(12) **PATENT**

(11) **343367** (13) **B1**

NORWAY

(19) NO

(51) Int Cl.

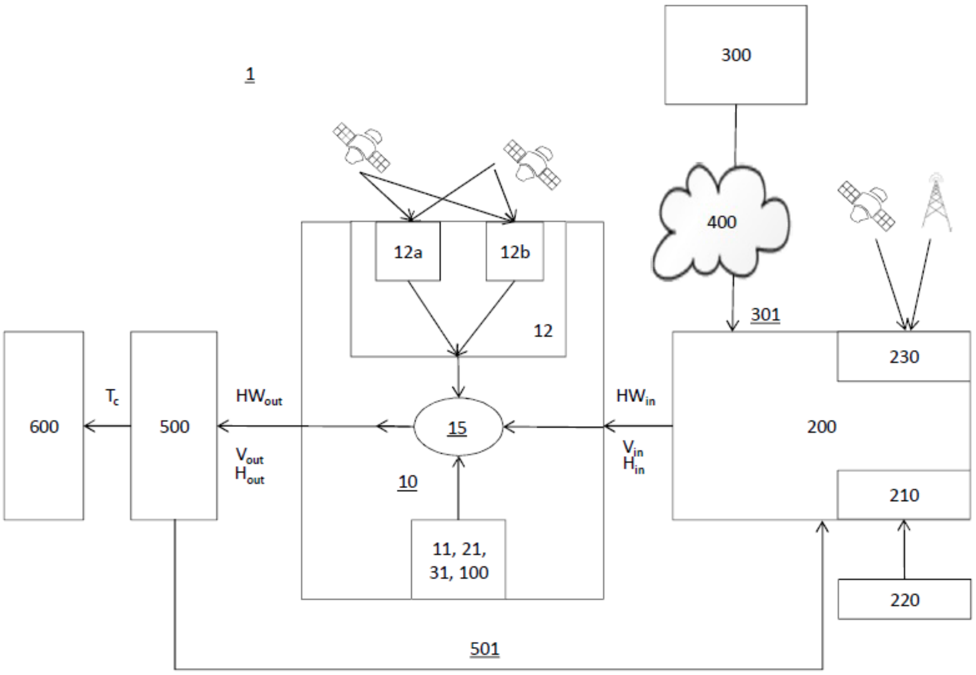
B60R 16/023 (2006.01)
G06F 21/00 (2013.01)
H04L 29/06 (2006.01)

Norwegian Industrial Property Office

(21)	Application nr.	20171854	(86)	International Filing Date and Application Number
(22)	Date of Filing	2017.11.21	(85)	Date of Entry into National Phase
(24)	Date of Effect	2017.11.21	(30)	Priority
(41)	Publicly Available	2019.02.11		
(45)	Granted	2019.02.11		
(73)	Proprietor	Rolls-Royce Marine AS, Deck Machinery - Brattvaag, Årsundvegen 24, 6270 BRATTVÅG, Norge		
(72)	Inventor	Richard Murrell, 3 Persian Close, DE241AS DERBY, Storbritannia Carl JOHANSSON, Sølvgade 23, 1307 KØBENHAVN, Danmark		
(74)	Agent or Attorney	ZACCO NORWAY AS, Postboks 2003 Vika, 0125 OSLO, Norge		

(54)	Title	**MARINE VESSEL CYBER-ATTACK PREVENTION SYSTEM, CONTROL SYSTEM AND METHOD**
(56)	References Cited:	US 2017149820 A1, US 2017313332 A1, US 2017227639 A1, US 2017045887 A1
(57)	Abstract	

A marine vessel cyber-attack prevention system, control system and method comprising a storage medium with hard-coded definitions of an allowable sailing path with an operating envelope for the vessel, wherein the cyber-attack prevention system is configured for receiving a vessel new waypoint control signal and further configured for reading the allowable sailing path for the vessel and comparing the new waypoint control signal with the allowable sailing path, wherein the cyber-attack prevention system is configured for forwarding the new waypoint control signal unaltered to the dynamic positioning system only if the vessel new waypoint control signal is within the operating envelope.



MARINE VESSEL CYBER-ATTACK PREVENTION SYSTEM, CONTROL SYSTEM AND METHOD

TECHNICAL FIELD

[0001] The present invention relates to cyber-attack protection of marine vessels that can be operated remotely, such as a remote controlled or autonomous ship where the ships route, position, speed etc. can be set from a remote operations center communicating with the ship over a communication link.

BACKGROUND

[0002] Remote and autonomous shipping is by many seen as the future of the maritime industry, especially for cargo. Common for both remotely operated and autonomous ships, is that the ships can be unmanned during long periods of time when the ships are at sea, which in turn can reduce human based errors and reduce costs considerably, since the accommodation and the deckhouse can be removed.

[0003] Remotely operated ships are manually operated from a remote control center over a communications interface, such as satellite communication system to ensure sufficient geographical coverage during the entire voyage, and a land based communication network for a higher bandwidth and lower latency communication close to harbor and land.

[0004] According to a strict definition of the highest level of autonomy, remote control should not be required for a fully autonomous ship. However, in real life, the operation of the ship can be subdivided into subtasks, which may have a varying degree of autonomy, and the subtasks with the least degree of autonomy will usually require more bandwidth. The degree of autonomy for a subtask will typically vary over time, depending on the state of the vessel, or the mission being executed. Therefore, a communications interface is still needed for e.g., real time supervision of the ship, for mooring, for route adjustments and ship control underway for some legs, and as part of a fallback strategy. The communication systems therefore become crucial, also for operation of autonomous ships.

[0005] The communication interface may become a substantial security risk if its control falls into the hands of hackers, which could have the intention to hijack the ship or take control of the ship with the intention to perform malicious or terrorist attacks by means of the ship.

[0006] The actors for malicious acts may be external to, or come from inside the organization. Traditionally execution of malicious acts has required physical presence of the actors and intrusion into the target system. The growing usage of networked information and communications technology, however, has made it possible to try to access systems virtually through network interfaces and gain unauthorized remote capability to manipulate or exploit the system or its particular elements in some undesired manner.

[0007] Cyber hijackers could for instance have the intention to redirect the ship to a different location under their control, where the cargo could be offloaded. Another common way pirates operate, is to hide the ship in an unknown location, requesting a ransom from the ship-owner to let it free.

[0008] Cyber terrorists could have the intention to run the ship under their control in high speed into other ships or into harbors or cities located by the waterfront to create damage and destruction.

[0009] In addition to hacking into systems, operation of autonomous ships could also be threatened by intentional jamming or spoofing of e.g. Automatic Identification System (AIS) or Global Positioning System (GPS) signals or the data communication between the ship and the shore control center.

[0010] Remote and Autonomous ships and an Autonomous navigation System Architecture are described in AAWA Whitepaper: http://www.rolls-royce.com/~/media/Files/R/Rolls-Royce/documents/customers/marine/ship-intel/aawa-whitepaper-210616.pdf, which is hereby incorporated by reference in its entirety.

[0011] US 2017149820 A1 describes a device for detection and prevention of an attack on a vehicle via its communication channels, having: an input-unit configured to collect real-time and/or offline data from various sources such as sensors, network based services, navigation applications, the vehicles electronic control units, the vehicle's bus-networks, the vehicle's subsystems, and on board diagnostics; a database, for storing the data; a detection-unit in communication with the input-unit; and an action-unit, in communication with the detection unit, configured for sending an alert via the communication channels and/or prevent the attack, by breaking or changing the attacked communication channels.

[0012] The autonomous vehicle system described in US 2017313332 includes a mobile platform that moves under remote and/or autonomous control, a sensor package supported by the mobile platform that obtains information relating to a component of a transportation network, and one or more processors that receive the sensor information and analyze the information in combination with other information that is not obtained from the sensor package. A hazard to one or more vehicles traveling within the transportation network may be identified.

[0013] US 2017227639 A1 discloses a system that may display resulting sonar data and/or imagery to a user through the user interface, and/or use the sonar data and/or imagery to control operation of a mobile structure, such as controlling steering actuator and/or propulsion system to steer the mobile structure according to a desired heading

[0014] US 2017045887 A1 describes a remote controlled boat system with a first central processing unit operably coupled to a communication unit and a first global positioning unit operably coupled to the first central processing unit. The system also includes at least one controller configured to control the boat via remote communication with the first central processing unit via the communication unit of the boat, the controller including a second central processing unit operably coupled to a second global positioning unit.

[0015] In order to set up secure communication between the remote operation center and the ship, common encryption protocols, such as symmetric or private key encryption are used. However, it is widely recognized that no encrypted communication is guaranteed secure.

[0016] While, encryption denies the intelligible content to an interceptor, as long as the interceptor does not break the encryption, it does not itself prevent interference. Therefore, the communication protocol for communication with the ship may become available to the interceptor if he/she manages to break the encryption.

[0017] Thus, there is a need to prevent the interceptor from taking full control of the vessel, in the case that encryption is broken.

[0018] It is further a need to regain remote control of a ship where the interceptor has been able to gain access to the communication protocol.

SHORT SUMMARY

[0019] A goal with the present invention is to disclose a marine vessel cyber-attack prevention system solving or alleviating the above-mentioned problems.

[0020] The invention addressing the above-mentioned problems is a marine vessel cyber-attack prevention system, a marine vessel control system with cyber-attack prevention, and marine vessel cyber-attack prevention method according to the independent claims.

[0021] One of the advantages of the invention is that a potential hacker or interceptor being able to get access to the communication protocol between the remote operations center and the ship will be limited in performing malicious actions related to piracy or terrorism.

[0022] Another advantage of an embodiment of the invention is that control can be re-gained if it is detected that the ships behavior is outside predefined parameters.

BRIEF DESCRIPTION OF THE DRAWINGS

[0023] Fig. 1 illustrates in a high level block diagram a marine vessel control system (1) with cyber-attack prevention according to an embodiment of the invention.

[0024] Fig. 2a illustrates in an example a path (20, 20a, 20b) and a corresponding allowable operating area (21a) of a vessel (S). The vessel (S) is illustrated in two positions. In the lower position the vessel is within the allowable operating area (21), while it in the upper position is on the way out, or has intended to leave the allowable operating area (21a) and has been stopped by the cyber-attack prevention system.

[0025] Fig. 2b illustrates how a path (20) and the allowable operating area defined by edges of an envelope (22a, 22b) may be defined by waypoints or geographical coordinates.

[0026] Fig. 3 illustrates a vessel following a path (20) into a harbor, where the area close to the harbor and a neighboring city has been divided into operating areas (21b, 21c, 21d, 21e, 21f) associated with different speed limits (V1, V2, V3, V4).

[0027] Fig. 4 illustrates how a path envelope defining an allowable operating area (21a) can be combined with the operating areas (21b, 21c, 21d, 21e, 21 f) associated with speed limits (V1, V2, V3, V4) from Fig. 3

EMBODIMENTS OF THE INVENTION

[0028] In the following description, various examples and embodiments of the invention are set forth in order to provide the skilled person with a more thorough understanding of the invention. The specific details described in the context of the various embodiments and with reference to the attached drawings are not intended to be construed as limitations. Rather, the scope of the invention is defined in the appended claims.

[0029] The invention is in an embodiment a marine vessel cyber-attack prevention system (10) comprising:
path limitation parameters (100) for the vessel, wherein
the cyber-attack prevention system (10) is configured for receiving an input headway control signal (HW_{in}) and further configured for reading the path limitation parameters (100) and comparing the input headway control signal (HW_{in}) with the path limitation parameters (100), and wherein
the cyber-attack prevention system (10) is configured for forwarding the input headway control signal (HW_{in}) unaltered as an output headway control signal (HW_{out}) only if the input headway control signal (HW_{in}) is within the allowable path limitation parameters (100), wherein
the cyber-attack prevention system (10) comprises a digital storage medium (11), and the path limitation parameters (100) are hard-coded on the digital storage medium (11).

[0030] The digital storage medium may be any type of data storage that allows the data stored in the memory to be restricted from write access from the navigation system and the cyber-attack prevention system (10) itself, e.g., such that it is only the CPU in the cyber-attack prevention system (10) that has read-only access to the data. An example of such memory could be PROM (Programmable read-only memory).

[0031] Fig. 1 illustrates how the cyber-attack prevention system (10) according to an embodiment receives the input headway control signal (HW_{in}) and reads the allowable path limitation parameters (100) to determine whether the input headway control signal (HW_{in}) should be allowed to pass through the cyber-attack prevention system (10) as the output headway control signal (HW_{out}).

[0032] The input and output headway control signals (HW_{in}, HW_{out}) may comprise any of speed (V_{in}, V_{out}), acceleration, retardation, position and heading (H_{in}, H_{out}) signals

[0033] The marine vessel cyber-attack prevention system (10) according to this embodiment comprises a processor (15) arranged for performing the determination described above.

[0034] In an embodiment that can be combined with any of the embodiments above, the marine vessel cyber-attack prevention system (10), comprises a dedicated position reference system (12) configured to determine a current position (Pc) of the vessel, wherein the current position is used in determining if the input headway control signal (HW_{in}) is within the allowable path limitation parameters (100).

[0035] The dedicated position reference system (12) can be e.g. global or regional navigation satellite systems, which can be e.g. GPS and Galileo typically used at open sea. Land based external reference systems for positioning may also be used, especially in port areas.

[0036] The dedicated position reference system (12) provides the Central Processing Unit (CPU) of the cyber-attack prevention system (10) with any of vessel position, heading and speed data.

[0037] In a related embodiment, the dedicated position reference system (12) comprises two satellite receivers (12a, 12b) configured to be arranged a fixed distance apart on board said vessel (S).

[0038] In an embodiment that can be combined with the embodiment above, the fixed distance is hard-coded on the digital storage medium (11).

[0039] Since the two satellite receivers, e.g. two GPS receivers are placed at a known and fixed distance from each other on the vessel, the CPU (15) of the cyber-attack prevention system (10) can calculate if any of the GPS receivers has been tampered with by e.g. spoofing signals, to provide an incorrect GPS signal. The satellite receivers may in addition use e.g. cryptography and distortion detection to detect spoofing.

[0040] If the CPU detects that one or multiple GPS receivers has been tampered with it may block any signals from the input interface. This may be achieved by:
- calculating whether the received signals, e.g., coordinates, from the two satellite receivers (12a, 12b) are in accordance with the fixed distance;
- forwarding the input headway control signal (HW_{in}) unaltered as an output headway control signal (HW_{out}) only if the received signals from the two satellite receivers (12a, 12b) are in accordance with the fixed distance

[0041] The CPU (15) may then use the received signals, e.g., coordinates, as a reliable reference to determine any of the vessels current position, speed and heading.

[0042] In an embodiment that can be combined with any of the embodiments above, the path limitation parameters (100) comprise one or more allowable or not allowable operating areas (21a, 21b,...) for the vessel. An allowable operating area may typically be a geographical area at sea where the vessel is allowed to operate, and a not allowable operating area may be a geographical area at sea where the vessel is not allowed to operate.

[0043] Different types of data structures can be used to describe the operating area. In a simple implementation the operating area (21f) may be described by an envelope of a path (20) intended for the vessel as illustrated in Fig. 2a and 2b. Thus, in this case the operating area can be described as anywhere from the intended path (20) to a pre-defined distance, such as e.g. 1 km to either side of the intended path. If the intended path is given as a set of waypoints, the edges of the envelope (22a, 22b) can be described as two sets of waypoints, where a waypoint on the path corresponds to a pair of waypoints equidistant on respective sides of the path waypoint of the path on each side as illustrated in Fig. 2b. The distance may be measured perpendicularly to a leg associated with a waypoint, e.g. entering leg as shown in Fig. 2b.

[00044] It is also possible to define alternative paths (20a, 20b) as illustrated in Fig. 2a. The operator could then send new commands to the vessel to take either an alternative path, e.g. for maintenance, head back or adjust position on the current path. In the embodiments above, the operating areas have been defined by an area falling within a certain definition.

[00045] However, an operating area can also be described as any area falling outside a certain definition. E.g. if all land in Fig. 2a is defined as an area, the allowable operating area could in principle be defined as anything that is not land. Further, coastal areas close to land associated with pirate activities could be defined as areas that are not allowable operating areas.

[0046] If the current vessel position, as determined by the dedicated position reference system (12) is outside the path operating area (21), the CPU (15) may output zero speed as the output headway control signal (HW_{out}) on an output interface. Typically to a Dynamic Positioning (DP) (500) System and/or Thruster Control System and/or Rudder Control System (600).

[0047] In an embodiment that can be combined with the embodiment above, one or more allowable operating areas (21) are associated with speed limitation parameters (31) read-only accessible from the digital storage medium (11).

[0048] Fig. 3 illustrates how the operating areas (21a, 21b, 21c, 21d, 21e) can be associated with speed limits (V1, V2, V3, V4). It can be seen that the maximum speed limit for operating area 21b and 21f is V1, for 21c it is V2, for 21d it is V3 and for 21e it is V4, where V1 is the lowest speed limit used in operating areas close to land.

[0049] Thus, in normal operation the controlled or autonomous vessel (S) coming in towards the harbor along the path (20) in Fig. 3 will reduce the speed gradually before entering the harbor.

[0050] Only in a situation where the speed is not reduced sufficiently will the associations between operating areas and speed limits come into effect. In such a situation the cyber-attack prevention system (10) will not forward the input speed signal (V_{in}) unaltered as the output speed signal (V_{out}) if the input speed signal (V_{in}) is above a speed limitation (V1, V2, V3, V4) for a current operating area (21a, 21b, ...) among the one or more operating areas (21a, 21b, ...).

In an embodiment the input headway control signal (HW_{in}) therefore comprises an input speed signal (V_{in}), and the cyber-attack prevention system (10) is configured for:
- comparing the input speed signal (V_{in}) with a speed limitation parameter (V1, V2,...), and
- forwarding the input speed signal (V_{in}) unaltered as an output speed signal (V_{out}) only if the input speed signal (V_{in}) is within a speed limitation (V1, V2,...) for a current operating area (21a, 21b,...) among the one or more operating areas (21) .

[0051] If the current vessel speed, as determined by the dedicated position reference system (12) is outside the speed limitation parameter (V1, V2,...), the CPU (15) may then output zero speed to the external output interface. Typically to a Dynamic Positioning System (500) and/or Thruster Control System and/or Rudder Control System (600).Fig. 4 illustrates how an envelope defined operating area (21a) as defined above can be combined with the operating areas (21b, 21c, 21d, 21e, 21f) associated with speed limitation parameters (V1, V2,V3 and V4).

[0052] The operating areas (21b, 21c, 21d, 21e, 21f) associated with speed may be common for different vessels and paths, while the envelope based operating area (21a) may be specific for the path and/or vessel. When the two are overlaid, the vessel will have to both stay within the envelope and respect the speed limitations of each operating area. At open sea, there might not be any speed limitation, and the path envelope may be the only constraint.

[0053] The operating areas (21b, 21c, 21d, 21e, 21f) associated with speed may be combined with an envelope based operating area (21a) with alternative paths (20a, 20b) as illustrated in Fig. 2a.

[0054] The invention also allows for definition of allowable ports. E.g., the vessel is only allowed to go into pre-coded ports or harbors. A minimum distance to the coastline could be pre-defined for all other areas. This could be used as a single condition for preventing cyber-attacks, or in combination with pre-defined paths and/or pre-defined speed areas described above.

[0055] Preferably, to ensure its integrity, the cyber-attack prevention system (10) is, as much as possibly, operating independently, and without the possibility to control any other systems on board the ship.

[0056] In an embodiment, the cyber-attack prevention system (10) blocks the incoming input headway control signal (HW_{in}) if it is not within path limitation parameters (100), and no signal is sent further to e.g. the dynamic positioning (DP) system.

[0057] However, the cyber-attack prevention system (10) may have a certain capacity to analyze the behavior of the ship and take certain decisions, in order to improve the current state of a vessel where the input headway control signal (HW_{in}) has fallen outside the allowable path limitation parameters (100).

[0058] In an embodiment, alternative to the embodiment above, the cyber-attack prevention system (10) is arranged for limiting the output speed signal (V_{out}) to the pre-defined vessel speed limitation parameter (V1, V2,...) for the current operating area (21a, 21b, ...). Thus, independent of the cause of the increased value of the speed signal, the vessel will only be allowed to sail on with the maximum speed allowed in the current operating area (21a, 21b, ...).

[0059] In another embodiment, that can be combined with any of the embodiments above, the cyber-attack prevention system (10) comprises an attack counter with a predefined upper limit, wherein the cyber-attack prevention system (10) is configured to increment the attack counter if the headway control signal (HW_{in}) is outside the allowable path limitation parameters (100). The upper-limit of the attack counter defines how many times the path limitation parameters (100) can be exceeded before the system is blocked and no further signals will be passed through to the next system, e.g. DP. This allows a small number of input signals, such as speed or heading to be outside the pre-defined limits, and the next signal within the path limitation parameters (100) to be accepted and forwarded to the DP.

[0060] In an embodiment that can be combined with any of the embodiments above, the cyber-attack prevention system (10) is arranged for sending a hold position command to the DP. This may be after a first attack, or when the attack counter reaches the upper limit. As a result the vessel will not move until it has been visited by technicians or skilled persons able to remove the cyber-attack prevention system (10) from the control loop.

[0061] Alternatively a "no thrust command" in order to stop propulsion, can be sent to the DP or Thruster system. The vessel will then slowly decrease the speed from the resistance of the water/wind.

[0062] In an embodiment that can be combined the previous two embodiments above, the marine vessel cyber-attack prevention system (10) is configured to block further headway control signal (HW_{in}) when the upper limit is reached.

[0063] In an embodiment that can be combined with any of the embodiments above, the marine vessel cyber-attack prevention system (10) is configured to issue a next encryption key command to the communication system (400).

[0064] In an embodiment the communication system (400) may have a list of encryption keys available, and when receiving the command from the marine vessel cyber-attack prevention system (10) it will start using the next encryption key in the list.

[0065] On the Remote Operations Centre (300), having a similar list of encryption keys, the encryption protocol attempts to contact the vessel with the next encryption key in the list as soon as communication is lost. The encryption protocol could also start a communication test with sequential use of the encryption key in the list, and if communication is successful, remain on the successful encryption key.

[0066] In an alternative embodiment one or more encryption keys is pre-defined and hard-coded on the digital storage medium (11), and the next encryption key command to the communication system comprises one of said encryption keys. In this way the spare encryption keys are never accessible from the communication system when not in use, adding an additional layer of security.

[0067] With the communication re-established with the new encryption keys control has been re-gained of the vessel, and the mission may continue, or additional measures, such as updating the communication software can be taken.

[0068] The invention is also a marine vessel control system (1) with cyber-attack prevention as illustrated in Fig. 1. The control system comprises in addition to a marine vessel cyber-attack prevention system (10) according as described in any of the embodiments above:
- a navigation system (200) configured for being controlled from a remote operation centre (300) via a communications system (400) and issuing a vessel input headway control signal (HW_{in}) to the marine vessel cyber-attack prevention system (10),
- a dynamic positioning system (500) configured for receiving the output headway control signal (HW_{out}) from the marine vessel control system (10) and issuing thruster control signals (Tc) to a propulsion control system (600).

[0069] In normal autonomous mode the ship executes the planned mission (e.g., navigation to the next waypoint) according to the defined plan. In this mode the data transfer between the ship and control center is minimized and limited to only relevant status data such as ship's location, heading, speed, Estimated Time of Arrival (ETA) to next way point (or area of closer supervision) and key information from the situational awareness systems as well as critical ship systems. While the interaction requirement between the ship and operator is minimal in this normal state, it is possible for the operator to supervise more than one vessel at the time. This means that the autonomy level of the vessel is high as long as the mission execution is proceeding according to the plan made by the operator. If the mission execution is not proceeding according to the original plan, the autonomy level may be lowered, where more operator interaction is required.

[0070] The communication system (400) illustrated in Fig. 1 may be any communication system allowing communication between a control center and a vessel, such as the satellite communication systems Inmarsat, Iridium, Thuraya, OrbComm, or a combination of land based and satellite communication.

[0071] A navigation system onboard the vessel, and more specifically an autonomous navigation system, is responsible for planning a collision free path for the autonomous ship through an environment of static and/or moving obstacles. The navigation system also takes into account the kinematic and dynamic constraints of the vessel to allow execution of the planned maneuvers.

[0072] The navigation system (200) may rely on a number of different input data that is used in calculation of the path:

- Input data from Situational Awareness (210) systems and sensors (220), such as LIDARs, Radars, cameras, weather sensors, environment sensors, microphones, etc.

- Electronic maps, i.e. nautical and terrain maps.

- Position input data (230) from positioning systems, such as global or regional navigation satellite systems, which can be e.g. GPS and Galileo typically used at open sea. Land based external reference systems for positioning may also be used, especially in port areas.

- DP input data (501) from the DP system (500).

- Control input data (301) from the remote control center (300) via the communication system (400).

[0073] In order to reach best possible autonomous navigation reliability, other available data sources which can help the navigation, may be used, such as Automatic Identification System (AIS), Automatic Radar Plotting Aid (ARPA) and Electronic Chart Display and Information System (ECDIS).

[0074] Based on the different input data the navigation system (200) may then calculate a path for the ship and send a next waypoint to the Dynamic Positioning system. This will be a dynamic process, and in congested areas, the waypoints may be updated more frequently than at open sea where spatial and temporal object tracking as explained above, can be applied to provide a continuous situational awareness for reactive collision damage or avoidance.

[0075] The responsibility of the dynamic positioning system is to maintain the vessels desired position and/or heading by using its propellers, rudders and thrusters, where the desired position is defined by the any of the new waypoint, speed and heading commands from the navigation system. The DP system is a major contributor to safe and accurate operations of the autonomous ship.

[0076] The typical thruster system of an autonomous ship typically comprises thrust elements needed to control both protrusion and heading, such as propellers (controllable pitch, fixed pitch and adjustable bolted), tunnel thrusters, azimuth thrusters, electric pod propulsors, flap rudders, rotary vane steering gear, monitoring and control, stabilizers and waterjets.

[0077] For the purpose of the invention, DP and thruster systems (500, 600), as well as interworking between these two systems are considered part of common available technology.

[0078] In addition to the above, the invention is also a marine vessel cyber-attack prevention method for a vessel comprising:
- a marine vessel cyber-attack prevention system (10),
- a navigation system (200) configured for being controlled from a remote operation centre (300) via a communications system (400) and issuing a vessel input headway control signal (HW_{in}) to the marine vessel cyber-attack prevention system (10),
- a dynamic positioning system (500) configured for receiving the output headway control signal (HW_{out}) from the marine vessel control system (10) and issuing thruster control signals (Tc) to a propulsion control system (600),

[0079] The method comprises the steps of:
- providing a digital storage medium in the marine vessel cyber-attack prevention system (10) with hard-coded path limitation parameters (100) for the vessel,
- receiving an input headway control signal (HW_{in}) from the navigation system,
- reading the path limitation parameters (100),
- comparing the input headway control signal (HW_{in}) with the path limitation parameters (100), and
- forwarding the input headway control signal (HW_{in}) unaltered as an output headway control signal (HW_{out}) only if the input headway control signal (HW_{in}) is within the allowable path limitation parameters (100).

[0080] In an embodiment that can be combined with the embodiment above, the path limitation parameters (100) comprises one or more allowable operating areas (21a, 21b,...) for the vessel, and wherein the method comprises the step of:
- forwarding the input headway control signal (HW_{in}) unaltered as an output headway control signal (HW_{out}) only if the input headway control signal (HW_{in}) is within the allowable one or more operating areas (21a, 21b).

[0081] In an embodiment that can be combined with the embodiment above, the path limitation parameters (100) wherein said one or more allowable operating areas (21a, 21b,...) are associated with speed limitation parameters (V1, V2,...) that are read-only accessible from on the digital storage medium (11) and the input headway control signal (HW_{in}) comprises an input speed signal (V_{in}), wherein the method comprises;
- comparing the input speed signal (V_{in}) with a speed limitation parameter (V1, V2,...), and
- forwarding the input speed signal (V_{in}) unaltered as an output speed signal (V_{out}) only if the input speed signal (V_{in}) is within a speed limitation (V1, V2,...) for a current operating area (21a, 21b,...) among the one or more operating areas (21) .

[0082] In an embodiment that can be combined with the embodiment above, the method comprises the step of:
- limiting the output speed signal (V_{out}) to the pre-defined vessel speed limitation parameter (V1, V2,...) for the current operating area (21).

[0083] In an embodiment that can be combined with any of the method embodiments above, the method comprises the step of:
- incrementing an attack counter if the headway control signal (HW_{in}) is outside the allowable path limitation parameters (100).

[0084] In an embodiment that can be combined with the embodiment above, the method comprises the step of:
- sending a hold position command if the attack counter reaches the upper limit.

[0085] In an embodiment that can be combined with the two previous embodiments above, the method comprises:
- blocking further headway control signal (HW_{in}) when the upper limit is reached.

[0086] In an embodiment that can be combined with any of the method embodiments above, the method comprises the step of:
- issuing a next encryption key command.

[0087] In an embodiment that can be combined with the embodiment above, the method comprises the step of:
- reading a next encryption key from the digital storage medium (11), and the next encryption key command comprises the encryption key.

[0088] In an embodiment that can be combined with any of the method embodiments above, the method comprises the step of:
- determining a current position of the vessel from a dedicated position reference system (12), wherein the current position is used in determine if the input headway control signal (HW_{in}) is within the allowable path limitation parameters (100).

[0089] In an embodiment that may be combined with the embodiment above the method comprises the step of:
- determining the current position of the vessel from two satellite receivers (12a, 12b) comprised by the dedicated position reference system (12), wherein two satellite receivers (12a, 12b) are arranged a fixed distance apart on board said vessel (S).

[0090] In an embodiment that may be combined with the embodiment above, the method comprises the step of:
- calculating whether the received signals from the two satellite receivers (12a, 12b) are in accordance with the fixed distance;
- forwarding the input headway control signal (HW_{in}) unaltered as an output headway control signal (HW_{out}) only if the received signals from the two satellite receivers (12a, 12b) are in accordance with the fixed distance.

[0091] In this case we cannot trust the GPS anymore. A hold position command may be sent to the Dynamic Position or Thruster Command System.

[0092] Other operating areas and speed limitations, as well as combinations of the two could of course be defined within the context of the invention. The actual configuration of these parameters may be case dependent and depend on different factors, such as path, vessel type and size, local regulations etc.

[0093] In an embodiment that may be combined with any of the system or method embodiments above, wherein any of the path limitation parameters (100), the one or more encryption keys and the fixed distance are hardcoded on the digital storage medium (11).

[0094] In the exemplary embodiments, various features and details are shown in combination. The fact that several features are described with respect to a particular example should not be construed as implying that those features by necessity have to be included together in all embodiments of the invention. Conversely, features that are described with reference to different embodiments should not be construed as mutually exclusive. As those with skill in the art will readily understand, embodiments that incorporate any subset of features described herein and that are not expressly interdependent have been contemplated by the inventor and are part of the intended disclosure. However, explicit description of all such embodiments would not contribute to the understanding of the principles of the invention, and consequently some permutations of features have been omitted for the sake of simplicity or brevity.

CLAIMS

1. A marine vessel cyber-attack prevention system (10) comprising:
- path limitation parameters (100) for the vessel (S), wherein the cyber-attack prevention system (10) is configured for receiving an input headway control signal (HW_{in}) and further configured for reading the path limitation parameters (100) and comparing the input headway control signal (HW_{in}) with the path limitation parameters (100), and wherein
the cyber-attack prevention system (10) is configured for forwarding the input headway control signal (HW_{in}) unaltered as an output headway control signal (HW_{out}) only if the input headway control signal (HW_{in}) is within the allowable path limitation parameters (100), wherein
the cyber-attack prevention system (10) comprises a digital storage medium (11) with read-only access for the cyber-attack prevention system (10), wherein the digital storage medium (11) comprises the path limitation parameters (100).

2. The marine vessel cyber-attack prevention system (10) of claim 1, comprising a dedicated position reference system (12) configured to determine a current position of the vessel, wherein the current position is used in determining if the input headway control signal (HW_{in}) is within the allowable path limitation parameters (100).

3. The marine vessel cyber-attack prevention system (10) of claim 2, wherein the dedicated position reference system (12) comprises two satellite receivers (12a, 12b) configured to be arranged a fixed distance apart on board said vessel (S).

4. The marine vessel cyber-attack prevention system (10) of claim 3, wherein the fixed distance is read-only accessible from the digital storage medium (11).

5. The marine vessel cyber-attack prevention system (10) of any of the claims above, wherein the path limitation parameters (100) comprises one or more allowable or not allowable operating areas (21a, 21b,...) for the vessel.

6. The marine vessel cyber-attack prevention system (10) of claim 5, wherein said one or more operating areas (21a, 21b,...) are associated with one or more speed limitation parameters (V1, V2,...) that are read-only accessible from the digital storage medium (11).

7. The marine vessel cyber-attack prevention system (10) of claim 6, wherein
the input headway control signal (HW_{in}) comprises an input speed signal (V_{in}), and the cyber-attack prevention system (10) is configured for
- comparing the input speed signal (V_{in}) with one of said speed limitation parameters (V1, V2,...), and
- forwarding the input speed signal (V_{in}) unaltered as an output speed signal (V_{out}) only if the input speed signal (V_{in}) is within a speed limitation (V1, V2,...) for a current operating area (21a, 21b,...) among the one or more operating areas (21) .

8. The marine vessel cyber-attack prevention system (10) of claim 7, wherein the cyber-attack prevention system (10) is arranged for limiting the output speed signal (V_{out}) to the pre-defined vessel speed limitation parameter (V1, V2,...) for the current operating area (21).

9. The marine vessel cyber-attack prevention system of any of the claims above, wherein the cyber-attack prevention system (10) comprises an attack counter with a predefined upper limit, wherein the cyber-attack prevention system (10) is configured to increment the attack counter if the headway control signal (HW_{in}) is outside the allowable path limitation parameters (100).

10. The marine vessel cyber-attack prevention system (10) of claim 9, wherein the cyber-attack prevention system (10) is arranged for sending a hold position command if the attack counter reaches the upper limit.

11. The marine vessel cyber-attack prevention system (10) of claim 9 or 10, configured to block further headway control signal (HW_{in}) when the upper limit is reached.

12. The marine vessel cyber-attack prevention system (10) of any of the claims above, configured to issue a next encryption key command.

13. The marine vessel cyber-attack prevention system (10) of claim 12, wherein one or more encryption keys is pre-defined and stored on the digital storage medium (11), and the next encryption key command comprises one of said encryption keys.

14. The marine vessel cyber-attack prevention system (10) of any of the claims above, wherein any of the path limitation parameters (100), the one or more encryption keys and the fixed distance are hardcoded on the digital storage medium (11)

15. A marine vessel control system (1) with cyber-attack prevention comprising:
- a marine vessel cyber-attack prevention system (10) according to any of the claims 1 to 13,
- a navigation system (200) configured for being controlled from a remote operation centre (300) via a communications system (400) and issuing a vessel input headway control signal (HW_{in}) to the marine vessel cyber-attack prevention system (10),
- a dynamic positioning system (500) configured for receiving the output headway control signal (HW_{out}) from the marine vessel control system (10) and issuing thruster control signals (Tc) to a propulsion control system (600).

16. A marine vessel cyber-attack prevention method for a vessel comprising
- a marine vessel cyber-attack prevention system (10),
- a navigation system (200) configured for being controlled from a remote operation centre (300) via a communications system (400) and issuing a vessel input headway control signal (HW_{in}) to the marine vessel cyber-attack prevention system (10),
- a dynamic positioning system (500) configured for receiving the output headway control

signal (HW_{out}) from the marine vessel control system (10) and issuing thruster control signals (Tc) to a propulsion control system (600),
the method comprising;
- providing a digital storage medium in the marine vessel cyber-attack prevention system (10) with hard-coded path limitation parameters (100) for the vessel,
- receiving an input headway control signal (HW_{in}) from the navigation system,
- reading the path limitation parameters (100),
- comparing the input headway control signal (HW_{in}) with the path limitation parameters (100), and
- forwarding the input headway control signal (HW_{in}) unaltered as an output headway control signal (HW_{out}) only if the input headway control signal (HW_{in}) is within the allowable path limitation parameters (100).

17. The method of claim 16, wherein the path limitation parameters (100) comprises one or more allowable or not allowable operating areas (21a, 21b,...) for the vessel, and wherein the method comprises;
- forwarding the input headway control signal (HW_{in}) unaltered as an output headway control signal (HW_{out}) only if the input headway control signal (HW_{in}) is within the one or more operating areas (21a, 21b).

18. The method of claim 17, wherein the path limitation parameters (100) wherein said one or more allowable operating areas (21a, 21b,...) are associated with one or more speed limitation parameters (V1, V2,...) that are read-only accessible from the digital storage medium (11) and the input headway control signal (HW_{in}) comprises an input speed signal (V_{in}), wherein the method comprises:
- comparing the input speed signal (V_{in}) with one of the speed limitation parameters (V1, V2,...), and
- forwarding the input speed signal (V_{in}) unaltered as an output speed signal (V_{out}) only if the input speed signal (V_{in}) is within the speed limitation (V1, V2,...) for a current operating area (21a, 21b,...) among the one or more operating areas (21a, 21b,...) .

19. The method of claim 18, comprising the step of:
- limiting the output speed signal (V_{out}) to the pre-defined vessel speed limitation parameter (V1, V2,...) for the current operating area (21).

20. The method of any of the claims 16 to 19, comprising the step of:
- incrementing an attack counter if the headway control signal (HW_{in}) is outside the allowable path limitation parameters (100).

21. The method of any of the claim 20, comprising the step of:
- sending a hold position command if the attack counter reaches the upper limit.

22. The method of any of the claim 20 or 21, comprising the step of:
- block further headway control signal (HW_{in}) when the upper limit is reached.

23. The method of any of of the claims above, comprising the step of:
- issuing a next encryption key command.

24. The method of any of the claim 23, comprising the step of:
- reading a next encryption key from the digital storage medium (11), and the next encryption key command comprises the encryption key.

25. The method of any of the claims above, comprising the step of:
determining a current position of the vessel from a dedicated position reference system (12), wherein the current position is used in determine if the input headway control signal (HW_{in}) is within the allowable path limitation parameters (100).

26. The method of claim 25, comprising the step of:
- determining the current position of the vessel from two satellite receivers (12a, 12b) comprised by the dedicated position reference system (12), wherein two satellite receivers (12a, 12b) are arranged a fixed distance apart on board said vessel (S).

27 The method of claim 26, comprising the steps of:
- calculating whether the received signals from the two satellite receivers (12a, 12b) are in accordance with the fixed distance;
- forwarding the input headway control signal (HW_{in}) unaltered as an output headway control signal (HW_{out}) only if the received signals from the two satellite receivers (12a, 12b) are in accordance with the fixed distance.

PATENTKRAV

1. Marinefartøy-cyberangrepsforebyggingssystem (10) omfattende:
- banebegrensningsparametre (100) for fartøyet (S), hvori cyberangrepsforebyggingssystemet (10) er konfigurert for å motta et inngangsfremdriftsstyresignal (HW_{in}) og ytterligere konfigurert for å lese av banebegrensningsparametrene (100) og å sammenligne inngangsfremdriftsstyresignalet (HW_{in}) med banebegrensningsparametrene (100), og hvori cyberangrepsforebyggingssystemet (10) er konfigurert for å videresende inngangsfremdriftsstyresignalet (HW_{in}) uendret som et utgangsfremdriftsstyresignal (HW_{out}) bare hvis inngangsfremdriftsstyresignalet (HW_{in}) er innenfor de tillatte banebegrensningsparametrene (100), hvori cyberangrepsforebyggingssystemet (10) omfatter et digitalt lagringsmedium (11) med kun lesetilgang for cyberangrepsforebyggingssystemet (10), hvori det digitale lagringsmediet (11) omfatter banebegrensningsparametrene (100).

2. Marinefartøy-cyberangrepsforebyggingssystemet (10) ifølge krav 1, omfattende et dedikert posisjonsreferansesystem (12) konfigurert for å bestemme en aktuell posisjon til fartøyet, hvori den aktuelle posisjonen anvendes til å bestemme om inngangsfremdriftsstyresignalet (HW_{in}) er innenfor de tillatte banebegrensningsparametrene (100).

3. Marinefartøy-cyberangrepsforebyggingssystemet (10) ifølge krav 2, hvori det dedikerte posisjonsreferansesystemet (12) omfatter to satellittmottakere (12a, 12b) konfigurert for å anordnes med en fast avstand ombord på fartøyet (S).

4. Marinefartøy-cyberangrepsforebyggingssystemet (10) ifølge krav 3, hvori den faste avstanden er tilgjengelig kun lesbart fra det digitale lagringsmediet (11).

5. Marinefartøy-cyberangrepsforebyggingssystemet (10) ifølge hvilke som helst av kravene ovenfor, hvori banebegrensningsparametrene (100) omfatter ett eller flere tillatte eller ikke tillatte operasjonsområder (21a, 21b,...) for fartøyet.

6. Marinefartøy-cyberangrepsforebyggingssystemet (10) ifølge krav 5, hvori det ene eller de flere operasjonsområdene (21a, 21b,...) er assosiert med én eller flere hastighetsbegrensningsparametre (V1, V2,...) som er tilgjengelige kun lesbart fra det digitale lagringsmediet (11).

7. Marinefartøy-cyberangrepsforebyggingssystemet (10) ifølge krav 6, hvori inngangsfremdriftsstyresignalet (HW_{in}) omfatter et inngangshastighetssignal (V_{in}), og cyberangrepsforebyggingssystemet (10) er konfigurert for
- å sammenligne inngangshastighetssignalet (V_{in}) med én av hastighetsbegrensningsparametrene (V1, V2,...), og
- å videresende inngangshastighetssignalet (V_{in}) uendret som et utgangshastighetssignal (V_{out}) bare hvis inngangshastighetssignalet (V_{in}) er innenfor en hastighetsbegrensning (V1, V2,...) for et aktuelt operasjonsområde (21a, 21b,...) blant det ene eller de flere operasjonsområdene (21).

8. Marinefartøy-cyberangrepsforebyggingssystemet (10) ifølge krav 7, hvori cyberangrepsforebyggingssystemet (10) er anordnet for å begrense utgangshastighetssignalet (V_{out}) til den forhåndsdefinerte fartøyhastighetsbegrensningsparameteren (V1, V2,...) for det aktuelle operasjonsområdet (21).

9. Marinefartøy-cyberangrepsforebyggingssystemet ifølge hvilke som helst av kravene ovenfor, hvori cyberangrepsforebyggingssystemet (10) omfatter en angrepsteller med en forhåndsdefinert øvre grense, hvori cyberangrepforebyggingssystemet (10) er konfigurert for å inkrementere angrepstelleren hvis fremdriftsstyresignalet (HW_{in}) er utenfor de tillatte banebegrensningsparametrene (100).

10. Marinefartøy-cyberangrepsforebyggingssystemet (10) ifølge krav 9, hvori cyberangrepsforebyggingssystemet (10) er anordnet for å sende en kommando om å holde posisjonen hvis angrepstelleren når en øvre grense.

11. Marinefartøy-cyberangrepsforebyggingssystemet (10) ifølge krav 9 eller 10, konfigurert for å blokkere ytterligere fremdriftsstyresignal (HW_{in}) når den øvre grensen er nådd.

12. Marinefartøy-cyberangrepsforebyggingssystemet (10) ifølge hvilke som helst av kravene ovenfor, konfigurert for å sende ut en neste krypteringsnøkkelkommando.

13. Marinefartøy-cyberangrepsforebyggingssystemet (10) ifølge krav 12, hvori én eller flere krypteringsnøkler er forhåndsdefinert og lagret på det digitale lagringsmediet (11), og den neste krypteringsnøkkelkommandoen omfatter én av krypteringsnøklene.

14. Marinefartøy-cyberangrepsforebyggingssystemet (10) ifølge hvilke som helst av kravene ovenfor, hvori hvilken som helst av banebegrensningsparametrene (100), den ene eller de flere krypteringsnøklene og den faste avstanden er hardkodet på det digitale lagringsmediet (11)

15. Marinefartøystyresystem (1) med cyberangrepsforebygging, omfattende:
- et marinefartøy-cyberangrepsforebyggingssystem (10) ifølge hvilke som helst av kravene 1 til 13,
- et navigasjonssystem (200) konfigurert for å styres fra et fjernoperasjonssenter (300) via et kommunikasjonssystem (400) og å sende ut et inngangsfremdriftsstyresignal (HW_{in}) for fartøyet til marinefartøy-cyberangrepsforebyggingssystemet (10),
- et dynamisk posisjoneringssystem (500) konfigurert for å motta utgangsfremdriftsstyresignalet (HW_{out}) fra marinefartøystyresystemet (10) og å sende ut drivkraftsinnretningsstyresignaler (Tc) til et drivkraftsstyresystem (600).

16. Fremgangsmåte for marinefartøy-cyberangrepsforebygging for et fartøy, omfattende
- et marinefartøy-cyberangrepsforebyggingssystem (10),
- et navigasjonssystem (200) konfigurert for å styres fra et fjernoperasjonssenter (300) via et kommunikasjonssystem (400) og å sende ut et inngangsfremdriftsstyresignal (HW_{in}) for fartøyet til marinefartøy-cyberangrepsforebyggingssystemet (10),
- et dynamisk posisjoneringssystem (500) konfigurert for å motta utgangsfremdriftsstyresignalet (HW_{out}) fra marinefartøystyresystemet (10) og å sende ut drivkraftsinnretningsstyresignaler (Tc) til et drivkraftsstyresystem (600),

der fremgangsmåten omfatter;

- å tilveiebringe et digitalt lagringsmedium i marinefartøy-cyberangrepsforebyggingssystemet (10) med hardkodede banebegrensningsparametre (100) for et fartøy,
- å motta et inngangsfremdriftsstyresignal (HW_{in}) fra navigasjonssystemet,
- å lese av banebegrensningsparametrene (100),
- å sammenligne inngangsfremdriftsstyresignalet (HW_{in}) med banebegrensningsparametrene (100), og

å videresende inngangsfremdriftsstyresignalet (HW_{in}) uendret som et utgangsfremdriftsstyresignal (HW_{out}) bare hvis inngangsfremdriftsstyresignalet (HW_{in}) er innenfor de tillatte banebegrensningsparametrene (100).

17. Fremgangsmåten ifølge krav 16, hvori banebegrensningsparametrene (100) omfatter ett eller flere tillatte eller ikke tillatte operasjonsområder (21a, 21b,...) for fartøyet, og hvori fremgangsmåten omfatter;

å videresende inngangsfremdriftsstyresignalet (HW_{in}) uendret som et utgangsfremdriftsstyresignal (HW_{out}) bare hvis inngangsfremdriftsstyresignalet (HW_{in}) er innenfor det ene eller de flere operasjonsområdene (21a, 21b).

18. Fremgangsmåten ifølge krav 17, hvori banebegrensningsparametrene (100) hvori det ene eller de flere tillatte operasjonsområdene (21a, 21b,...) er assosiert med én eller flere hastighetsbegrensningsparametre (V1, V2,...) som er kun lesbart tilgjengelige fra det digitale lagringsmediet (11), og inngangsfremdriftsstyresignalet (HW_{in}) omfatter et inngangshastighetssignal (V_{in}), hvori fremgangsmåten omfatter:

- å sammenligne inngangshastighetssignalet (V_{in}) med én av hastighetsbegrensningsparametrene (V1, V2,...), og
- å videresende inngangshastighetssignalet (V_{in}) uendret som et utgangshastighetssignal (V_{out}) bare hvis inngangshastighetssignalet (V_{in}) er innenfor hastighetsbegrensningen (V1, V2,...) for et aktuelt operasjonsområde (21a, 21b,...) blant det ene eller de flere operasjonsområdene (21a, 21b,...).

19. Fremgangsmåten ifølge krav 18, omfattende trinnet:

- å begrense utgangshastighetssignalet (V_{out}) til den forhåndsdefinerte hastighetsbegrensningsparameteren (V1, V2,...) for fartøyet for det aktuelle operasjonsområdet (21).

20. Fremgangsmåten ifølge hvilke som helst av kravene 16 til 19, omfattende trinnet:
- å inkrementere en angrepsteller hvis fremdriftsstyresignalet (HW_{in}) er utenfor de tillatte banebegrensningsparametrene (100).

21. Fremgangsmåten ifølge hvilke som helst av krav 20, omfattende trinnet:
- å sende en kommando om å holde posisjonen hvis angrepstelleren når den øvre grensen.

22. Fremgangsmåten ifølge hvilket som helst av kravene 20 eller 21, omfattende trinnet:
- å blokkere ytterligere fremdriftsstyresignal (HW_{in}) når den øvre grensen er nådd.

23. Fremgangsmåten ifølge hvilke som helst av kravene ovenfor, omfattende trinnet:
- å sende ut en neste krypteringsnøkkelkommando.

24. Fremgangsmåten ifølge hvilke som helst av krav 23, omfattende trinnet:
- å lese en neste krypteringsnøkkel fra det digitale lagringsmediet (11), og den neste krypteringsnøkkelkommandoen omfatter krypteringsnøkkelen.

25. Fremgangsmåten ifølge hvilke som helst av kravene ovenfor, omfattende trinnet:
å bestemme en aktuelle posisjon til fartøyet ut fra et dedikert posisjonsreferansesystem (12), hvori den aktuelle posisjonen anvendes til å bestemme om inngangsfremdriftsstyresignalet (HW_{in}) er innenfor de tillatte banebegrensningsparametrene (100).

26. Fremgangsmåten ifølge krav 25, omfattende trinnet:
- å bestemme den aktuelle posisjonen til fartøyet ut fra to satellittmottakere (12a, 12b) omfattet av det dedikerte posisjonsreferansesystemet (12), hvori to satellittmottakere (12a, 12b) er anordnet med en fast avstand ombord på fartøyet (S).

27. Fremgangsmåten ifølge krav 26, omfattende trinnene:

- å beregne om de mottatte signalene fra de to satellittmottakerne (12,a 12b) er i overensstemmelse med den faste avstanden;

å videresende inngangsfremdriftsstyresignalet (HW_{in}) uendret som et utgangsfremdriftsstyresignal (HW_{out}) bare hvis de mottatte signalene fra de to satellittmottakerne (12a, 12b) er i overensstemmelse med den faste avstanden.

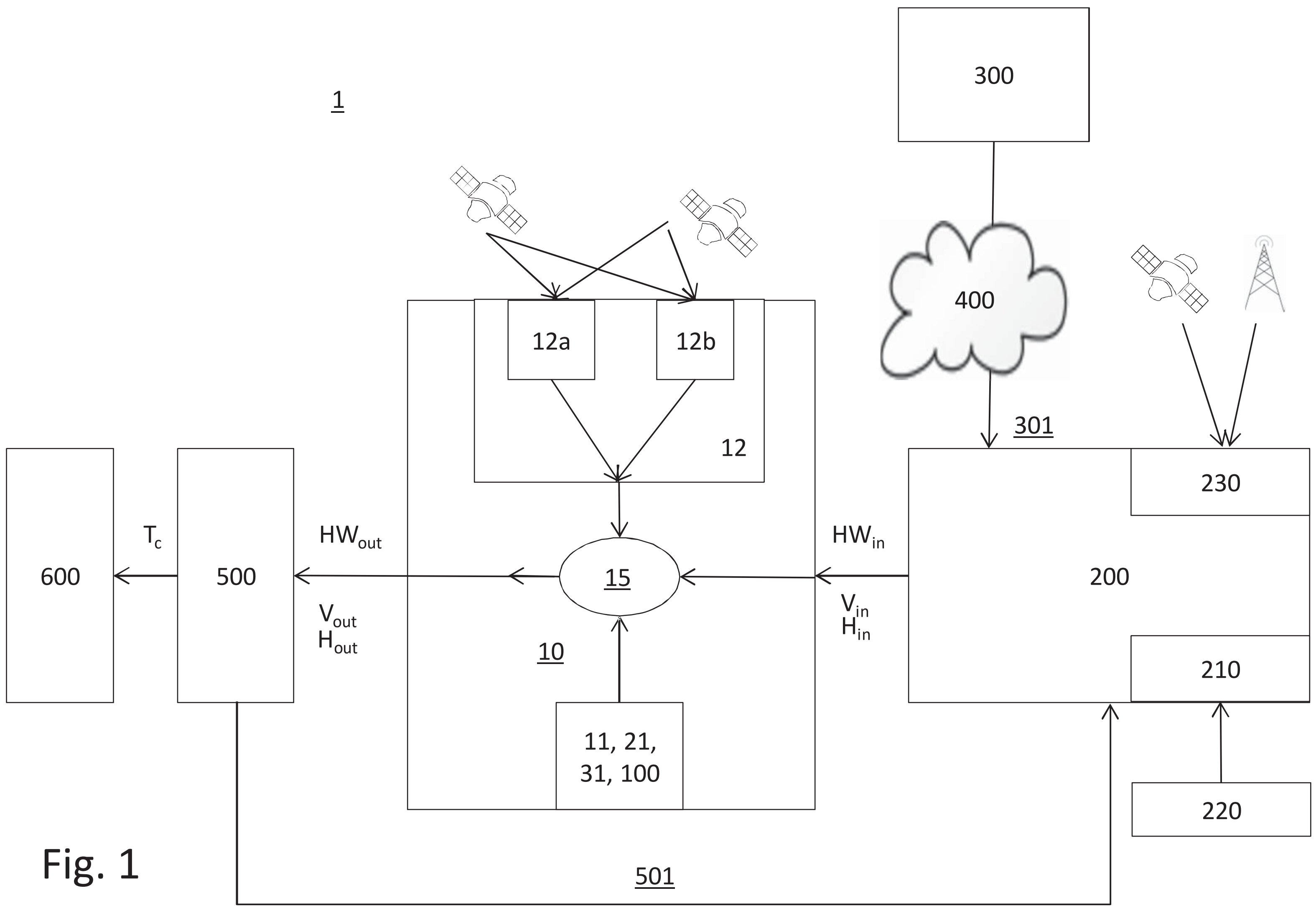

1
300
400
301
230
200
210
220
12a
12b
12
15
10
11, 21,
31, 100
HW$_{in}$
V$_{in}$
H$_{in}$
HW$_{out}$
V$_{out}$
H$_{out}$
500
T$_c$
600
501

Fig. 1

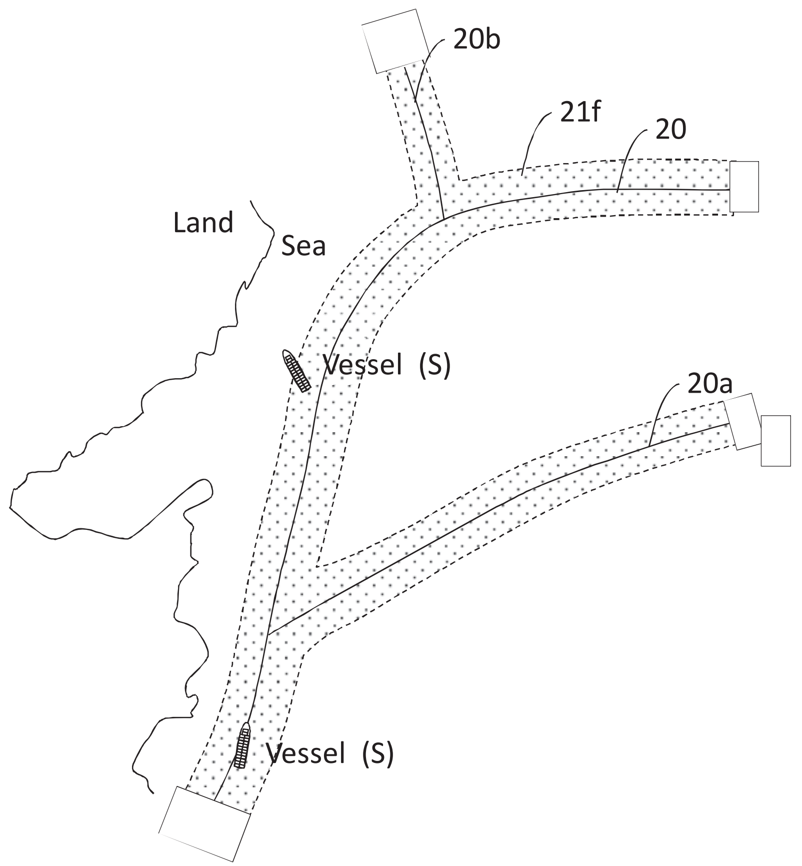


Fig. 2a

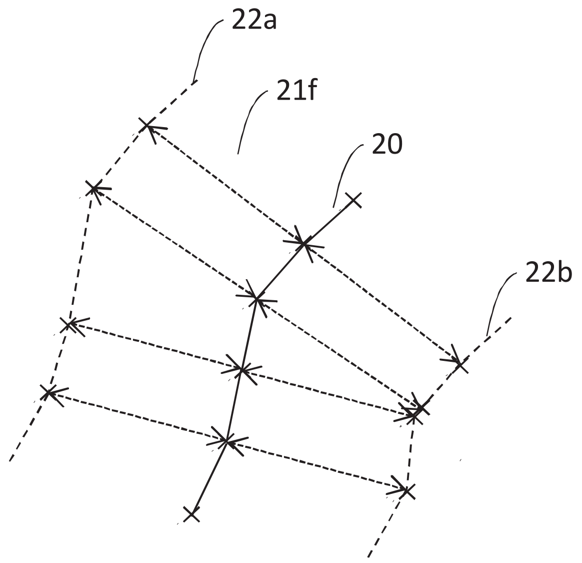


Fig. 2b

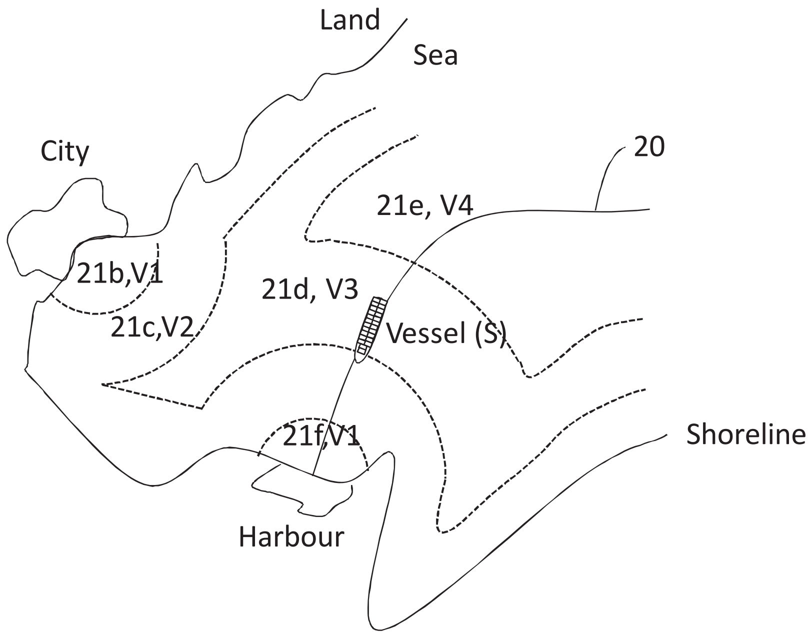

Land
Sea
City
20
21e, V4
21b,V1
21d, V3
Vessel (S)
21c,V2
21f,V1
Shoreline
Harbour

Fig. 3

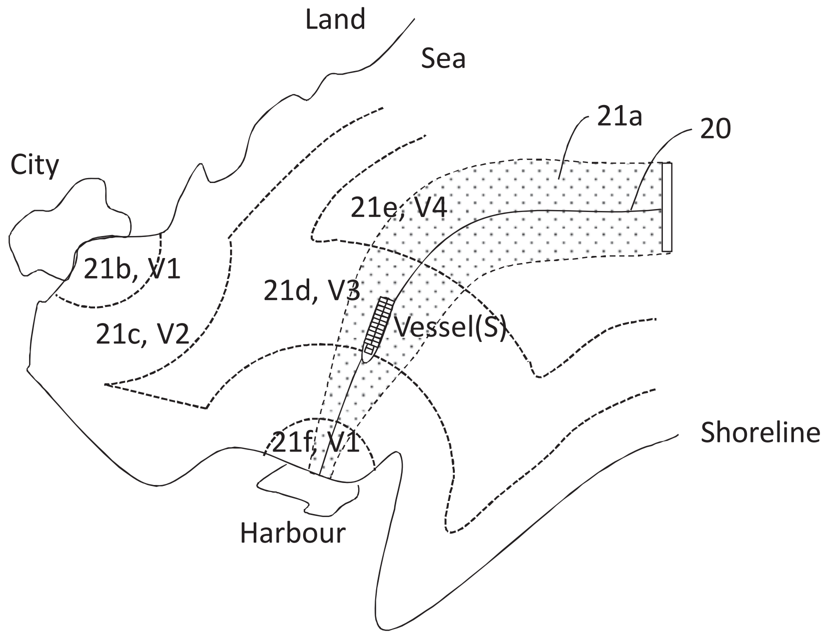

Land
Sea
21a
20
City
21e, V4
21b, V1
21d, V3
Vessel(S)
21c, V2
21f, V1
Shoreline
Harbour

Fig. 4