Connect and Protect: Requirements for Maritime Autonomous Surface Ship in Urban Passenger Transportation

Ahmed Amro[1], Vasileios Gkioulos[1], and Sokratis Katsikas[1,2]

[1] Norwegian University of Science and Technology, Gjøvik, Norway
ahmed.amro@ntnu.no; sokratis.katsikas@ntnu.no; vasileios.gkioulos@ntnu.no
[2] Open University of Cyprus, Faculty of Pure and Applied Sciences, Nicosia, Cyprus
sokratis.katsikas@ouc.ac.cy

Abstract. Recent innovations in the smart city domain include new autonomous transportation solutions such as buses and cars, while Autonomous Passenger Ships (APS) are being considered for carrying passengers across urban waterways. APS integrate several interconnected systems and services that are required to communicate in a reliable manner to provide safe and secure real-time operations. In this paper, we discuss the APS context, stakeholders, regulations, standards and functions in order to identify communication and cybersecurity requirements towards designing a secure communication architecture suitable for APS.

Keywords: autonomous ship · communication system · communication security · cyber security

1 Introduction

According to the most recent report from the Norwegian Shipowners' Association, exactly half of the global shipping companies will implement autonomous ships by 2050, while Rolls-Royce aims to operate autonomous unmanned oceangoing ships by 2035 [25]. In this direction, the International Maritime Organization (IMO) started to address the regulatory scope for autonomous ships [8]. Norway is leading the autonomous shipping industry by opening several testing areas for the development of this technology, in addition to the production of Yara Birkland, the worlds first all-electric and autonomous cargo ship [27], and other projects aiming to operate autonomous passenger ferries in different locations [5,28]. Many other initiatives all around the globe are taking place towards the development of autonomous ships; for instance, in 2018, Rolls-Royce and a Finish ferry operator demonstrated the world's first fully autonomous ferry in Finland [26].

The Norwegian Forum for Autonomous Ships (NFAS) has provided definitions for autonomous ships, their context, and functions in [33]. A classification of autonomous maritime systems was suggested, depending on the operational area (underwater or surface), the control mode (remote control or autonomous) and the manning levels (from continuously manned to continuously unmanned).

This paper is targeting a specific autonomous maritime system which is the Maritime Autonomous Surface Ship (MASS) with a specific application for passenger transportation in urban waterways, to which we refer to as Autonomous Passenger Ship (APS). A comprehensive definition for a ship is suggested by NFAS: "a vessel with its own propulsion and steering system, which execute commercially useful transport of passengers or cargo and which is subject to a civilian regulatory framework". Consequently, an autonomous ship is defined as "a ship that has some level of automation and self governance". The typically expected operational mode of autonomous ships that is appropriate for APS is called “autoremote" and refers to a a ship operating in a fully autonomous mode with the ability for a human intervention in case of emergency to take over full control of the ship operations [19].

With the increased research in the maritime industry focused at autonomous ships, the technological improvements were directed toward benefiting the development of smart cities through the smart transportation domain. The city of Trondheim which was recently stamped by EU as smart city [10] has opened the Trondheim Fjord as the world's first testing area for autonomous ships [39]. The idea behind the development of a smart city includes suggesting solutions for improving the citizens quality of life [38]. In this direction, the city of Trondheim is considering the application of a new technology i.e the autonomous ferry (*Autoferry*) [1] through the Trondheim canal to improve residents' life as an alternative to a high-cost bridge [40]. In this paper we focus on this new type of autonomous ships that will be used for passenger transportation in urban waterways.

Operating an autonomous passenger ship in a highly congested area is challenging for many reasons. Such a ship is expected to require the development of new technologies, while maintaining security and safety for the surrounding environment, the ship itself, and its passengers. Designing a suitable communication architecture is a crucial factor for safe operations, since improper communications is considered a primary factor for maritime casualties [11]. Additionally, according to ship owners, the most significant challenges for the usage of unmanned ships are rules and regulations, in addition to competence, compatible ports and fairways, and cyber security [27]. Therefore, the APS' communication architecture should satisfy certain requirements, deriving from the applicable rules and regulations and should be compatible with the views of the stakeholders of the APS ecosystem. Accordingly, this paper aims to identify requirements for a secure communication system in the specific case of APS. To this end, we identify the APS's stakeholders and their views and goals; we analyze existing regulations, guidelines and standards governing the design and operation of autonomous vessels; and we consider the functionality that such vessels should have to be able to operate safely.

The remaining of the paper is organized as follows: In Section 2 we review relevant research works. In Section 3 we discuss the APS's context, stakeholders, functions, relevant regulations, standards and guidelines. In Section 4 we present the identified requirements for the APS secure communication architecture. Finally, in Section 5, we summarize our conclusions and we present directions for future work.

2 Related Work

Several studies targeted the design and development of autonomous vessels. A master thesis proposed a design for a small autonomous passenger ferry that aims to be used for transporting passengers across the Trondheim city canal [22]. Another work proposes a technique for carrying out autonomous vessel steering tasks in coastal waters by implementing an agent system; each agent is deployed to perform specific tasks controlled by an agent platform installed on a computer on shore [24]. Neither of these works discussed communication or cybersecurity in their design proposals. Reliable communication capabilities are considered crucial toward the development of autonomous passenger vessels [22,24]. The literature is rich in various works targeting the communication architecture for autonomous ships, focusing on different operational areas, vessel types, and functional requirements. Furthermore, several navigation solutions known as e-navigation have been introduced by IMO in order to reduce human and traditional machine errors, and improve safety related to navigation on board ships, toward better protection for passengers, crew, maritime systems and the environment [30]. The e-navigation solutions targeted SOLAS (International Convention for the Safety of Life at Sea)-based ships, making them inapplicable to the APS. Nonetheless, a previous work discussed the integration of e-navigation solutions for non-SOLAS manned ships [12].

Moving toward autonomous ships, Maritime Unmanned Navigation through Intelligence in Networks (MUNIN) was a project that targeted the technical aspects in the operation of unmanned merchant vessels, and the assessment of their technical, economic and legal feasibility [31]. The project produced many deliverables, including the ship and communication architecture, remote bridge, autonomous engine room, and shore control center. The MUNIN project also produced a communication architecture for unmanned merchant ships, also suggesting communication and legal requirements to carry out unmanned operations in close to shore areas [32]. The MUNIN communication architecture is expected to influence the design and implementation of the communication architecture for the APS. Bureau Veritas, a member of the maritime classification society, published a document providing guidelines for suggested functions and components in autonomous ships [15]. The document aimed to provide guidelines for achieving the most essential functionality and improved reliability, being helpful in the process of studying related communication and cybersecurity requirements. The document also provided communication requirements for functionality and increased reliability. Although the document focused on satellite communications, which is not relevant for urban passenger transportation, the proposed considerations can be adjusted to radio frequencies in close to shore operations. Although the guidelines exclude ships smaller than 20m, we believe that the suggested guidelines related to communication are relevant for the APS. Additionally, DNV GL published several documents discussing aspects of autonomous ships. In their position paper they discussed the expected change in navigation, the regulatory scope, safety assurance, and social and ethical assurance [21]. Another related document from DNV GL is the class guidelines for autonomous and remotely operated ships [19]. In this document, DNV GL discussed several aspects including navigation functions, communication functions and cybersecurity considerations.

Several works discuss the lack of a regulatory framework that governs the operation of autonomous ships and suggests solutions to adapt to such technology. The Danish maritime authorities published a report on the regulatory barriers to the use of autonomous ships, suggesting suitable steps toward tackling these barriers, such as creating new laws for autonomous ships or amending existing ones [17]. Another work surveyed relevant regulations that might affect the operational capacity of autonomous ships [23]. The authors discussed regulations like SOLAS, COLREGS (International Regulations for Preventing Collisions at Sea), and others in detail, and pointed out that the regulations in their current form limit the deployment of autonomous ships. The work presented in [23] suggested generic communication requirements in order to satisfy certain regulations such as the availability of delay-free, reliable, fast and secure communication between the ship and control center.

3 The APS ecosystem

3.1 System Context

A general system context for the operation of a MASS as shown in Fig. 1 was suggested by NFAS. A brief description of the context components and their relevance to the APS is given below:

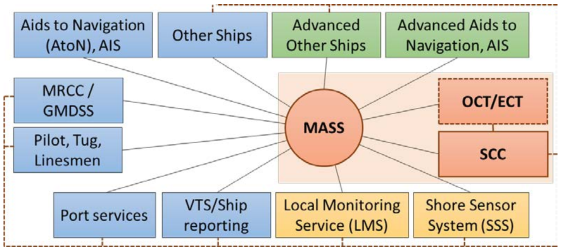
Aids to Navigation (AtoN), AIS
Other Ships
Advanced Other Ships
Advanced Aids to Navigation, AIS
MRCC / GMDSS
Pilot, Tug, Linesmen
MASS
OCT/ECT
SCC
Port services
VTS/Ship reporting
Local Monitoring Service (LMS)
Shore Sensor System (SSS)

Fig. 1. Context diagram for autonomous ship operation [33].

– **Remote Control Center(RCC)**: The implementation of such controlling entity is common across most works involving autonomous ships. Some refer to this entity as Shore Control Center (SCC), others as Remote Control Center

(RCC); herein we adopt the latter term. An RCC functions as an observer, by monitoring the APS status, but in some cases it might be forced to take control of the ship in order to avoid accidents. For this reason, it was concluded that certain manning requirements are important for the RCC to operate [36]. Additionally, a single or a chain of RCCs might be expected to serve several ships concurrently. The location of the RCC might be on shore or it can reside on-board another vessel (e.g. an escort vessel).

- **Emergency Control Team (ECT)**: a team which is expected to intervene in case of emergencies endangering the passengers or the surrounding environment. For instance, a passenger falling into water, or the ship not responding to remote commands and heading on a collision course.
- **Shore Sensor System (SSS)**: A collection of sensors are expected to be mounted on shore to aid some functions of the APS. For instance, ship automatic docking, charging, and other functions related to passenger embarking and disembarking.
- **VTS/RIS**: Ships are expected to establish contact with Vessel Traffic Services (VTS) for guidance and reporting. Moreover, the European Parliament has defined activities towards establishing harmonized River Information Services (RIS) for inland waterways to facilitate navigation [13].
- **Aids to Navigation (AtoN)**: Collection of systems expected to provide real-time information for the ship navigation system regarding weather, other ships, location awareness, etc. Examples of such systems are the Automatic Identification System (AIS), the Global Navigation Satellite System (GNSS), Radar, LIght Detection and Ranging (Lidar), etc.
- **Other Ships**: The APS is expected to communicate with other ships in the area for sharing navigational information using several agreed upon communication systems, such as Very high frequency (VHF), the more advanced VHF Data Exchange System (VDES) or AIS.
- **Port Services**: Some services, such as electric charging, maintenance, passenger embarking and disembarking, might be provided to the APS at the port or quay.

Other components in Fig.1, such as the Maritime Rescue Coordination Centre (MRCC), Global Maritime Distress and Safety System (GMDSS), and Service vessels (Pilot, tug, etc.) are less relevant to the case of the APS, due to the smaller size of its operational area.

3.2 APS Stakeholders

It is important for the development of the APS communication system to grasp an overview of all the system's stakeholders and understand their requirements. Several works discussed the stakeholders of autonomous ships; some focused on the regulator's perspective [17], whilst others provided an overview of all stakeholders from the shipping industry perspective [41]. In the context of APS, we identified seven categories of stakeholders, as shown in Fig. 2. Detailed descriptions of each stakeholder category, their interactions and their interest in the system are provided below:

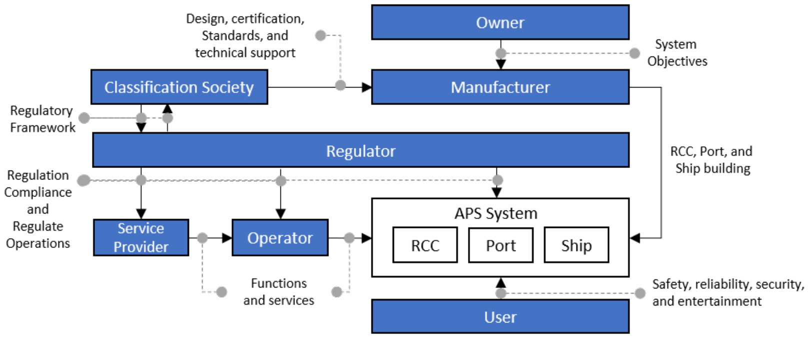

Fig. 2. APS stakeholders and their interactions

- **Owner**: The entire APS or parts of it might be owned by one or several entities. Usually, system owners dictate the objectives to be realized by the manufacturer.
- **Manufacturer**: All entities involved in the design and the implementation of APS, RCC, and port systems and facilities. Such entities are expected to follow standards and requirements related to functionality, reliability, safety, cybersecurity set by the classification society.
- **Classification Society**: Entities that contribute to the maritime domain, including through providing recommendations and suggesting relevant standards for ship manufacturers. The International Association of Classification Societies (IACS) consists of twelve members (including Bureau Veritas and DNV GL) that contribute to the classification design, construction, and rules and standards compliance for more than 90% of the world's ships. IACS is also recognized by IMO as the principal technical advisor [3].
- **Regulator**: A crucial component for the operation of APS is a relevant civilian legal framework. While such a framework does not exist at the time of writing this paper, its development is an ongoing task carried out by IMO [8], assisted by several other entities [19]. Additionally, the operations of APS are expected to be regulated through ship registration and instructions from several entities such as local maritime authorities and traffic regulators (VTS, RIS, etc.). Ensuring regulatory compliance is another task performed by some regulatory entities.
- **Operator**: All entities responsible for realizing the functions of the different components of the APS ecosystem; these are mainly the RCC, ship, and port. It must be noted that in some cases the system might be operated by its owner.
- **Service providers**: Supporting entities that provide additional functions and services for the system's operators. Services may include maintenance, connectivity, insurance, technical support, ship movement in and outside water, etc.

- **User**: Passengers constitute an important component of the APS ecosystem. Their safety and well being is the top priority when designing and operating the ship. Passengers expect such a ship to be safe, reliable, secure, and entertaining.

3.3 Regulations, Standards, and Guidelines

As mentioned earlier, the definition of a ship includes a regulatory framework that governs its operation, mainly to ensure safety, security and protection of the environment. Internationally, such responsibility falls upon the IMO, while regional or national regulatory entities are entitled to issue their own regulations within their jurisdiction [21]. Several international regulations need to be considered while moving forward toward autonomous ships. The identified international regulations and their applicability to APS is depicted in Table 1.

Table 1. International Regulations and Standards relevant to APS

Regulations

Title	Section/Chapter	Scope	APS Applicaple
SOLAS		International voyages	✗
	ISM		✗
	ISPS		✗
	GMDSS		✗
UNCLOS		Sea	✗
STCW			✗
MARPOL			✗
SAR			✗
COLREG		Sea Connected	✓*
Standards			
IEC 61162	1 (NMEA 0183)	Serial Communication	✓
	3 (NMEA 2000)		✓
	450	Ethernet	✓
	460	Ethernet and Security	✓
IEC 61850	90-4	LAN Engineering	✓
MSC.252	83	Integrated Navigation System	✓
IEC 62443	3-3	Security of Industrial Control Systems	✓
ISO/IEC 27000	27001	Information Security Management Systems	✓
	27002		✓
IEC 62940		Communication between on-board systems and external computer systems	✓

✓*: Require modifications

In the case of APS in urban transportation, the most related regulations are the Convention on the International Regulations for Preventing Collisions at Sea (COLREG) which applies to all vessels operating at sea or waterways connected to the sea and accessed by seagoing vessels [29]. This can apply to APS operating in rivers and canals linked to the sea. An important regulation that affects the core functionality of the autonomous vessels to operate safely at water is Rule 5 in COLREG. The rule basically requires that the ship shall maintain proper lookout by proper means to avoid collision [29]. Considering that 48.9% of 1522 reported maritime accidents in the Republic of Korea between 2013-2017 were related to improper lookout, [41] it is evidently crucial to address this issue in autonomous ships. Additional regulations concerning passenger vessels differ between regions and countries. The European Union enforces several regulations regarding the cybersecurity of ships and ports like the NIS directive (EU 2016/1148) and the General Data Protection Regulation (GDPR) for processing data of EU citizens, in addition to some other regulations that are related to ships in international voyages. In the Nordic region, each country specifies the passenger vessel types that require an operation certificate. Finland and Norway require all vessels of all sizes to acquire certificates, whilst in Sweden and Denmark certificates are required only for vessels carrying more than 12 passengers. Additionally, all passenger vessels that require certificates must comply with the regulations set by the maritime administration in that country. In Norway, for instance, such administration is the Norwegian Maritime Authorities (NMA) [4].IACS [2,6,7], DNV GL [19], and Bureau Veritas [15], the most referenced standards that are suggested to be followed are also depicted in Table 1. Additionally, the most referenced guidelines to be considered in providing cybersecurity protections for autonomous ships come from the National Institute of Standards and Technology (the NIST Framework) [37], from IMO in resolution MSC.428(98) (MSC-FAL.1/Circ.3) [16], and from the French National Cybersecurity Agency (ANSSI) [14].

3.4 APS Functions

In order for the APS to operate safely, it must support functions that include navigation, machinery and passenger management, and communications. In this paper we focus on the communication functions and cybersecurity considerations for the APS to perform its intended functions, with an increased focus on navigation. DNV GL discussed the navigation functions that are expected of a vessel in autoremote operation [19]. These are listed below:

- **Voyage Management**: This function includes tasks such as the planning, updating, and recording of voyage data.
- **Condition Detection and Analysis**: This function includes tasks such as proper lookout and situational awareness (e.g determination of position)
- **Contingency Planning**: A critical safety feature that is expected of any APS is referred to as Minimum Risk Condition (MRC). MRC is a state with the lowest possible risk where the ship should be programmed to enter in case of abnormal situation during operations such as the loss of communication links [19]. MRC can also be referred to as fail-safe condition.
- **Safe Speed**: The human in control or in supervisory mode must receive sufficient information regarding the situational awareness to keep the ship's speed within regulated limits.
- **Maneuvering**: To enable maneuvering for collision avoidance or voyage route change, an effective two way communication to provide sufficient situational awareness for either the autonomous system or the RCC in control to make correct decisions.
- **Docking**: An effective two way communication with the docking stations on board and on the shore (e.g. SSS).
- **Alert Management**: An alerting functionality through a Central Alert Management system (CAM) is crucial to achieve safety.

To realize such functions, a combination of systems are expected to be integrated within the APS. These systems require a certain level of connectivity and cybersecurity protection, which should be provided by the communication functions and protected using cyber security controls.

4 Communication and Cybersecurity Requirements

Based on [15,19] and on our analysis of the APS ecosystem in Section 3, this section presents the extracted communication and cybersecurity requirements of the APS to perform its expected functions (cf section 3.4). These requirements derive from the perspective of each stakeholder (cf section 3.2), and their presentation is organized accordingly.

4.1 Requirements deriving from the regulators' perspective

At the time of writing this paper there exist no specific regulations that govern the operations of autonomous ships. Nevertheless, the main aim of the regulators of APS is to ensure safety, security and environmental protection. This implies that autonomous ships must achieve a level of safety and security that is at least equivalent to that of a traditional ship.

4.2 Requirements deriving from the Classification Society's perspective

Both DNV GL [19] and Bureau Veritas [15] have offered communication and cybersecurity requirements for autonomous ships to operate in compliance with the related regulations, especially COLREG and SOLAS. Bureau Veritas suggested requirements focusing on the functionality and reliability of autonomous ships, whereas DNV GL focused more on safety. An overarching requirement is that *An efficient and secure communication network should be implemented to enable communication between internal and external systems of the autonomous ship.*

In the sequel, we discuss in detail the requirements for (efficient) and (secure) communication in the APS case. Three main communication categories have been identified for the APS to perform its intended functions: 1. External communication including connection with the RCC and external systems and stakeholders; 2. internal communication between on-board ship components; and 3. communication with other vessels in the vicinity. This subsection discuss the communication requirements for each communication category in addition to general requirements that apply across all categories. Additionally, this subsection discusses cybersecurity requirements mapped to the relevant NIST framework function as suggested by Bureau Veritas [15]. Each requirement in this section is titled with a three level coding scheme. The first level is related to the domain (communication (C) or Cybersecurity (S)). The second level is related to the sub-domain. The communication sub-domains are external (X), internal

(N), with other ships (O) or general (G). The cybersecurity sub-domains are identification (I), protection (P), detection (D), response and recovery (R). The third level refers to the relative numbering of the requirement within its category.

Communication Requirements: This subsection discusses external and internal communication requirements, in addition to the communication with other ships and other general communication requirements.

– External Communication
  First, *a dedicated physical space must be allocated separately from the controlled vessel*, which can be on the shore or on-board another ship. The required level of reliability, availability, and security of the communication link will increase with increased control of the RCC over the APS, depending on the latter's autonomy level. Additional communication with off-ship systems is required. Examples of off-ship systems that are leveraged for operational purposes are SSS, AtoN, VTS and RIS communication (cf Section 3.1). Additionally, other systems may require access to the ship's systems, to provide services such as maintenance, processing insurance claims, etc. Communication with external stakeholders is expected by the APS either by automated systems on the vessel itself, or by the personnel on the RCC. The requirements for the aforementioned communication are discussed below:
  - **C-X-1**: *The link's minimum acceptable network latency and maximum required bandwidth should be calculated, documented and implemented.* MUNIN provided minimum accepted requirements of latency and bandwidth [34]. In total 4Mbps accumulated link is considered the minimum link bandwidth for ship to shore communication. The required bandwidth is expected to be larger in the case of APS due to the implementation of new technologies with high data requirements such as the lidar. For instance, the targeted lidar for implementation in the *Autoferry* project [1] requires local transfer rate between 9-20 Mbps. Although the amount of data to be transmitted to the RCC is expected to be much less, in case of an increased control of the RCC over the vessel, the full lidar data might be expected for transmission. Additionally, the accepted latency suggested by MUNIN ranges from 0.05 seconds for ship to ship communication up to 2.5 seconds for HD video.
  - **C-X-2**: *A dedicated, permanent and reliable link for emergency push buttons for passengers should exist.* Such button should be used to indicate passenger related emergency and is expected to initiate intervention of the available ECT (cf Section 3.1) in the area or to change the autonomy level to provide the RCC full control of the APS if appropriate.
  - **C-X-3**: *The link with the RCC should be fault-tolerant so that it operates at full capacity even in case of failure in a single component*
  - **C-X-4**: *Traffic in the link with the RCC should be prioritized according to a pre-defined prioritization policy to enable traffic with higher priority to be forwarded in case of reduced bandwidth.* DNV GL suggested a prioritization policy so that the traffic is prioritized in the following order, from highest to lowest priority: 1. Control messages for emergency (e.g. MRC activa-

tion); 2. commands for remote control of key vessel functions; 3. situational awareness data for remote control of key vessel functions; 4. supervision data; 5. maintenance data.

- **C-X-5**: *The operator should be able to seamlessly switch and distribute different vessel data between the different communication channels without a negative effect on the operations* e.g. situational awareness data on one channel, the rest on another.
- **C-X-6**: *Communication links should operate according to appropriate QoS requirements and adapt with signal degradation.* The QoS requirements are case dependent based on the implemented systems on board the APS. For instance, a rule could be established that delay sensitive systems (i.e. collision avoidance) should be carried through an appropriate communication channel that provides the lowest delay whereas delay tolerant systems (i.e. HD video) could be channeled through a communication channel with higher but still appropriate delay.
- **C-X-7**: *The network should integrate monitoring and notification systems for real-time or near real-time link quality analysis, based on data collection and aggregation subsystems which satisfy intrinsic and contextual Quality of Information requirements to support such real-time/near real-time situational awareness and incident response.* The notification functionality is expected to be integrated within the ship's CAM.
- **C-X-8**: *The operator should have independent troubleshooting capabilities over each one of the communication links.* Troubleshooting one link should not interrupt the operations of another.
- **C-X-9**: *Communication link with RCC should be established using redundant communication channels, including main and backup channels, preferably using different communication technologies and service providers.* The communication architecture presented by MUNIN was mainly focusing on deep sea operations. This entails the application of satellite communication for carrying ship to shore operations as a primary communication channel; this is different compared to inland or short sea shipping such as the APS, where high communication requirements are needed. In this case, mobile communication or Wi-Fi channels can be primarily used [35].

– Internal Communication
  - **C-N-1**: *The Communication network design should comply with the applicable requirements in the relevant standards.* (cf table 1)
  - **C-N-2**: *A Segregated network design should exist to avoid failure cascading.* DNV GL suggested a specific network arrangement that applies network segregation [19]. They suggested that the following systems should not be connected to the same network: 1. Navigation system; 2. Communication system; 3. Machinery control and monitoring system; 4. Safety systems; 5. Control systems that serve redundant vessel services; 6. Auxiliary systems not related to vessel key functions; 7. Other systems from different system suppliers. Suggested network segmentation methods include air-gap, VLAN, firewalls etc.

  - **C-N-3**: *A redundant network design should exist with automatic transition/activation/restoration between the main and backup system components.*
  - **C-N-4**: *It should be possible to divert connectivity to local resources upon loss of remote resources.* (e.g in case of distributed network or cloud services providing data storage, backup local storage for critical data are expected to be implemented)
  - **C-N-5**: *Connectivity to several systems on-board, such as passenger management system, alert system (CAM), log book, and local sensors should exist.* The passenger management system provides certain services to the passengers on-board such as voice communication, trip status, and internet-access. Local sensors may include weather sensors, positioning sensors and others.
  - **C-N-6**: *If several wireless communication links are expected to operate closely on-board with a risk of interference, a frequency coordination plan should be made and documented and then tested on board.*
- Communication with other vessels
  - **C-O-1**: *The APS should be able to communicate with other vessels. For such communication, line of sight (LOS) communication system mainly based on AIS or digital VHF with range of at least two kilometers should be used.* This communication includes position and route advertisement which is essential for safe navigation and collision avoidance.
- General Communication Requirements
  - **C-G-1**: *Important communicated data should be recorded and logged to be analyzed when needed.* DNV GL proposed the minimum data that is required to be recorded [19]: 1. The status of the vessel's key functions including the communication links; 2. Alerts; 3. Manual orders or commands; 4. All input and output data to or from the decision support and automation systems. In case the data is recorded on board, an early alert should be raised in case storage capacity exceeds a certain threshold and it should be possible for it to be transferred to shore.
  - **C-G-2**: *The network components and equipment should be type-approved in compliance with the related certification policy.* For technologies implemented in autonomous vessels to be certified by DNV GL, type approval is discussed in a specified class program for cybersecurity [20]. Type approval according to Bureau Veritas includes compliance with the IEC 61162 standards (all parts) and the MSC.252(83) performance standards.
  - **C-G-3**: *The transmission protocol in each link should comply with a relevant international standard*, for example, 802.11 or 802.15 series for wireless communication.
  - **C-G-4**: *Wireless data communication should employ an internationally recognized system with the following features:* 1. Message integrity including fault prevention, detection, diagnosis, and correction; 2. Device configuration and authentication by permitting the connection only for devices that are included in the system design; 3. Message encryption to maintain mes-

sage confidentiality; 4. Security management to protect network assets from unauthorized access.
- **C-G-5**: *A coverage-analysis of the different wireless communication systems must be performed in order to determine its effectiveness.* To this end, a wireless communication testbed that simulates or emulates the communication architecture of the APS can be leveraged.
- **C-G-6**: *All protocols and interfaces implemented in the communication links should be documented.*

Cybersecurity Requirements: This section discusses requirements for the cybersecurity of the APS communication system. A recognized framework should be applied to prevent or mitigate cybersecurity incidents, and in this paper we approach and discuss the identified cybersecurity requirements in the context of the NIST framework [37].

- Identification
  - **S-I-1**: *An up-to-date cybersecurity management framework should exist to govern the operations of cyber systems. It should include necessary policies, procedures and technical requirements.* According to the IMO resolution MSC.428(98), ship owners/operators must address cybersecurity risks in their management systems [16]. This can be achieved through an Integrated Ship Security and Safety Management System (IS3MS).
  - **S-I-2**: *A regularly updated map of the IT installations and the network architecture should be established with a list of the equipment specified by model number and software specified by software version number.*
  - **S-I-3**: *Network user accounts should be inventoried with the associated privileges, reflecting actual authorization.*
- Protection
  - **S-P-1**: *User access management should exist and support the best practices in secure authentication, avoidance of generic and anonymous accounts, secure password and password change policies.*
  - **S-P-2**: *Regular network software updates must be performed, according to an update policy that includes a list of components, responsibilities, means of obtaining and assessing updates, updates verification, and a recovery processes in case of failure.*
  - **S-P-3**: *The network should be protected using secure protocols*, e.g. encrypted transmission, and/or authentication as appropriate.
  - **S-P-4**: *Protection from malware should be implemented to prevent spreading between systems or network segments.*
  - **S-P-5**: *Any personnel who shall access the system should be trained on relevant cybersecurity policies.* It has been determined that a major cause of cybersecurity incidents is the lack of awareness [19].
  - **S-P-6**: *Software-based components should go through regular security analysis with suitable update policy.*
- Detect
  - **S-D-1**: *Monitoring capabilities should be put in place to detect abnormal events.* Abnormal events such as several log-in failures, or massive data

transfer. Monitoring capabilities might include Intrusion Prevention Systems, Firewalls, etc. Additionally, such monitoring capabilities should adapt to the existence of encrypted traffic through utilizing best practices such as SSL/TLS proxies and/or anomaly detection.

– Response and Recovery
  - **S-R-1**: *An incident response plan should be formulated, including the isolation of infected components and detailed reporting.* First action after the isolation of all infected machines from the network, for each detected incident a feedback should be documented, and lessons learned sessions should be arranged, to improve defensive measures for similar events in the future.
  - **S-R-2**: *Availability of backup facilities for essential information should be made available with a suitable backup plan.*

4.3 Requirements deriving from the Service Providers' perspective

Additional cybersecurity considerations should be given regarding the service providers, especially in the case of them being provided from an external party rather than the systems operators. A list of identified possible service providers categories and their related cybersecurity considerations is given below:

– **Ship Registry**: secure authentication controls should exist for ship certification and revocation of certificates.
– **IT Service Providers**: controls regarding authorization and access control should exist.
– **System installation**: controls to verify proper and secure systems installation according to a defined list of configuration parameters should exist.
– **Maintenance**: access to the system to provide software and/or hardware maintenance services should be controlled, monitored, and verified.
– **Financial services**: controls should exist to protect processes related to passengers payments.
– **Insurance services**: controls should exist to secure access or disclosure of certain data in case of accidents.

4.4 Requirements deriving from the Users' perspective

Essentially, passengers safety should be guaranteed by all means during trips. Communication solutions for passengers to communicate with the ship operators and vise versa should be made available. Additionally, certain regulations exist to protect passengers privacy, for instance in Europe, compliance with GDPR is expected and in Norway there exist regulations including Privacy Law and personal data act that are set forth by The Norwegian Data Protection Authority (Datatilsynet) [9] governing tracking (The use of WiFi, Bluetooth, beacons and intelligent video analytic.), video surveillance and anonymity [18]. So, passengers should be protected against tracking, and their information should be processed with privacy considerations.

5 Conclusion and Future Work

A special type of autonomous ships is the Autonomous Passenger Ship. APSs operating in urban waterways constitute a case of increased interest when it comes to the design and implementation of their communication system. In order to define communication and cybersecurity requirements in this case, we defined and analyzed the APS ecosystem in terms of context, stakeholders, regulations, standards, and functions. By leveraging this analysis, we extracted communication and cybersecurity requirements that need to be satisfied so as the APS may perform its required functions. This work is part of an ongoing project called *Autoferry* [1]. Our future work will design and implement a communication architecture and an IS3MS for the *Autoferry* as a use case of an APS system, according to the requirements defined in this paper.

References

1. Autonomous all-electric passenger ferries for urban water transport. =https://www.ntnu.edu/autoferry
2. Iacs rec 164 - communication and interfaces - new nov 2018. IACS
3. International association of classification societies. =http://www.iacs.org.uk/
4. Nordic boat standard. =https://www.sdir.no/en/guides/nordic-boat-standard/
5. Projects carried out by members of nfas. =http://bit.ly/NFASProjects
6. IACS rec 158 - physical security of onboard computer based system - new oct 2018. =http://www.iacs.org.uk/download/8782
7. IACS rec 159 - network security of onboard computer based systems - new sep 2018. =http://www.iacs.org.uk/download/8652
8. IMO takes first steps to address autonomous ships. =http://bit.ly/IMOAutonomous
9. Tracking in public spaces. =http://bit.ly/DatatilsynetTracking
10. Trondheim blir smartby. =http://bit.ly/Trondheimkommune
11. Focus on risks 2018. =http://bit.ly/sdirRisks2018 (Nov 2017)
12. An, K.: E-navigation services for non-solas ships. International Journal of e-Navigation and Maritime Economy **4**, 13–22 (2016)
13. Andrés, S., Piniella, F.: Aids to navigation systems on inland waterways as an element of competitiveness in ulcv traffic. International Journal for Traffic and Transport Engineering **7**(1) (2017)
14. ANSSI: Information systems defence and security: France's strategy (2011)
15. Bureau Veritas: Guidelines for autonomous shipping. http://bit.ly/BureauVeritas641NI2017 (2017)
16. Committee, T.M.S.: Maritime cyber risk management in safety management systems (2017)
17. Danish Maritime Authority: Analysis of regulatory barriers to the use of autonomous ships. Danish Maritime Authority," Final Report, December (2017)
18. Datatilsynet: The anonymisation of personal data. =http://bit.ly/DatatilsynetAnonymisation
19. DNV GL: Dnvgl-cg-0264: Autonomous and remotely operated ships (2018)
20. DNV GL: Dnvgl-cp-0231: Cyber security capabilities of control system components (2018)

21. DNV GL – Maritime: Remote-controlled and autonomous ships position paper (2018)
22. Havdal, G., Heggelund, C.T., Larssen, C.H.: Design of a Small Autonomous Passenger Ferry. Master's thesis, NTNU (2017)
23. Komianos, A.: The autonomous shipping era. operational, regulatory, and quality challenges. TransNav: International Journal on Marine Navigation and Safety of Sea Transportation **12** (2018)
24. Łebkowski, A.: Design of an autonomous transport system for coastal areas. TransNav: International Journal on Marine Navigation and Safety of Sea Transportation **12** (2018)
25. Levander, O., Marine, R.R.: Ship intelligence–a new era in shipping. In: The Royal Institution of Naval architects, Smart Ship Technology, Internation-al Conference proceedings. pp. 26–27 (2016)
26. MI News Network: Rolls-royce and finferries demonstrate world's first fully autonomous ferry. =http://bit.ly/marineinsightRollsRoyce (Dec 2018)
27. Norwegian Shipowners' Association: Maritime outlook 2018. Tech. rep., Norwegian Shipowners' Association (2018)
28. Olsen, S.: Autonom ferge ballstadlandet. =http://bit.ly/lofotenmatpark
29. Organization, I.M.: Convention on the international regulations for preventing collisions at sea, 1972 (colregs) (1972)
30. Patraiko, D.: The development of e-navigation. TransNav, International Journal on Marine Navigation and Safety od Sea Transportation **1**(3) (2007)
31. Porathe, T., Burmeister, H.C., Rødseth, Ø.J.: Maritime unmanned navigation through intelligence in networks: The munin project. In: 12th International Conference on Computer and IT Applications in the Maritime Industries, COMPIT'13, Cortona, 15-17 April 2013. pp. 177–183 (2013)
32. Rødseth, Ø., Burmeister, H.: Munin deliverable d10.1: Impact on short sea shipping. =http://www.unmanned-ship.org/munin/wp-content/uploads/2015/10/MUNIN-D10-1-Impact-on-Short-Sea-Shipping-MRTK-final.pdf (2015)
33. Rødseth, Ø., Nordahl, H.: Definitions for autonomous merchant ships. In: Norwegian Forum for Unmanned Ships (2017)
34. Rødseth, Ø.: Munin deliverable 4.3: Evaluation of ship to shore communication links. http://www.unmanned-ship.org/munin/wp-content/uploads/2014/02/d4-3-eval-ship-shore-v11.pdf (2012)
35. Rødseth, Ø.J., Kvamstad, B., Porathe, T., Burmeister, H.C.: Communication architecture for an unmanned merchant ship. In: OCEANS-Bergen, 2013 MTS/IEEE. pp. 1–9. IEEE (2013)
36. Rødseth, Ø.J., Tjora, Å.: A system architecture for an unmanned ship. In: Proceedings of the 13th International Conference on Computer and IT Applications in the Maritime Industries (COMPIT) (2014)
37. Sedgewick, A.: Framework for improving critical infrastructure cybersecurity, version 1.1. Tech. rep., National Institute of Standards and Technology (2019)
38. Sikora-Fernandez, D., Stawasz, D., et al.: The concept of smart city in the theory and practice of urban development management. Romanian Journal of Regional Science **10**(1), 86–99 (2016)
39. SINTEF: Test site opens for unmanned vessels. =http://bit.ly/sintefTestSites
40. Skille, A., Lorentzen, S.: Foreslår førerløs passasjerferge i trondheim. =http://bit.ly/nrkTrondheim
41. Yoon, I.: Technology assessment - autonomous ships (09 2018). https://doi.org/10.13140/RG.2.2.36778.88009