the said either message 8 or 6, the string of 10 24 messages so obtained being finally sent through said communication system. Preferably according to embodiments of the invention, said secret information is a cryptographic key.

15 Preferably according to embodiments of the invention, each of said one or more devices utilises a GPS and a geographical localisation module, which is suitable to detect any deviation of the corresponding co-operating ship to be protected from the boundaries of a pre-determined secure area and/or the navigation plan in case of capture of the co-operating ship by pirates, and is also suitable to transmit such deviation to a shore-based control system.

20 There is also disclosed a device for maritime surveillance data extraction from maritime surveillance sensors mounted on a ship, characterised in that it comprises:

- a module for connecting to said maritime surveillance sensors, by means of data bus or by direct connection;
- 25 - a gateway module for connecting to a data transmission module mounted on board of the ship for the sending of the extracted data to a shore centre through said communication system.

30 Preferably according to embodiments of the invention, the device comprises a extracted data elaboration module, suitable to prepare elaborated data to be transmitted through said gateway module.

Preferably according to embodiments of the invention, said extracted data elaboration module functions also as an on board tracker, in particular in the case of data extracted from on board radar sensors.

35 Preferably according to embodiments of the invention, said gateway module is suitable to operate towards a VHF radio data transmission module mounted on board of said ship.

Preferably according to embodiments of the invention, said gateway module is suitable to operate towards a satellite and/or U/VHF radio transmission

module, mounted on board of said ships for sending of data to shore.

Preferably according to embodiments of the invention, said modulo gateway comprises a sub-module for the management of commands and parameters relevant to the radio communication, such as for example the hand-over in the selection of the frequencies and radio channels to be utilised in the communication to shore.

Preferably according to embodiments of the invention, the device comprises two modules for connection to said maritime surveillance sensors:

- a direct connection module, which extracts the data and represents them in a pre-defined format;
- a bus indirect connection module (ETH), which is a sniffer for data extraction and data representation in a standard protocol.

The invention will be now described, by way of illustration but not by way of limitation, making reference to the figures of the attached drawings, wherein:

- figure 1 shows the general architecture of the system according to the invention;
- figure 2 shows the information elaboration flow in the system according to the invention (shore part);
- figure 3 shows a video processing elaboration chain, in the pixel domain, i.e. optical domain, (segmentation of background/foreground, object tracking and classification/extraction of features to the semantic domain (data fusion and scene description) according to the invention;
- la figure 4 shows the features extraction technique for the classification of ships;
- la figure 5 shows the connection of a "safety box" device according to the invention;
- la figure 6 shows the modules of the safety box according to the invention.

The function performer by the system 100 according to the present invention (anti-naval-piracy function) is based on the analysis and tracking of targets based on various sources of information about scattered targets 30, 31, 50, to provide to the final user the possibility of obtaining a secure navigation channel in the economic exclusive zone EEZ, managed by the VTS centres or equivalent coastal centres.

10

Making reference to figure 2, the system utilizes, according to a preferred embodiment, three different data sources:

- cameras 11 (typically high-sensitivity cameras adapted to low level of light and infrared) to the ground and/or on-board level;
- 5 - shore radar 12 and on board radar 12';
- Automatic Identification System AIS 13.

Traditionally, only the shore radar and more recently the AIS have been utilized to obtain the position of the target and its identification. Such traditional systems have the disadvantage of using only kinematics data and therefore do not allow a precise identification of the watercrafts of various nature (commercial or potentially pirate) in the watched zone. The AIS is mandatory only on big ships larger than 15t, therefore the potentially more dangerous small targets can be detected only by the radar that does not allow a precise identification since it manages only kinematics information.

The system according to the invention instead utilizes also the data coming from the ship's radar, and optionally from the cameras at shore level and/or on board, to allow the improving of the data fusion coming from all the sensors, and therefore improve the possibility of a correct identification and positioning both of the watched ship and the watercrafts surrounding it to the end of effect an early warning about the presence of potential pirate threats.

It should also be observed that within an area already surveilled by a classical VTS system, the present invention provides the anti-piracy functionality without the necessity of adding additional sensors in the surveillance area (owing to the fact that each interesting watercraft already possesses at least an on-board radar). It makes use of complementary information coming from different sensors (radar, AIS, cameras).

It is here to be stressed that the use of the only on-board radar to anti-piracy ends is all alone already a remarkable innovation with respect to the prior art, because this extends the radar investigation field without the need of mounting additional sensors on any part of the system. As we will see in the following, this functionality is assured by the "safety box" (or device 90 for extraction of maritime surveillance data) according to the invention, which optionally can also exploit the data from on-board camera.

On a real scenario, the following statements are true:

11

- the AIS 70 is mandatory usually for ships larger than 15 t in accordance with the IMO regulation and therefore does not provide any information for the smaller ships;
- the AIS 70 could be illicitly manipulated to provide deceptive information;
- the radar 12 or that on board 12' provide kinematic information, usually without information concerning the identity of the targets of the same targets (for example, it is difficult to discriminate, with the help of the only radar, between a still small watercraft and a buoy);
- the shore camera 11 or those on board provide the video information about the target wherefrom the identification data for any specific target can be extracted (in the above example, the possibility of adding the optical information, by means of the use of the cameras, to the radar data allows to discriminate immediately between a still ship even if of small size and a buoy).

The input data are elaborated in a module called enhanced Multi Sensor data Fusion module (e-MSF) 21 to the end of providing an evaluation of the threat corresponding to the operative scenario 22, that is used by the operator of the shore headquarter 20.

#### Shore-based level

The shore-based level (first level) 20 is installed in the calculation nodes of the VTS system or equivalent system of coastal surveillance and is devoted to the performing of the anti-piracy functionalities mentioned in the following, which have as input the radar 12,12', the AIS 13 ("Automatic Identification System") and the electro-optical data 11,11' as shown in figure 2. This level comprises therefore the data received from the sensors of the co-operating ship.

The processing of the optical images 11,11' defines video signals elaboration steps from levels of low semantic significance (raw data flow coming from the camera(s)) to the semantically more descriptive levels. This electro-optical process is composed by (cf. figure 3):

- a module of segmentation 23 whose aim is the isolation of the interest targets from the background;
- a module of optical tracking 24 whose aim is to attribute to each of the objects isolated in the previous step an univocal identifier that is needed for identifying the same object in subsequent images of the

12

video flow;

- a feature extraction module 25 whose aim is the calculation of the main features of the isolated targets;
- a module of target classification 26 that works on the target silhouettes. The features obtained from the feature extraction module (license plate, colour, form) are the input for this module, which will compare the target silhouette with the ships silhouettes in a reference database (DB) 27 (cf. figure 4).

After the step of image elaboration, the system according to the invention effects the fusion of the optical information with AIS and radar information, in the e-MSF module 21. To this end, an algorithm has been developed to use optical data in the fusion process. The difficulty of such process is that of correctly associate the image data with the corresponding AIS or radar tracks, since the image data do not contain the distance information. To overcome this difficulty, an algorithm has been implemented, which uses geo-referenced reference points that are defined by operator and, by means of geometrical transformations, succeeds to associate positional information to an optical target.

The data fusion has a twofold functionality: on one hand, information are associated to the target, which are functional to the subsequent threat evaluation processes 22 (see below), on the other hand the interaction with the optical images allows to validate the radar information. The validation scheme provides that, starting from the single radar track, once the cameras are positioned so as to frame the point where the same radar track finds itself, the traditional algorithms for object detection are executed, in such a way to verify effectively that the radar track is corresponding to a watercraft.

As already said, after the data fusion process, each track is associated to information of position (AIS or radar) and therefore each target is also correlated with extension data (length, height).

Starting from all the available information:

- data deriving from video (license plate, colour, form);
- radar or AIS kinematic data (position, course and speed);
- data relevant to the union of radar/AIS and video position information (length, height);
- data that come from available archives (for example Lloyd's or other watercrafts databases),

13

The threat evaluation module can operate in two modes.

In the first mode, the system is trained to recognize anomalous behaviours without the intervention of the operator. In such a mode, the operator should only define important features to track (for example position, speed and course) and the system will:

- 1) learn (off-line) the "normal" behaviour of the system (in order to make the system understand what a normal behaviour is, the system is trained on real data without anomalous situations);
- 2) detect anomalous situations comparing the current data with the data utilized during the training sessions.

In the second mode, the operator defines (by using a language with pre-defined rules) the anomalous situation that it wish to prevent.

The utilized technology to implement such a system is based on the Description Logics (DL). The Knowledge Based (KB) system will contain a pre-defined assertions set (usually called T-box assertions) constructed (only once) by person skilled in the art. The data coming from the sensors, once suitable elaborated, will provide information on the actual state of the system (A-box assertion). Starting from these structures, the system will provide a semantic description of the current situation.

On the basis of the evaluation of the threat 22, the anti-piracy function is directly activated and managed by the component of support to decision of the VTS system or equivalent coastal control centre, for:

- indicating the tools more adapted to face the threat;
- indicating the minimum path to reach the sensible target;
- evaluating the possible escape path and starting the hunting mission.

#### Connection of secure communication (second level)

The secure connection level 60 defines a secure approach path through a secure transit channel (of any extension and form, possibly even an area) inside an AIS certified area. This certified area has an extension equal to the normal AIS radar range (the fact of "certifying the AIS data does not decrease the intrinsic efficiency of the AIS system). The AIS 13, 70 is a co-operating transponder that provides a ship-shore communication channel on a VHF connection which is intrinsically unsecure (all the details of the structure of the messages are in the regulation ITU-R M.1371-1).

14

Said AIS unsecure connection allows the sniffing, spoofing and phishing, for example the pirates could simulate an attack to a non-existing ship to distract the attention making the emergency means and the allies units converge in a geographical zone which is distant from the point where the attack is actually delivered. The "time factor" can be highly determining for the outcome of an attack (usually the pirates does not have means suitable to face a reaction by the reinforcement means, they play instead on the surprise factor to attack merchant ship, oil tanker or the like). The innovative concept of "certified track" is introduced to the end of validating any information relevant to a track.

In the framework of the above-mentioned AIS standard (24 messages), the present invention uses some of the messages to assure the integrity of the communication. To this end, the invention utilises indifferently one or the other of the messages No. 8 and 6, which are available as text messages freely usable by anybody. A secret information (for example a key) is appended to the string of the 24 messages and a hash of the whole string is calculated. Afterwards, this hash is inserted in the chosen message (either No. 8 or No. 6) and the 24-messages string is sent to the wished user (shore headquarters).

The secret information is shared with the wished user, so that he/she can recognize the ship that is communicating.

The message 6 is used in the prior art to address oneself to the addressee, the message 8 is utilized to broadcast the information (all the AIS apparatuses). A further message 7 can be utilized by the headquarters to acknowledge receipt.

In this way, the AIS according to the invention will not function only for identifying the co-operating ship in the anti-piracy system, rather also for authenticating the identity provided by the AIS of the prior art. The VTS alone cannot provide this authentication, owing to the fact that the AIS could have been stolen or cloned or manipulated and installed on a ship that wishes to simulate to be co-operating. This because the identification information is not kept in the AIS.

It is here to be specified that the choice of the messages 6 and 8 is only a preferred embodiment of the authentication (preferred since it allows not to modify the current standard of the AIS messages and therefore the nowadays installed AIS infrastructure, which remains absolutely compatible with all the existing installations, by utilising

15

precisely those messages that in the AIS standard are reserved as "free text"). It can be made in many different ways, reaching the same goal (for example in case of standard evolution).

5 In addition to the technical details utilized to secure the AIS connection, it is possible to compare the available information in the starting ports or in the international registers such as the navigation plan (spatial trajectory and time schedule) and the starting protocol with the information exchanged through the AIS connection and the data arriving from the optical processing (current navigation trajectory) to validate the  
10 correspondence of the dynamical information with the static information (for example the navigation plan) in real time.

#### Naval Level (third level)

15 In order to face the most critical events, the system according to the invention proposes to utilise a dedicated device called hereafter "safety box" (SB) 90, which has to be connected to the radar (and/or other sensors) already installed on the ship (typically utilising a limited set of standard interfaces) for example to the end of:

- localizing the ship at any time;
- 20 - detecting any deviation from the boundaries of the secure area and/or the navigation plan (in case of capture of the ship by the pirates), and possibly transmitting it to the VTS centres;
- transmitting to the VTS centres the surveillance data about the watercrafts around the ship, acquired to improve the tactical  
25 framework extending the radar coverage (cf. figures 5 and 6).

In order to perform the second operation of the list, the safety box can comprise a GPS or exploit the one already mounted on board, and comprises a geographical localisation module that comprises all the maps suitable to the end.

30 It is also utilised for extending the radar coverage from shore with the "ARPA" on board tracks (Automated Radar Plotter Aid) that arrive from the ship towards shore (making use of the safety box as described in the following). The safety box (SB) is a computerised device (commercial Windows® o Linux PC) that is equipped with dedicated software modules.

35 In particular, there are two software modules of interest:

- the tracker 91, and
- the gateway 92 for the interface of the VHF subsystem, called VHF-

15

GW (that could also be a gateway for a satellite connection for the data transmission).

5 The safety box 90 receives data from two input interfaces, one for the tracker 91 and another one 92 directly from the LAN (Local Area Network) of the ship, also called ship data bus (e.g. a serial data bus at 4800 baud), and sends its output to the VHF console (i.e. console or interface for the satellite system), which is the console of the VHF subsystem, again through the LAN of the ship.

10 The communication on the LAN of the ship is based on Ethernet technologies with standard protocols such as the NMEA messages (NMEA 0183 and 2000 managed by the national naval electronic association, [www.nemea.org](http://www.nemea.org)). On the other hand, if the ship does not have a modern data bus (LAN) but only an on-board radar connected directly to the ARPA console, a second input interface of the safety box is utilised to connect  
15 such an ARPA console directly to the tracker inside the safety box, producing radar tracks by means of a tracker 91 inside the safety box. Such tracks are produced in a pre-defined format and sent to the VHF-GW 92, which can transform them in a standard message such as the NMEA and then passes it to the VHF console of the subsystem VHF, or sends  
20 them directly through a dedicated interface whenever the VHF sub-system be predisposed and compatible. In this second scenario, the connection between the console of the ship (or of the merchant ship) and the safety box is realised by using a serial connection such as the standard connection RS-232 that could be suitable considering the short distance to  
25 cover. One observes here that the safety box is installed on board of the ship and usually could be positioned near the console of the ship.

Summarising, the aim of the safety box 90 is to produce radar and/or optical tracks (or of different type if the sensors on board are different) preferably in a standard format (for example NMEA). To this end,  
30 if the ship is – let us assume – a modern ship and already has radar tracks in the commercial format (for example NMEA) and a local network (Ethernet technology), the safety box is simply connected to the LAN of the ship and the tracks are forwarded to the VHF subsystem by using a sniffer. On the contrary, in all the other cases where there is not a tracker  
35 on the ship or there is no standard radar processing unit on the ship, ~~the~~ the safety box is connected by using a serial cable (RS-232 or equivalent) directly to the naval console (ARPA) keeping the raw radar data and

From: Barzanò &amp; Zanardo

To: 00498923994465

Page: 24/40

Date: 15/05/2012 16.17.51

PCT/IT 2011/000 286 - 15-05-2012

17

performing the same tracking function. In both cases, the output of the safety box is constituted by standard radar tracks (for example in the format NMEA) or in a proprietary format, which are sent to the shore system of the present invention utilising the VHF subsystem.

5           The commercial idea is based on the remark that the protection against piracy is an economical opportunity that is attractive for the clients and could be of interest for the VTS national administration and the ships' owners. Moreover, the assurance companies could reduce the fares for the cargo navigation and ships within areas affected by piracy as soon as  
10 they accept to subscribe said security service.

In the foregoing, the preferred embodiments have and variations of the present invention been described, but it is to be considered that those skilled in the art will be able to make modifications and other variations without departing from the scope of the invention, as defined by the  
15 enclosed claims.

## CLAIMS

1. Maritime anti-piracy system, for the recognition of suspect watercrafts around one or more co-operating ships to be protected, comprising:

- 5       - a shore-based control system, comprising:
  - one or more centres, geographically distributed, comprising shore sensors for detecting watercrafts surveillance data;
  - a central station for collecting and elaborating watercrafts surveillance data;

10       the shore-based control system comprising a bi-directional communication network between said one or more centres and said central station, in such a way that the central station be able to send commands to said shore-based sensors;

- a communication system between said one or more centres and said one or more co-operating ships to be protected,

The anti-piracy system being characterised in that it comprises:

- one or more devices, mounted on board of corresponding said one or more co-operating ships to be protected, for maritime surveillance data extraction from maritime surveillance sensors, which are mounted on board of corresponding said one or more co-operating ships to be protected and are suitable to watch over the space around said one or more co-operating ships, said one or more devices for data extraction being suitable to send said maritime surveillance data to at least one of said one or more centres through said communication system;
- an identification and authentication system of said one or more co-operating ships to be protected, which functions through said communication system and is shared among said one or more centres and each of said one or more co-operating ships to be protected,

said central station for collecting and elaborating data elaborating the data coming from said one or more centres, and therefore also from said one or more co-operating ships to be protected, and launching the relevant alarms in the case of recognition of suspected watercrafts.

2. System according to claim 1, characterised in that said maritime surveillance sensors comprise the radar mounted on board of said one or more co-operating ships to be protected.

5 3. System according to claim 1 or 2, characterised in that said identification and authentication system comprises one or more AIS transmission devices mounted on corresponding said one or more co-operating ships, and at least a shore AIS receiving device, said one or more AIS transmission devices being suitable to transmit information of authentication of the identity of said corresponding said one or more co-operating ships to said at least a shore AIS receiving device.  
10

4. System according to claim 3, characterised in that to each of said one or more AIS transmission devices and said at least a shore AIS receiving device a encryption unit is associated, which generates a key for the authentication of the AIS messages, without changing the structure of the exchanges messages, i.e. within the AIS systems standards.  
15

5. System according to claim 3, characterised in that said identification and authentication system comprises or is constituted by a VHF communication with encrypted signature.

6. System according to any claim 2 to 5, characterised in that said shore-based sensors comprise at least a shore camera and said maritime surveillance sensors comprise at least a camera, said central station elaborating the video data coming from said shore-based sensors and said maritime surveillance sensors to obtain watercrafts video tracks, including said suspected watercrafts and said one or more co-operating ships, which are elaborated together with at least a track coming from said at least a shore AIS receiving device and said radar relevant to the same watercrafts, to the end of improving the recognition of the same watercrafts.  
20  
25

7. System according to claim 6, characterised in that said central station elaborates video data from camera to additionally obtain the watercrafts silhouettes and compares them with a series of pre-defined silhouettes relevant to known ships.  
30

8. System according to any claim 2 to 7, characterised in that each of said one or more devices for data extraction comprises:  
35 - a module for connecting to said maritime surveillance

sensors, by means of data bus or by direct connection;

- a gateway module for connecting to a data transmission module mounted on board of said one or more co-operating ships for the sending of the extracted data to shore through said communication system.

9. System according to claim 8, characterised in that each of said one or more devices for data extraction comprises an extracted data elaboration module, which is suitable to prepare elaborated data to be transmitted through said gateway module.

10. System according to claim 9, characterised in that said extracted data elaboration module functions also as on board tracker, in particular in the case of data extracted from on board radar sensors.

11. System according to any claim 8 to 10, characterised in that said gateway module is suitable to operate towards a VHF radio data transmission module mounted on board of said one or more co-operating ships.

12. System according to any claim 8 to 10, characterised in that said gateway module is suitable to operate towards a satellite and/or U/VHF radio transmission module, mounted on board of each of said one or more co-operating ships for sending of data to shore.

13. System according to any claim 8 to 12, characterised in that said gateway module comprises a sub-module for the management of commands and parameters relevant to the radio communication, such as for example the hand-over in the selection of the frequencies and radio channels to be utilised in said communication system.

14. System according to claim 8 to 13, characterised in that each of said one or more devices comprises two modules of connection to said maritime surveillance sensors:

- a direct connection module, which extracts the data and represents them in a pre-defined format;
- a bus indirect connection module (ETH), which is a sniffer for data extraction and data representation in a standard protocol.

15. System according to any claim 1 to 14, characterised in that said identification and authentication system utilises indifferently either message No. 8 or 6 of the AIS standard, being provided electronic elaboration means which append a secret information to the string of the

24 AIS messages and calculate a hash of the whole string so obtained, said a hash being inserted in said either message 8 or 6, the string of 24 messages so obtained being finally sent through said communication system.

5           16. System according to claim 15, characterised in that said secret information is a cryptographic key.

10           17. System according to any claim 1 to 16, characterised in that each of said one or more devices utilises a GPS and a geographical localisation module, which is suitable to detect any deviation of the corresponding co-operating ship to be protected from the boundaries of a pre-determined secure area and/or the navigation plan in case of capture of the co-operating ship by pirates, and is also suitable to transmit such deviation to a shore-based control system.

15           18. Device for maritime surveillance data extraction from maritime surveillance sensors including radar sensors, disposed within a ship to be protected against suspect watercrafts in said space and configured to watch over the space around the ship, said ship including a data transmission device for sending data to a shore centre through an associated communication system, the device being characterised in that it comprises:

- a connection module for connecting to said maritime surveillance sensors, comprising:
  - a direct connection module, which extracts the data and calculates tracks; and
  - 25       - a bus indirect connection module (ETH), which is a sniffer for tracks data extraction;

Which produce elaborated tracks by representing tracks in pre-defined formats;

- a gateway module connected to both said module for connecting to said maritime surveillance sensors and configured to be connected to said data transmission module;
- 30       -

, in such a way that, in use, said elaborated tracks are transmitted to shore through said gateway module.

35           19. Device according to claim 18, characterised in that said direct connection module calculates tracks for data from radar sensors and/or video sensors.

20. Device according to any claim 18 to 19, characterised in that it further comprises a geographical localisation module, which uses GPS information from the ship or from an integrated GPS, and comprises all the maps to detect any deviation from the boundaries of a secure area and/or a navigation plan, the deviation data being transmitted to shore through said gateway module.

21. Device according to any claim 18 to 20, characterised in that said gateway module is suitable to operate towards a satellite and/or U/VHF radio transmission module, mounted on board of said ships for sending of data to shore, in particular towards a VHF radio data transmission module inside an AIS device mounted on board of said ship.

22. Device according to any claim 18 to 21, characterised in that said gateway module comprises a sub-module for the management of commands and parameters relevant to the radio communication, such as for example the hand-over in the selection of the frequencies and radio channels to be utilised in the communication to shore.

23. Device according to any claim 18 to 22, characterised in that the device is used in the system according to any claim 1-17.