TRANSNAV
http://www.transnav.eu
the International Journal
on Marine Navigation
and Safety of Sea Transportation
Volume 13
Number 4
December 2019

DOI: 10.12716/1001.13.04.03

Preliminary Results of a System-theoretic Assessment of Maritime Autonomous Surface Ships' Safety

K. Wróbel & P. Krata
Gdynia Maritime University, Gdynia, Poland

J. Montewka
Gdynia Maritime University, Gdynia, Poland
Aalto University, Espoo, Finland

ABSTRACT: While a system-theoretic approach to the safety analysis of innovative socio-technical systems gains a growing acceptance among academia, safety issues of Maritime Autonomous Surface Ships (MASS) remain largely unexplored. Therefore, we applied a System-Theoretic Process Analysis to develop and analyze a preliminary model of the unmanned shipping system in order to elaborate safety recommendations for future developers of the actual system. Results indicate that certain advancements shall be undertaken in relation to MASS' software solutions in particular.

1 INTRODUCTION

The concept of unmanned shipping has been developing since 1970s, but it gained a considerable momentum in the second decade of 21st century, when several R&D projects have been funded to explore its feasibility.

Among these, the most notable are Maritime Unmanned Navigation through Intelligence in Networks (MUNIN) (Burmeister, Bruhn, and Walther 2015), Advanced Autonomous Waterborne Application Initiative (AAWA)(Wróbel, Montewka, and Kujala 2018b, 2018a), as well as several projects carried out by privately-owned companies.

It has been generally acknowledged that technical and organizational revolution of shifting merchant vessels' control from their crews to shore-based facilities or on-board computers will influence safety in multiple ways (Nautilus Federation 2018; Ramos et al. 2018; Utne, Schjølberg, and Roe 2019; Rødseth and Burmeister 2015). Nevertheless, due to unquestionable innovativeness of the concept and lack of full-scale prototypes operating in a real environment, a comprehensive safety evaluation of the concept could not be performed to date (Thieme, Utne, and Haugen 2018), particularly in a quantitative manner.

In an attempt to bridge this gap, we applied a System-Theoretic Process Analysis (STPA), a tool developed to analyze safety of large socio-technical systems regardless their development phase. It is based on the assumption that safety is not a value to be assessed but rather a feature to be controlled. Therefore, some principles of control engineering can be applied to model safety (Leveson 2011). STPA and related methods have previously been applied in various domains, including automated driving systems (Abdulkhaleq et al. 2018), aeronautics (Allison et al. 2017; Lower, Magott, and Skorupski 2018), maritime accidents' analysis (Filho, Jun, and Waterson 2019; Kim, Nazir, and Øvergård 2016) and maritime safety management (Valdez Banda and Goerlandt 2018). Its versatility made it a perfect candidate for conducting a safety analysis of a system still being under development at the time.

2 MATERIALS AND METHODS

A system-theoretic, holistic insight has originally been developed to address safety issues regardless organizational levels to which they relate, from top management through individual operators or actuators. By that, control over hazards in each point of the system's structure would be ensured (Kee et al. 2017; Leveson 2011). Within this approach, known as System-Theoretic Accident Model and Process (STAMP), it is not unreliability of particular components of the system in question but inadequacy of interactions between them that leads to accidents. Such interactions must be executed in an adequate, controlled manner which will ensure that the whole system maintains its safety pre-conditions (Kazaras, Kontogiannis, and Kirytopoulos 2014). Therefore, violation of safety constraints that shall be enforced on the system might develop a hazard (a system state or set of conditions that, together with a particular set of worst-case conditions, will lead to an accident) (Leveson 2011). Conditions that could in fact result in a hazard are investigated and ideas on how to mitigate them are explored. It is however recommended to renounce any quantitative research activity including risk calculation (Bjerga, Aven, and Zio 2016), mostly due to a potential lack of sufficiently reliable data, which is particularly apparent in initial phases of system development.

The above considerations are in line with Safety-II approach that focuses on making entire socio-technical systems capable of succeeding (in safety terms) under any circumstances (Hollnagel 2014). Therein, safety should be rooted in the system from its earliest design phases and throughout operation until decommissioning. STAMP and related tools (including STPA) are said to be more effective in achieving this goal (Altabbakh et al. 2014) than previously applied methods, including quantitative ones. With reference to unmanned shipping as an emergent technology, system-theoretic approach gives an opportunity to both perform a proactive safety analysis as well as assess its feasibility in this aspect. The latter could only be attained some period after unmanned vessels' implementation when the outcome could be validated, for instance through reality check or benchmarking (Goerlandt, Khakzad, and Reniers 2017).

Before the STPA could be performed, hazards to which it can be exposed are listed as well as safety-related interactions between its components being modelled and visualized through safety control structure (see Figure 1, depicting a generalized STPA procedure).

Thence, an identification of potentially inadequate interactions (control actions or feedback) between system's components is carried out. Those can occur because:

1 A control action required for safety is not provided or not followed;
2 A control action is provided in an unsafe manner;
3 A potentially safe control action is provided at the wrong time or in the wrong sequence;
4 A control action required for safety is stopped too soon or applied too long (Leveson 2011).

Subsequently, ways in which unsafe control action could occur are investigated. This consists of an examination of system's control loops in order to determine what factors could cause it to be inadequate and how. Furthermore, hazard mitigation measures can be elaborated at this stage, which is of particular significance from safety-driven design point of view. Therein, cooperation between system developers and safety analysts is iteratively utilized to design an ever-safe system (Fleming and Leveson 2015). When multiple controllers influence one component, particular attention must be paid to all relevant control loops so as to eliminate potential coordination problems.

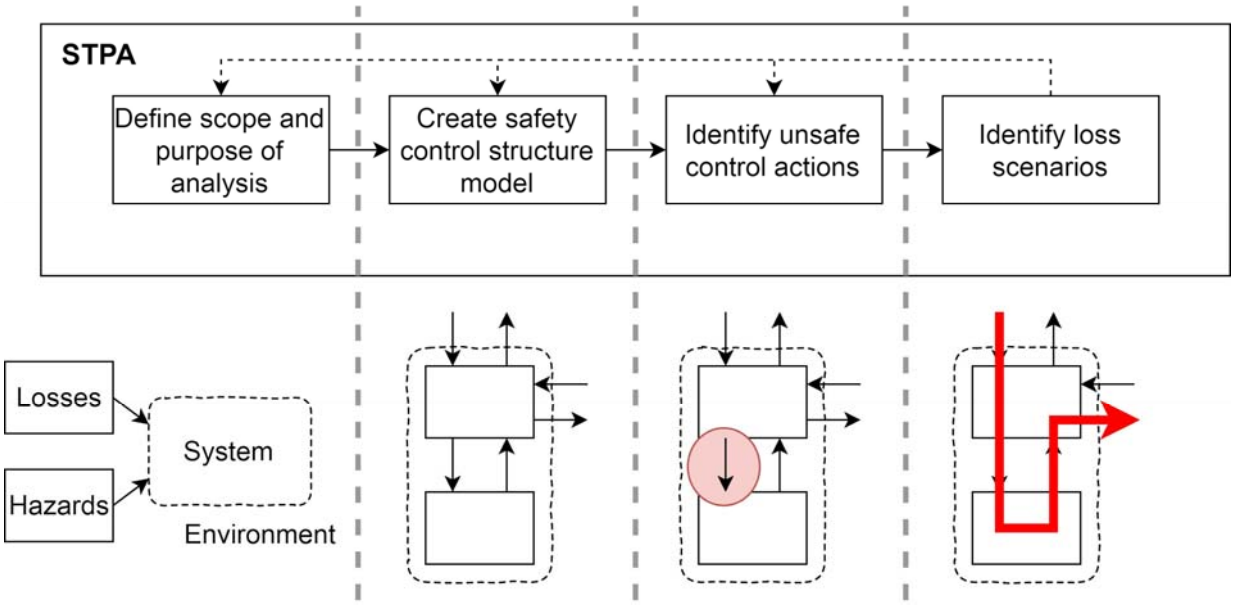

Figure 1. STPA standardized procedure, inspired by (Leveson and Thomas 2018)

The analysis presented in this paper is based on publicly available data pertaining to unmanned ships' system concept (Porathe, Prison, and Man 2014; Rødseth and Tjora 2014; Van Den Boogaard et al. 2016; Porathe 2016; Hogg and Ghosh 2016; Burmeister et al. 2014). These have been reviewed and compiled into a model of system safety control structure in line with STPA's principles. Therein developed model has been consulted with experts involved in R&D projects related to MASS. Thence, the proper part of STPA has been performed with identification of hazards, control actions and potential hazard mitigation measures. The herein-described analysis has been performed for a concept of fully-autonomous merchant vessel. Such a ship is expected to navigate herself without a direct control of shore-based operator and conduct all shipborne processes based on pre-programmed algorithms of artificial intelligence.

Additionally, uncertainties pertaining to the analysis have been analyzed as postulated in (Goerlandt and Reniers 2016; Bjerga, Aven, and Zio 2016).

The analysis procedure is outlined in Figure 2.

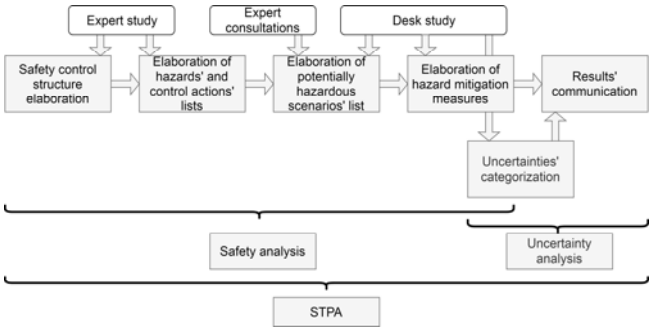

Figure 2. System-Theoretic Process Analysis outline as performed

3 MODEL AND RESULTS

The high-level safety control structure of fully-autonomous merchant vessel is given in Figure 3 while the list of identified hazards to which an autonomous merchant vessel can be susceptible is given in Table 1.

As can be seen in Table 1, most of the hazards are related to mechanical failures and dangerous physical interactions of an autonomous ship with other objects. Nevertheless, these can result from all different kinds of inadequacies of control actions, just to name improper safety culture implemented within a shipping company.

Thence, recommendations for future systems' developers have been elaborated, pertaining to potential ways of mitigating hazards. These are also referred to as mitigation measures. Their full list is given in (Wróbel, Montewka, and Kujala 2018b), while Figure 4 depicts their summary.

As can be seen in Table 1, most of the hazards are related to mechanical failures and dangerous physical interactions of an autonomous ship with other objects. Nevertheless, these can result from all different kinds of inadequacies of control actions, just to name improper safety culture implemented within a shipping company.

Table 1. List of hazards

#	Description of hazard
1	Physical hazards
1.1	Vessel collides with another ship, runs into element of infrastructure or damages other man-made objects
1.2	Vessel is incapable of properly containing dangerous chemicals or energy
1.3	Vessel causes death or injury to persons accidentally or illegally occupying her compartments
1.4	System does not detect a distress situation
1.5	Vessel loses her cargo at sea
1.6	Vessel is unable to maintain proper cargo stowage conditions
1.7	Vessel runs aground
1.8	Vessel suffers from propulsion/steering failure
1.9	Vessel's navigational capabilities are impaired by weather conditions
1.10	Vessel suffers from loss of stability
1.11	Vessel suffers from flooding
1.12	Vessel suffers from fire or explosion
1.13	Vessel suffers from loss of structural integrity
1.14	Vessel suffers from loss of power supply
1.15	System causes other vessel to ground, run into element of infrastructure or damage other man-made objects
2	Organizational hazards
2.1	Contact with the vessel cannot be established
2.2	Vessel is denied passage due to security concerns
2.3	Vessel contributes to delay of other ships' traffic
2.4	Vessel violates international or coastal state's regulations
2.5	System's communication subsystem unintentionally interferes with other assets
3	Environmental hazards
3.1	Vessel is unable to maintain integrity of tanks containing oils or oily mixtures
3.2	Vessel is unable to maintain proper fuel combustion parameters
3.3	Vessel is incapable of properly containing dangerous chemicals or energy

Thence, recommendations for future systems' developers have been elaborated, pertaining to potential ways of mitigating hazards. These are also referred to as mitigation measures. Their full list is given in (Wróbel, Montewka, and Kujala 2018b), while Figure 4 depicts their summary.

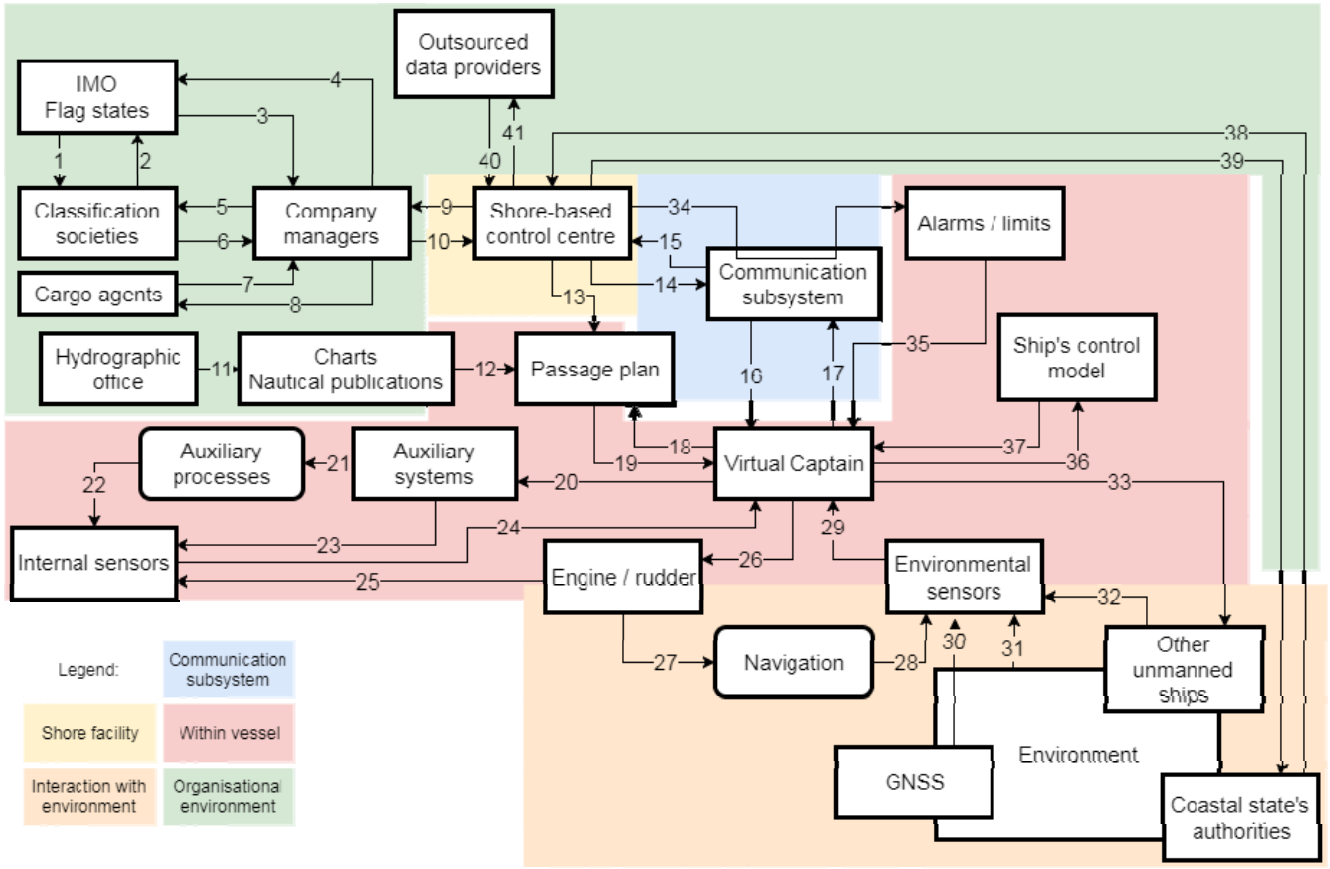

Figure 3. High-level safety control structure of fully-autonomous merchant vessel system

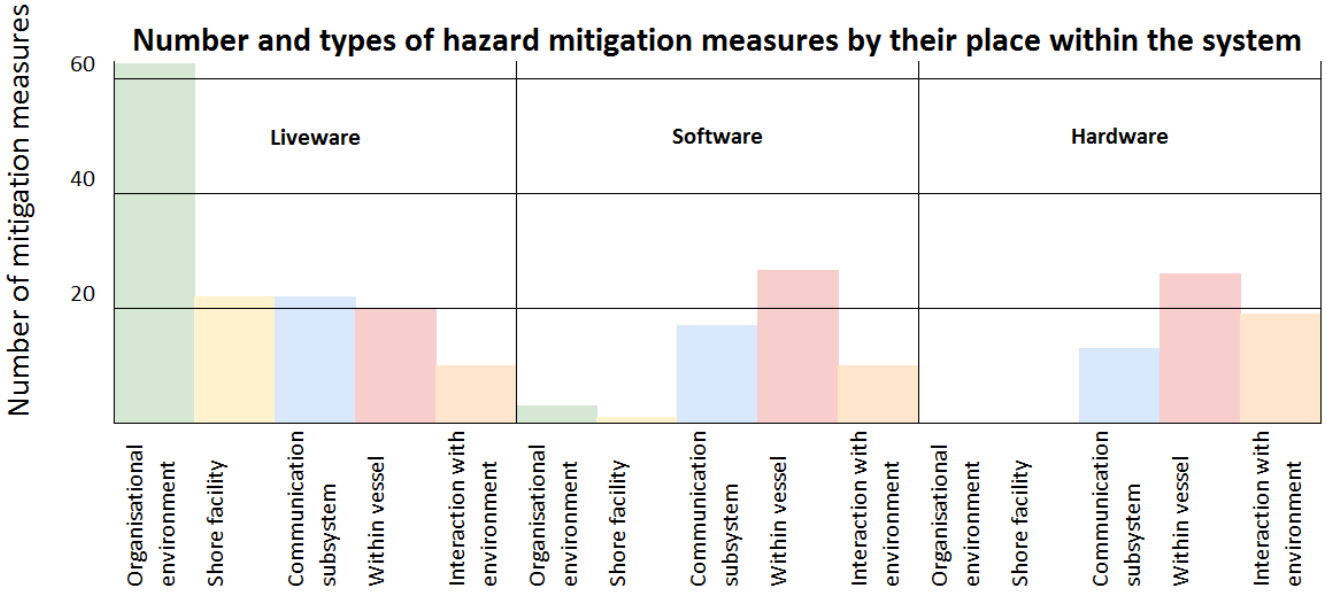

Figure 4. Summary of hazard mitigation measures for Maritime Autonomous Surface Ships

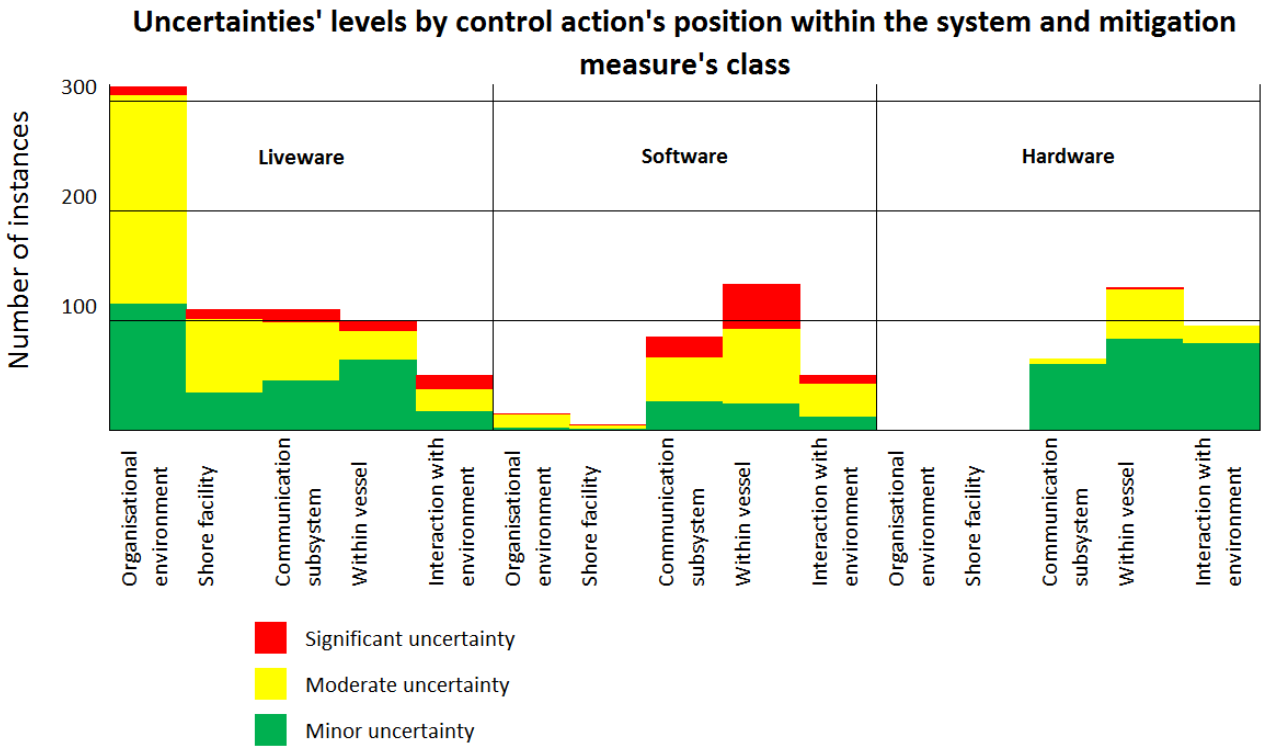

Figure 5. Results of uncertainty assessment

The relevant mitigation measures have been structured into three categories: those pertaining to liveware, software and hardware. As can be seen in Figure 4, the number of suggested solutions is significant, particularly for the shore-side part of the system.

Furthermore, results' uncertainties have been evaluated according to the method introduced in (Flage and Aven 2009) and refined in (Wróbel, Montewka, and Kujala 2018b). The uncertainties pertaining to background knowledge supporting any given mitigation measure implementation has been assessed as either significant, moderate or minor. The results of this part of study are given in Figure 5.

The mitigation measures related to software solutions can be characterized as more uncertain than others. This can result from a fact that autonomous vessels would operate based on innovative software, perhaps including artificial intelligence, development of which is still ongoing with promising results. Similar issues had been encountered during the development of driverless cars (Waldrop 2015). Meanwhile, the use of same hardware solutions as in manned shipping is expected which brings about a limited uncertainty.

4 DISCUSSION

Throughout the analysis, some high-level recommendations on MASS safety solutions have been elaborated and assessed with relation to the uncertainties potentially affecting the feasibility of their implementation. As can be seen in Figure 4, such recommendations can be applied to almost any aspect of MASS operation ranging from organizational factors through environment sensing.

Despite the autonomous merchant vessels being expected to operate with no crew on board, stating that human factor will be removed from the system is misguiding. In fact, human operators will remain in loop one way or another through design, fleet management, remote supervision or control tasks (Kobyliński 2018; Ahvenjärvi 2016). The number of mitigation measures involving liveware is significant and applicable to all aspects of MASS operation, and organizational environment in particular.

Although the number of mitigation measures involving software solutions is comparable to these of hardware, it must be noted that software is likely to have much greater influence on autonomous ships' safety performance than it has on today's merchant vessels (Lloyd's Register 2017; Komianos 2018; Man et al. 2018). Virtually all components of the system will rely on software to the extent that cannot be determined at the point. The fact that some significant uncertainties have been identified pertaining to software solutions feasibility, a further, more comprehensive study on this matter is required (Thieme, Utne, and Haugen 2018). Close cooperation between systems' developers, researchers and practitioners such as seafarers may be extremely beneficial in this matter.

5 CONCLUSIONS

An application of a qualitative, systemic method instead of quantitative ones to analyze safety issues of autonomous merchant vessel allowed for obtaining a high-level, universally applicable results. These do not depend on the actual design of MASS system which is still being developed by various industry actors, but should rather be considered as general guidelines for the developers of such systems.

As opposed to quantitative sets of safety assessment methods, no determination of safety of risk values has been performed as these are believed to be misleading (Leveson 2011) or unnecessary (Condamin, Louisot, and Naïm 2007). Instead, some general recommendations have been elaborated on how to ensure that MASS system retains safety as its feature in any conditions. Nevertheless, the results must be considered incomplete as these pertain to some idealistic model of autonomous ship systems retrieved from publicly available materials.

Nevertheless, they can be validated as soon as the concept of autonomous shipping enters a full-scale implementation phase.

REFERENCES

Abdulkhaleq, Asim, Markus Baumeister, Hagen Böhmert, and Stefan Wagner. 2018. "Missing No Interaction—Using STPA for Identifying Hazardous Interactions of Automated Driving Systems." *International Journal of Safety Science* 02 (01): 115–24. https://doi.org/10.24900/ijss/0201115124.2018.0301.

Ahvenjärvi, S. 2016. "The Human Element and Autonomous Ships." *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation* 10 (3): 517–21. https://doi.org/10.12716/1001.10.03.18.

Allison, Craig K., Kirsten M. Revell, Rod Sears, and Neville A. Stanton. 2017. "Systems Theoretic Accident Model and Process (STAMP) Safety Modelling Applied to an Aircraft Rapid Decompression Event." *Safety Science* 98 (October). Elsevier Ltd: 159–66. https://doi.org/10.1016/j.ssci.2017.06.011.

Altabbakh, Hanan, Mohammad A. AlKazimi, Susan Murray, and Katie Grantham. 2014. "STAMP - Holistic System Safety Approach or Just Another Risk Model?" *Journal of Loss Prevention in the Process Industries* 32. Elsevier Ltd: 109–19. https://doi.org/10.1016/j.jlp.2014.07.010.

Bjerga, Torbjørn, Terje Aven, and Enrico Zio. 2016. "Uncertainty Treatment in Risk Analysis of Complex Systems: The Cases of STAMP and FRAM." *Reliability Engineering and System Safety* 156. Elsevier: 203–9. https://doi.org/10.1016/j.ress.2016.08.004.

Boogaard, Maurits Van Den, Andreas Feys, Mike Overbeek, Joan Le Poole, and Robert Hekkenberg. 2016. "Control Concepts for Navigation of Autonomous Ships in Ports." In *10th Symposium on High-Performance Marine Vehicles*. Cortona.

Burmeister, Hans-Christoph, W C Bruhn, and L Walther. 2015. "Interaction of Harsh Weather Operation and Collision Avoidance in Autonomous Navigation." *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation* 9 (1): 31–40. https://doi.org/10.12716/1001.09.01.04.

Burmeister, Hans-Christoph, Wilko C Bruhn, Ørnulf Jan Rødseth, and Thomas Porathe. 2014. "Can Unmanned Ships Improve Navigational Safety?" In *Proceedings of the Transport Research Arena*. Paris.

Condamin, Laurent, Jean-Paul Louisot, and Patrick Naïm. 2007. *Risk Quantification: Management, Diagnosis and Hedging*. Chichester: John Wiley & Sons, Ltd.

Filho, A, GT Jun, and P Waterson. 2019. "Four Studies, Two Methods, One Accident—another Look at the Reliability and Validity of Accimap and STAMP for Systemic Accident Analysis." *Safety Science* 113. Elsevier: 310–17. https://doi.org/10.1016/j.ssci.2018.12.002.

Flage, Roger, and Terje Aven. 2009. "Expressing and Communicating Uncertainty in Relation to Quantitative Risk Analysis." *Reliability & Risk Analysis: Theory & Application* 2 (13): 9–18.

Fleming, Cody Harrison, and Nancy Leveson. 2015. "Integrating Systems Safety into Systems Engineering during Concept Development." In *25th INCOSE International Symposium*, 989–1003. Seatlle, WA. https://doi.org/10.1002/j.2334-5837.2015.00111.x.

Goerlandt, Floris, Nima Khakzad, and Genserik Reniers. 2017. "Validity and Validation of Safety-Related Quantitative Risk Analysis: A Review." *Safety Science* 99 (November): 127–39. https://doi.org/10.1016/j.ssci.2016.08.023.

Goerlandt, Floris, and Genserik Reniers. 2016. "On the Assessment of Uncertainty in Risk Diagrams." *Safety Science* 84: 67–77. https://doi.org/10.1016/j.ssci.2015.12.001.

Hogg, Trudi, and Samrat Ghosh. 2016. "Autonomous Merchant Vessels: Examination of Factors That Impact the Effective Implementation of Unmanned Ships." *Australian Journal of Maritime & Ocean Affairs* 8 (3): 206–22. https://doi.org/10.1080/18366503.2016.1229244.

Hollnagel, Erik. 2014. "Is Safety a Subject for Science?" *Safety Science* 67: 21–24. https://doi.org/10.1016/j.ssci.2013.07.025.

Kazaras, Konstantinos, Tom Kontogiannis, and Konstantinos Kirytopoulos. 2014. "Proactive Assessment of Breaches of Safety Constraints and Causal Organizational Breakdowns in Complex Systems: A Joint STAMP-VSM Framework for Safety Assessment." *Safety Science* 62. Elsevier Ltd: 233–47. https://doi.org/10.1016/j.ssci.2013.08.013.

Kee, Dohyung, Gyuchan Thomas Jun, Patrick Waterson, and Roger Haslam. 2017. "A Systemic Analysis of South Korea Sewol Ferry Accident - Striking a Balance between Learning and Accountability." *Applied Ergonomics* 59. Elsevier Ltd: 504–16. https://doi.org/10.1016/j.apergo.2016.07.014.

Kim, Tae-eun, Salman Nazir, and Kjell Ivar Øvergård. 2016. "A STAMP-Based Causal Analysis of the Korean Sewol Ferry Accident." *Safety Science* 83: 93–101. https://doi.org/10.1016/j.ssci.2015.11.014.

Kobyliński, Lech. 2018. "Smart Ships – Autonomous or Remote Controlled?" *Scientific Journals of the Maritime University of Szczecin* 53 (125): 28–34. https://doi.org/10.17402/262.

Komianos, Aristotelis. 2018. "The Autonomous Shipping Era. Operational, Regulatory, and Quality Challenges." *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation* 12 (2): 335–48. https://doi.org/10.12716/1001.12.02.15.

Leveson, Nancy G. 2011. *Engineering a Safer World - Systems Thinking Applied to Safety*. Cambridge, MA: MIT Press.

Leveson, Nancy G., and John P. Thomas. 2018. *STPA Handbook*. https://doi.org/10.2143/JECS.64.3.2961411.

Lloyd's Register. 2017. "Cyber-Enabled Ships. ShipRight Procedure Assignment for Cyber Descriptive Notes for Autonomous & Remote Access Ships." Southampton.

Lower, Michał, Jan Magott, and Jacek Skorupski. 2018. "A System-Theoretic Accident Model and Process with Human Factors Analysis and Classification System Taxonomy." *Safety Science*.

Man, Yemao, Reto Weber, Johan Cimbritz, Monica Lundh, and Scott N. MacKinnon. 2018. "Human Factor Issues during Remote Ship Monitoring Tasks: An Ecological Lesson for System Design in a Distributed Context." *International Journal of Industrial Ergonomics* 68. Elsevier: 231–44. https://doi.org/10.1016/j.ergon.2018.08.005.

Nautilus Federation. 2018. "Future Proofed? What Maritime Professionals Think about Autonomous Shipping." London.

Porathe, Thomas. 2016. "A Navigating Navigator Onboard or a Monitoring Operator Ashore? Towards Safe, Effective, and Sustainable Maritime Transportation: Findings from Five Recent EU Projects." *Transportation Research Procedia* 14 (2352). Elsevier B.V.: 233–42. https://doi.org/10.1016/j.trpro.2016.05.060.

Porathe, Thomas, Johannes Prison, and Yemao Man. 2014. "Situation Awareness in Remote Control Centres for Unmanned Ships." In *Human Factors in Ship Design & Operation*. London.

Ramos, Marilia, Ingrid Bouwer Utne, Jan Erik Vinnem, and Ali Mosleh. 2018. "Accounting for Human Failure in Autonomous Ships Operations." In *Safety and Reliability - Safe Societies in a Changing World ESREL 2018*, edited by Stein Haugen, Anne Barros, Coen van Gulijk, Trond Kongsvik, and Jan Erik Vinnem, 355–63. Trondheim: CRC Press.

Rødseth, Ørnulf Jan, and Hans-Christoph Burmeister. 2015. "Risk Assessment for an Unmanned Merchant Ship." *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation* 9 (3): 357–64. https://doi.org/10.12716/1001.09.03.08.

Rødseth, Ørnulf Jan, and Åsmund Tjora. 2014. "A System Architecture for an Unmanned Ship." In *13th International Conference on Computer and IT Applications in the Maritime Industries (COMPIT 2014)*, 291–302. Redworth. http://www.ssi.tu-harburg.de/doc/webseiten_dokumente/compit/dokumente/compit2014_redworth.pdf.

Thieme, Christoph Alexander, Ingrid Bouwer Utne, and Stein Haugen. 2018. "Assessing Ship Risk Model Applicability to Marine Autonomous Surface Ships." *Ocean Engineering* 165. Elsevier Ltd: 140–54. https://doi.org/10.1016/J.OCEANENG.2018.07.040.

Utne, Ingrid B., Ingrid Schjølberg, and Emery Roe. 2019. "High Reliability Management and Control Operator Risks in Autonomous Marine Systems and Operations." *Ocean Engineering* 171. Elsevier Ltd: 399–416. https://doi.org/10.1016/J.OCEANENG.2018.11.034.

Valdez Banda, Osiris A, and Floris Goerlandt. 2018. "A STAMP-Based Approach for Designing Maritime Safety Management Systems." *Safety Science* 109. Elsevier: 109–29. https://doi.org/10.1016/j.ssci.2018.05.003.

Waldrop, M. Mitchell. 2015. "Autonomous Vehicles: No Drivers Required." *Nature* 518: 20–23. https://doi.org/10.1038/518020a.

Wróbel, Krzysztof, Jakub Montewka, and Pentti Kujala. 2018a. "System-Theoretic Approach to Safety of Remotely-Controlled Merchant Vessel." *Ocean Engineering* 152: 334–45. https://doi.org/10.1016/j.oceaneng.2018.01.020.

Wróbel, Krzysztof, Jakub Montewka, and Pentti Kujala. 2018b. "Towards the Development of a System-Theoretic Model for Safety Assessment of Autonomous Merchant Vessels." *Reliability Engineering & System Safety* 178: 209–24. https://doi.org/10.1016/j.ress.2018.05.019.