Autonomy for Ships: System Thinking and Engineering

Dittmann, Kjeld

Published in:
Proceedings of International Conference on Software, Telecommunications and Computer Networks 2022

Link to article, DOI:
10.23919/SoftCOM55329.2022.9911446

Publication date:
2022

Document Version
Peer reviewed version

Autonomy for Ships: System Thinking and Engineering

Kjeld Dittmann[1]

***Abstract*— Marine autonomy research has focused on algorithmic and technical developments, targeting autonomous craft in restricted areas where international rules and regulations are not prioritised. This paper addresses the system engineering aspect of a highly complex system in which the seamless, predictable, and secure interoperability of vendor-specific hardware and software subsystems is a fundamental requirement for designing and implementing cyber-physical systems with artificial intelligence to assist or replace the navigating officer, such as autonomous marine surface vehicles. It addresses international rules in the sector and exhibits a system architecture that can fulfil the criteria for safe behaviour in foreseen occurrences and the capacity to request human aid if the autonomous system cannot manage a problem. The system thinking and engineering provided in this article have been applied to The GreenHopper, a harbour bus currently under construction and intended to undergo certification and enter commercial service.**

I. Introduction

Diverse domains are gaining momentum for technical solutions supporting autonomous and unmanned crafts, and the maritime domain is no exception. The challenges of marine transport differ from those of land-based transport not only in terms of the number of vehicles produced annually, but also in terms of international rules, regulations, and approval processes. Moreover, due to the small number of identical vessels, maritime automation systems are frequently designed on a project-by-project basis. As there is currently no regulatory framework for the operation of Maritime Autonomous Surface Ships (MASS), trials have been conducted in designated test areas [1], [2]. At the MSC 105 in April 2022, the International Maritime Organization (IMO) agreed to develop a non-mandatory goal-based MASS [3], [4] framework as an interim measure. According to [5] the implementation of MASS has the potential to increase safety, enhance the vessel's environmental performance, and make shipping more cost-effective. Trials with highly automated vessels, such as [6], [7], [8], have shown the concept's feasibility. The potential danger of installing vast and complicated automation systems on board ships, on the other hand, is a persistent subject of worry. The increasing cognitive demands of the system design process necessitate the implementation of measures that reduce software defects, malfunctions, and cyber-interference risks and consequences. For a system to be resilient to these risks, it must be able to isolate and encapsulate abnormal behaviours. Furthermore, extreme dependability is required even for infrequent occurrences. The complexity of system design and implementation is one of the consequences of introducing autonomous systems. Thus, the risk factors shift to software development and validation [9], [10] and cyber-physical dimensions [11], [12]. To meet these challenges, system-wide design principles and tools are in demand. In addition, the introduction of new technologies in a highly regulated safety domain poses additional challenges that must be carefully considered. This paper focuses on the difficulties associated with system design in a highly regulated and safety-critical domain. It focuses on the design case of an autonomous, surface marine vehicle, where high-quality autonomy functions are essential for obtaining the approval of periodical unattended bridge operation with the option of remote operation by a human if required. The paper addresses central risk elements in the development and approval of autonomous systems, analyses the challenges associated with testing, commissioning, and maintenance of the highly complex system, and detail system design principles. The paper shows how such a design can be obtained. A variety of autonomy-related projects have been initiated in global maritime hubs. There is, however, a general lack of published material on the implementation of autonomous vessels designed for daily service.

The remainder of the paper is structured as follows: Section II introduces the project, while liability and regulatory framework are discussed in Section III. Section IV introduce the engineering framework. Section V addresses the application of such design principles to the ShippingLab project. Section VI offers the conclusions.

II. The Project Vessel - The GreenHopper

The GreenHopper is the result of three years of collaboration between equipment suppliers, a shipyard, universities, maritime academies, and government agencies.

The vessel design follows current rules and regulations and is certified by the Danish flag state. The hull is a double-ended catamaran with a length of 12.2 meters. With a capacity of 25 passengers, one wheelchair, four bicycles, and a baby carriage. In addition, the design provides space for two crew members. The propulsion configuration is two electric-powered rotateable thrusters capable of providing a cruising speed of up to 8 knots. Batteries provide energy storage.

The systems and modules described throughout this article were completed in the first quarter of 2022. The integration

*This research was funded by the Danish Innovation Fund through the ShippingLab project, grant 8090-00063B, (the Work Package on Autonomy) and by the The Danish Maritime Fund, Orients Fund and the Lauritzen Fund.

[1]Kjeld Dittmann is with the Automation and Control Group, Department of Electrical and Photonics Engineering, Technical University of Denmark, 2800 Lyngby, Denmark (e-mail: kjeditt@dtu.dk)

Fig. 1. The GreenHopper under construction - March 2022 status. Photo courtesy of Tuco Shipyard

test is underway, and trials will begin in August 2022. However, the GreenHopper will enter service in autumn 2022, with a human on the loop.

III. Liability and Regulatory Framework

Terms and definitions for maritime autonomous surface ships are not yet settled, and the term autonomous vessel does not mean unmanned vessel in this article. Similarly, a floating structure with its own propulsion and steering system serves as a definition of a vessel, and when self-governing capabilities are added, it is classified as *autonomous*.

A. Liability

According to [13], [14] and [15] autonomous vessels engaged in international trade have the same liability and navigational rights as conventional human-crewed vessels as long as they adhere to the same rules and regulations [16], [17]. While outside the scope of this article, the underlying premise is that a human proxy will likely be held accountable at an Remote Control Centre (RCC).

B. Regulatory framework

The operation and coexistence of ships at sea are governed by international law. The United Nations (UN) agency in charge of the maritime domain is the IMO [16]. Ships are only permitted to operate in international waters if they comply with international law. The objective of the IMO is to create a level playing field, i.e. no favourable treatment. Given that the goal of an autonomous system is to replace or supplement a vessel's navigating crew, it is crucial to note that IMO regulations rely on and utilise the framework of professional seafarers [18]. Conformity with the United Nations Convention of Law of the Sea (UNCLOS) and IMO conventions is ensured by the framework, which represents the vessel owner and the flag state. The certification of equipment, materials, and ultimately the final vessel is a collaborative effort between the flag state and a recognised class society, i.e., an International Association of Classification Societies (IACS) member [19]. In accordance with the IMO's principle of non-discrimination, proof must be provided that the autonomous system provides the same level of safety, security, and environmental protection as a conventional manned vessel. Combined with the current rules and regulations, the lack of standardised vessel "models" poses significant validation and certification challenges. During sea trials, each ship is formally approved. The majority of products and solutions applied to vessels are currently certified and approved under a regime of prescriptive rules and procedures, i.e. performance and test standards, despite the changing risk perception. Almost all test standards arose from a hardware-centric perspective, i.e., expose, observe, measure, and document. The autonomous and non-autonomous vessels will coexist, so it is crucial that the autonomous system be designed and implemented in accordance with and with the approval of the regulatory regime. As a consequence of the development of autonomous systems, IMO has published guidelines for conducting trials [1]. At the MSC 105 in April 2022, IMO agreed to develop a non-mandatory goal-based MASS [3], [4] framework as an interim measure. The degrees of autonomy are likely to be defined not to address ship-wide definitions of autonomy but cover specific functions and systems of the ship. The various mode of operation or conditions, e.g., normal operations, emergency operations, or maintenance, will impact when the degree of autonomy can be engaged.

IV. System Engineering Framework

The system view provided by a systems engineering process approach is crucial for achieving the system safety required by an autonomous vessel operating in unrestricted areas, i.e., conforming to rules and regulations [20]. There are several steps involved in the systems engineering process. Defining the system's objectives and the criteria to rank alternative designs, including safety objectives and design constraints, is the starting point and provides the evaluation criteria. Despite the fact that the depicted process is greatly simplified and iterative in practise, it illustrates the engineering process used to develop the GreenHopper.

When implementing MASS, it is generally acknowledged that a goal- and risk-based assessment will be required [5], [21]. The associated risk can be divided into four categories, the first two of which are beyond the scope of this paper.

- The liability risk when the humans are 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 the integration of the onboard & Ship-Shore systems.
- The risk associated with the electronic solutions and the design & reliability thereof.

Approximately two-thirds of all incidents involving ships have been attributed to human error, according to incident reports [22]. Efforts have been made to address the problem, with system integration being one of the most important factors. By adopting a higher level of Information and Communications Technology (ICT), a shift in the sources of risk is observed, i.e. the design and software development & implementation are becoming major areas of concern [5], [11], [10], [12]. However, many of these accidents could be more accurately attributed to the working conditions of the crew, their situational awareness, and their interaction with the system. It is indicative of a deeper problem within the system. Predictability, transparency, and intuitive responses are essential system design elements. Minimising the risk

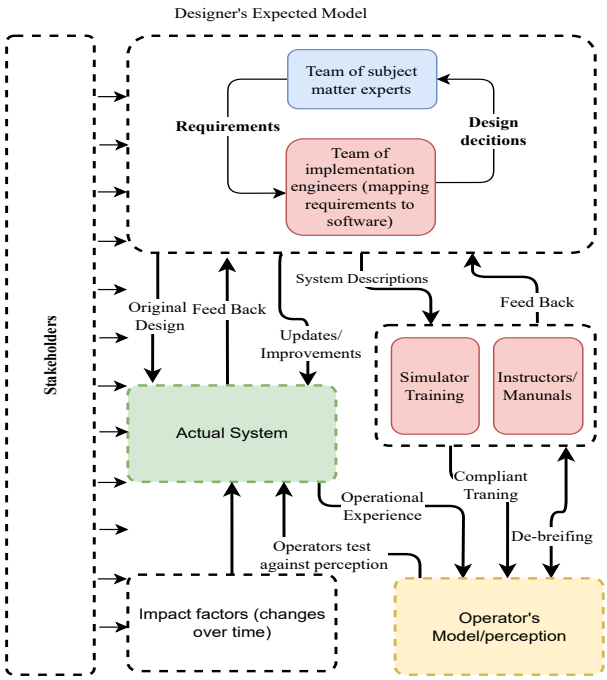

Fig. 2. Stakeholder System Perception and Relations

associated with human-automation system interactions is a challenging task. Section V discusses the functional mapping onto a control hierarchy [23] and utilising the Seafarers Training Certification and Watch-keeping (STCW) principles, see [18]. Fig. 2 illustrates some of the impacting factors that cause the operator's lack of predictability, transparency, and intuitive responses in critical situations, i.e., the alternation from the domain expert to the operator.

Evaluation of hazards and risks are essential elements in a safety assessment. A hazard is *"A condition with a potential for human injury, damage to property, damage to the environment or some combination of these"*, and risk is defined as *"The likelihood of a specified undesired event occurring within a specified period or in specified circumstances (frequency or probability)"* [24]. The limitations of probabilistic consequence are that, although the approach simplifies that mathematics, it struggles with the fundamental lack of imperial data on the likelihood and impact. A definition of operation and system structure forms the basis for hazard and risk assessment [20]. One of the essential parts of dealing with risks is to set up a structure and interface standards for the systems that are generally accepted. This gives a framework for where the different sub-functions belong, in terms of a control hierarchy, and makes sure that the systems can communicate, i.e. by locating the functions and aggregating the information [23].

Decomposition and modularity have proved to be effective ways of accommodating abstraction, automated testing and certification. In [25], [26], it is highlighted that bad design and/or high complexity are more likely to cause problems or breakdowns than faulty hardware. In addition to lowering cognitive challenges, a rigorous modular architecture facilitates the frequently incremental certification procedure. It enables the required test strategy of module and regression tests and the development of an automated consistency and interoperability verification tool that can evaluate the vessel-specific configuration before actual integration.

A reference model can be used to solve various problems; in the case of GreenHopper, a reference model also served to improve communication between partners.

V. Autonomy Enabling Sub-Systems

The design decision to separate the control of the vessel's movement from the autonomy function facilitates regulatory assessment by enabling differentiation between characteristics that are fundamentally similar to those of a traditional ship and those that are significantly different. Consequently, the method of defining the path to follow [27] and the performance & test criteria for control systems [28] were adopted from conventional IMO vessels to guide the distribution of functions between vessel control, virtual captain, and shore-side supervision. Fig. 3 illustrates the additional components required to support autonomous operation.

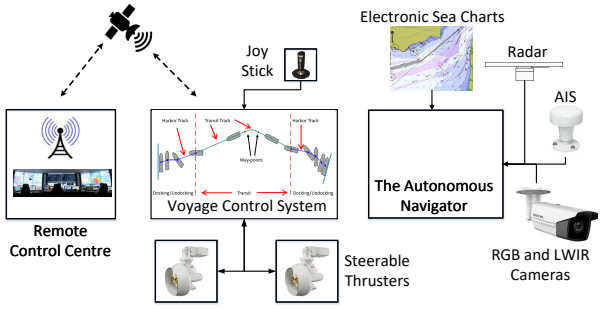

Fig. 3. Enabling components required to support autonomous operation.

The project placed a significant emphasis on proving the architecture, interface, and integration mechanism.

A. Architecture

In this paper, the term "architecture" is used to describe the structure of a vessel ICT, that is, a structure composed of entities, their properties, and their relationships. The selection, creation, and implementation of the proposed solutions are guided by a pragmatic combination of the following criteria:

- 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)

During this design phase, the primary system interfaces, the topology of the subsystem interfaces, and the functions and constraints, such as safety constraints, that guide the design of each subsystem are determined.

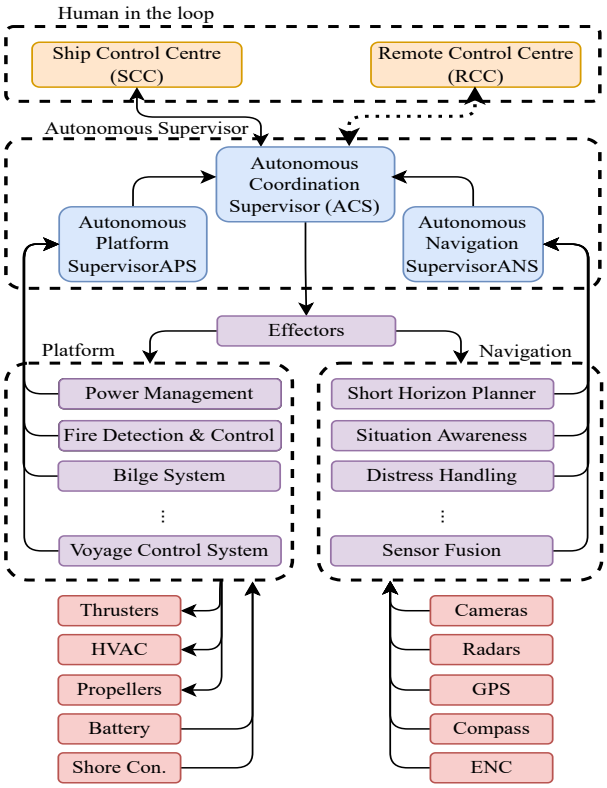

Fig. 4. Allocation of modules in the Control Hierarchy. A dotted line indicates outside vessel communication to the RCC

B. Functional boundaries

The interfaces define the system components' functional boundaries. Interfaces must improve visibility and control while also isolating components that can be implemented independently and to support delegation of authority and responsibility. Interfaces must support separate independent functions while facilitating system integration, testing, and operation. Therefore, safety is an important consideration when designing interfaces. The system interface analysis should include a safety analysis. Because interfaces are particularly vulnerable to design errors, simplicity is a primary goal of interface design. Properly designed interfaces help ensure that, analysed and tested prior to integration and that interface responsibility is clearly defined.

C. Onboard communication

Data harvesting required for operational optimisation has been driving the creation of ship-wide networks that provide the normalised data needed. Therefore, one of the fundamental requirements for designing and implementing a MASS system is to provide interoperability between domain-specific hardware and software platforms in a seamless, predictable and secure way. The topology of the A and B net in each segregated application area can be a ring, a star or a combination utilising managed switches.

D. The Transport Protocol

One of the primary design criteria for ICT systems for MASS is worst-case performance, as opposed to the more common average performance.

In the implementation of the GreenHopper project, a ring topology with automatic reconfiguration is used in the event of a cable failure. This redundancy feature is however supplemented by the application of an A- and B-segment in which the connection-oriented transport protocol monitors the communication quality between entities [29], [30]. During the initialisation phase, the system's integrity is validated by establishing a connection to the node and subscribing to all application topics. Using the flow of data and heartbeat messages, the connection is continuously monitored and confirmed. The required matching of information captured on different physical devices and for the chronological sorting of events, the Middle-Ware (MW) provides an accurate system-wide clock service. All nodes in the system can become the clock master. Absolute time is not required; however, the node connected to an external clock system is the default master. The service that synchronises the local operating system clock and the immediate acknowledgement is as illustrated in Fig 5 part of the transport layers Protocol Data Unit (PDU) parser to secure the required accuracy without significant overhead. The updates of topics are event-driven, i.e. if there is no change in value, then no updates are being communicated. It is prohibited for a node that comes online to time-stamp a piece of information and share it as long as the node has not been time synchronised.

E. Security Policies

Cybersecurity must be integrated into the design process alongside quality and testing, as opposed to being "bolted on" later. Standard services, such as e-mail and file transfer, are frequently the root cause of cybersecurity issues. To mitigate this, the use of external communication services provided by the operating system on the node is prohibited, and all ports below 49,152 are closed.

F. Integration Service Extensions

The onboard equipment can be considered a system of systems from different vendors. The individual systems are optimised 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 [31]. Furthermore, subscription-based exchange of information

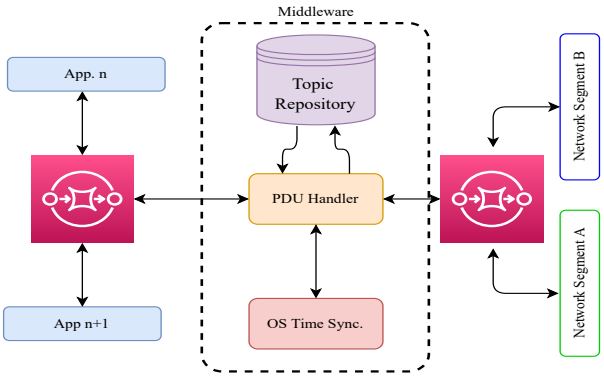

Fig. 5. Network node structure

combined with a symmetric client-server architecture facilitates service access from multiple sources.

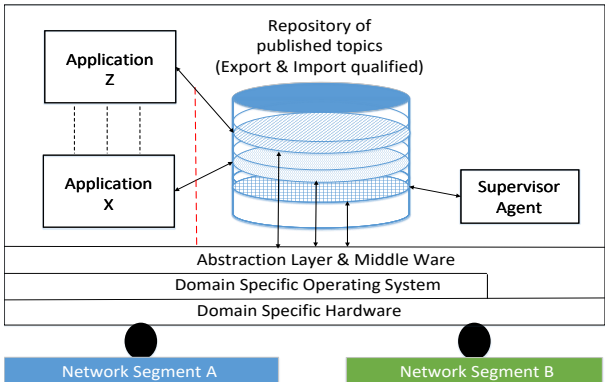

Fig. 6. Elements of a node

A publish-subscribe communication protocol is used to pass messages between modules. Each module is located on one or several physical nodes in the system, where each node contains an instance of the MW [29], [30], which primary task is to enable and ensure secure communication between modules. Fig. 6 shows an example of such a node. In addition, each node system holds a local data repository, which contains a local copy of all the data either sent from or received by the modules running on the node. 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 module instance is placed on different physical nodes and activated if no higher priority instance is running. Hence, this design enables redundancy at both the hardware and software levels. The supervisor agent is responsible for gathering the performance of the MW, the applications, and statistics & metrics used to monitor the health of the node and the hosted applications. In addition, the status of agents is collected, monitored and acted upon by the Autonomous Coordination Supervisor (ACS). Guarding the modules by strict entry control will isolate, channel, and simplify the application interaction and ease the integration process. A comprehensive assessment of existing frameworks like ZeroMQ, RabbitMQ and ROS revealed a high level of complexity and dependency on a central message exchange service. Therefore, this approach does not meet our system criteria for an effective and robust integration framework.

A rigid policy for joining the networked autonomy system is supported by features 10, 12, and 13, reducing the surface of the attack. Asset mobility [32] has been addressed by features 4 and 15, enabling floating hosting of services, while features 2, 3, and 5 address the more general cyber-related risks. In addition, features 7, 8, 9, and 14 support system integrity, and features 1, 6, and 11 support the applications.

G. Autonomy Enabling Modules

The autonomy system employs the *Voyage Control System*, which provides closed-loop control and distributes forces among the vessel's actuators. Moreover, the Voyage Control System (VCS) automates the execution of an optimised vessel trajectory, as defined by the planned path and speed.

TABLE I
KEY FEATURES - SYSTEM INTEGRITY AND CYBER RESILIENCE

Feature	Middleware Key Features
1	Worst-case performance design.
2	No "master" component.
3	Segmentation.
4	Redundancy.
5	End–to–end message encryption.
6	System wide accurate time synchronisation (1 ms)
7	Connection oriented protocol
8	Immediate acknowledge
9	System integrity monitoring
10	Connection to external systems via white-list mapping
11	Network segment re-routing within 5ms
12	All standard service ports are close
13	Only entry via the Middle-Ware message parser
14	Manage the topic updates and flag in case of malfunction
15	Manage the active-running and hot application topic update

A series of way-points define a route to follow [27] connected by line segments, as shown in Fig. 7. When an evasive manoeuvre is required to reduce the risk of a collision, the autonomous system changes the way-points to follow. During periods of unattended bridge operation of the vessel, i.e., when the crew onboard the vessel is performing other duties, the shore-based crew of the *Remote Control Centre* will assume the responsibilities of the Watch Keeping Officer. A critical factor is the shared and sliding responsibility, as described in [33], which describes the mapping from STCW competence requirements to autonomy module functionality. The system engineering process must include the RCC and the autonomy system onboard the vessel, as illustrated in Fig. 2. The situational awareness requirements of RCC impose stringent reliability and capacity requirements on *External Connectivity*. In [34], typical external communication hazards are enumerated alongside design guidelines, typical capacity requirements, and anticipated latency.

The *Autonomous Navigator* is responsible for navigational safety during unattended bridge operations. The autonomous navigator verifies data from the Electronic Navigational Chart (ENC), Global Navigation Satellite Systems (GNSS), and Automatic Identification System (AIS) with object detection from a 360-degree camera setup (daylight and infrared), radar (X and W bands), and two lidars. The Autonomous Navigation Supervisor (ANS) module evaluates information regarding detected objects within a vessel's awareness zone. The objects detected by the ANS identify other ships, their expected course and speed, and potential threats. If the ANS detects a need for route modification, it will offer a

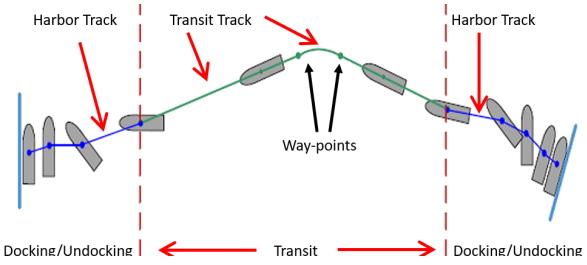

Fig. 7. The route to follow

rerouting suggestion to the ACS. Then, depending on the operational mode, the ACS will either instruct the VCS to follow the newly suggested route or forward the suggestions to a human proxy (onboard or RCC-based). The Sensor Fusion (SFU) uses radar, AIS and camera-based object detection to track objects. Situational awareness includes the sub-modules of comprehension and anticipation. The understanding module assigns semantic meaning to data to identify the present circumstance. The anticipation module forecasts the development of the present circumstance. The understanding sub-module evaluates data and determines the risk of collision based on the closest predicted distance between objects and compliance with Convention on the International Regulations for Preventing Collisions at Sea (COLREG). The ACS and Autonomous Platform Supervisor (APS) supervisor modules provide the ship-wide coordinator with the information required for a ship-wide assessment. If an evasive manoeuvre is necessary, the Short Horizon Planner (SHP) will suggest up to three alternative routes. The ACS arbitrates between the alternatives and, in autonomous mode, will initiate activation of a new route within the COLREG boundaries or notify the human proxy otherwise.

VI. Conclusions

This article addressed safety, resilience, and cyber security as inherent components of the design and implementation of autonomous systems for surface marine vessels. Development of autonomy for the strictly regulated marine area was discussed, and architecture that could meet the requirements of this field was suggested. An architecture was presented that facilitates the safety and dependability requirements of maritime autonomy: the ability to integrate subsystems from different vendors and system-level testability. The autonomy system developed for an autonomous harbour bus, which is currently undergoing factory acceptance testing and will be commissioned and demonstrated in the fall of 2022, exemplifies the concepts.

References

[1] IMO, "Interim Guidelines For MASS Trials," IMO, Tech. Rep. MSC.1/Circ.1604, 2019.

[2] DNV-GL, "Autonomous and remotely operated ships," DNV-GL, Tech. Rep. CLASS GUIDELINE DNVGL-CG-0264, 2018.

[3] IMO, "Outcome of the Regulatory Scoping Exercise for the Use of Maritime Autonomous Surface Ships (MASS)," IMO, Tech. Rep. MSC.1/Circ.1638, 2021.

[4] Lloyd's Register of Shipping, "IMO Maritime Safety Committee One Hundred and Fifth session (MSC 105) Summary Report," Lloyd's Register of Shipping, Tech. Rep. MSC 105, 2022.

[5] J. V. Earthy and M. Lützhöft, "Autonomous ships, ICT and safety management," *Managing Maritime Safety*, pp. 141–165, 2018.

[6] Rolls-Royce, "Remote and Autonomous Ship – The next steps," Rolls-Royce, Tech. Rep., 2016.

[7] Rochelle Beighton - CNN, August 2021, world's first crewless, zero emissions cargo ship will set sail in Norway. [Online]. Available: https://edition.cnn.com/2021/08/25/world/yara-birkeland-norway-crewless-container-ship-spc-intl/index.html

[8] Wartsila, "Wartsila-tests-remote-control-vessel-from-8000-km-away," 2017. [Online]. Available: https://www.offshore-energy.biz/wartsila-tests-remote-control-vessel-from-8000-km-away/

[9] J. Earthy, B. S. Jones, and N. Bevan, "The improvement of human-centred processes - Facing the challenge and reaping the benefit of ISO 13407," *International Journal of Human Computer Studies*, vol. 55, no. 4, pp. 553–585, 2001.

[10] C. A. Thieme, "Risk Analysis and Modelling of Autonomous Marine Systems," Ph.D. dissertation, Norwegian University of Science and Technology, Trondheim, 2018.

[11] B. Rokseth, O. I. Haugen, and I. B. Utne, "Safety Verification for Autonomous Ships," *MATEC Web of Conferences*, vol. 273, p. 02002, 2019.

[12] S. Vander Maelen, M. Buker, B. Kramer, E. Bode, S. Gerwinn, G. Hake, and A. Hahn, "An Approach for Safety Assessment of Highly Automated Systems Applied to a Maritime Traffic Alert and Collision Avoidance System," *2019 4th International Conference on System Reliability and Safety, ICSRS 2019*, pp. 494–503, 2019.

[13] A. Chircop, "Testing International Legal Regimes : The Advent of Automated Commercial Vessels," *The German Yearbook of International Law*, pp. 1–34, 2018.

[14] M. Shiokari and S. Ota, "Considerations on the regulatory issues for realization of Maritime Autonomous Surface Ships," *Journal of Physics: Conference Series*, vol. 1357, no. 1, 2019.

[15] R. Veal and H. Ringbom, "Unmanned ships and the international regulatory framework," *Journal of International Maritime Law, 23 (2)*, vol. 23, no. 23, pp. 100–118, 2017. [Online]. Available: http://urn.nb.no/URN:NBN:no-64241

[16] UN, "United Nations Convention on the Law of the Sea," United Nations, Tech. Rep., 1982.

[17] IMO, "Guidelines for the Approval of alternatives and equivalents as provided for in various IMO instruments," IMO, Tech. Rep. MSC.1/Circ.1455, 2013.

[18] ——, "The Manila Amendments to STCW," IMO, Tech. Rep. STCW/CONF.2/34, 2010.

[19] J. V. Bjørn, S. Rolf, and L. S. Asun, "DNV GL–Maritime Remote-Controlled and Autonomous Ships," *DNV GL - Maritime*, p. 36, 2018. [Online]. Available: https://maritimecyprus.files.wordpress.com/2018/09/dnv_gl_autonomous_ships_2018-08.pdf

[20] Nancy G. Leveson, *Engineering a Safer World : Systems Thinking Applied To Safety*. The MIT Press, 2012.

[21] C. A. Thieme, A. Mosleh, I. B. Utne, and J. Hegde, "Incorporating software failure in risk analysis – Part 1: Software functional failure mode classification," *Reliability Engineering and System Safety*, vol. 197, no. January, p. 106803, 2020.

[22] EMSA, "Annual Overview of Marine Casualties and Incidents 2014," EMSA, Tech. Rep., 2019.

[23] M. Blanke, M. Staroswiecki, and N. E. Wu, "Concepts and Methods in Fault-tolerant Control," *American Control Conference*, vol. 4, no. June, p. 15, 2001.

[24] D. A. Jones, *Nomenclature for Hazard and Risk Assessment in the Process Industries, Institution of Chemical Engineers*, 2nd ed. The Institution of Chemical Engineers, 2003.

[25] M. Brinkmann and A. Hahn, "Testbed architecture for maritime cyber physical systems," *Proceedings - 2017 IEEE 15th International Conference on Industrial Informatics, INDIN 2017*, pp. 923–928, 2017.

[26] R. Obermaisser and B. Huber, "A multi-core platform for integrated modular avionics derived from a cross-domain embedded system architecture," *SAE Technical Papers*, 2009.

[27] IEC, "IEC 61162-1:2016 Maritime navigation and radio communication equipment and systems - Digital interfaces - Part 1: Single talkers and multiple listeners," IEC, Tech. Rep., 2016.

[28] ——, "IEC 62065:2014 Maritime navigation and radio communication equipment and systems – Track control systems – Operational and performance requirements, methods of testing and required test results," IEC, Tech. Rep., 2014.

[29] Peter Karstensen, Luc Pierre Etienne Christin and Kjeld Dittmann, "ShippingLab Software implementation of core infrastructure: Middleware Functional Specification," Technical University of Denmark, Tech. Rep. SL.WP02.01.05.01.063.001, 2022.

[30] ——, "ShippingLab Software implementation of core infrastructure: Protocol and Service Specification," Technical University of Denmark, Tech. Rep. SL.WP02.01.01.01.063.001, 2022.

[31] H. Kopetz, "A Conceptual Model for the Information Transfer in Systems-of-Systems," *Proceedings - IEEE 17th International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing, ISORC 2014*, pp. 17–24, 2014.

[32] NIST, "Developing Cyber-Resilient Systems:A Systems Security Engineering Approach," National Institute of Standards and Technology, Tech. Rep. 800-160, 2021.

[33] K. Dittmann, N. Hansen, D. Papageorgiou, S. Jensen, M. Lützen, and M. Blanke, "Autonomous surface vessel with remote human on the loop: System design for stcw compliance," *IFAC-PapersOnLine*, vol. 54, no. 16, pp. 224–231, 2021.

[34] BV, "Guidelines for Autonomous Shipping - Guidance Note NI 641 DT R01 E," Bureau Veritas, Tech. Rep. NI 641 DT R01 E, 2019.