Autonomy for Ships: A Sovereign Agents Architecture for Reliability and Safety by Design

Dittmann, Kjeld; Hansen, Nicholas; Papageorgiou, Dimitrios; Blanke, Mogens

Published in:
Proceedings of 5th International Conference on Control and Fault-Tolerant Systems

Link to article, DOI:
10.1109/SysToT52990.2021.9595889

Publication date:
2021

Document Version
Peer reviewed version

Link back to DTU Orbit

Citation (APA):
Autonomy for Ships: A Sovereign Agents Architecture for Reliability and Safety by Design*

Kjeld Dittmann1, Peter Nicholas Hansen1, Dimitrios Papageorgiou1 and Mogens Blanke1

Abstract—Autonomous systems strive to obtain salient features that include computer intelligence for obtaining situation awareness, decision support to a human navigator, or for facilitating autonomous decision-making in unmanned vehicles. This paper considers the case of autonomous marine surface vehicles, where high-quality decision support will be instrumental for obtaining a periodically unattended bridge and for approval of unmanned bridge operation with fallback through remote operation. The proposed design focuses on a sovereign-based architecture that facilitates safety, resilience and cyber-security. We address central elements of risk in the development and approval of autonomous systems; we analyze the challenges associated with testing, commissioning and maintenance of a highly complex cyber-physical system, and describe design principles for the sovereign agents architecture.

I. INTRODUCTION

The rapid development in autonomy for vehicles on land promises radical changes in the transport and the handling of goods, e.g. the size of transporting units and the frequency of service. The challenges in marine transport differs from those for vehicles on land, both in terms of number of vehicles manufactured per year and the size of the units, but also in international rules, regulations and approval procedures. With the small number of identical vessels, i.e. sister ships, the maritime automation systems are designed on project conditions, often utilizing parts of previously approved hardware and software designs.

Trial experiments with a highly automated vessel have demonstrated that the on-board control system has the ability to control a vessel from the quay in one port and to berth it in another [1], [2]. Similar trials have been conducted in the field of remote operation, where the bridge crew on offshore vessels and tugs has been substituted by a crew at a Remote Control Center (RCC) [3]. The regulatory regime for operation of Maritime Autonomous Surface Ships (MASS) is currently not in place and therefore trials have been performed in assigned test areas [4], [5]. The introduction of MASS has the potential to increase safety, improve the environmental performance of the vessel and enable more cost-effective shipping. However, the potential risk associated with the introduction of large and complex automation systems on board ships is of continuous concern. The authors in [6] address the need for a risk-based design method.

The increasing cognitive challenges associated with the system design process require measures that reduce the risks and consequences of software defects, malfunction and harmful cyber-interference. Resilience to these risks require the system to be able to isolate and encapsulate not-normal behaviours. Moreover, extreme dependability is needed even for rarely occurring events. The sources of risk have changed towards the software development and validation [7], [8], and to the cyber-physical dimensions [9], [10]. The pace of the development in MASS is difficult to predict, but the first generation of autonomous vessels might be in operation by the end of 2021 [11]. To make this happen without compromising safety, a fundamental paradigm shift is needed in the design of the on-board system.

This paper focuses on the challenges of control system design for identifying ways of applying new technologies in a safe way. More specifically, the paper addresses the design case of an autonomous, over-actuated surface marine vehicle, where high-quality decision support is instrumental for obtaining a periodically unattended bridge. The same level of decision support is fundamental for the approval of unmanned bridge operation with a possibility of fall-back to remote operation by a human, if this should be needed. The proposed approach concerns a sovereign-based architecture for obtaining safety, resilience and cyber-security. We address central elements of risk in the development and approval of autonomous systems; we analyze the challenges associated with testing, commissioning and maintenance of the highly complex cyber-physical system, and detail system design principles. We show how such a design can be obtained through a novel sovereign-based architecture. An actual implementation shows the efficacy of the concepts.

The remainder of the paper is structured as follows: Section II introduces the context of the problem at hand, while design constraints and guidelines are discussed in Section III. Section IV shows how challenges associated with testing, commissioning and maintenance of a high-complexity cyber-physical system are made easier with a sovereign-based design. Section V addresses the application of such design principles on the ShippingLab ship. Section VI provides a first-hand impression of the system performance and Section VII offers the conclusions.

II. THE AUTONOMOUS SYSTEM IN CONTEXT

A ship or a vessel is often defined as a floating construction above 15 meters in length with its own propulsion and steering system. When adding self-governing capabilities, the ship is categorised as autonomous.
The main drivers for introducing autonomous technologies, as discussed in [12], are:

1) Data collection and big data.
2) Operational efficiency.
3) Operational safety, minimizing human errors [13].
4) Reduction of crew costs.

The current international rules require an onboard crew with well-defined roles and responsibilities. When introducing electronic-based solutions with the aim of replacing parts of the onboard statutory crew, a substitute crew will need to resume responsibility. A RCC, often shore-based, is likely to assume that role. Fig. 1 shows a simplified block diagram that illustrates the key elements of an autonomous ship.

The shore-based crew of a RCC is assumed to consist of master mariners undertaking the role of Master/Captain, Chief Engineering Officer and the Officer of the Watch. The manning of the RCC will need a level of situation awareness as if being on the vessel, in order to fulfil that assignment. The derived functional requirement to a RCC and its communication link imposes stringent reliability and capacity requirements, however this is considered outside of the scope of this paper. The primary areas of interest of this paper are the sub-systems related to vessel movement e.g., power automation, Voyage Control System (VCS) and the electronic solution substituting the bridge crew.

The voyage planning for the autonomous vessel will be performed, as for a conventional vessel, based on optimization criteria e.g., weather, tide and required arrival time. The transit part of the route will be equivalent to a route for a track control system [14], but the harbor and berthing track will need to be included. The VCS has three modes: automatic, joystick/tiller and manual mode. The automatic mode has three sub-modes i.e., transit, harbor and berthing. The joystick mode has two sub-modes, i.e. local and RCC control.

The Autonomous Navigation Supervisor (ANS) monitors the situation by information from cameras, radar, Automatic Identification System (AIS), own vessel navigational data i.e., speed, heading, position, wind & depth, and the Electronic Navigational Chart (ENC). If the ANS detects a need for route alteration, it will provide the Autonomous Coordination Supervisor (ACS) with a rerouting suggestion. The ACS will, depending on the operational mode either; instruct the VCS to follow the newly suggested route, or forward the suggestions to a human proxy (either on-board or RCC based).

III. GUIDING DESIGN CRITERIA

Computer-based solutions have been applied in the maritime industry for decades. In this paper we use the term architecture to describe the structure of a vessel Information and Communications Technology (ICT), i.e. a structure consisting of entities, their properties, and relationships.

The criteria that guides the selection, creation, and implementation of the proposed solutions are a pragmatic combination of:

- Cyber security in cyber-physical systems
- The regulatory regime
- Dealing with risk and complexity
- Fault-tolerant control
- Real-time on-board communication
- External communication to other vessels and shore (outside the scope of this paper)
- Design of the shore based control center (outside the scope of this paper)
- Training and education (outside the scope of this paper)

A. Cyber security in cyber-physical systems

Two significant issues have gradually changed the impact of utilizing computer-based solutions. The first notable difference is that various automation systems installed on ships have historically had limited inter-system integration and, until recently, the same applied to the integration between navigation and automation systems. This configuration of non-homogeneous systems protected the vessel from computer-viruses spreading from one system to another, thereby limiting the risk of a complete vessel breakdown [15], [16]. The second notable change is the adoption of development frameworks, tools, libraries, public domain components and operating systems. The adoption has enabled innovative solutions, which have drastically reduced the product cost and the development cycle. However, gradually moving away from proprietary hardware and software solutions has exposed the systems to a previously non-existing threat, i.e. computer-viruses which are able to spread throughout the entire system, since the individual sub-systems have adopted a homogeneous technology and are no longer isolated.

Among corporate enterprises, it is common to have a homogeneous infrastructure and apply regular updates and virus protection regimes. This protection regime is, for several reasons, currently not applied on-board vessels. One issue is the difficulty of assessing and validating potential side effects of the software upgrade. Another issue is that a virus scan will detect industrial application software as suspicious software of unknown origin, e.g. the dedicated automation and navigation applications, and it might flag/remove these. Potential re-certification of the installed system is also an issue; as described earlier in this paper, vessel design and
constructions have not been standardized i.e., the selection of sub-systems, their configurations and certification are unique. The currently applied solutions of protection mechanisms, i.e. firewalls and Virtual Private Networks (VPN), have in numerous cases shown to be insufficient [17].

Vessels are often operated 24/7 between the five year mandatory docking intervals and the ability to perform on-line changes are often highlighted as a desired feature. For example, when performing service and upgrades of Heating, Ventilation, and Air Conditioning (HVAC) and Emergency Shot-Down Systems (ESD) on large passenger ships with short port stay. This has introduced highly standardized interpreted programming languages or scripts designed for on-line changes at the expense of the system robustness towards threats from cyber attacks targeted Integrated Ship Control (ISC) systems [18].

B. The Regulatory Regime

The International Maritime Organization (IMO) is the domain agency of the United Nations (UN) being responsible for creating a fair and effective regulatory maritime framework. According to United Nations Convention of Law of the Sea (UNCLOS), vessels are only granted permission to operate in international waters if they comply with international regulation [19]. The conventions of UNCLOS and IMO utilize the principle of skilled seafarers [20] who manage the ship and ensure compliance with regulations on behalf of the flag state and the owner. The certification of equipment, material and ultimately the final vessel is a joint effort of the flag state and a recognised class society, i.e. a member of the International Association of Classification Societies (IACS) [21]. According to IMO’s principle of no favorable treatment, evidence must be provided that the autonomous system offers the same degree of safety, security and protection of environment as a conventional manned vessel.

The limited number of marine vessels constructed per annum and the lack of standardization "models", combined with the current rules and regulations, impose significant validation and certification challenges. Each vessel is formally approved during sea trial; however, this type of approval regime leads to a certification process that strongly relies on individually type-approved sub-systems. Despite the change in the risk image, the majority of products and solutions applied on vessels is currently certified and approved under a regime of prescriptive rules and procedures, i.e. performance and test standards. Nearly all the test standards originated from a hardware mind-set i.e., expose, observe, measure and document. The autonomous and non-autonomous vessels will co-exist, thus alignment with, and endorsement of the regulatory regime is important when designing and implementing the autonomous system.

Due to the rapid development of autonomous systems, IMO has published guidelines for conducting trials [4]. When not having the complete regulatory regime in place, the IMO’s Strategic Plan [22] provides strategic directions by stating, "Integrate new and advancing technologies in the regulatory framework” [23] in connection with [24] that introduces a modular design, certification standards & rules.

C. Dealing with Risk and Complexity

It is generally accepted that a goal and risk based assessment will be required when implementing MASS, [25], [12] and [6]. The associated risk can be grouped into four main categories, with the first two categories being outside the scope of this paper.

- The liability risk when the human is replaced by electronics, e.g. is the supplier of the electronic solution liable for a collision between two vessels?
- The conventional vessel risk of fire, flooding, etc.
- The cyber risk originated from on board & Ship-Shore integration.
- The risk associated with the electronic solutions and the design & reliability thereof.

Incident reports have documented that up to two-thirds [13] of all incidents involving ships could be referred to as caused by human errors. Efforts have been made to improve the issue of human error, with the strong integration of systems being one of the dominating factors. By adopting an increased level of ICT, a shift in the sources of risk can be observed, i.e. the design and the software development and implementation are becoming major areas of concern [12], [9], [8], [10].

![Fig. 2. Modular hierarchy in an architecture with supervisor as a meta-level between process layer with control and plant wide coordination [26]](image)

One of the corner elements of the risk handling is to establish a generally accepted structure and interface standards of the systems in order to obtain a framework for where the individual sub-functions belong, i.e. the allocation of functions in terms of a control hierarchy, and to ensure correct communication and interoperability [26]. Fig. 2 illustrates how to deal with increasing complexity, i.e. by locating the functions and aggregating the information.

Decomposition and modularity has proved to be an effective way of accommodating abstraction, automated testing and certification. Problems/failures more frequently arise due to poor design and/or high complexity rather than hardware malfunction [27], [28]. In addition to reducing the cognitive
challenges, a stringent modular design supports the often-incremental certification process. It supports the needed test strategy of module and regression test, as well as the creation of an automated consistency and interoperability verification tool, which can validate the vessel specific configuration prior to the actual integration.

D. Real-time on-board communication

Data harvesting required for operational optimization has been driving the creation of ship-wide networks that provide the normalized data needed. Therefore, one of the fundamental requirements to the design and implementation of a MASS system is to provide interoperability between domain specific hardware and software platforms in a seamless, predictable and secure way. Migrating from a collection of non homogeneous sub-systems towards a platform concept is illustrated in Fig. 3 and has accelerated the need for domain specific solutions. This has been utilized on advanced patrol vessels operated by modern navies, as well as by some innovative large commercial ship owners as part of the digitisation and optimization strategy. The routing of inter-system connection - illustrated by a red line - is done in separated fire zones, as this is one of the requirements in the "safe return to port" rules. The topology of the A and B net in each of the segregated application areas can be a ring, a star or a combination utilizing managed switches. Significant development has taken place within the area of communication technology, strongly supported by the general development in office automation and household use. The requirements originating from the maritime industry has, due to the size of the industry, limited visibility. One of the overlooked requirements within the maritime industry is the demand for worst-case performance in contrast to the majority of users that appreciates average performance. This has fostered proprietary solutions that complicate the integration process in a multi-vendor environment. Significant efforts were assigned to the development of standards facilitating the increasing needs for industrial communication and interoperability [29], [30]. These standardized communication protocols aimed at providing solutions for safe and predictable connectivity in a multi-vendor system with demands to worst-case performance.

The ATOMOS I/II/III/IV projects, funded by the EU under the FP4-Transport and FP5-Growth programs, spearheaded the understanding of technology-driven development within the areas of vessel operation, system interoperability, human factors and risk. In the context of vessel automation, the concept from MMS [31] and ISO’s Time Critical Communication Architecture group (TCCA) [32] was carried forward and implemented on ISC systems, resulting in - among other findings - a Token Bus based [33] transport profile. Although being available at the time of design, as a chip from recognized manufacturers, a common issue of these application optimized protocols is that they are no longer available.

The project Maritime Unmanned Navigation through Intelligence in Networks (MUNIN) [34] under the EU FP7 aimed at developing a framework for the unmanned vessel. The communication standards applied was Ethernet [35] adopted from MITS [36] with the main focus on vessel to vessel and vessel to shore functional communication.

IV. THE SOVEREIGN BASED VESSEL OPERATING SYSTEM (VOS)

A variety of autonomy related projects have been launched in maritime hubs around the world; however, there is limited published work available on the implementation of autonomous vessels intended for daily service. The proposed solution is provided by:

- Ship-wide network with security policies.
- A dedicated transport protocol with real-time capabilities and accurate time synchronization.
- A minimized local operating system with integration and protection services as extensions.
- Fault tolerant control and highly advanced sensor fusion techniques.

The term operating system is used in connection with computers, networks and in the case of this paper as VOS, i.e. the combination of the above four key elements that constitute the infrastructure.

A. Security Policies

The cyber security needs to be embedded in the design process in parallel to quality and testing rather than “bolted on” at a later stage.

On a network, the term port is used to determine where the incoming traffic should be directed and establish connection to standard services. These built-in standard services, e.g. mail and file transfer services, are often the root cause of cyber security related problems. In order to minimize that, the utilization of external communication services provided by the operating system on the node is prohibited, i.e. the port numbers below 49,152 must be closed.
The closing of standard ports supplemented with an end-to-end message authentication, will provide a cyber-resilient system design [37], [38]. It is recommended that the ability to perform on-line changes should be limited and only utilized under strict policies and only with physical presence on the vessel.

B. The Transport Protocol

One of the fundamental design criteria of ICT systems for MASS is worst-case performance in contrast to the often applied average performance in the general domain of computers and communication. In the implementation of the proposed system, a ring topology with automatic reconfiguration in case of a cable defect is being utilized. However, this redundancy feature is supplemented by applying an A- and a B-segment where the quality of the communication between entities is being monitored by the implemented connection oriented transport protocol. Secure delivery of information is of paramount importance in a MASS system. It has therefore been decided to utilize the User Datagram Protocol (UDP) supplemented with an immediate acknowledgement at the entry of the Middle-Ware (MW) Protocol Data Unit (PDU) parser, and the path-connection is flagged unavailable if an acknowledgement is not received. In case a re-transmission on the other network segment is not successful, all subscribed topics originating from that entity is flagged ”connection lost” in the local repository. Integrity of the system is verified during the initialization phase by establishing a connection to the node and to all the topics that the application needs to subscribe to. The connection is continuously being monitored and validated by the flow of data and heartbeat messages.

An accurate system-wide clock service is required for matching information captured on different physical devices and for the chronological sorting of events. All nodes in the system have the ability to become the clock master/leader. Absolute time is not required, however the node connected to an external clock system is the default master. It was decided, as illustrated in Fig. 4, to implement the service that synchronise the local operating system clock as part of the transport layers PDU parser along with the immediate acknowledgement service in order to get the required accuracy without significant overhead. The communication delay between entities that are being synchronized is measured by a series of ping/echo sequences and used to adjust the time message being exchanged. The updates of topics is event driven, i.e. if there is no change in value, then no updates are being communicated. Therefore, a node that comes online is prohibited from time-stamping a piece of information and share it as long as the node has not been time synchronized.

System messages, supervisor related messages and application message exchange are only granted via the symmetric subscription server/repository. The proposed system design does not depend on any single component or service; the system design supports the elimination of central functions by the distributed allocation of functions. The connection oriented communication protocol is securing integrity of the system, enabling exchange of changes and not full data sets, and thereby keeping the traffic load at a minimum. This communication principle also applies for the link to the RCC.

C. Integration and Protection Service Extensions

The cyber-physical system on an autonomous vessel can be considered as a system of systems, often from different vendors. The individual systems are optimized to serve a specific purpose with dedicated hardware and software. From the domain of real-time system design, the exchange of information, in the form of message passing, provides the needed execution independence [39]. Subscription based exchange of information combined with a symmetric client-server architecture utilizing an actor/agent approach facilitates service access from multiple sources. Messages between modules are based on a publish/subscribe communication protocol. This design choice of a ”pub/sub” protocol is motivated by the wish to remove the dependency between producers, e.g. a module that read sensory information and publish data (a topic), and consumers, i.e. other modules or sub-systems that use the produced data. This also enables the framework to easily add many consumers of a single topic, without changing the configuration of the producer.

Each module is placed on one or several physical ”nodes” in the system, where each node contains a singleton of a MW, which primary task is to enable and ensure secure communication between modules. The secure message transport between modules is abstracted away by the MW, leaving
the modules to focus only on the sending and receiving of data. Fig. 5 shows an example of such a node, where the "Supervisor Agent" is located on the node, and it is able to communicate with the rest of the system, through the local MW. Each node in the system also has a local data repository, which contains a local copy of all the data that is either sent from or received by the modules running on the node. The information items in the distributed repositories will collectively hold the current state of the combined system with validity information and accurate time stamp for value and state change.

The MW enables modules to exist across several physical nodes. Modules can be defined in a hierarchy of priority: active, hot-spare, cold-spare. Each instance of a module is placed on different physical nodes and is activated if no higher priority instance is running. Hence, this design enables redundancy at both the hardware and software level.

The supervisor agent will be responsible for gathering the performance of the MW and the applications. This includes gathering of statistics and metrics that are used to monitor the health of the MW and the hosted applications. The status from agents will be collected, monitored and acted upon by the ACS.

Guarding the components/modules by strict entry control will isolate, channel, and simplify the interaction between applications and ease the integration process as a whole.

D. Ensuring integrity of safety critical modules

The outer shells of defense have the purpose to ensure dependable and safe operation of the vessel in all conditions, including unintended issues caused by on-board software, or hostile cyber events. These are core obligations by the sovereign architecture of modules. These outer bastions can fail, however, when supplementing the safety critical modules with a model-based detection and fault-handling mechanisms the integrity can be maintained. Model-based detection and fault-handling mechanisms were addressed extensively in the literature on diagnosis and fault-tolerant control, see [40]. These principles have found their way to the space [41] and aircraft industry [42], and to some extent to marine vessels [43]. Model-based methods were also considered in connection with cyber threats for electrical power systems in [18], who advocated for combined cyber security and model-based methods for on-line validation of signals and control actions.

An autonomous vessel needs to be resilient to temporal artefacts, faults or failures, irrespective of whether these origin in software-based functions, in instruments, in on-board hardware or they are caused by external events or direct cyber attacks. In addition to the aforementioned techniques based on models of the physical system, an autonomous system has more possibilities. Equipped with intelligent sensor monitoring of the surroundings, including object detection with cameras in both infrared and visible part of the spectrum, radars with cm and mm wavelengths, automated cross validation of information is feasible. Used for fault-tolerant sensor fusion, suspect sensor signals are excluded for navigation before safety and dependability become at risk. The means to do so include cross validation between observations done with 360-degree camera and radar coverage, ENC and AIS messages. Conditions with spoofing or denial of service from the Global Navigation Satellite Systems (GNSS) are frequently occurring, and AIS messages are being tampered with. Alternative sources for position information are automatically utilised by fault-tolerant sensor fusion, such as positions of buoys and beacons from the ENC, and land contours from radar if in near coast conditions. Generic techniques exist [44] to cross validate the combined information that is available.

To show-case the design principles, Fig. 6 shows a schematic overview of essential functionalities. An ANS module assess the information about detected objects within an awareness zone around the vessel. This information is provided to a Situation Awareness Service (SAS) module based on a dynamic list of detected and classified objects. The Sensor Fusion (SFU) tracks objects using radar, AIS, camera based object detection, and ENC. The SFU provides position, heading, speed and include object situation/condition when this is available.

The situation awareness comprises understanding and anticipation sub-modules. The understanding module attaches semantic meaning to data to identify the current situation. The anticipation module predicts the evolution of the current situation. Updates to the object list are signalled to the relevant topic in the MW that distributes information to modules authorized to subscribe to this information. Trajectory prediction forecasts future position, velocity and bearing of
detected objects. The understanding sub-module evaluates data and assesses the current situation with respect to risk of collision, based on closest predicted distance between objects and compliance with Convention on the International Regulations for Preventing Collisions at Sea (COLREG).

The publish/subscribe based communication protocol design patterns are used to ensure that modules do not impose constraints on the configuration and communication between other modules in the system. This implies that, although the understanding and anticipation sub-modules are part of the same overarching module, the sub-modules need not be located on the same physical hardware node. Furthermore, the publish/subscribe based design allows the system to function in the event of module failures since each module is independent of other modules in the system. For example, if the anticipation sub-module goes offline, the understanding sub-module will still be fully operational, allowing the autonomous supervisor to decide how to proceed, knowing that the anticipation module is offline. On top of enhanced reliability, this design also enables good testability as modules can be tested in isolation, without the entire system being available.

V. APPLYING THE VOS ON THE SHIPPINGLAB SHIP

Fig. 7 shows the allocation of functions in an autonomous ship. A key component of the system is the perception, which provides a consolidated list of objects or targets. In this specific implementation, perception is derived from 7 RGB cameras arranged to provide a 360-degree coverage, 3 LWIR cameras, a pan-tilt-zoom camera, an X-band radar, a short range 79 GHz radar, an AIS receiver, a motion reference unit and navigational information from gyro, speed log, echo sounder, wind speed/direction and GNSS. A sensor fusion, data association and an object trajectory prediction is performed along with a verification against the electronic sea chart where possible.

The VCS executes the planned route and has three modes of operation; transit according to the track-control standard [14]; slow speed track follower for vessel control in the harbour area and related waters; berthing for the final approach. The planned and verified active route is hosted in the short horizon planner that also suggests route alternation triggered by the SAS module.

The SAS module is constantly monitoring the actual situation based on information from the consolidated object subscription server, the ENC service and the COLREG service module. Two supervisor modules, the ACS and the Autonomous Platform Supervisor (APS) provide the ship-wide coordinator with the information needed for a ship-wide assessment. In case an evasive manoeuvre is required, the Short Horizon Planner (SHP) will suggest up to three deviations to the current route. The ACS arbitrates between the alternatives and will in autonomous mode initiate activation of a new route when within the COLREG boundaries or otherwise notify the human proxy. When in non-autonomous mode the ACS will forward the suggested actions to the decision support application.

VI. THE MW PERFORMANCE TEST

Version 1.0 of the MW has been implemented in C++ with application support for C++ and Python. In the current C++ implementation, a one millisecond internal clock accuracy can be maintained with an update interval of five minutes. The target system is intended for autonomy of a Harbour Bus in the ShippingLab project. Node mapping for the target ship test:

- interface to the VCS
- to the general automation system through APS
- to the shore connection
- to Camera, short range and X-band radar servers
- to ACS, ANS and SAS
- to SFU
- to SHP, base load and spare

The integration process is on-going and the own ship navigational data, the SHP and SFU modules have successfully been integrated. Performance tests are currently being performed, including application-to-application network communications loss, latency (min/max/average), bandwidth/throughput/capacity, and delay caused by retransmission (segment switch over time). The initial tests utilize a system of standard HP laptops with Linux Ubuntu 20.04 (Intel Core i7-9700 CPU 3.0GHz) running the C++ implemented MW and a Python test application generating a base load with a symmetric update rate of 2000 topics/s. The average latency has been measured to 150 µs with a payload size of 111 bytes. The recovery time for the case where the current network path is flagged unavailable and a change of network segment is initiated has been measured to 5 ms.

VII. CONCLUSIONS

This paper addressed the design and implementation of autonomous systems for marine vessels. A sovereign-based architecture was suggested to facilitate safety, resilience and
cyber security. The architecture helped satisfying design constraints originating from safety requirements to autonomous systems. Guidelines were described for testing, commissioning and maintenance of a highly complex cyber-physical system. The applicability of the concept was demonstrated by an implementation of the situation awareness service module for autonomous navigation.

ACKNOWLEDGMENT

The authors would like to thank Luc Christin, Jakob Garde and Peter Karstensen for great discussions surfacing as part of their implementation of the MW.

REFERENCES