Communication Architecture for Autonomous Passenger Ship

Journal of Risk and Reliability (JRR)
XX(X):1–??

DOI: 10.1177/ToBeAssigned
www.sagepub.com/
SAGE

Ahmed Amro[1] and Vasileios Gkioulos[1] and Sokratis Katsikas[12]

Abstract
Novel innovations have been witnessed in the past few years in the field of technology for autonomous vehicles. These have been exploited in various applications in the maritime domain; one such application is the proposal to develop autonomous passenger ships (APS) or ferries for carrying passengers in urban waterways. Such technology requires the integration of several components to support the safe and secure operation of the ferries. In this paper, a communication architecture is proposed, that satisfies pre-established communication requirements and supports autonomous and remotely controlled functions of an APS. The architecture was designed using the Architecture Analysis and Design Language (AADL); this enabled an iterative design process to be followed and allows for future improvements. The proposed architecture is verified by showcasing the role of the different architectural components in addressing the requirements and in supporting the expected functions in a number of operational scenarios based on the expected operations of an APS use case called "Autoferry". Furthermore, the proposed architecture has been evaluated by demonstrating its ability to achieve the expected performance according to the requirements, in simulated experiments using the network simulator GNS3.

Keywords
Autonomous Passenger Ship, communication Architecture, Reliable Communication, Safe Navigation

1 Introduction

Schallmo et al. (1) provide a brief history and some of several existing definitions of digital transformation, summarizing that it as a process which aims at novel value creation, process optimization, enhancement of experience, and establishment of new foundational capabilities. In the maritime domain, as discussed by Heilig et al. (2), digital transformation found its first significant applications within port management and logistics. Soon after, the introduction of innovative Information and Communication Technologies (ICT) was also focused directly toward the ships, aiming to enhance how they are built, operated and maintained.

This process motivated research and innovation activities towards novel and sustainable maritime transport systems, promoting the development of remotely controlled, automated, and autonomous ships. Definitions and advancement towards their attainment can be found in Rødseth et al. (3). The Norwegian Forum for Autonomous Ships (NFAS) currently reports multiple active and completed projects (4) that aim to develop enabling technologies, and also complete platforms. One example of such is the Autonomous all-electric Passenger Ships (APS) for urban water transport (5), from which the work presented in this paper originates and is part of.

The challenges associated with developing an APS, including those specific to the interaction with the environment, and the navigation of the autonomous system, with the primary objective to maintain the safety and security of passengers, systems, and the surrounding environment were presented in an earlier study by Havdal et al. (6).

Multiple initiatives have focused on the development of E-Navigation, also coordinated through the International Maritime Organization (IMO) as described by Patraiko (7). E-Navigation has been defined by the International Association of Lighthouse Authorities (IALA) as "the harmonised collection, integration, exchange and presentation of maritime information aboard and ashore by electronic means to enhance berth-to-berth navigation and related services, safety and security at sea, and the protection of the marine environment" (8). Originally, E-navigation was suggested as an open sea navigation solution. However, as presented by Kwang (9), the examination of the IMO's e-navigation Strategy Implementation Plan (SIP) and of Korea's national SIP for e-navigation reveals that E-navigation services are essential also for inland navigation. Kwan (9) also argued that digital communication services such as Long-Term Evolution (LTE) and Automatic Identification System (AIS) are key enablers for the implementation of E-navigation services. This is also the case for APSs used for inland transportation of passengers.

Supporting E-navigation within the context of the APS raises various system-specific requirements, which have been extracted and analysed by the authors in earlier work

[1]Norwegian University of Science and Technology, Gjøvik, Norway
[2]Open University of Cyprus, Faculty of Pure and Applied Sciences, Nicosia, Cyprus

Corresponding author:
Ahmed Amro, Norwegian University of Science and Technology, Gjøvik, Norway
Email: ahmed.amro@ntnu.no

(10); therein, in addition to communication and security-related requirements, the system context, the involved stakeholders, and the relevant regulations, standards, and guidelines were discussed. The extracted requirements were proposed by the stakeholders with a focus on regulatory compliance, functionality, reliability and safety of autonomous ships. The work in (10) leads to the conclusion that ICT technologies implemented in contemporary ships are not sufficient for autonomous all-electric passenger ferries for urban water transport, given the operational conditions and requirements of the latter.

Accordingly, in this paper, a tailored Communication Architecture is proposed, that aims to satisfy the communication requirements established in (10), and to address the needs of the various stakeholders. The architecture is designed so as to include elements to allow the design and development of a complementary security architecture that will address the security requirements established in (10).

Using modeling and design languages is an observed approach in the literature on autonomous ships. For instance, Rødseth and Tjora (11) referred to the extensive use of Unified Modeling Language (UML) and scenario-based modeling in the MUNIN project to describe functionality. Additionally, the application of system modeling methods during the development of autonomous ship systems has been explored by Basnet et al. (12). Particularly, the authors explored both System Modelling Language (SysML) and Object Process Methodology (OPM) and argued that both methods were suitable to handle the system complexity and communication of system information. Moreover, the Architecture Analysis Design Language (AADL) (13), which can complement SysML, has been proposed for the analysis of critical systems due to its ability to combine information related to hardware, operating system, and code to implement functions. This allows AADL to be applied at advanced stages during the system development (14; 15). This specific capability deemed AADL as the most suitable in this work, especially to support the efforts during the development of the complementary security architecture. Therefore, the presented communication architecture is modeled using AADL for the description and analysis of the architecture in four abstraction layers, namely i) model, ii) service, iii) protocol and interface, iv) implementation. In the paper, the various components, along with their connections and dependencies, are presented, with details on selected aspects across the four abstraction layers. Furthermore, the architecture is conceptually verified against the requirements of (10), and a use case is presented in order to highlight further the functionalities of the various architectural components. Finally, the IP-based network of the architecture is evaluated using the GNS3 simulator, demonstrating capabilities such as increased availability of the internal and external network; and network segregation and traffic prioritization capability.

The remaining of the paper is structured as follows: In Section 2 related work and background information is given. The architecture development methodology is presented in Section 3. In Section 4, the Autoferry use case is described, so as to put the proposed communication architecture into an operational context. In Section 5, we present our proposal for the communication architecture. Section 6 discusses the verification of the proposed architecture against its design requirements, as well as its applicability to other use cases, including of a larger scale. Finally, Section 7 summarises our conclusions and outlines directions for future work.

2 Background

E-navigation entered the IMO's agenda officially in 2006, with initial work been aided by IALA due to their expertise in the areas of navigational aids and Vessel Traffic Services (VTS). IALA identified three primary objectives for E-navigation, namely the development and provisioning of infrastructure for transferring information onboard ships; between ships; and between ships and onshore stakeholders (7).

As regards autonomous merchant ships, Rødseth et al. (16) proposed four operational modes, namely i) autonomous execution, ii) autonomous control, iii) remote control, and iv) fail to safe. Autonomous execution is the routine operational mode where the ship follows a pre-established set of instructions, transitioning to autonomous control when independently resolving minor problems. Remote control by shore operators is required when occurring circumstances fall outside the predetermined operational envelope. Finally, the fail-to-safe mode is entered when the remote control is necessitated but can not be achieved. E-Navigation is essential across all operational modes and therefore adopted and expected to be supported by the communication architecture proposed in this paper.

Placing these modes in the context of the APS, continuous transmission of real-time telemetry to a Remote Control Center (RCC) is necessitated for remote monitoring during autonomous execution. In case of minor changes, such as changing route or speed for dynamic positioning relative to moving objects, the APS transitions to the autonomous control mode where it keeps performing autonomously but transmits supplementary situational awareness data to the RCC and can expect to receive minor control commands. In case of unresolved hazardous situations such as possibly unavoidable collisions, the APS must transmit data to the RCC for enhanced and complete situational awareness, also receiving real-time control commands from the RCC. Finally, in case of loss of communication with the RCC or if the passenger emergency push button (EPB) is pressed, the APS is expected to initiate an appropriate fail to safe procedure (F2S). Several F2S procedures are expected to be available in the operational envelope, such as calling the nearby Emergency Control Team (ECT) to approach the ship and take control of it, while maintaining a fixed position.

These operational modes can only be achieved using E-navigation services based on reliable communication, with low latency and sufficient bandwidth to accommodate the amount of data generated and transmitted by the sensors. In this direction, many communication architectures have been proposed in the literature for maritime operations including autonomous maritime vessels (16; 17; 18; 19; 20). A reference architecture for crewless merchant ships has been proposed by Rødseth et al. (16) as part of the Maritime Unmanned Navigation through Intelligence in Network (MUNIN) project (21). This architecture, shown in Fig 1 was based on explicit assumptions related to

redundancy, security, network segregation and multiple RCCs, where having redundant communication links is realized by providing a main, a backup, and a dedicated link for rendezvous with ECT. Moreover, this reference architecture suggested an autonomous ship controller (ASC) as an entity that performs the autonomous and remotely controlled operations, in addition to controlling the mapping between the available communication resources and the control mode of the ship.

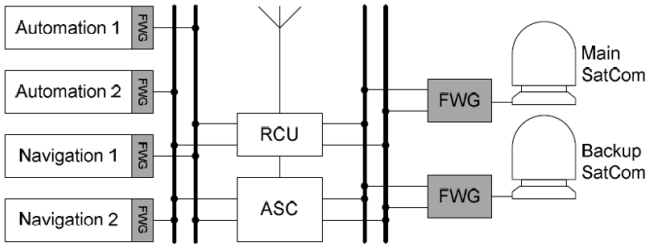


Figure 1. On board Reference Architecture (16)

Zolich et al (17) conducted a survey of communication and networks for autonomous marine systems, including autonomous vessels. The authors discussed the observed communication technologies and protocols used in different applications within the maritime domain. They highlighted that mobile communication technologies, as well as WiFi communication, are widely adopted in applications requiring large throughput and low latency.

In more recent works, Höyhtyä (18) aimed to address the challenges of navigating in port areas. Such areas are susceptible to accidents due to their increased traffic and limited manoeuvrability space, that raises the need for manoeuvres to be done accurately to avoid damaging the pier area; a similar challenge faces the operations of the APS. Höyhtyä argued that a reliable communication solution based on mobile communication technologies is needed to address this challenge. To this end, he proposed a high-level communication architecture consisting of satellite and terrestrial components for data transmission. Höyhtyä also suggested including in the architecture an intelligent entity called *connectivity manager*, which would be responsible for managing connectivity over multiple carriers, prioritizing traffic, cooperating with other ships, etc. Later, Höyhtyä (19) described an architecture of the connectivity manager as well as its functionalities, such as quality of service measurements, prioritization, and spectrum sharing. The connectivity manager component proposed by Höyhtyä (18) (19) is considered highly relevant to the case of APS communication, as it addresses a number of the requirements established in (10). Consequently, it has been adopted as a component of the architecture proposed herein.

Another communication architecture, utilizing LTE technology for maritime communications, was proposed by Jo and Shim (20). The authors argued that LTE can be reliably used to increase the range of ship-to-shore communication up to a range of 100 km. However, communication for autonomous operations was not the main focus of their work. Regarding LTE performance, some concerns have been raised by Mir and Filali (22). The authors performed an evaluation of LTE in comparison to IEEE 802.11p technology. They argued that LTE outperformed IEEE 802.11p in aspects such as reliability, scalability and mobility. However, LTE failed to satisfy delay requirements in networks with high traffic loads.

Stelzer and Jafarmadar (23) have proposed a multi-stage communication architecture for autonomous sailboats. The authors highlighted the benefits of using several technologies to employ in the boat-to-shore link for providing reliable and cost-effective monitoring and control capabilities. In the first stage, a WiFi connection was proposed and exhibited the best performance. In the second stage, GPRS and UMTS cellular connections were made available to increase coverage in a cost-effective manner. For the last stage, satellite communication was suggested and implemented using the Iridium satellite services.

The reference architecture proposed by Rødseth et al (16) was found to be the most relevant to our work since it addressed several of the communication requirements established in (10). This architecture constitutes a significant part of the current state of the art, but it lacks certain elements necessary in the context of the APS case. Differences in operational conditions as well as in functional and non-functional requirements between the APS case and the cases considered in (16) require notable enhancements and modifications, that were made to design the architecture proposed herein. Such enhancements and modifications of significant importance are the protocols and interfacing, the integrated communication technologies, and the provided services. Some other aspects, such as the concept of the connectivity manager, and the utilization of mobile communication technologies rather than satellite communication, were influenced by other works in the literature and have been adapted and integrated into the proposed architecture. The proposed architecture was also influenced by the network engineering and design principles introduced by Cisco Inc., which are related to Hierarchy, Modularity, Resilience and Flexibility. Defining a suitable network hierarchy is a critical factor. Computer networks usually comprise a three-tier hierarchical model consisting of access, distribution, and core. Furthermore, the core and the distribution tiers can be merged into a collapsed tier, which, as described by Papic (24) can reduce costs and complexity while also increasing redundancy. Additionally, having a modular design is beneficial due to the isolation it provides, and the ability to update or upgrade technologies seamlessly. The resilience principle refers to maintaining an operable status under normal and abnormal conditions, and one way of realizing it is through redundancy, by avoiding single points of failure. Lastly, due to continuous changes in technology, the network design should leave room for flexibility in the choice of technologies.

In our study, AADL and OSATE, an open-source tool that supports it (25), have been utilized for developing and modelling the proposed architecture. AADL is a language that enables early system's architecture analysis, providing a comprehensive set of notations for the description of system components, modes, properties, information flows and events (13). The developed model of the architecture describes all the entities in the APS context. Custom AADL properties were developed in order to

describe several aspects of the architecture, including communication properties of the connections between components, functional requirements, as well as security requirements. Having a model of the communication architecture in AADL enables its structured analysis, and the model is expected to be used in the future for performing threat and risk analyses. The model has been made accessible online [1].

Notes

1. APS communication architecture AADL model: https://github.com/ahmed-amro/APS-Communication_Architecture.git

3 Methodology

The architecture presented in this article is based on a stable and pre-specified set of requirements, aiming to field early initial operational capabilities concerning communications (main scope of this article) and security (only highlighted here). Accordingly, an adapted pre-specified multistep model of incremental and evolutionary development is utilized, as suggested in (26). The generic system life cycle model (27) has adapted ISO/IEC 15288:2015 (28) and ISO/IEC 24748-1:2010 (29) suggesting a series of steps for the specification, development, operation and retirement of systems. For the purposes of our study and the current Technology Readiness Level of the Autoferry project, this study is focused on the two initial stages, namely:

- **Concept definition:** "Developing the concept of operations and business case; determining the key stakeholders and their desired capabilities; negotiating the stakeholder requirements among the key stakeholders and selecting the system's non-developmental items (NDIs)" (27). These have been primarily addressed earlier at (10), and are further detailed here, in appendix B.
- **System Definition:** "Developing system architectures; defining and agreeing upon levels of system requirements...Performing system analysis in order to illustrate the compatibility and feasibility of the resulting system definition" (27). This is the main contribution of this article, namely presenting the development of the system architecture in section 5, and the initial system analysis in section 6.

The concept definition phase refers both to communications and security, in order to identify and reconcile conflicting objectives and requirements, while the first system definition phase is referring to communications, as presented in the remainder of the article, also carrying security implications given the common concept definition phase. The second system definition phase, focusing purely on security is outside the scope of this article and will be presented in future work. The main contributions and methods used for each phase can be further detailed as follows:

3.1 Concept definition

This topic has been primarily addressed in earlier work. In the current article, we expand upon this, focusing primarily on the pre-established requirements by defining:

1. their prioritization according to the MoSCoW method (Must have, Should have, Could have, Won't have)
2. their classification according to their nature:
    - Quantitative property: a requirement indicating a property that can be described with certain units of measurements, such as latency or bandwidth.
    - Qualitative property: a requirement indicating a property that can be observed but not measured, such as redundant design.
    - Support of capability: a requirement indicating the capacity to perform a certain activity, such as network troubleshooting.
    - Action (i.e. operational activity): a requirement indicating performing a certain activity, such as frequency coordination planing.
3. their corresponding verification criteria at the design and implementation levels, under the limitations with respect to metric quantification due to the phrasing of the requirements by external stakeholders;
4. the architectural components that provide the functions which satisfy the requirements;
5. the verification methods used for system analysis;
6. future work directions.

3.2 System Definition

3.2.1 Development of the system architecture: An overview of the system definition process is depicted in Figure 2. To define the architecture's functions and structure, we initially followed the Goal Tree Success Tree (GTST) functional decomposition framework proposed by Kim and Modarres (30). The functional hierarchy described by the GTST includes a Goal Tree (GT) and a Success Tree (ST). In the GT, three basic levels can be formulated: the goal or functional objectives, functions, and sub-functions. In the ST, the system structure is formulated as a collection of subsystems utilized to realize the functions identified in the GT.

Firstly, in the GT, the goal functions with relevance to the needed communication architecture have been established in our previous work from the views of the different stakeholders (10)—namely, safe and secure navigation as well as reliable and secure communication. Then, the goal functions are decomposed to functions and sub-functions assuring that the goal functions are achieved. The functions can be described in several ways, such as main and supporting functions. The main functions can be derived from the goal functions, and the supporting functions can be suggested toward the fulfillment of the goal functions. Furthermore, the functions can be decomposed into further sub-functions (more details in Section 4).

Secondly, in the ST, the identification of system structure was influenced by different works in the literature each proposing some design artifacts that deemed relevant to the needed communication architecture. Additionally, joint work with the other project members in the Autoferry project (5) provided guidelines for the proposition of the navigation and machinery systems as well as the emergency modules. The resulted GTST is presented in Figure 3. Then, the interactions of the system functions and the component distribution over the operational context were specified

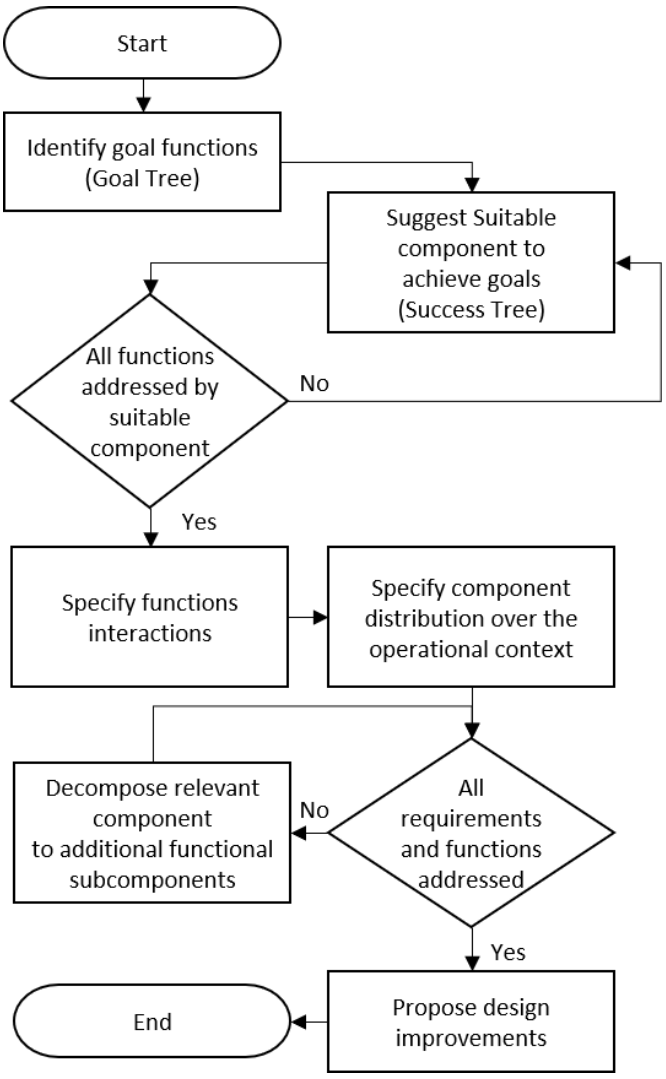


Figure 2. The system definition process

according to the expected operational modes specified in the literature.

Afterward, AADL was utilized in the development of the architecture components by undergoing through several iterations of system decomposition to ensure the realization of the system functions as well as the fulfillment of the established requirements. Moreover, certain design decisions were carried to introduce design improvements related to flexibility, scalability ad expandability in a way that doesn't contradict with design requirements. The detailed description of this step is presented in Section 5.

3.2.2 System analysis: Such an analysis is performed not only in the system definition stage but at any stage across the life cycle that engineering or technical decisions are made. This allows for the quantitative and qualitative assessment of available architectural choices, and the affirmation of compliance with the elicited system requirements (31). In this article we focus on the effectiveness analysis of the proposed architecture, utilizing the use case described in section 4 to establish the operational context, and the scenarios presented in section 6 for the conceptual and experimental affirmation of the established requirement verification criteria. The assessment criteria, use case, and scenarios have been selected according to the anticipated context of use of the system and in accordance with the current Technology Readiness Level of the Autoferry project, which is currently in the early technology development stage. Where operational or technical assumptions have been made due to the current maturity state, these have been captured and documented across sections 5 and 6.

4 Use case

The Autoferry, (Fig 4), will be developed to transport passengers across the Trondheim city canal as an alternative to a high-cost bridge. The operational area of the autonomous ferry is shown in Fig 5a. The ferry goes in both directions across the canal and its route is approximately 110m long. The canal witnesses traffic of mostly small size boats and, occasionally, of kayaks. The ferry will be monitored and able to be controlled by a main RCC stationed at the NTNU campus in Trondheim, at an approximate distance of 1.9 km from the operational area of the ferry, as shown in Fig 5b. A 5G mobile communication infrastructure is being built in the operational area to support the operation of the Autoferry.

The autonomous ferry is expected to carry passengers (max 12 on each trip) from one side of the canal to the other. A number of E-navigation functions is expected to be needed to support different operational modes, similar to the ones proposed by Rødseth et al (16) and previously discussed in Sec 2. Moreover, the ferry is expected to communicate with other vessels in the area, and to offer the necessary traffic services to maintain safe navigation routes according to the requirements established in (10). Furthermore, the ferry will be all electric and is expected to integrate new technologies that are highly interconnected; this makes it susceptible to cyber attacks. Therefore, a communication architecture is needed to support the identified goal functions specified earlier, namely safe and secure navigation; and secure and reliable communication.

During the decomposition of the goal functions, the identification of the main, supporting and system functions and sub-functions for the first goal function was based on the relevant literature and influenced by the stakeholders' viewpoints. Specifically, the notion for the decomposition of navigation functions is influenced by the proposed operational modes by Rødseth et al. (16), functions proposed in the MUNIN project (33) as well as DNV.GL's proposed "autoremote" operational mode (34). For the second goal function, the identification of functions and sub-functions was based on the established communication requirements (10). Each function and sub-function was derived to address a certain requirement until all requirements are addressed.

A logical view of the functions and their interactions is shown in Fig 6. In this figure, "Engine Monitoring and Control" refers to the capabilities to monitor the engines status and control them, "Navigation" refers to the capabilities to receive navigation data, establish situational awareness and define safe routes. "Remote" refers to the capabilities being carried through RCC operators, "Autonomous" refers to the capabilities being carried by the APS itself, while "Emergency Remote" refers to the capabilities being carried by the ECT. "Passenger Safety" refers to the capabilities to initiate emergency signals

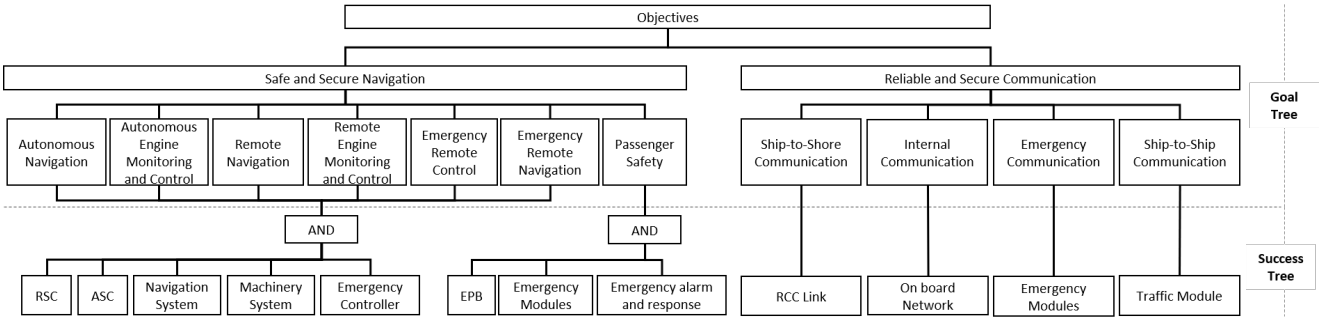
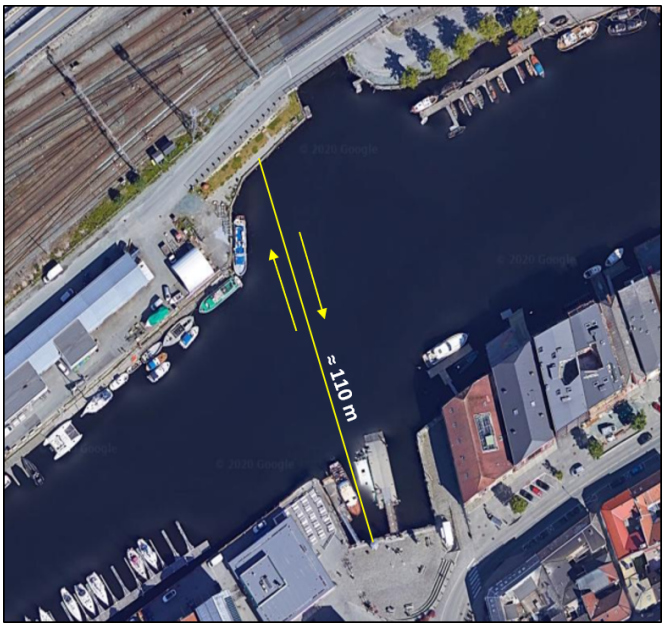


Figure 3. The GTST of the Communication Architecture

Figure 4. APS Use case: the autonomous ferry (Autoferry)



(a) Close view

(b) Wide view

Figure 5. APS Operational Area (Photos by Google Earth(32))

indicating safety-critical event related to passengers. The arrows indicate the direction of networked interactions between the different functions, but they do not capture the transitive interactions between the different functions at the service layer. The functions for safe and secure navigation rely on the communication functions and other supporting functions such as power, security, control and emergency response. Each supporting function is provided by a dedicated system or personnel. On the other hand, the functions for reliable and secure communication enable the navigation functions as well as other functions necessary for network and system management (NSM). A detailed list of the functions that aim to provide safe and secure navigation as well as reliable and secure communication is shown in Table 2 in Appendix A.

5 Communication Architecture

As outlined by Large et al. (35), communication architectures describe both logical and physical interconnections of all the identified elements in an ecosystem from the signal generation to its termination. In this section, the proposed communication architecture is presented, describing the ecosystem of a generic APS, the constituent systems and their subsystems. The architecture is modelled using AADL (13), thus enabling an extended analysis on one hand, and design modifications in the future on the other. In this paper, the modelling and analysis are presented at the

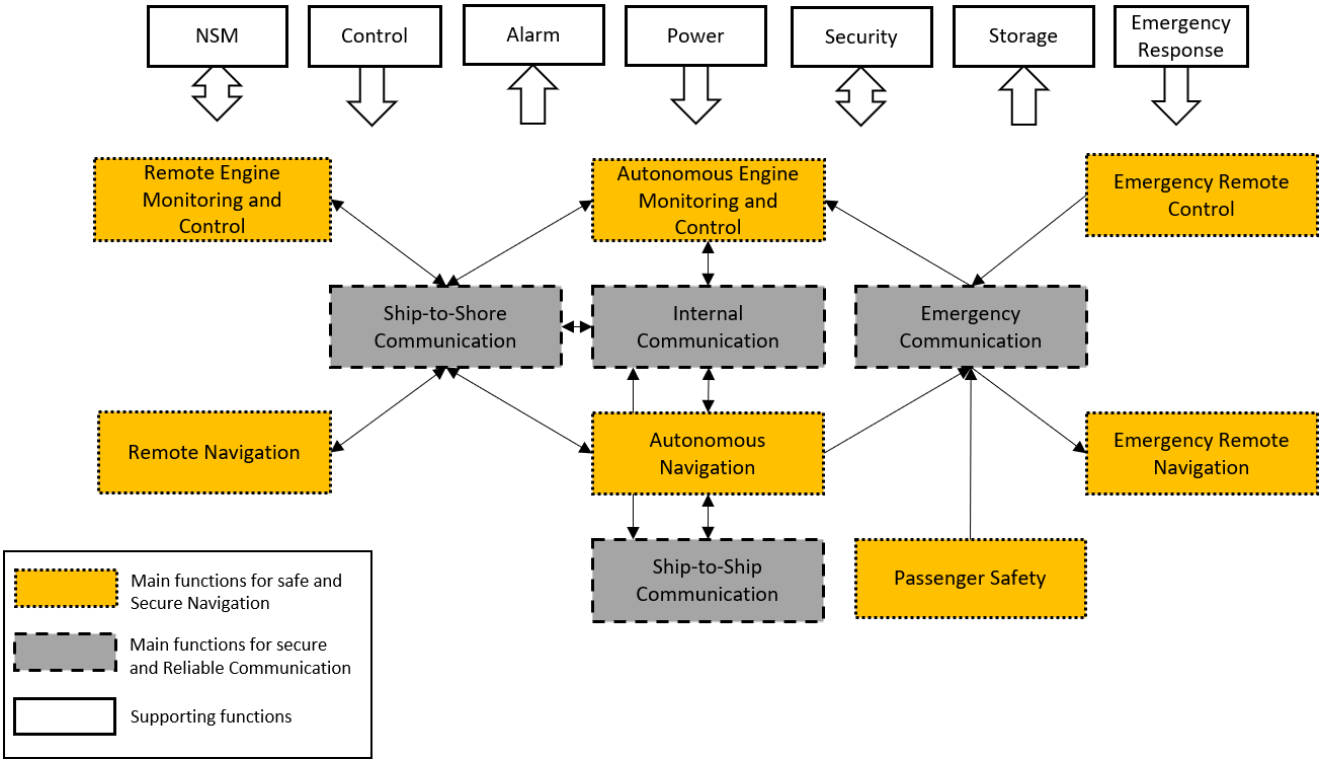


Figure 6. Logical view of the Autoferry functions and their interactions

level of system components, including their properties and interconnections.

5.1 Context View

Initially, the identified system structure reflected in the ST in Figure 3 was distributed across the APS context identified in (10). The distribution was based on the appropriate interactions across the different system functions, which are reflected in Figure 6. Moreover, additional context entities which were not discussed in (10) were suggested to provide design improvements towards realizing the system functions. Namely, mobile network, and Cloud Component (more details in section 5.6 and section 5.5 respectively). The outcome of this initial stage represents the highest level of abstraction with regards to the architecture components, reflected in Figure 7. This view aids the understanding of the various interacting entities in the APS context; explicit details related to each system are discussed in the following subsections.

5.2 APS

The APS itself is the central element of the communication architecture, as it is involved in all the main functions, with the remaining context components supporting its operation. In this section, four subcomponents of the APS onboard architecture are discussed, namely, the onboard network, the Autonomous Ship Controller (ASC), the navigation system, and the machinery system.

The onboard network is responsible for facilitating the different communication functions, while the ASC hosts the logic responsible for autonomous, remote and emergency navigation as well as engine monitoring and control functions, in addition to other system and network management components. Furthermore, the navigation system is the largest source of data to be traversing through the network and to be processed toward aiding the autonomous, remote and emergency navigation functions. Finally, the machinery system is responsible for supporting the movement ability of the APS and realizing the autonomous, remote, and emergency engine monitoring and control functions. Further discussion for the main sub-components as well as a brief discussion regarding additional expected systems is provided below.

The onboard network architecture presented in Fig 8 utilises two core/distribution tiers for high availability of communication functions, dividing the network into two main segments. The first segment provides ship-to-shore communication functions and limited internal communication functions. It connects the internal system components with the components on the RCC and components hosted on other entities in the context, using high-speed network access. The second segment provides more internal communication functions as well as emergency communication functions through connecting the internal APS systems and subsystems, in addition to integrating some low-speed connections from parts of the context (Aids to navigation, and ECT). Further description for each component in the network architecture is provided below.

5.2.1 The core/distribution tier : This component consists of two parts named A and B, for redundancy and to support network scalability as per the adopted network design principles (36). The main reason for having two parts for the core/distribution tier is to allow the ship network to operate both when communication with the RCC is possible and in the case of communication outage. While the

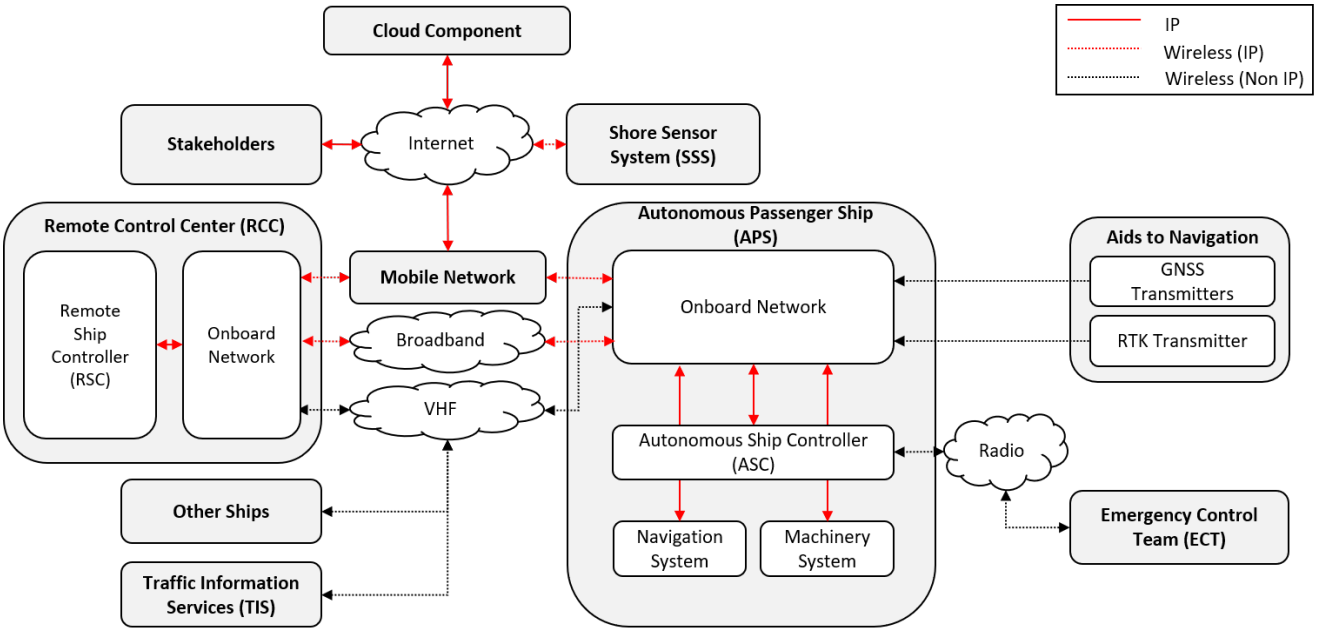


Figure 7. Overview of the APS Context

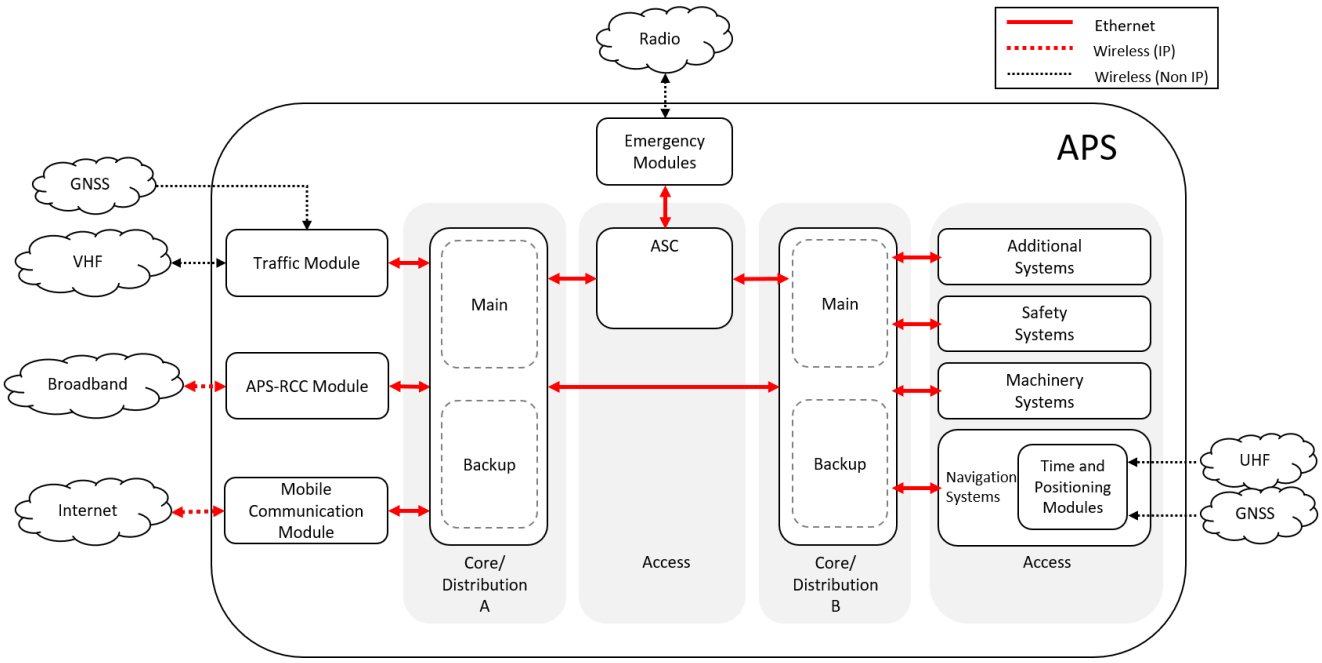


Figure 8. On board Network architecture

communication with the RCC is available, part A will handle the core/distribution related tasks while part B will primarily handle the distribution tasks to the internal networks. In case of loss of communication with the RCC or total failure of part A, part B will take responsibility for the core/distribution tasks, connecting the ASC with the internal networks. Two redundant units are proposed in each part. The units can utilise load sharing according to a load balancing policy, or one of them can be the main and the other stands as a backup. We propose the application of Layer 3 switches with load balancing and inter-VLAN (Virtual Local Area Network) routing capabilities to handle the core connectivity in addition to traffic distribution. This arrangement provides high availability of external and internal connectivity, in addition to satisfying pre-established requirements related to fault-tolerance, redundancy and capacity. Additionally, appropriate traffic distribution is governed by inter-VLAN routing to satisfy the requirements related to network segregation.

5.2.2 Gateways : A gateway in this architecture operates as a bridge between two networks. Accordingly, the proposed architecture includes several gateways to carry ship-to-shore, ship-to-ship and emergency communication as well as supporting navigation functions. The gateways are represented as modules in the architecture to comply with modular network design principles. Each module represents

a gateway for a communication link without restricting the technology to be used for its implementation.

- **Mobile Communication Module (MC Module)**: Provides connectivity to high-speed mobile networks for carrying ship-to-shore functions. 5G is a possible implementation option due to the expected larger bandwidth and lower latency. Additionally, as observed in the literature, LTE and 4G have been evaluated for E-navigation services and showed positive signs with some challenges related to latency. This module will provide the ferry with internet access in order to connect to the cloud component and the RCC.
- **APS-RCC Module**: To satisfy the requirement for redundancy of the link with the RCC, a backup module that provides direct connectivity to the RCC for carrying ship-to-shore communication functions is proposed. Broadband communication technology such as Wi-Fi, Mobile Communication, or the Maritime Radio Broadband (MRB) technology by Kongsberg (37) are considered for implementation of this module since they are internationally recognised wireless communication technologies which are indicated in the requirements. Wi-Fi is suggested if the RCC location is within proximity to the APS while mobile communication can be utilised when out of range of Wi-Fi. However, challenges related to latency are expected when using mobile communication.
- **Traffic Module**: This module aims to provide ship-to-ship communication functions, including communication with Traffic Information Services (TIS) such as the Vessel Traffic Service (VTS), or the River Information Service (RIS). In order to satisfy the ship-to-ship communication requirement, VDES, or AIS are considered for implementation in this module since they provide Line-of-Sight (LoS) communication, and they have been proposed by Kwan (9) as digital communication technologies needed to implement E-navigation services. The traffic module is expected to receive signals from the Global Navigation Satellite System (GNSS) for positioning and timing.
- **Emergency Modules**: Two modules are proposed for providing emergency communication functions. The first module is connected to ASC to provide emergency remote control and navigation functions over radio communication connected with the ECT. The second module, as desired in the requirements, provides a dedicated link over a mobile communication system (e.g. The Universal Mobile Telecommunications System (UMTS)) that allows the transmission of an emergency signal when a passenger onboard the APS press an emergency push button.
- **Time and Positioning Modules**: Two modules are leveraged for supporting the navigation system with positioning and timing data. The expected implementation technologies are GNSS and Real-time kinematic (RTK) receivers. The GNSS receiver provides positioning and timing data while the RTK receiver provides position correction data.

5.2.3 ASC : The Autonomous Ship Controller hosts the logic responsible for performing the functions related to autonomous, remote, and emergency navigation, engine monitoring and control. The proposed architecture of the ASC system includes a main and a backup system, each of which consists of several subsystems. This arrangement can utilise the server virtualization technology to simplify the management of such systems in addition to providing the required high availability. The proposed architecture for the ASC is shown in Fig 9 and is discussed in detail below:

- **ANS**: The Autonomous Navigation System (ANS) hosts the logic to carry the navigation functions in the different operational modes such as collision avoidance, situational awareness, and operational mode alteration. Additional features in the backup unit are the connectivity to the emergency control module to enable emergency remote control by the ECT in case of emergency and loss of ship-to-shore communication with the RCC. Additionally, the backup unit is expected to host the routines for the several Minimum Risk Conditions (MRC) that governs the APS operations under the Fail-to-safe operational mode.
- **AEMC**: The Autonomous Engine Monitoring and Control (AEMC) system hosts the logic for performing engine monitoring and control functions through retrieving engine data and forwarding commands to control the movement of the ship. Similar to the ANS backup unit, the AEMC backup unit is provided with connectivity to the emergency control module.
- **Network and System Management**: is a group of components that host required services. These components include User Access Management (UAM); Connectivity Management (more details below), the ship's Digital Logbook; and additional network and system management entities. Such entities include the Domain Controller; remote access (jump) servers; backup servers; and a system and network documentation repository. The digital logbook is expected to host recording and logging capabilities of important data, as indicated in the requirements.
- **Integrated Ship Safety and Security Management System (ISM3S)**: is a group of components that host services related to the safety and security of the ship and provide supportive safety and security functions. Possible components are Security Information Event Management (SIEM), primary Intrusion Detection and Prevention Systems (IDS/IPS), and the ship's Central Alarm Management (CAM) which hosts the systems responsible for safety-related alarms in compliance with the pertinent safety regulations.
- **Connectivity Manager** : The concept of a connectivity manager was proposed by Höyhtyä et al (18) as an intelligent entity responsible for ensuring the robustness of the ship's communications in any and all environments. Its application was proposed in satellite-terrestrial integration by Höyhtyä (19). We adopt the notion for the need of an intelligent network management entity in the APS ecosystem due to the increased autonomy, and we propose the APS Connectivity Manager as an autonomous network manager with functions aiming to reduce the need for human

network operators. The proposed Connectivity Manager will be hosted in the ASC network and is expected to provide the identified communication functions (see Appendix A) to satisfy a number of the communication requirements established in (10). Several components are proposed as part of the APS Connectivity Manager; these are discussed in the sequel:

- **Quality of Service Controller (CM-QoSC)**: This component is responsible for maintaining the required level of service quality. Other than managing the QoS rules through the establishment, enforcement, and management of rules, this module is responsible for enabling traffic prioritization and traffic re-direction. It handles the establishment of a prioritization policy, its communication to the appropriate network devices and any additional tasks related to traffic prioritization. Moreover, this component is responsible for managing the functionality for diverting communication paths within the network, depending on the available communication resources. This can be achieved by monitoring the status of the network links and updating routing and Inter-VLAN routing tables based on the connectivity state to direct traffic from the available sources to the available destinations. Additionally, this controller is responsible for managing the traffic load over the links, based on a pre-established load balancing rule or managed by the operator.
- **Network Monitor and Troubleshooter (CM-NMT)**: This component is responsible for collecting the relevant network-related logs, performance indicators, in addition to providing automatic network self-checking and to triggering network troubleshooting by the operator. The component is also responsible for generating, along with the CAM software, the appropriate alarms.
- **Network Software Updater (CM-NSU)**: This component is responsible for managing the retrieval, installation, verification of updates and recovery from them in case of failure.
- **Network Segmentation Manager (CM-NSM)**: One of the most critical aspects of the proposed architecture is the segregation by design for reliable and secure network operation. This component is responsible for managing the network segregation feature through the establishment and enforcement of the segregation policies, as well as validating their enforcement.
- **Network Security Coordinator (CM-NSC)**: The need for a dedicated entity for managing cybersecurity risks was established in (10) and is proposed in this paper, as is also the case with the IS3MS. The communication networks play an essential role in managing cyber-attacks, especially wireless networks. Accordingly, coordination between the connectivity manager and the IS3MS related to the communication of unexpected events and the enforcement of the various policies is expected.
- **Network Device Backup Controller (CM-NDBC)**: This component is responsible for retrieving and maintaining the backups of the network devices, in accordance with a backup policy. Additionally, it provides access to these backups for the other Connectivity Manager components, for example for CM-NI, CM-NSU and others, if needed.

We propose the development of the Connectivity Manager based on the FCAPS network management model (38) with appropriate adjustments, so as to take into account the autonomous operational environment.

5.2.4 Navigation Systems : As discussed earlier, the navigation system is a critical component of the APS that is responsible for collecting the required data for sensing the surroundings and enabling the APS to make informed decisions. No standardised navigation system has hitherto been proposed for the APS. The main design decisions related to the communication network is to avoid traffic congestion due to the transmitted data from the extensive amount of sensors (lidars, radars, video cameras, EO cameras) and to support scalability if the required amount of supporting components is to increase (e.g. more sensors). This could be achieved by applying two solutions. The first solution is to utilise Sensor Processing Units (SPU) to reduce the amount and frequency of transmitting sensor data. However, such a solution has been proven incapable of providing sufficient operational guarantee in case of faults (39), in addition to the expected increased latency that may hinder the control operation (40). The second solution is to connect the SPUs or to distribute sensors across multiple switches so that the traffic flowing to the switch stack in Core/Distribution B is distributed over multiple interfaces. Such an arrangement would add resilience to the navigation system by providing multiple access paths for the sensor data since even in the case that few SPUs or sensor switches failed, the remaining units will still be able to communicate some sensor data to the ASC.

The Global Navigation Satellite System (GNSS) and the inertial measurement unit (IMU) play a crucial role in the ship navigation system to provide accurate and timely positioning and timing data. At the same time, both components rely on external signals received through GNSS and RTK receivers, respectively. GNSS signals are susceptible to various attacks such as spoofing and jamming, and they require additional processing to ensure their security (41). A possible arrangement for the navigation system and its connectivity to the APS internal network is shown in Fig 10a: the navigation system transmits the sensor data as well as the GNSS processed information to the ANS, to aid the navigation functions.

5.2.5 Machinery Systems : Similar to the navigation systems, there is no standardized machinery system proposed for the APS. A possible arrangement of the machinery system and its connectivity to the APS internal network is depicted in Fig 10b. The Dynamic Positioning (DP) system

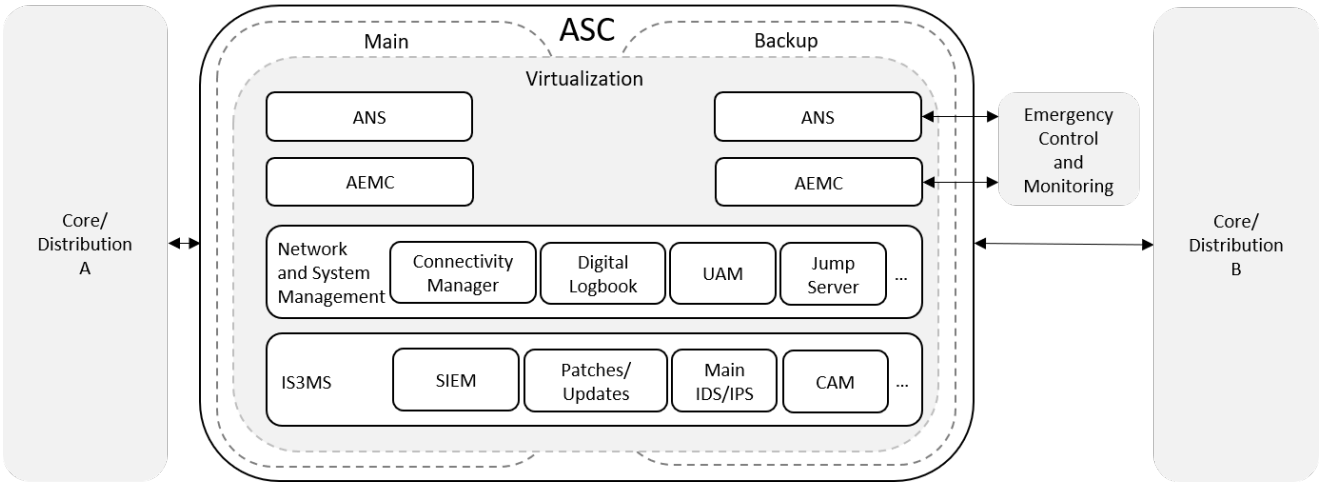
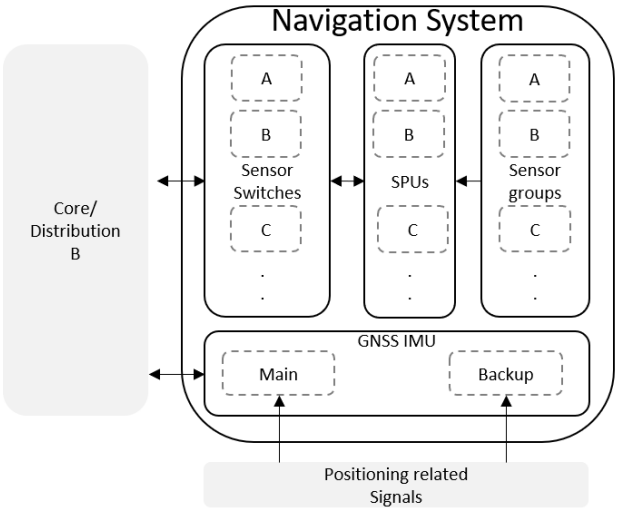
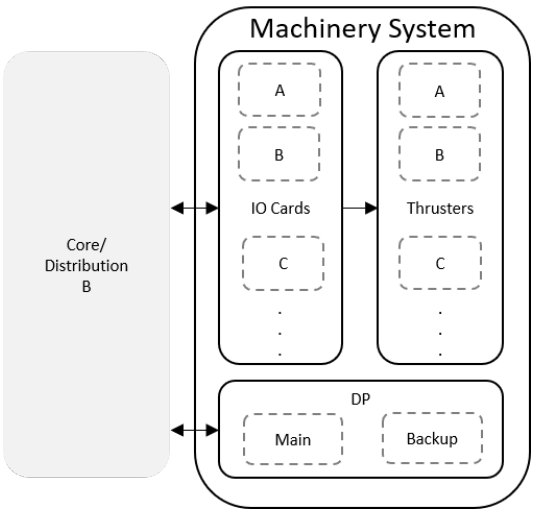


Figure 9. ASC architecture



(a) Navigation System



(b) Machinery System

Figure 10. Simplified Overview of the navigation and machinery systems

is responsible for maintaining the floating structure of the APS in a fixed position as well as on its established route by utilizing active thrusters. Furthermore, for functional redundancy, multiple thrusters are expected to be utilized and be connected to the core/distribution part B through Input/Output (IO) cards (42) which convert packet data (e.g. commands) coming from the control function (e.g. DP system), and send them to the thrusters to navigate the APS. The machinery system, together with the AEMC perform the engine monitoring and control functions through sending engine performance parameters and receiving route specification and control commands from the AEMC.

5.2.6 Additional APS Systems : Additional systems are expected to be attached to the APS internal network to provide supporting functions, as mentioned in Sec 4; these may include safety systems, power management systems, and passenger management and entertainment systems. Specifically, systems dedicated to providing safety functions for the APS and passengers include anchor drop, horn, alarm, lantern and user panel to control such systems manually. The systems are connected to the ship's network through General IO module, such as a PLC, while further security mechanisms are expected to monitor the commands going toward the machinery and safety systems to protect them from malicious attacks. By having the Core/Distribution part B separated from Core/Distribution part A, the network topology enables the network to be scalable and able to accommodate new systems in the future. Such systems can be added to the network by connecting a system's gateway or IO Card to the switch stack in Core/Distribution part B and having a dedicated VLAN created for them. Consequently, proper inter-VLAN routing is to take place to route the traffic to and from those systems appropriately.

5.3 RCC

In order to support remote navigation, as well as remote engine monitoring and control functions, it has been determined that a remote controlling entity located in a separate physical location is required. This entity can be hosted onshore or onboard another ship (10). In Fig 11, we propose a possible network architecture for the RCC

that is compatible with the previously proposed network architecture on board the APS. Further description for each component in the network architecture is provided below:

5.3.1 On board network : In this system, we propose a similar arrangement to the one discussed in Sec 5.2 for the Core/Distribution tier and gateways, with the exception that there is no need for two Core/Distribution parts, due to the anticipated small number of integrated systems on the RCC and the fact that the traffic module is only needed if the RCC is hosted onboard another ship.

5.3.2 RSC : The Remote Ship Control (RSC) consists of components responsible for carrying the remote functions in addition to managing the RCC and APS networks, systems and security. The proposed architecture of the RSC system as shown in Fig 12 consists of a main and a backup system, each of which consists of several subsystems. Similar to the ASC, this arrangement can also utilise the server virtualization technology, for the same reasons (refer to the discussion of the ASC architecture in 5.2). Another advantage for the application of server virtualization technology would be to facilitate the migration of RSC from one RCC to another. The systems and subsystems in the RSC and the ASC perform similar tasks. The Remote Navigation System (RNS) and Remote Engine Monitoring and Control (REMC) are expected to perform similar tasks to their equivalent autonomous systems ANS and AEMC, respectively. The main difference is that in the RNS and REMC, the analysis and control can be performed by an operator. Also, the Network and System Management and the IS3MS perform similar tasks, but with a focus on the RCC network, and they support the operations of their corresponding systems onboard the APS.

5.4 ECT

As described in Sec 5.2, there are two emergency-related modules onboard the APS that are utilised to establish emergency communication with the ECT. We propose a simplified architecture of the ECT, as shown in Fig 13a. The Emergency Alarm and Response system is responsible for performing the required tasks when the passenger emergency button on board the APS is pressed, while the emergency signal is received over a mobile communication link. A possible response action could be to raise a vocal and illuminated alarm so that the ECT notice an emergency and make their way toward the APS. The Emergency controller is a separate control system for managing the APS by a human operator through a LoS or short-range communication as suggested by MUNIN (21). In order to perform emergency navigation and engine monitoring and control functions, the emergency controller should be compatible with the backup ANS and AEMC (refer to the ASC architecture in Sec 5.2).

5.5 Cloud Component

Several cloud components such as the Maritime Connectivity Platform (MCP) (43), and DNV.GL's Veracity platform (44) have been utilised in maritime operations. In this work, we propose the utilization of such online applications to provide several functionalities. One goal for the application of a cloud component in the architecture proposed herein is to facilitate communication among the different APS stakeholders as described in (10); this can be accomplished through a dedicated portal for the APS ecosystem. An additional service could be utilised for the APS and RCC registration and binding in order to establish communication links between them. Additional services can be leveraged in the case of utilizing a cloud service such as online storage to backup the APS's and RCC's digital logbooks and other essential data. Furthermore, the application of a cloud component can facilitate the connection of additional context entities to the APS ecosystem without requiring changes in the proposed architecture. For instance, a Shore Sensor System (SSS) is expected to be implemented to aid the autonomous navigation functions, and a possible communication channel with the APS could be through a cloud service that pulls sensor data from the SSS and pushes this data or a processed version of these data to the APS through the APS MC module. Additional cloud services related to the connectivity manager and IS3MS could be utilised through the cloud component. A simplified architecture for the cloud component is shown in Fig 13b.

5.6 Mobile Network

The operational area of the APS in inland waterways enables the APS ecosystem to utilise the high-speed mobile communication infrastructure. As observed in the literature (Sec 2), many works have proposed, and some have evaluated the application of various mobile communication technologies in the maritime domain and for autonomous vehicles as well. 5G has yet to be evaluated in such applications, but it has been proposed by many. On the other hand, LTE and 4G technologies have shown promising results in previous communication architectures for traditional ship navigation. We propose the utilization of mobile communication technologies (see Fig 14); this satisfies the requirement for minimum bandwidth of 4 Mbps and maximum latency of 1 second for remote control and up to 2.5 seconds for HD video. To achieve flexibility in the architectural design, the mobile communication has been modelled as a forwarder of communication between the connected context entities, i.e. APS, RCC, SSS, and cloud component as well as a gateway to internet access. Thus, we pose no restriction on the communication technology to be employed (4G, LTE, or 5G), and we leave the implementation option to the technology that best satisfies the pertinent requirements. Nonetheless, it must be noted that an appropriate Service Level Agreement (SLA) of the ASP operator with the service provider of the mobile communication should be established, to maintain the required Quality of Service (QoS). We support the suggestion proposed by Höyhtyä et al (18) regarding the utilization of the mobile edge computing (MEC) technology supported by mobile communication infrastructures such as LTE, 4G and expected to be improved in 5G. The possible implementation of MEC in the APS architecture would move the suggested cloud component into the Mobile Communication infrastructure, which could drastically reduce the latency (see Fig 14).

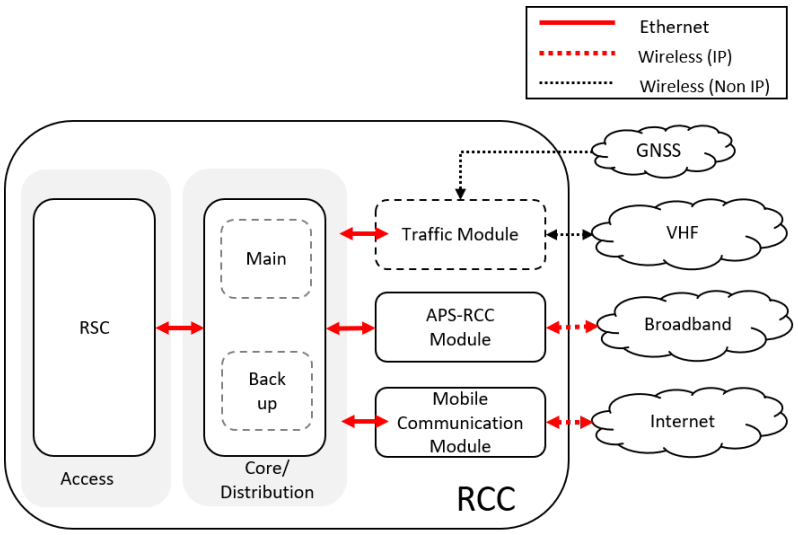


Figure 11. Remote Control Center Network Architecture

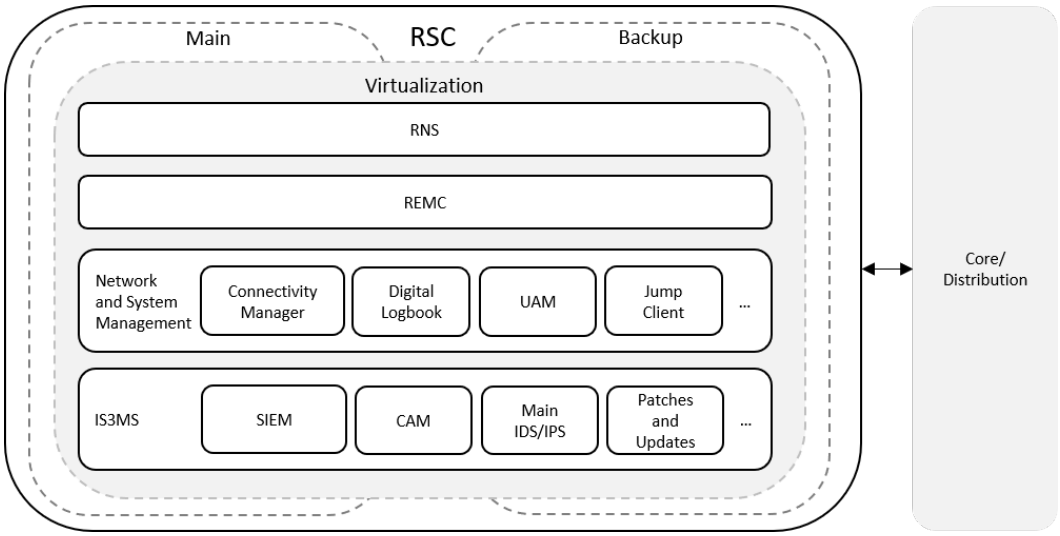


Figure 12. RSC architecture

5.7 SSS

A group of sensors are expected to be mounted on the shore side to aid several functions related to navigation, docking/undocking, passenger loading/unloading, etc. The arrangement of the SSS is still under development, and in this paper, we suggest that the SSS utilises the application of a cloud component to transfer the sensor data to the APS without adding additional communication modules onboard the APS. Such an arrangement enables other APSs approaching the shore to utilise the SSS as well.

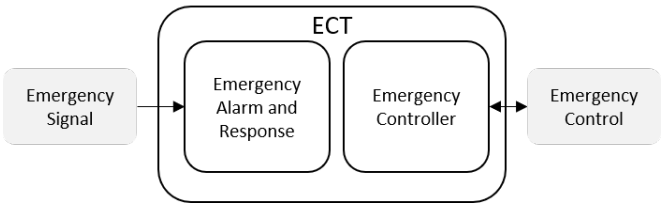
6 Verification

In order to verify that the proposed architecture meets the requirements in (10) that relate to communications, a number of operational scenarios were defined. By leveraging these, we showcase how the architecture provides the required functionality. Additionally, the IP network part of the proposed architecture was implemented in a network simulator; this allowed experimentation that also showed the architecture's ability to meet the established communication requirements of the APS.

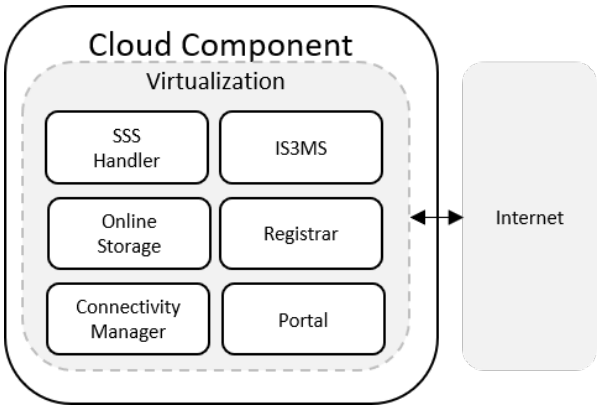
6.1 Verification Scenarios

In this section, a number of operational scenarios that use the communication capabilities of the architecture, and are drawn from the expected operations of the Autoferry (Fig (5)) and influenced by a number of scenarios delivered by the MUNIN project (33) are described.

6.1.1 ***Traffic Communication:*** A crucial requirement for the APS is the ability to communicate with the surrounding ships using LoS communication. It is also recommended that the ship follows the guidance provided by traffic services in the area, such as broadcast messages from VTS. At all times, the APS is expected to receive broadcast traffic messages through the traffic module (Section 5.2.2) and use them to determine safe routes. At the same time, the traffic module is used to broadcast the APS status to surrounding ships for



(a) ECT



(b) Cloud Component

Figure 13. Architectures of ECT, and cloud component

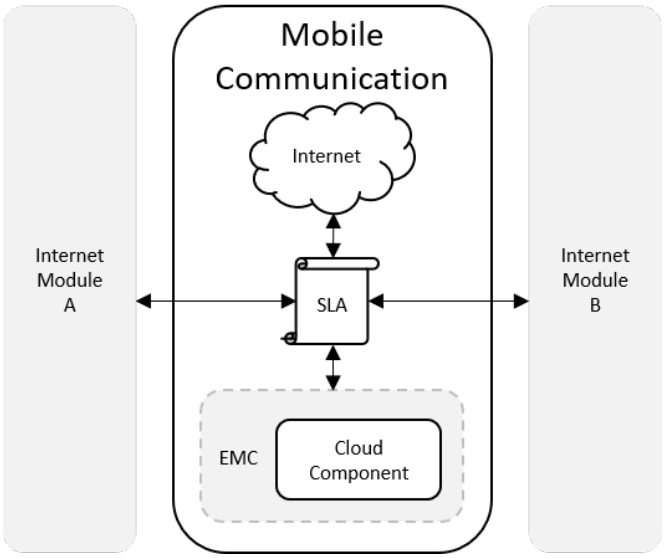


Figure 14. Mobile Communication Utilization

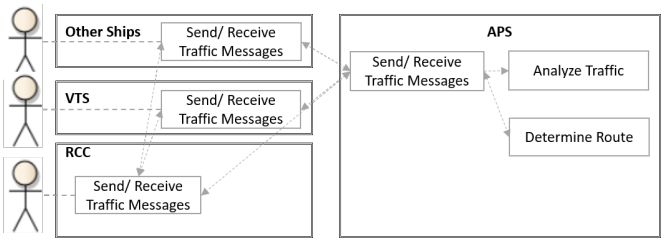


Figure 15. Traffic communication Scenario

safe navigation. Fig 15 shows a scenario of a typical ship-to-ship communication between the APS, other ships and VTS. Moreover, the RCC is expected to communicate with the surrounding ships if the ship-to-ship communication was not sufficient.

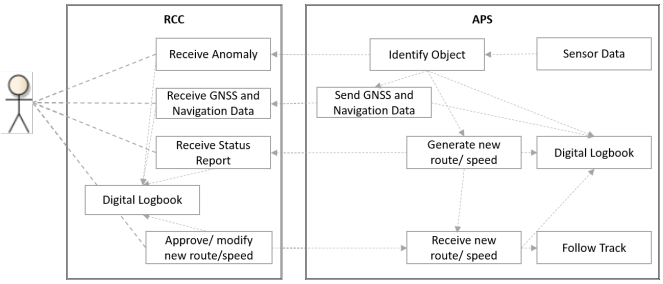


Figure 16. Collision detection and Avoidance Scenario

6.1.2 ***Collision detection and Avoidance:*** During the voyage, the APS operates in autonomous execution mode, and this includes the ability of the ship to perform autonomous and remote navigation functions and engine monitoring and control functions. Fig 16 reflects a scenario of expected communication within the APS and with the RCC to carry out those functions. The ANS collects data from different sensors to perform autonomous navigation functions. In case of a detected object that poses a possible collision threat, the ANS generates a new navigation plan that may include another safe route or modified speed. Meanwhile, a summary of the navigation and GNSS data is sent to the RNS for monitoring together with the newly generated navigation plan. The operator in the RCC receives the navigation data and decides whether to approve or modify the ANS plan for collision avoidance. The ANS waits for the RNS approval or modification for a specific time. If received, the ANS adopts the commands and forwards them to the machinery system. Otherwise, the ANS carries on with its own new navigation plan.

In order to successfully realize such a scenario, both internal and external communications are expected to operate reliably according to the established requirements. For instance, high availability of the communication link with the RCC is needed for the remote navigation, engine monitoring and control functions; this is realized through defining the MC module and the APS-RCC module as a redundant pair. Moreover, a fault-tolerant network is required to reliably carry autonomous navigation, engine monitoring and control operations, even in case of a single component failure. This requirement is addressed by the proposal of redundant network design and redundant devices in both of the core/distribution tiers, the ASC, redundant sensors, redundant thrusters, etc.

6.1.3 ***Loss of Communication:*** An APS is prone to communication loss. To maintain safe operations, the APS is expected to operate in a fail to safe mode in case of communication loss. Fig 17 describes a scenario showing the APS internal communication and emergency communication with the ECT to handle the loss of communication with the RCC and to maintain safe operations. Initially, as long as the ship-to-shore communication with the RCC is available, the ANS receives continuous updates of several MRC plans which govern the ship operations under fail to safe mode

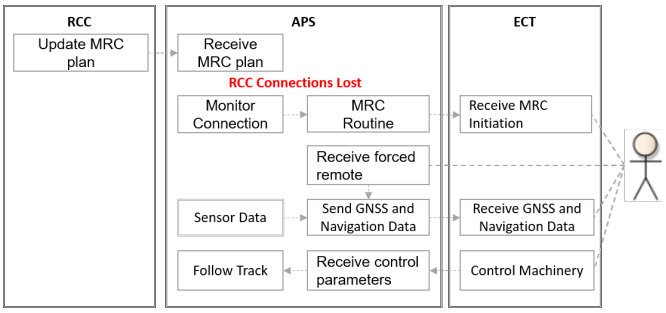


Figure 17. Loss of Communication Scenario

depending on several factors (location, wind, etc). The CM-NMT module that is part of the connectivity manager on the APS has implemented a feature to monitor the connection with the RCC continuously. When the connection is lost, the most appropriate MRC plan is initiated by the ANS, and a signal is sent to the ECT of this action. When the personnel on the ECT receives this signal and have the ability to respond, they send a forced remote signal to the APS forcing it to operate under remote control mode in order to perform emergency navigation and control functions by sending the navigation and GNSS data to the operator on board the ECT; the operator uses these data to navigate the ship safely.

To successfully realize the operation in the described scenario, several requirements need to be met. The requirement related to link quality monitoring and notification is met by the CM-NMT module (Section 5.2.3). Additionally, during the fail to safe mode, it is crucial that the internal network is available for autonomous navigation, engine monitoring and control.

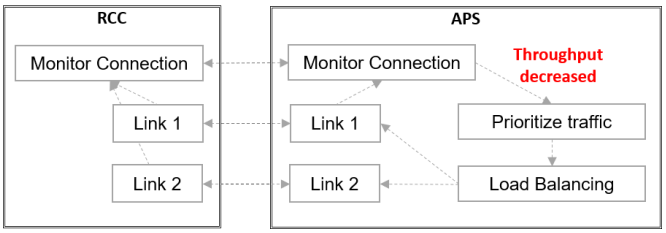


Figure 18. APS and RCC Link Degradation Scenario

6.1.4 ***APS and RCC Link Degradation:*** The communication links between the RCC and the APS are prone to quality degradation resulting from the loss of one of them or due to regular link performance issues. Fig 18 describes a possible scenario of the APS ability to deal with link quality degradation. A communication service (CM-NMT) on the APS continuously monitors the quality of the connections with the RCC. The service initiates an alarm of a quality degradation related to decreased throughput, which may affect the quality of the establishment of situational awareness of the RCC operators and may also reduce their ability to intervene in case of emergency. Therefore, the CM-QoSC service prioritizes the traffic based on a pre-established prioritization policy and utilizes a load balancer to distribute the traffic across the multiple links with the RCC by pushing the traffic with the highest priority in the better link and the traffic with the lower priority in the link with lower quality, if it is still active.

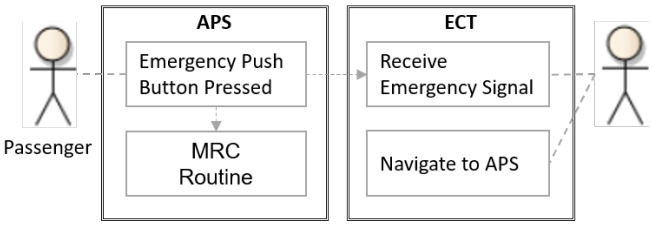


Figure 19. Pressing of Emergency Push Button Scenario

6.1.5 ***Emergency Push Button:*** The highest priority in the APS ecosystem is the safety of the passengers. Therefore, one of the main requirements is the establishment of a communication link for an emergency push button (EPB). Fig 19 describes a scenario of the tasks performed when the EPB is pressed. If pressed, due to a situation perceived by passengers as dangerous (e.g. a passenger falls off the ship), passenger safety functions are invoked, including the initiation of the appropriate MRC routine and the transmission of an emergency signal to the ECT. Then, the ECT will navigate to the ship to intervene and perform a rescue operation.

6.2 IP network simulation

In this section, we provide an evaluation of the IP-based network of the proposed architecture by means of experimentation using the GNS3 simulator. GNS3 (Graphical Network Simulator-3) is a software capable of emulating real devices (routers, switches, servers, PCs, etc) using real software images. It allows users the ability to flexibly configure, test, develop their networks without the high cost of real device (45). We implemented and configured the IP-based network in a manner that allows verifying that the proposed architecture meets its design requirements as established in (10).

As shown in Fig 20, both the networks of the APS and the RCC were implemented as well as their interconnections. Moreover, virtual servers were integrated into the network toward implementing the different ASC components (ANS, AEMC, IS3MS etc.). The core/distribution tiers A and B in the APS network as well as the single-tier in the RCC network were implemented using redundant Layer-3 switches. The implemented redundancy protocol is the Gateway Load Balancing Protocol (GLBP). The MC module and the APS-RCC modules were implemented as gateway routers since GNS3 does not directly support wireless communication. However, for the purpose of verifying the architecture, it has been decided that any routing device capable of routing incoming and outgoing traffic through a third network would suffice. The implemented IP routing protocol is Open Shortest Path First (OSPF). Moreover, to satisfy a requirement related to the employed transmission protocol, the implemented transmission protocol is Transmission Control Protocol (TCP) which is compliant with an international standard (46).

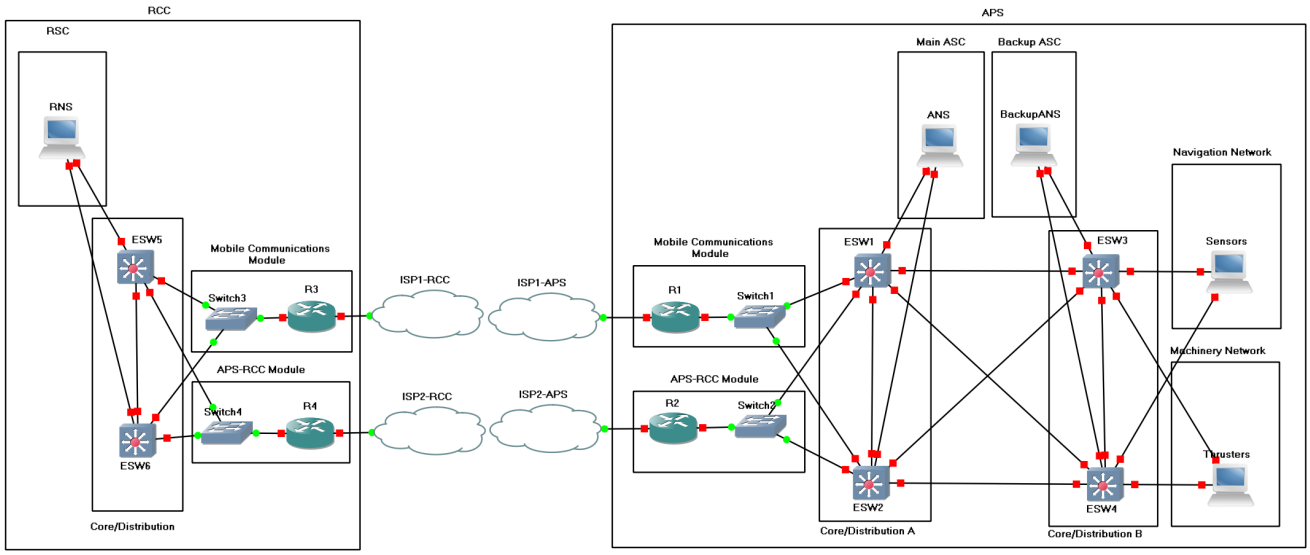


Figure 20. Implementation of the IP network in the proposed architecture using GNS3

Within the capabilities of GNS3, a number of experiments were carried in the simulated architecture to verify that the requirements related to **RCC link redundancy**, **fault tolerance**, **network segregation**, **network redundancy**, **network troubleshooting**, **QoS**, **link quality monitoring and notification**, **traffic prioritization** and **traffic redirection** are addressed.

The results can be inferred from Table 1 which depicts the connectivity matrix for all the hosts in the different implemented networks in GNS3. The table reflects the minimum and the maximum number of routing devices allowing traffic between the hosts in each network and the hosts in the other networks. Between each network, there is a maximum number of routing devices. For instance, there exist eight maximum possible routing devices between the main ASC network and the RSC network while only two between the backup ASC and both the machinery and navigation network. For each network pair, the minimum number of nodes required to maintain connectivity was calculated by performing a systematic shutdown of routing devices between them until the connectivity is completely lost without the ability for automatic recovery. For instance, the connectivity between the main ASC network and the RSC network can withstand up to four routing devices to fail (with maximum 1 out of each 2 redundant pair), while the connectivity between the backup ASC and both the machinery and navigation networks can only withstand one routing device to fail. Nevertheless, the results reflect that both internal and external networks are fault-tolerant, and the connectivity with the RCC is redundant. Moreover, the traffic redirection requirement is implicitly satisfied due to the automatic redirection of traffic implemented by the enforcement of weighted load balancing between each network device pair. Moreover, the implementation of network segregation according to the requirement is indicated in Table 1. The network segregation policy has been implemented in this work by creating a virtual LAN (VLAN) for each network; the connectivity between those networks is governed by defining Access Control Lists (ACLs). For instance, the hosts in the RSC network in the RCC can only access the hosts in the main ASC network, while the hosts in the main ASC can access the hosts in all the networks.

The IP network behaviour in the scenario mentioned in Sec 6.1.3 is simulated during these experiments. When two routers in the pairs (R1 and R2) or (R3 and R4) were shut down, loss of communication between APS and RCC occurred. The ”track” feature implemented by the CM-NMT in the Core/Distribution tier A detected that a link had been lost. This feature can be used to notify the ANS to alter the operational mode. Notably, the internal network was not affected by the loss of communication; this enables the ship to perform all the functions that do not require RCC interference. Further, the scenario mentioned in Sec 6.1.4 is also simulated. When one of the routers R1 or R2 was shut down, the ”track” feature detected that a link had been lost and the CM-QoSC applied a load balancing policy to prioritize traffic, thus meeting the Traffic Prioritization requirement. The link with the RCC was restored automatically using the redundant module, thus showcasing the high availability of the link between APS and RCC.

Moreover, to satisfy the Network Troubleshooting, quality monitoring and notification as well as the operator-triggered traffic redirection requirements, most of the implemented network devices are managed with the Secure Shell (SSH) protocol enabled; this allowed troubleshooting and configuration using SSH within GNS3 from both the RCC and APS networks. Moreover, the notification capability is implemented using the ”track” feature that notifies when a link status is changed. The monitoring and troubleshooting capabilities should be hosted in the main ASC network as it has oversight over all other networks, as shown in Table 1. Advanced troubleshooting and monitoring capabilities are targeted for implementation as part of the Connectivity Manager (Section 5.2.3) in future work.

Table 1. Connectivity Matrix for hosts in the implemented networks

Networks	Main ASC	Backup ASC	Nav. Network	Mach. Network	RSC
Main ASC	N/A	2/4	2/4	2/4	4/8
Backup ASC	2/4	N/A	1/2	1/2	0
Nav. Network	2/4	1/2	N/A	0	0
Mach. Network	2/4	1/2	0	N/A	0
RSC	4/8	0	0	0	N/A

For detailed information regarding the verification criteria in the simulation for the targeted requirements, the reader may refer to Table 3 in Appendix B.

6.3 Applicability

The architecture design leveraging the network design principles related to Hierarchy, Modularity, Resilience and Flexibility (see Section 2) enables it to support a wide range of use cases, different than the one targeted in the Autoferry project (see Section 4). In the near future, it is expected to have several APSs operating in the same area. Such operation requires coordination with the RCC and communication among the ships. The proposed architecture can accommodate this operation by virtue of the cloud component: A cloud service can be developed to bind different APSs to the appropriate RCCs. Additionally, other cloud services can be developed to facilitate communication among different APSs. The topology of the scaled network will be a hybrid between centralized star topology with the RCC in the centre managing several APSs, and P2P topology with Ship-to-Ship communication.

Furthermore, avoiding restrictions regarding the choice of the implementation of technology in the gateway modules provides flexibility for various APS routes. For instance, the implementation of high bandwidth, low latency mobile communication technology such as 5G could enable longer routes for the APS.

6.4 Limitations

In this section, we discuss the limitations in the communication architecture design and verification processes and the efforts to overcome them. The limitations are related to the following:

1. Although the APS system functions and expected operations have been previously defined, the APS systems are still under development. This limited the ability to customize design decisions to that would be more suitable in the future APS and confined the architect with best-judgment decisions based on previous experience, discussions with other project members, and future expectations discussed in the literature.
2. Some requirements lack qualitative or/and quantitative metrics to sufficiently verify their satisfaction in the architecture design. Examples of such limitations:
   (a) No verification metrics for reliability in C-X-2.
   (b) No QoS requirements have been defined to verify C-X-6.
   (c) Measurable metric for redundancy is not provided in C-X-9.

   Efforts to overcome this limitation were made by formalizing design-level and implementation-level verification metrics of the requirements as well as suitable verification method as shown in Table 3 in Appendix B.
3. Limited simulation capabilities exist to simulate heterogeneous networks consisting of IP and Non-IP components. Because of this, we were unable to verify the proposed non-IP components using simulation. Therefore, we utilized scenarios to demonstrate the functionality of such components. Furthermore, a testbed that includes the proposed IP and non-IP components in the architecture is undergoing and considered for future work.
4. Additional architecture analysis methods such as technical risk analysis, trade-off studies, cost analysis, usability, dependability, and maintainability analysis were deemed out of the scope of this paper. Nevertheless, a range of these methods, inter alia, are considered in later stages of the architecture development.

7 Conclusions and future work

Many aspects of our modern life are undergoing digital transformation. Autonomous Passenger Ship (APS) is an example of such transformations. APS relies on many interconnected components to carry passengers in urban water channels safely and securely; this requires the definition of a communication architecture capable of connecting all these components. Therefore, a multidimensional design is required to capture the architecture from different perspectives within the APS operational context. Furthermore, with many involved stakeholders in such technology, the communication architecture needs to achieve the goals and satisfy the requirements communicated by these stakeholders.

An adapted and pre-specified multistep model of incremental and evolutionary development was utilized to develop the architecture by following a generic system life cycle model starting with defining the concept and subsequently the system that aims to realize it. In this regard, the Architecture Analysis and Design Language AADL as well as a network simulator were leveraged in the development and analysis of the architecture design.

At the time of writing this paper, there exists no operational APS to fully evaluate the proposed architecture fully. Instead, we relied on a description of an APS use case, namely the Milliampere ferry, as well as a group of operational scenarios to verify the architecture's ability to perform the intended functions. Finally, some

aspects of the architecture have been verified using a network simulator (GNS3); this showed that the architecture meets requirements related to RCC link redundancy, fault tolerance, network segregation, network redundancy, network troubleshooting, QoS, link quality monitoring, and notification, traffic prioritization, and traffic redirection.

The methodology followed for the development of the communication architecture allowed the integration of stakeholders' communicated goals and addressed their requirements in a verifiable manner. Additionally, it allowed the influence and adoption of design artifacts from the literature and relevant best practices and standards in the industry. This allowed the architecture to integrate and suggest features that make it scalable, flexible, and expandable.

As regards directions of future work, note that the work presented in this paper is part of the ongoing Autoferry project (5). An instance of the proposed communication architecture will be implemented to support the operations of a real autonomous passenger ferry (Milliampere). The Milliampere and its supporting systems (Navigation, Machinery, etc) are still under development. Complete evaluation of the proposed architecture will become possible when these systems become available. Until then, the proposed communication architecture will be complemented by a cybersecurity architecture to reduce the risk of cyberattacks. Additionally, a testbed will be developed with real network devices, to allow experimentation with different options for implementing the APC-RCC and the MC modules. The technologies targeted for experimentation are LTE, 4G, 5G and different WiFi versions. Additionally, the testbed will enable further evaluation of the architecture's ability to perform expected functions such as Ship-to-Ship communications, as well as several Internal and ship-to-shore communication functions.

Furthermore, integration between the implemented GNS3 architecture and real situational awareness systems under development by other project members is underway, in addition to adding visual simulation capabilities to the Autoferry. This setup will enable penetration testing of the APS network and of some of its sub-systems, with the ability to observe the result of cyber attacks on the simulated Autoferry. This feature will be useful in studying the effect of cyber attacks on the security and safety of the Autoferry systems.

References

[1] Schallmo DR and Williams CA. History of digital transformation. In *Digital Transformation Now!* Springer, 2018. pp. 3–8.

[2] Heilig L, Lalla-Ruiz E and Voß S. Digital transformation in maritime ports: analysis and a game theoretic framework. *Netnomics: Economic research and electronic networking* 2017; 18(2-3): 227–254.

[3] Rødseth ØJ and Burmeister HC. Developments toward the unmanned ship. In *Proceedings of International Symposium Information on Ships–ISIS*, volume 201. pp. 30–31.

[4] Projects carried out by members of nfas. http://bit.ly/NFASProjects.

[5] Autonomous all-electric passenger ferries for urban water transport. https://www.ntnu.edu/autoferry.

[6] Havdal G, Heggelund CT and Larssen CH. *Design of a Small Autonomous Passenger Ferry*. Master's Thesis, NTNU, 2017.

[7] Patraiko D. The development of e-navigation. *TransNav, International Journal on Marine Navigation and Safety od Sea Transportation* 2007; 1(3).

[8] IMO M. 85/26/add. 1 report of the maritime safety committee on its eighty-fifth session. *International Maritime Organization, London* 2008; .

[9] An K. E-navigation services for non-solas ships. *International Journal of e-Navigation and Maritime Economy* 2016; 4: 13–22.

[10] Amro A, Gkioulos V and Katsikas S. Connect and protect: Requirements for maritime autonomous surface ship in urban passenger transportation. In *Computer Security*. Springer, 2019. pp. 69–85.

[11] Rødseth ØJ and 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)*. Verlag Schriftenreihe Schiffbau, 2014 Redworth, UK.

[12] Basnet S, Banda OAV, Chaal M et al. Comparison of system modelling techniques for autonomous ship systems. In *Proceedings of the International Seminar on Safety and Security of Autonomous Vessels (ISSAV) and European STAMP Workshop and Conference (ESWC) 2019*. Sciendo, pp. 125–139.

[13] Feiler PH, Gluch DP and Hudak JJ. The architecture analysis & design language (aadl): An introduction. Technical report, Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst, 2006.

[14] de Saqui-Sannes P, Hugues J et al. Combining sysml and aadl for the design, validation and implementation of critical systems. *ERTS 2012* 2012; .

[15] Kordon F, Hugues J, Canals A et al. *Embedded systems: analysis and modeling with SysML, UML and AADL*. John Wiley & Sons, 2013.

[16] Rødseth ØJ, Kvamstad B, Porathe T et al. Communication architecture for an unmanned merchant ship. In *OCEANS-Bergen, 2013 MTS/IEEE*. IEEE, pp. 1–9.

[17] Zolich A, Palma D, Kansanen K et al. Survey on communication and networks for autonomous marine systems. *Journal of Intelligent & Robotic Systems* 2019; 95(3-4): 789–813.

[18] Höyhtyä M, Huusko J, Kiviranta M et al. Connectivity for autonomous ships: Architecture, use cases, and research challenges. In *2017 International Conference on Information and Communication Technology Convergence (ICTC)*. IEEE, pp. 345–350.

[19] Höyhtyä M. Connectivity manager: Ensuring robust connections for autonomous ships. In *2019 2nd International Conference on Intelligent Autonomous Systems (ICoIAS)*. IEEE, pp. 86–90.

[20] Jo SW and Shim WS. Lte-maritime: High-speed maritime wireless communication based on lte technology. *IEEE Access* 2019; 7: 53172–53181.

[21] Porathe T, Burmeister HC and Rødseth ØJ. 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.

[22] Mir ZH and Filali F. Lte and ieee 802.11 p for vehicular networking: a performance evaluation. *EURASIP Journal on Wireless Communications and Networking* 2014; 2014(1): 89.

[23] Stelzer R and Jafarmadar K. Communication architecture for autonomous sailboats. In *Proceedings of International Robotic Sailing Conference*. pp. 31–36.

[24] Papić S. Achieving optimal redundancy in a small business network. *International Journal of Digital Technology & Economy* 2016; 1(1): 13–23.

[25] Team SA et al. An extensible open source aadl tool environment (osate). *Software Engineering Institute* 2006; .

[26] Boehm B and Lane J. DoD Systems Engineering and Management Implications for Evolutionary Acquisition of Major Defense Systems. Technical report, USC-CSSE-2010-500, SERC RT-5 report, March 2010.

[27] Forsberg K, Turner R and Adcock R. *in SEBoK Editorial Board. 2020. The Guide to the Systems Engineering Body of Knowledge (SEBoK), v. 2.2 R.J. Cloutier (Editor in Chief). Hoboken, NJ: The Trustees of the Stevens Institute of Technology. www.sebokwiki.org. BKCASE is managed and maintained by the Stevens Institute of Technology Systems Engineering Research Center, the International Council on Systems Engineering, and the Institute of Electrical and Electronics Engineers Computer Society.*, chapter Generic Life Cycle Model. March 2010.

[28] *Systems and Software Engineering - System Life Cycle Processes. Geneva, Switzerland: International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC)/Institute of Electrical and Electronics Engineers. ISO/IEC 15288:2015.* .

[29] *Systems and Software Engineering, Part 1: Guide for Life Cycle Management. Geneva, Switzerland: International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 24748-1:2010.*

[30] Kim I and Modarres M. Application of goal tree-success tree model as the knowledge-base of operator advisory systems. *Nuclear Engineering and Design* 1987; 104(1): 67–81.

[31] Faisandier A, Madachy R and Adcock R. *in SEBoK Editorial Board. 2020. The Guide to the Systems Engineering Body of Knowledge (SEBoK), v. 2.2 R.J. Cloutier (Editor in Chief). Hoboken, NJ: The Trustees of the Stevens Institute of Technology. www.sebokwiki.org. BKCASE is managed and maintained by the Stevens Institute of Technology Systems Engineering Research Center, the International Council on Systems Engineering, and the Institute of Electrical and Electronics Engineers Computer Society.*, chapter System Analysis. May 2020.

[32] Google earth. https://earth.google.com/.

[33] Munin scenarios. http://www.mits-forum.org/munin/index.htm.

[34] DNV GL. Dnvgl-cg-0264: Autonomous and remotely operated ships 2018; .

[35] Large D and Farmer J. *Broadband cable access networks: the HFC plant*. Morgan Kaufmann, 2008.

[36] Pueblas M, Gyurinda S, Strik J et al. Small enterprise design profile reference guide. *CISCO, Capitulo* 2010; 5.

[37] Maritime broadband radio - mbr. https://www.kongsberg.com/maritime/products/bridge-systems-and-control-centres/broadband-radios/maritime-broadband-radio.

[38] Hegering HG, Abeck S and Neumair B. *Integrated management of networked systems: concepts, architectures and their operational application*. Morgan Kaufmann, 1999.

[39] Steinbaeck J, Steger C, Holweg G et al. Next generation radar sensors in automotive sensor fusion systems. In *2017 Sensor Data Fusion: Trends, Solutions, Applications (SDF)*. IEEE, pp. 1–6.

[40] Gürses E and Akan ÖB. Multimedia communication in wireless sensor networks. In *Annales des Télécommunications*, volume 60. Springer, pp. 872–900.

[41] Albrektsen SM, Bryne TH and Johansen TA. Robust and secure uav navigation using gnss, phased-array radio system and inertial sensor fusion. In *2018 IEEE Conference on Control Technology and Applications (CCTA)*. IEEE, pp. 1338–1345.

[42] Løvø E. Marine technologies' control networks analysis and optimization for failsafe operations examined for class certification ; .

[43] platform Consortium MCC MC. Maritime connectivity platform. https://maritimeconnectivity.net/.

[44] DNV G. Veracity–an open industry platform, 2017.

[45] Neumann JC. *The book of GNS3: build virtual network labs using Cisco, Juniper, and more*. No Starch Press, 2015.

[46] Hunt C. *TCP/IP network administration*, volume 2. " O'Reilly Media, Inc.", 2002.

Appendices

A Appendix A: Navigation and communication Functions

A comprehensive list of expected functions and sub-functions needed to achieve the goals of the Autonomous Passenger Ship (APS), together with the source or requirement proposing the functions as well as the proposed architectural component to realize them, is depicted in Table 2.

B Appendix B: Verification of Requirements

A detailed analysis of the communication requirements verification has been conducted and is depicted in Table 3 to demonstrate the architecture satisfaction of the communicated requirements. The table describes the addressed requirements, the required verification criteria, the relevant architectural components, efforts made to verify as well as future efforts for evaluation.

Table 2. Functions for safe and secure navigation and secure and reliable communication

Goal Function	Functions		Sub-functions	Proposed/ Requirement	Architectureal Components	Goal Function	Functions		Sub-functions	Requirement	Architectureal Components
Safe and Secure Navigation	Main Functions	Autonomous Navigation	Initiate MRC plan	Literature and Stakeholders goals	ANS	Secure and Reliable Communication	Main Functions	Internal and Ship-to-Shore Communication	Establish communication links	C-*-*	- Gateways - Core/distribution tiers
			Receive navigation data						Establish access policies	C-N-5, C-G-4	CM-NSC
			Receive requests						Establish routing tables	C-*-*	CM-QoSC
			Upload new route						Establish prioritization policy	C-X-4	CM-QoSC
			Send reports						Updating Inter-VLAN routing table	C-X-(4,5,6)	CM-QoSC
			Send requests						Establish traffic balancing policy	C-X-(4,5,6)	CM-QoSC
			Receive traffic messages		- ANS - Traffic Module				Establish segmentation policy	C-N-2	CM-NSM
			Send traffic messages						Validate segmentation policy	C-N-2	CM-NSM
			Send navigation data		- Navigation System - ANS				Generating security alarm	C-X-7, C-G-4	CM-NSC
		Autonomous Engine Monitoring and Control	Initiate control parameters		AEMC				Enforcement of security policies	C-G-4	CM-NSC
			Receive requests						Collecting devices configuration backup	C-N-4	CM-NDBC
			Send requests						Storing devices configuration backup	C-N-4	CM-NDBC
			Send Engine Data		- Machinery System - AEMC				Establish backup policy	C-N-4	CM-NDBC
		Remote Navigation	Receive MRC plan		- ANS - RNS				Send device configuration backup	C-N-4	CM-NDBC
			Receive navigation data						Collecting network logs	C-N-5	CM-NMT
			Receive requests						Calculate performance indicators	C-X-7	CM-NMT
			Receive new route						Network troubleshooting	C-X-8	CM-NMT
			Send reports						Generate alarms	C-X-7	CM-NMT
			Send requests						Establish QoS rules	C-X-6	CM-QoSC
			Receive traffic messages		- ANS, RNS				Manage conflicting QoS rules	C-X-6	CM-QoSC
			Send traffic messages		- Traffic Module			Emergency Communication	Transmit navigation data	C-X-2	Emergency Module
			Send navigation data		- Navigation System - ANS				Receive control parameters	C-X-2	Emergency Module
					REMC				Transmit emergency signal	C-X-2	Emergency Module
		Remote Engine Monitoring and Control	Send control parameters					Ship-to-Ship Communication	Receive traffic messages	C-O-1	Traffic Module
			Receive control parameters		AEMC				Send traffic Messages	C-O-2	Traffic Module
			Receive requests					Security		S-*-*	Security Architecture (Future work)
			Send requests		- Machinery System - AEMC		Supporting Functions	Power		Out-of-Scope	
			Send Engine Data					Alarm			
		Emergency Remote Navigation	Receive MRC plan		Backup ANS Emergency Controller			Storage			
			Receive navigation data					Network			
			Receive requests					Control			
			Receive new route								
			Send reports								
			Send requests		- Backup ANS - Traffic Module						
			Receive traffic messages								
			Send traffic messages		- Navigation System - Backup ANS						
			Send navigation data								
		Emergency Remote Control	Send control parameters		Emergency Controller						
			Receive control parameters								
			Send requests		- Backup AEMC						
			Receive requests								
			Send Engine Data		- Machinery System - AEMC						
		Passenger Safety	Initiate emergency signal	C-X-2	EPB						
	Supporting Functions	Security		Project	Security Architecture (Future work)						
		Network			The communication architecture						
		Power									
		Alarm									
		Emergency Response			Out-of-Scope						
		Control									

Table 3. Detailed Requirement Analysis

Code as in (10)	Requirement Description	Priority*	Related to	Verification Criteria		Architecture Components	Verified by		Evaluation	Verification and Evaluation method	Plan forward
				Design-level	Implementation-level		Scenario	Simulation	Testbed		
C-X-1	Link bandwidth and latency	S	Quantitative property	Minimum latency and maximum bandwidth are estimated	A minimum bandwidth of 9Mbps and minimum latency of 0.05 seconds for the ship-to-ship link and 2.5 seconds for the video link	Gateways	-	-	Y	Bandwidth and latency tests	Speed and latency tests will be carried in the testbed across the different implemented gateway links to determine the satisfaction of the requirement.
C-X-2	Emergency push button	S	Capability	A dedicated component that provides the capability exists	A permanent and reliable link is implemented for the EPB	- EPB - Emergency Module - Emergency Alarm and Response	Y 6.1.5	-	Y	Reliability tests	Several implementation choices are being discussed and efforts to integrate this capability to the testbed will be made
C-X-3	Fault tolerant RCC link	S	Qualitative Property	Fault-tolerance property is designed for the RCC link	Link still operates at full capacity in case of a failure in a single component.	- MC Module - APS-RCC Module - Core/distribution tier - ASC - RSC	Y 6.1.4	Y	Y	Network performance tests	Several performance tests will be carried in the testbed to evaluate the ability of the RCC link to tolerate different types of failures
C-X-4	Traffic prioritization	S	Capability	Traffic prioritization capability exists in the proposed component for the RCC link	Traffic prioritization according to a defined policy is implemented	CM-QoSC	Y 6.1.4	Y	Y	Network configuration test	After the implementation of the capabilities, several tests will be carried in the testbed to evaluate their effectiveness
C-X-5	Operator triggered traffic redirection	S	Capability	Traffic balancing capability exists in the proposed component for the RCC link	The operator is able to seamlessly switch and distribute traffic between different communication channels without negative effect		-	Y	Y		
C-X-6	Quality of Service	S	Capability	The capability to provide QoS exists in the proposed components for all external links	The link operates according to a defined QoS metrics		Y 6.1.4	Y	Y		
C-X-7	Link quality monitoring and notification	S	Capability	The design integrates monitoring and notification systems for Information Quality analysis	Real-time or near real-time quality analysis is implemented based on QoI requirements	CM-NMT	Y 6.1.4, 6.1.3	Y	Y		
C-X-8	Network Troubleshooting	S	Capability	Independent troubleshooting capabilities exists for each link	Troubleshooting can be performed by the operator across all the links.		-	Y	Y		
C-X-9	Redundant RCC Link	S	Qualitative Property	Link with RCC is designed to be redundant having at least main and backup	The link with RCC is maintained even with the loss of one of the links	- MC Module - APS-RCC Module	Y 6.1.4	Y	Y	Network performance test	Several implementation choices will be tested using the testbed to propose the most suitable technologies for the main and backup RCC links
C-N-1	Standard aligned design	S	Qualitative Property	The design achieves compliance with applicable requirements in relevant standards	N/A	- On board topology - CM-NSM	-	-	-	Compliance checking	N/A
C-N-2	Segregated network design	S	Qualitative Property	Segregated network design exists	Failure doesn't propagate across segregated networks		-	Y	Y	Network performance test	The feasibility of the segmentation policy after the implementation of the system components will be evaluated
C-N-3	Redundant network design	S	Qualitative Property	Redundant network design exists	Automatic transition/activation/restoration between main and backup systems is implemented		Y 6.1.3	Y	Y		The efficiency of the transition/activation/ restoration process will be evaluated for each system and its backup component
C-N-4	Event triggered traffic redirection	S	Capability	Traffic redirection capability exists in the internal network	Traffic redirected upon loss of remote resources	CM-QoSC	Y 6.1.3	Y	Y	Network configuration test	The effectiveness of the implemented capability will be evaluated in the testbed
C-N-5	Network capacity	S	Capability	Internal Network has the ability to connect several systems	Connectivity is achieved for the different APS components in the internal network	On board topology	-	Y	Y	Existence	The capacity of the implemented network shall be evaluated
C-N-6	Frequency coordination plan	S	Action	N/A	Frequency coordination plan is made, documented, and tested	Implementation-level requirement	-	-	Y	Wireless signal interference testing	After the implementation of several wireless technologies, a frequency coordination plan will be constructed
C-O-1	LoS communication	S	Capability	Ship-to-ship capability exists in the APS	Ship-to-ship communication achieved through LoS communication system (AIS or DVHF) for a range of at least 2km	Traffic module	Y 6.1.1	-	Y	AIS operation, security, and range testing	Several tests will be conducted to evaluate the effectiveness of the AIS technology for implementation in the traffic module. Special focus will be given to its security.
C-G-1	Data recording	S	Capability	Recording and logging capabilities of important data is designed in the APS	Recording and logging of important data is implemented	- Digital Logbook - Online Storage	-	-	Y	Existence	The recording capability will be implemented and evaluated in the testbed.
C-G-2	Type approved components	S	Qualitative Property	N/A	All network components and equipment are type-approved	Implementation-level requirement	-	-	Y	Compliance checking	Efforts will be made to ensure that all testbed equipment are type-approved.
C-G-3	Transmission protocol	S	Qualitative Property	N/A	The transmission protocol for each link is compliant with a relevant international standard		-	Y	Y	Existence	The transmission protocols across all links shall be relevant to an international standard.
C-G-4	Wireless data communication	S	Qualitative Property	N/A	Wireless data communication across the links employ an internationally recognized system with pre-specified features		-	-	Y	Performance and security testing	Several performance and security tests will be carried to verify that the implemented wireless communication technology includes the required features.
C-G-5	Coverage analysis	M	Action	N/A	The effectiveness of the wireless communication systems is determined		-	-	Y	Coverage Analysis	Several tests will be conducted using the testbed to evaluate the coverage of the links in different geographical areas and weather conditions
C-G-6	Network documentation	S	Action	N/A	Documentation of the implemented protocols and interfaces is performed		-	-	Y	Inventory of System-wide protocols and interfaces	After the implementation of all protocols and interfaces, such documentation will be made available.

* MoSCoW rule (S: Should, M: Must)