Paving the way toward autonomous shipping development for European Waters – The AUTOSHIP project

V Bolbot, G Theotokatos, E Boulougouris Maritime Safety Research Centre, University of Strathclyde, Glasgow, UK
LA L Wennersberg, H Nordahl, Ø J Rødseth SINTEF, Trondheim, Norway
J Faivre, BUREAU VERITAS Marine & Offshore, Paris, France
M Molica Colella CiaoTech (PNO Group), Rome, Italy

SUMMARY
New developments in maritime industry include the design and operation of autonomous ships. The AUTOSHIP project is one initiative promoting the use of autonomous ships in European waters focusing on two specific use cases, a Short Sea Shipping (SSS) cargo vessel and an Inland Waterways (IWW) barge. The AUTOSHIP objectives include thorough regulatory, societal, financial, safety and security analyses for the two investigated use cases as well as the development of a novel framework and methods for the design of autonomous vessels. This objective is achieved with the support of a number of activities, including supply chain, regulatory, risk and gaps analyses. Some results and findings from these activities are presented in this paper. The results demonstrate that the supply chain analysis is important to understand the complex relationships between different partners and phases for the effective design of maritime autonomous systems. Furthermore, a number of regulatory gaps needs to be addressed for the wider adoption of the AUTOSHIP use cases. There is a number of essential hazards associated with each of the two use cases; measures to mitigate these hazards are presented.

1. INTRODUCTION

Paving the way towards the development of the Maritime Autonomous Surface Ships (MASS) requires innovative and bold initiatives. Such a collaborative initiative is the AUTOSHIP project [1], which aims at converting two conventional vessels in remotely controlled and autonomous vessels as well as testing and operating them; in particular, a Short Sea Shipping (SSS) cargo vessel and an Inland Waterways (IWW) barge. AUTOSHIP is a €27M budget project funded by EU with a duration of 42 months, which started on 1st June 2019. The AUTOSHIP consortium involving 10 partners gathers the technological excellence as well as the market, industry and academic knowledge and know-how to analyse and define the extended framework related to MASS adoption and acceptance.

The main aim of AUTOSHIP project is the promotion of autonomous shipping in Europe. The project specific objectives focus on the development of key enabling technologies, including shore/remote control centres, autonomous navigation, intelligent maintenance, operation and safety based on Artificial Intelligence algorithms. In addition, communication technology enabling a prominent level of cyber security**,** will be developed and experimentally validated targeting both retrofitting of existing vessels and new ships design.

Moreover, another project objective is the development and use of new tools including simulators and decision support tools for operators training, cost assessment and optimisation of the next generation autonomous ships. It is expected that the developed tools and methods will support the operation and optimisation of conventional vessels as well. The project objectives also include the review of the environmental and socio-economic aspects for the autonomous shipping transportation and scaling up at a global level. This will allow for quantification of societal, environmental and financial impact stemming from modal-shifts from road to waterborne transport, jobs shifting towards higher-skills positions, and new business cases.

The safety and security (including cyber-security) is another objective of paramount importance for the development of MASS. Two work packages led by the Maritime Safety Research Centre (MSRC) of the University of Strathclyde [2] are dedicated to activities, which include comprehensive regulatory, societal, economic, (cyber)security and safety analyses, thus leading to the development of a roadmap, methodologies, advanced methods and standards for planning and design of next generation MASS, duly motivated by the two full-scale demonstrators testing. Based on the project results a proposal to IMO for amending and improving the existing regulatory framework is planned.

The realisation of the last-mentioned objective of the AUTOSHIP project is implemented according to the following steps. First, the two investigated vessels supply chains are analysed including the operating phases and the involved actors. Subsequently, the existing regulatory framework for the two use cases is analysed. Based on the available information for the two use cases, a risk assessment is implemented and risk control measures are defined. These investigations support the development of a novel safety, security and cybersecurity framework focusing on autonomous ships. Based on these steps the major gaps for scaling-up the demonstrators are provided. These steps are elaborated further in the next sections and some of the project findings are presented.

2. SUPPLY CHAIN ANALYSIS

This is a task led by SINTEF [3], aiming at the supply chain analysis to provide the foundation for following-up analyses on: (a) the impact of autonomy introduction on

regulations; (b) the societal and economic scenarios; (c) definition of the basic operational scenarios for the risk assessment. This analysis also provides input for determining the operations, functions and controls for the two use cases along with the vessels routes, including segments with remote controlled/monitored sailing and totally unmanned bridge.

This study and analysis are based on information from semi-structured interviews carried out with staff from the AUTOSHIP project operators, specifically, Blue Line Logistics [4] and Eidsvaag [5]. The survey was built up to capture all stages of the investigated vessels supply chains according to the multi-stage supply chain model described in [6]. Emphasis was put on distribution and logistics chain, but also to capture relevant interactions with production planning and inventory control. The results of the semi-structured interviews were then used to map the supply chains by using flowchart models that describe both the sequence and relationships between the flow of goods and the flow of information.

Some indicative results for the IWW use case are provided in the flowchart of Figure 1. As it is deduced, the supply chain includes several actors: customers, sales department, logistics department, the transporting truck and IWW manager. The transportation by ship is arranged only after a coordination between the land transport and ship transport. This understanding is important for the financial analysis. The results of the detailed supply chain analysis are available in the public project deliverable [1].

3. COMPLIANCE FRAMEWORK ANALYSIS

The AUTOSHIP project use cases are considered to operate in a specific regulatory and legislative environment, one in the inland waterways in Belgium and one in national waters as well as in a route between Norway and Denmark. The introduction of autonomous ship operations requires the understanding of the gaps that exist in the regulatory framework.

This need is addressed through task led by Bureau Veritas (BV) [7]. This task identifies and maps the existing regulatory framework including the prevailing regulations, rules and standards (international and national) for the SSS and IWW use cases considered in the AUTOSHIP project.

A systematic review approach and direct interaction with the relevant partners have been employed for identification and analysis of all the relevant information/material. This has allowed for mapping the compliance framework of the two use cases design and operation against the existing rules, regulations, standards and codes.

The analysis has been limited to mandatory instruments related to maritime safety and maritime security:

- Safety Of Life At Sea (SOLAS), International Convention on Load Lines (CCL), Tonnage, International Convention on Standards of Training, Certification and Watchkeeping (STCW), Convention on the International Regulations for Preventing Collisions at Sea (COLREG), Safety And Rescue (SAR) operations, Maritime Labour Convention (MLC), European Directives, National and Local regulations.
- Policy Regulations for the Navigation of Rhine (RPNR), European Code for Inland Waterways (CEVNI), Strasbourg Convention on the limitation of liability in inland navigation (CLNI), the Strasbourg Convention on the collection, deposit and reception of waste (CDNI), European Directives, Regional, National and Local regulations for the IWW use case.

IMO Interim Guidelines for MASS trials, IMO Guidelines on maritime cyber risk management and Bureau Veritas Guidelines for Autonomous Shipping [8] have also been considered. It should be noted that it does not include all codes and standards relevant for such SSS & IWW use cases (e.g. land based regulations for remote control centre located at shore).

The main identified areas where amendments or new developments are required are the following:

- Definition and responsibilities of the master, crew and responsible person in new context.
- Regulations requiring the presence and actions of human operators on-board, manual operations or indication/alarm on the bridge.
- No provisions for compulsory systems, devices and procedures that would facilitate crewless vessel

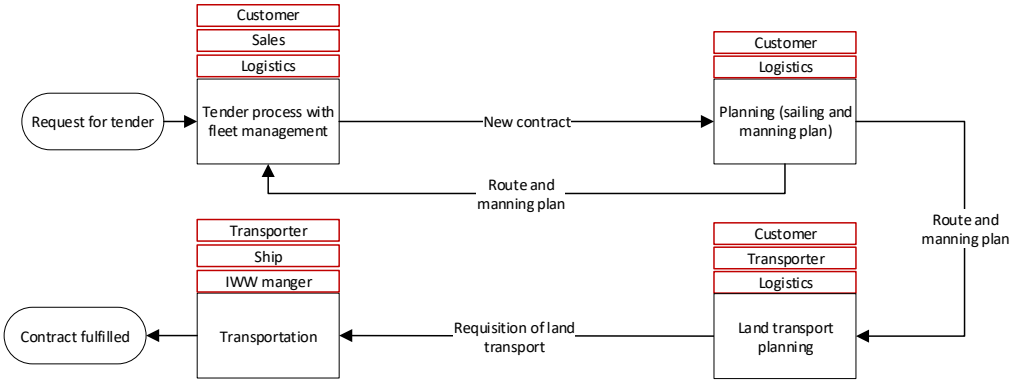

Figure 1 IWW Supply chain overview.

operation (all tasks will be not moved from crew to remote operators, some tasks will be performed by systems on board).
- Functions, rights and responsibilities of Remote Control Centre, including personnel qualification.

More detailed results of regulatory framework analysis are provided in the pertinent deliverable [1].

4. RISK ASSESSMENTS

The introduction of autonomous ships is accompanied with a number of challenges related to safety, security and cybersecurity. The safety challenges can be attributed to increased complexity related to the interactions between the autonomous ships systems/components and environment [9]. Furthermore, cybersecurity has been an important issue, as a cyber-attack can exploit vulnerabilities in the communication links and directly affect the integrity or availability of the data and control systems, leading to accidents [9, 10]. A number of incidences with unauthorised people gaining remote access to the ship control systems was recently reported [11]. Terrorists or pirates could potentially board an autonomous vessel trying to take control, which might lead to hazardous/inadvertent situations (e.g. collision with another ship or requests for significant ransom).

The availability of different methods for safety, security and cybersecurity analysis might create a confusion on their suitability and applicability as well as for the required sequence. For the purposes of this analysis, a classic HAZID as proposed according to the BV rules [8] with some modifications was selected. In addition, alternative approaches employed in other industries and their marinisation (customisation to the requirements of the maritime industry) are investigated. These include the SAE ARP4761 standard for development of civil aircrafts and systems as well as the ISO/PAS21488 and the approach of Safety of Indented Functionality (SOTIF). The risk assessment focuses mainly on the autonomous vessels and associated remote control centre functions during different operational phases. This task is primarily led by MSRC in close cooperation with BV and SINTEF.

The identification process focusing on system parts as shown in Figure 2 is implemented following the process presented in **Error! Reference source not found.**. First a specific group of functions is selected for the analysis. For this group of functions, a specific operating phase is considered. For each combination of functions and operating phases, a specific type of inadvertent event is considered either primarily related to safety, security or cybersecurity. The inadvertent event is identified by focusing on the output of a specific function. For identifying the potential hazards, guidance statements are used, such as provided wrong, not provided, provided in timely, provided results in conflict. For security/cybersecurity related events, different threat groups are considered. For each scenario, potential causes are considered in terms of safety (system error, failure, human error, inadvertent environment conditions, missing input), security (management failure, missing/faulty technical barrier, operating in dangerous area) and cybersecurity (potential cyberattacks types and vulnerabilities). For each cause and hazard, incident/accident categories are defined and potential consequences are identified in terms of safety, damage to environment or financial impact.

The main identified inadvertent events include the following:
- The surrounding situation is not properly (wrongly or not) determined e.g. Objects (small objects, navigation marks, ships, ship lights, floating objects, depth) are not detected and recognised, weather is not properly determined.

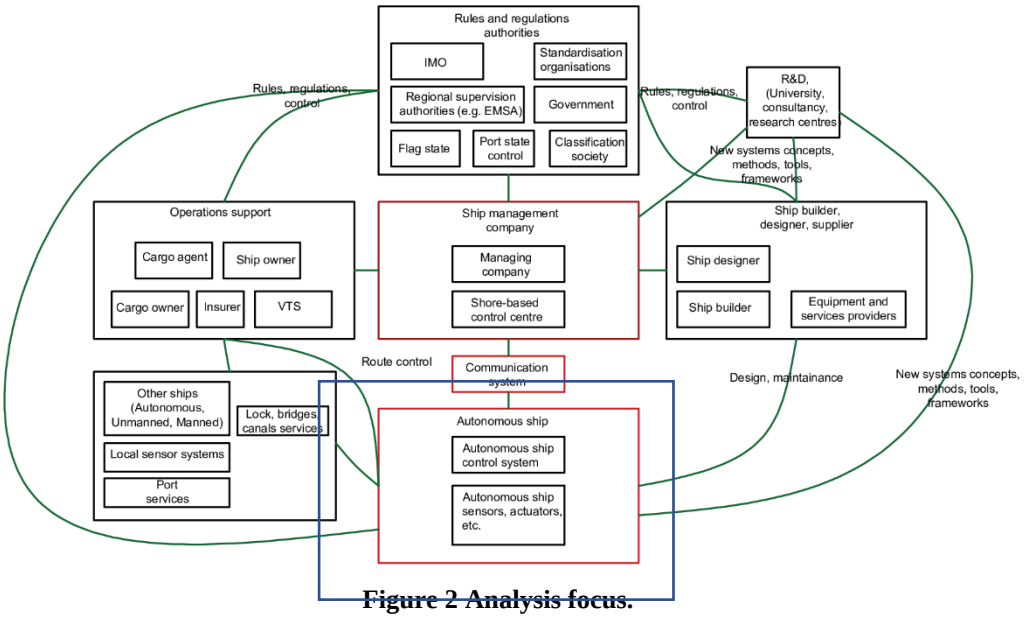

Figure 2 Analysis focus.

- Situation awareness equipment malfunction due to a generic cyberattack during berthing / sailing / manoeuvring.
- Ship on collision track with other vessels/on grounding track (no output / wrong output from collision avoidance system).
- Selecting route with heavy traffic/ bad weather conditions/ Close to shallow water/low visibility / close to obstacles.
- Vessel erratic operation/movements.

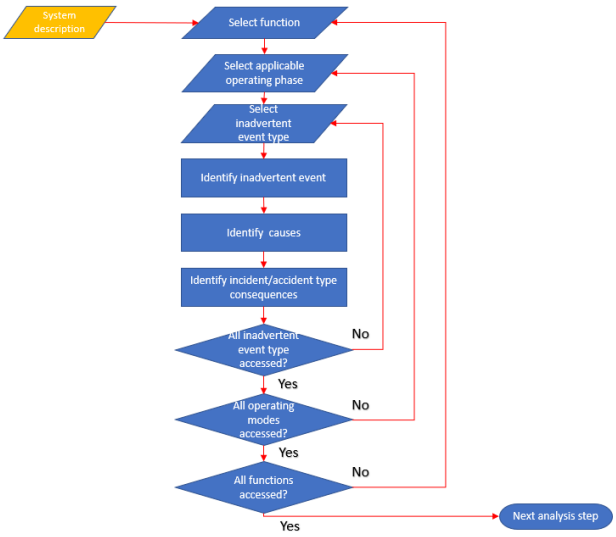

Figure 3 Risk analysis approach.

The potential risk mitigation measures include:

- Crosscheck of information coming from different sources using voting mechanisms.
- Installation of firewall and intrusion detection system in ship control network.
- Automatic remote-control centre personnel in case of serious malfunctions and take over.
- Double verification of selected route.
- Filters installed on sensors used for ship position control.

The results of the HAZID session along with detailed information for the risk and control measures will be provided in future publications.

5. NOVEL SAFETY, SECURITY, CYBERSECURITY ASSURANCE FRAMEWORK DEVELOPMENT

The MASS can be described as systems of Cyber-Physical Systems (CPSs). The additional complexity of the marine CPS on autonomous ships can be attributed to the novel components such as the shore control centre, the novel communication links, the novel human-machine interfaces, the extensive cyber (software) supported functions. It is expected that the existing safety assurance methods may have inherent weaknesses for supporting identification of all the potential hazardous scenarios [9, 12].

In this task, which is led by MSRC, a critical review of the methods and standards used for safety, security and cybersecurity assurance in different domains was implemented. Based on the standards and methods limitations, a novel safety assurance framework is proposed to support the design of safe, secure and cyber secure autonomous ships. The framework includes parallel but interacting processes for safety, security and cybersecurity of the MASS assurance. Each (safety, security, cybersecurity) assurance is double staged, proceeding from high-level analysis to lower, more detailed analysis and in parallel with Vee design process, as shown in **Figure 4**. The analysis results are also used to derive specific test scenarios for MASS and support the development of the safety, security and cybersecurity case, which is addressed in other project tasks. In addition, a number of novel and advanced safety, security and cybersecurity analysis methods such as STPA [13], Cyber-Risk Assessment for Marine Systems [14] fitting into the new safety assurance framework is proposed for overcoming the existing methods drawbacks.

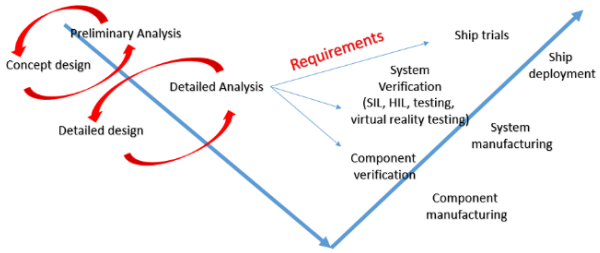

Figure 4 Proposed safety framework aligned with Vee design process.

6. GAP ANALYSIS

Using the output from previous tasks, the final purpose of this task led by MSRC is to identify gaps for wider adoption of the two demonstrators/use cases. This is carried out by implementing a multi-dimensional analysis.

The analysis is articulated in two steps. First the functional and operational requirements and Key Performance Indicators (KPIs) are defined considering the whole supply chain. Then, impact analysis of the identified scenarios is implemented for the two use cases. This is still work in process and results are anticipated to be published in the future studies.

7. CONCLUDING REMARKS

In this paper, the main objectives and some results of the AUTOSHIP project were presented. The results demonstrate that for the two use cases:

- The operation is implemented using a complex and highly interacting supply chain including several phases.
- A number of gaps exists in the existing regulatory framework, which need to be addressed to allow wider adoption of the use cases.
- Emerging hazards on the two use cases need to be addressed using appropriate control measures.
- The complexity of the autonomous ships requires the development of novel integrated design, safety, security, cybersecurity frameworks employing modern and advanced methods and tools for these systems analysis.
- The enhancement of operations and adoption for the novel use cases requires the definition of KPIs connected to the supply chain.

AUTOSHIP is an ongoing project and novel outputs are being constantly generated, such as methods, tools, concepts, results to support the design and operation of the two use cases. It is expected that these results will also support the general community of autonomous ships designers.

8. ACKNOWLEDGEMENTS

The study was carried out in the framework of the AUTOSHIP project (AUTOSHIP, 2019), which is funded by the European Union's Horizon 2020 research and innovation programme under agreement No. 815012. The authors greatly appreciate the AUTOSHIP partners reviewed and provided feedback for this paper. The authors affiliated with MSRC also greatly acknowledge the funding from DNV GL AS and RCCL for the MSRC establishment and operation. The opinions expressed herein are those of the authors and should not be construed to reflect the views of EU, DNV GL AS, RCCL or other involved partners in the AUTOSHIP project.

9. REFERENCES

1. AUTOSHIP. Autonomous Shipping Initiative for European Waters 2019 [Available from: https://www.autoship-project.eu/.
2. MSRC. The Maritime Safety Research Centre 2020 [Available from: https://www.strath.ac.uk/research/maritimesafetyresearchcentre/.
3. SINTEF. SINTEF 2020 [Available from: https://www.sintef.no/en/.
4. Blue Lines Logistics. Blue Lines Logistics News 2015 [Available from: http://www.bluelinelogistics.eu/news.
5. Eidsvaag. Eidsvaag 2020 [Available from: https://eidsvaag.no/.
6. BM B. Supply Chain design and analysis: Models and methods. Int J Production Economics. 1998:281-94.
7. BV. Bureau Veritas 2020 [Available from: https://www.marine-offshore.bureauveritas.co.uk/.
8. Guidelines for autonomous shipping - Guidance Note NI 641DT R01 E, (2019).
9. Bolbot V, Theotokatos G, Bujorianu LM, Boulougouris E, Vassalos D. Vulnerabilities and safety assurance methods in Cyber-Physical Systems: A comprehensive review. Reliability Engineering & System Safety. 2019;182:179-93.
10. Eloranta S, Whitehead A. Safety aspects of autonomous ships. In: Gl DNV, editor. 6th International Maritime Conference; Germany, Hamburg, 2016. p. 168-75.
11. Wingrove M. Shipborne systems most vulnerable to cyber-attack. Marine electronics & communications [Internet]. 2017; 11(3):[27 p.].
12. Bolbot V, Theotokatos G, Boulougouris E, Psarros G, Hamann R. A novel method for safety analysis of Cyber-Physical Systems - Application to a ship exhaust gas scrubber system. Safety. 2020.
13. Leveson N. Engineering a safer world: Systems thinking applied to safety. Moses J, de Neufville R, Heitor M, Granger M, Pate-Cornell E, Rouse W, editors. London, England: The MIT press; 2011. 560 p.
14. Bolbot V, Theotokatos G, Boulougouris E, Vassalos D. A novel cyber-risk assessment method for ship systems. Safety Science. 2020; Currently under review.

9. AUTHORS BIOGRAPHY

Victor Bolbot is a Research Associate at the Maritime Safety Research Centre (MSRC), Department of Naval Architecture, Ocean and Marine Engineering (NAOME), University of Strathclyde, Glasgow. His research focuses on safety and cybersecurity of marine autonomous and complex systems. His recent research output includes publications on safety analysis of power systems on cruise ships, scrubber systems, dual-fuel engines and cyber security risk assessments.

Gerasimos Theotokatos is the DNV GL Reader of Safety of Marine Systems at the Maritime Safety Research Centre (MSRC), Department of Naval Architecture Ocean and Marine Engineering (NAOME), University of Strathclyde, Glasgow. His research focuses on the development of scientific approaches to holistically capture the safety, energy and sustainability interplay of the complex marine systems including cyber-physical and autonomous systems by employing advanced model-based methods and tools for their design and optimisation pursuing life-cycle risk and energy management, efficiency improvement, and safety and sustainability enhancement.

Evangelos Boulougouris is the MSRC Director and RCCL Reader of Safety of Maritime Operations,

Department of NAOME, University of Strathclyde, Glasgow. His research focuses on the safety of ship operations, holistic design optimisation and design for safety. He is RINA Fellow and member of SNAME.

Lars Andreas Lien Wennersberg is a Research Scientist at SINTEF Ocean in Trondheim, Norway. He has a background from simulator-based testing of maritime control systems and engineering of maritime power, distribution and propulsion systems. His research focuses on design and test methods of autonomous ship systems.

Håvard Nordahl is a Research Scientist at SINTEF Ocean in Trondheim, Norway. He has a background from simulator based testing of maritime control systems and offshore modification projects. His research focuses on standardisation of simulations, design and cost evaluations of autonomous ship systems and autonomous shipping in general.

Ørnulf Jan Rødseth is a senior scientist at SINTEF Ocean and is the manager of Norwegian Forum for Autonomous Ships. He has more than 25 years' experience in maritime information and communication technology. In the last years, he has worked mainly with autonomous ship technology and maritime digitalization. He is a member of ISO TC8 and IEC TC80 and regularly meets at IMO as observer for ISO.

Jérôme Faivre is Smart Ships Rules Manager in the Development Department of BUREAU VERITAS Marine & Offshore Division. After 22 years as a naval senior surveyor, he has developed a large experience in Marine and Offshore fields and engineering management. His main responsibilities include development of Rules for autonomous and remote-controlled units.

Marco Molica Colella is Team Manager and Senior Innovation consultant in Italy at PNO Consultants. He has developed a large experience (+14) since his PhD as Engineer in the mechanical and aeronautics domain. He now supports the management, growth and finance of innovative projects in a large ecosystem made of primary actors in the energy and transport domain. He is the appointed AUTOSHIP coordinator.