Communication and Cybersecurity of Autonomous Passenger Ferry

Project extended abstract for SWITS Karlstad – June 2019
Ahmed Amro (ahmed.amro@ntnu.no)
PhD Candidate, Department of Information Security and Communication Technology, Gjøvik

1. Introduction

Autonomous ships are gaining increasing attention in research. According to the most recent report from the Norwegian Ship Owners Association, exactly half of the global shipping companies will implement autonomous ships by 2050 [1]. In this direction, Norway is leading the autonomous shipping industry by opening several testing areas for the development of this technology, in addition to the production of Yara Birkland, the world's first all-electric and autonomous cargo ship, which is planned to operate in 2019. According to ship owners, the most important challenges for the usage of unmanned ships are rules and regulations, in addition to competence, compatible ports and fairways, and cyber security [1].

With the increased research in the maritime industry focused at autonomous ships. The technological improvements were directed toward benefiting the development of smart cities through the smart transportation domain. The city of Trondheim, recently stamped by EU as" smart city [2]", opened the Trondheim Fjord as the world's first testing area for autonomous ships [3]. The idea behind the development of a smart city" is based in various decision-making areas related to the quality of life on the preference for savings, or obtaining the best long-term expenses-effects ratio, while considering the systemic approach to solving a given problem" [4]. In this direction, the city of Trondheim is considering the application of a new technology i.e the autonomous ferry (Autoferry), through the Trondheim canal to improve residents' life as an alternative to a high-cost bridge [5].

The work targeted in this research aims to provide a secure and reliable communication system between all the Autoferry system components to enable carrying real-time operational tasks, like navigation. Additionally, after January 1st, 2021, all ship owners must address cyber risk management in their safety management systems for compliance under the ISM code [6]; thus, this research will target the design and development of an Integrated Security, Safety and Ship Management System (IS3MS). In Norway, transportation, which is the main objective of the Autoferry, is considered part of the country's critical infrastructure. The US National Institute of Standards and Technology (NIST) issued a framework version for improving critical infrastructure cybersecurity [7]. The NIST Framework is considered to be appropriate to follow in implementing the cybersecurity components in this research by creating a cybersecurity framework profile for the Autoferry. Such a profile represents the road map for the Autoferry project to align its requirements, risk tolerances, and resources to the core cybersecurity functions of the NIST framework.

2. Project Goals

1. Define and implement a suitable communication architecture that:
    a. Complies with regulations and standards.
    b. Satisfies functionality, safety and cybersecurity requirements.
2. Apply a suitable risk assessment method in order to identify potential risks.
3. Elicit and integrate cybersecurity mechanisms required to enforce security policies.
4. Provide risk management capabilities through the design and implementation of a standard-aligned Integrated Ship Safety and Security Management System (IS3MS).

3. Breakdown of Work

Establishing State-of-the-Art

A preliminary literature review has been conducted to gain an overview of the state-of-the-art in the related areas to this research and to assess possible benefits toward achieving the research goals. Consequently, and after gaining an initial perspective of the Autoferry project goals, a more in-depth literature review will be conducted to identify and analyze related approaches in the literature.

Communication Architecture

The Autoferry project at its early stages has not defined a specific communication architecture of its own. So, a suitable communication architecture is essential to the development of the project. In this research, a survey of the existing communication architectures in the maritime domain will be conducted in addition to the communication architecture for smart ports and IoT transportation. It is believed that a combination of solutions from each field will be beneficial to this project. This is so because the Autoferry will include new all-electric components and such components will require communication requirements different from the other non-

electric components. Also, the operational conditions of the Autoferry are different than those in the open sea, the former being intended for highly congested urban water and city canals. It has been identified in the literature that for close-to-shore areas, the implementation of lower frequency communication channels is more convenient due to the existence of mobile cellular coverage and short distances between ships and ship control centers [8, 9, 10, 11]. However, the dependency on the mobile cellular network alone might not be suitable to the Autoferry project, due to possible high communication requirements such as live video feed, passenger entertainment, Wi-Fi, and others [12]. At the same time, the Autoferry project will operate in some areas side by side to other vessels having their own communication architectures. Therefore, the Autoferry communication architecture must be compatible with all of them. Fortunately, the Global Maritime Distress Safety System (GMDSS) requires all vessels operating close to shore (Area A1) to communicate through a defined set of communication equipment [13]. To meet all the aforementioned requirements, the communication architecture of a project called Maritime Unmanned Navigation through Intelligence in Networks and other network design principles and approaches will be studied and used toward designing and implementing a communication architecture for the Autoferry.

For evaluating the outcome communication architecture against the operational requirements of the Autoferry project, a mobile wireless communication testbed will be implemented and operated in different areas. The testbed is expected to provide measurements related to wireless communication coverage, bandwidth, latency, and others.

Cybersecurity Framework Profile

Identify Cybersecurity related assets and risk assessment

As stated regarding the NIST framework, which consists of five core functions, Identify, Protect, Detect, Respond, and Recover will be followed. Each function consisting of several categories, subcategories, and informative references. The first function in the creation of a cybersecurity framework profile is to identify risks, assets, business environment, governance, and risk management strategy. To do so, this research will refer to the International Maritime Organization (IMO) high-level guidelines on maritime cybersecurity risk management [14] in order to identify required security policies and procedures. Additionally, the United States Coast Guard have issued documents containing detailed implementations of the NIST framework in different profiles such as offshore operations, and passenger vessels [15]. Such documentations are considered closely related and useful toward the creation of a cybersecurity framework profile for the Autoferry project.

Cyber Security Protection mechanisms and Attack modeling

After all cyber related system components have been identified and cyber risks have been assessed, the NIST framework suggests the subsequent function of system protection. Implementing the protection function includes covering issues related to access control, data security, information protection, and personnel awareness. Then, relevant attacks can be modeled against the identified Autoferry system components within the existence of the required system protection mechanisms.

Detect, Response, and Recovery mechanisms

In addition to protection, the attack detection (Detect), incident response (Respond) and incident recovery (Recovery) functions must be implemented to achieve the agreed upon mission objectives. Performing such functions in a new system such as the Autoferry is expected to require new methods and techniques towards the creation of a cybersecurity framework profile. Initially, a set of cybersecurity detection mechanisms, such as anomaly detection, events identification, and continuous monitoring must be defined. After that, a response plan to carry out tasks such as communication of incident details to the appropriate authorities and involved stakeholders, incident analysis, mitigation and future improvement, during or/and after the occurrence of a cybersecurity incident should be designed. Later, a recovery plan targeting future improvement should be defined.

Implementation of Cybersecurity testbed and attack Scenarios

Finally, going through the aforementioned cybersecurity functions should pave the way into the implementation of a Cybersecurity testbed in addition to real attack scenarios, toward measuring the effectiveness of the performed cybersecurity functions. The attack scenarios should be feasible and thorough in order to safely claim having achieved a secure Autoferry system.

Integrated Security, Safety and Ship Management System (IS3MS)

When a clear view of the Autoferry systems and cybersecurity framework profile is in place, as a final outcome, the IS3MS should be implemented to provide cybersecurity risk management capabilities. The IS3MS will be designed in compliance with existing standards. A candidate standard for cybersecurity management system is the ISO27001 [16], as suggested by DNV GL [17].

For evaluating the implemented IS3MS, the previously implemented cybersecurity testbed for autonomous vessels will be used to launch various attacks, monitor, and assess the system's preparedness against them.

4. References

[1] N. S. Association et al., “Maritime outlook 2018,” Report March, 2018.

[2] “Trondheim blir smartby.” [Online]. Available: https://www.trondheim.kommune.no/trondheim-blir-smartby/

[3] SINTEF, “Test site opens for unmanned vessels.” [Online]. Available: https://www.sintef.no/en/latest-news/test-site-opens-for-unmanned-vessels/

[4] D. Sikora-Fernandez, D. Stawasz et al., “The concept of smart city in the theory and practice of urban development management,” Romanian Journal of Regional Science, vol. 10, no. 1, pp. 86–99, 2016.

[5] A. Skille and S. Lorentzen, “Foresl˚ar førerløs passasjerferge i trondheim.” [Online]. Available: https://www.nrk.no/trondelag/foreslar-forerlos-passasjerferge-i-trondheim-1.12990523

[6] C. Ramboll, “Advokatfirma: Analysis of regulatory barriers to the use of autonomous ships: Final report,” Danish Maritime Authority, Copenhagen, pp. 1374–1403, 2017.

[7] N. I. of Standards and Technology, “Framework for improving critical infrastructure cybersecurity,” 2014.

[8] M. Hoeft, K. Gier lowski, J. Rak, and J. Wo´zniak, “Netbaltic system– heterogeneous wireless network for maritime communications,” Polish Maritime Research, 2018.

[9] Y. Kim, J. Kim, Y. Wang, K. Chang, J. W. Park, and Y. Lim, “Applica tion scenarios of nautical ad-hoc network for maritime communications,” in OCEANS 2009, MTS/IEEE Biloxi-Marine Technology for Our Future: Global and Local Challenges. IEEE, 2009, pp. 1–4.

[10] Y. Xu, S. Jiang, and F. Liu, “A lte-based communication architecture for coastal networks,” in Proceedings of the 11th ACM International Conference on Underwater Networks & Systems. ACM, 2016, p. 6.

[11] L. Lambrinos and C. Djouvas, “Creating a maritime wireless mesh infrastructure for real-time applications,” in GLOBECOM Workshops (GC Wkshps), 2011 IEEE. IEEE, 2011, pp. 529–532.

[12] B. Rødseth, “Munin deliverable d10.1: Impact on short sea shipping, september 21st 2015,” Available from www. unmanned-ship. org. Accessed January 2019, 2015.

[13] Z. Kopacz, W. Morga´s, and J. Urban´ski, “The maritime safety system, its main components and elements,” The Journal of Navigation, vol. 54, no. 2, pp. 199–211, 2001.

[14] “Guidelines on maritime cyber risk management.” [Online]. Available: http://www.imo.org/en/OurWork/Security/GuidetoM aritimeSecurity/Documents/MSC.1 CIRC.1526(E).pdf

[15] “Cyber security.” [Online]. Available: https://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/Inspections-Compliance-CG-5PC-/Office-of-Port-Facility-Compliance/Domestic-Ports-Division/cybersecurity/

[16] G. Disterer, “Iso/iec 27000, 27001 and 27002 for information security management,” Journal of Information Security, vol. 4, no. 02, p. 92, 2013.

[17] A. J. Oliver, “Dnv gl works with tsakos for the in dustry’s first cybersecurity management plan.” [Online]. Available: https://www.dnvgl.com/news/dnv-gl-works-with-tsakos-for-the-industry-s-first-cybersecurity-management-system-66577