TRANSNAV
http://www.transnav.eu
the International Journal
on Marine Navigation
and Safety of Sea Transportation
Volume 17
Number 2
June 2023

DOI: 10.12716/1001.17.02.14

Integration Test Procedures for a Collision Avoidance Decision Support System Using STPA

S.A. Dugan[1], R. Skjetne[1], K. Wróbel[2], J. Montewka[3], M. Gil[2] & I.B. Utne[1]
[1] *Norwegian University of Science and Technology, Trondheim, Norway*
[2] *Gdynia Maritime University, Gdynia, Poland*
[3] *Gdańsk University of Technology, Gdańsk, Poland*

ABSTRACT: The transition from conventionally manned to autonomous ships is accompanied by the development of enhanced Decision Support Systems (DSS) for navigators. Such systems need to consider interactions among hardware, software, and humans and their potential effects on system performance, which require rigorous testing to verify the system's safe decision-making ability and operational limits. Testing requirements for verification are aimed at 1) assessing the system's reliability and failure handling performance, and 2) integration testing. This work uses the System-Theoretic Process Analysis (STPA) to develop integration tests for a novel DSS. STPA is a structured methodology to identify hazards from multiple sources, including hardware or software failures, system interactions, and human errors. The objectives of the study are to develop and assess the feasibility of integration test procedures based on STPA. The stability monitoring subsystem from the DSS is analyzed as a case study. The results are used to suggest functional and performance integration test procedures.

1 INTRODUCTION

The development of autonomous ships is accompanied by an increased focus on enhanced decision support systems (DSS). These systems support the safe operation of ships by performing various tasks onboard to reduce the workload of navigators [1]. Increasing complexity of such systems, including interactions between humans, software, and hardware, may lead to emergent behavior that is difficult to predict, detect, and mitigate.

Verification refers to the process of evaluating or providing evidence of a system's ability to satisfy its requirements [2]. In the maritime industry, classification societies set guidelines and procedures for verification. For ship control and monitoring systems onboard traditionally manned ships, verification is a three stage process [3], consisting of software verification, certification testing of software and hardware, and onboard testing focused on equipment functionality and communication. For verification of autonomous navigation systems (ANS), DNV proposes additional yet complementary guidelines [4]. Verification testing must be performed in two areas: 1) redundancy and failure response tests, and 2) testing of integrated systems and functions. Redundancy and failure response tests are typically generated from the results of a failure mode and effects analysis (FMEA), while the methods to generate integration tests and the procedures to evaluate their results are ambiguous.

Current methods for testing of complex systems are typically derived from hardware-in-the-loop (HIL) testing. HIL allows for systematic testing of system behavior through the aid of or use of simulation [5]. In the maritime industry, HIL testing has predominately been used for dynamic positioning (DP) system testing [5, 6]. For verification, an HIL test scope consists of several types of testing include functional, failure mode, and performance testing [6]. Functional testing assesses the compliance of a system's function to its functional requirements. Performance testing quantifies the level of performance of a function [5].

Simulation has been identified as a method of enabling large scale tests of scenarios for verification [7]. Simulation-based testing extends from the principles of HIL testing, and typically relies on comprehensive models of the ship, the environment, and a test management system [7]. The test management system is responsible for generation of test scenarios, specifying acceptance criteria, and evaluation of the results. Although simulation-based testing allows for testing system behavior in multiple scenarios, questions exist on its performance. Specifically, how should an efficient and relevant test scope be determined, and what procedures should be used to evaluate the test results [8].

The System-Theoretic Process Analysis (STPA) has been increasingly featured in research on verification and validation of maritime autonomous surface ships (MASS). STPA is a hazard assessment methodology based on control theory [9] and has been identified as particularly suitable for evaluating the safety level of complex systems [10]. The method focuses on the control structure of a system to better understand the system behavior. Compared to other hazard analysis methods, STPA is noted for its ability to identify the interactions between different failure types [11, 12].

The "systems-level" perspective of the STPA has also resulted in identifying several accident scenarios not captured by FMEA, which often investigates safety at a component level [13]. Rokseth et al. [14] uses STPA to analyze the safety of DP systems by deriving verification objectives based on the requirements elucidated by STPA. Rokseth et al. [15] expands the method to develop a verification program at different stages of system development, including suggesting test procedures for system performance. For each loss scenario, the aim, setup, execution, and acceptance criteria are provided for multiple stages in the system's verification process.

The research nevertheless indicates a gap in presenting guidelines for identifying and conducting tests for system integration. Therefore, the objective of this paper is to apply a methodology for developing such tests based on the results of an STPA. The principles of HIL testing are extended to improve verification objectives and procedures. The objective of the work is to present the development of targeted functional and performance tests for a DSS developed as part of the Endure research project (project-endure.eu). The purpose of the tests is to identify operational limits and practical settings for the system's operation. The approach is similar to that followed in Rokseth et al. [15]. However, instead of presenting verification objectives, we focus on functional and performance based aspects of integration testing.

The paper is organized as follows: the next section presents the methodology of the study, including STPA and the proposed approach to develop integration tests. The system of study is then described. Results include the steps of the STPA and the derivation of example integration tests for a selected loss scenario. The discussion focuses on the impact of the results for system verification, and the feasibility of STPA for generating test procedures.

2 METHODOLOGY

2.1 *Step 1: STPA*

STPA is a hazard analysis method derived from the System Theoretic Accident Model and Processes (STAMP) [16]. Before describing the purpose and methodology of STPA, a few words are dedicated to its precursor.

STAMP is an accident causality model that shifts the emphasis from preventing failures to enforcing behavioral safety constraints [16]. Although component failure accidents are still included, the ability to analyze and understand component interactions leads to a better understanding of the more complex systems of today. The introduction of the STAMP model requires the refinement of terminology, which is consistent in its related techniques. An accident is termed an unplanned and undesired loss event [16]. Safety is re-framed to a problem of control: safety constraints are placed to restrict emergent properties between component interactions. STAMP and its related techniques, STPA and Causal Analysis based on STAMP (CAST), have been used to analyze accidents and systems ranging from aircraft control to aquaculture [10].

STPA is chosen as the method for this analysis in order to capture the complex functional relationships between controllers, especially when emergent behaviors and competing objectives are expected to be revealed. Additionally, it can be used to model multiple types of controllers (human, software, hardware) and the interactions between them.

The four steps of STPA are detailed below [9]:

1. Define the purpose of the analysis. This step contains four parts: identify losses, identify system-level hazards, identify system-level constraints, and refining hazards (optionally). In this stage, it is important to describe the boundary of the system within its environment.
2. Model the hierarchical control structure. The control structure describes the functional relationships and interactions within the system through the use of feedback control loops.
3. Identify unsafe control actions (UCAs), or control actions that in particular environments and context will lead to a hazard [9]. UCAs are then used to create the requirements and constraints for the system. There are four ways that a control action can be considered unsafe [9]:
   - Not providing the control action leads to a hazard
   - Providing the control action leads to a hazard
   - Providing a potentially safe control action too early, too late, or in the wrong order
   - The control action lasting too long or stopping too soon
4. Identify loss scenarios (LS). The purpose of the scenario identification is twofold:

- to demonstrate how factors within the control structure cause UCAs and lead to losses
- how safe control actions might be executed improperly and lead to losses

These losses can further contribute to the development of requirements and constraints for the system.

2.2 *Step 2: Integration test development*

The purpose of integration testing is to prove that no emergent properties between system functions and their dependencies will degrade the system. Within HIL testing, two types of tests are primarily used to accomplish this: functional testing and performance testing [5, 6]. Functional testing is the testing of a function's ability to fulfil its requirements [5]. In the context of integration, this requires investigating the structure and process variables (PVs) of the system to identify any dependencies that may contribute to a function's failure. Typically, performance testing aims to quantify the performance level for a function. Again, within the context of integration, performance testing investigates the impact of different conditions (both internal and external) on the function's performance [5].

Integration testing is focused on the interactions between components in the system. We use the hierarchical control structure from the STPA as a basis for understanding the behavior of a controller within the context of the system. We identify interfaces by modeling the inputs and outputs of the controller. The unsafe control actions derived from STPA are used to generate safety constraints, or requirements, for functional testing. Loss scenarios provide insight on the dependencies or conditions that may lead to failures. These conditions are used to derive performance tests. Integration test procedures include descriptions of the setup, execution, and evaluation of the results in accordance with IEEE requirements [2].

To develop a test plan based on the results of the STPA, we perform the following additional steps:

1. For an unsafe control action (STPA, Step 3),
   - Identify PVs that contribute to the unsafe control action.
   - Develop functional test based on the generated safety requirement(s).
2. For a loss scenario (STPA, Step 4),
   - Identify PMV conditions that contribute to the LS.
   - Select key performance indicator(s) (KPIs) to evaluate function performance.
   - Develop performance tests for the identified PMV conditions.

Examples of functional and performance tests are presented in Section 4.

3 SYSTEM OF STUDY

The methodology is applied to a DSS for collision avoidance. The DSS is novel due to its consideration of vessel intact stability when evaluating evasive maneuvers for collision avoidance. This is motivated by the role of intact stability in two recent maritime accidents: the capsizings of the Golden Ray [17] and MV Sewol. The latter is one of the worst maritime disasters in recent history, with a death toll of 306 passengers [18].

Intact stability is governed by the interaction of weight and buoyancy [19]. The two primary parameters of interest are the locations of the centers of gravity and buoyancy. The weight and location of the ship's center of gravity is estimated by the officer of the watch (OOW) before each voyage. The center of buoyancy is a function of the ship's weight and hull shape. This information is typically used by the onboard stability computer to estimate the ship's intact stability.

Turning maneuvers, particularly at high speeds, create large heeling moments on the vessel that may cause capsizing [20]. Heeling moments act to move the ship away from the upright position. At large angles of heel, the factors influencing the probability of experiencing large roll motions include ship speed, rudder angle, and wave height, period, and direction [21].

The DSS system, developed as part of the Endure project, will be installed on the training vessel Horyzont II. The ship profile view is shown in Figure 1. Principal ship characteristics are below:

- Length overall: 56.34 m
- Length between perpendiculars: 48.37 m
- Breadth: 11.36 m
- Block coefficient: 0.60
- Service speed: 12 knots

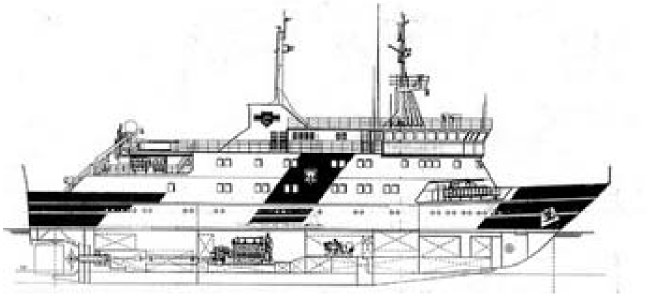

Figure 1. Horyzont II profile view

The system performs condition detection utilizing leading safety indicators [22], condition analysis, and action planning, but has no direct control over the ship's motion. For object detection, the system extracts ship speed, type, and size from static and dynamic AIS data. The OOW can manually input objects that are not detected or detectable by AIS. Condition analysis, the next phase, is performed by assessing the present target ship's behavior and planned own ship's action in order to select suitable, predefined collision avoidance dynamic critical areas (CADCA) , pre-computed for own ship encounters with the target ship's safety domain. Object classification is used for the situational analysis of potential conflicts. Lastly, action planning is performed by restricting the CADCAs to only consider evasive maneuvers with rudder angles that do not jeopardize the ship's intact stability for given wave conditions.

4 RESULTS

4.1 *Step 1. STPA*

The STPA was performed by researchers with domain knowledge and involved with the DSS's development. System architecture diagrams and flowcharts were consulted to model the system control structure diagram and better understand the system's behavior.

4.1.1 *Step 1.0: Define the system boundary*

The system of study is restricted to the behavior of the own ship (OS). This comprises the OOW, the DSS with its sensors and components, and the ship (including its propulsion and maneuvering equipment). The environment therefore consists of surrounding ships and obstacles. Evasive maneuvers are restricted to turns; speed reduction is not considered as a possible maneuver.

4.1.2 *Step 1.1: Define the purpose of the analysis*

The purpose of the DSS is to provide information to the OOW regarding potential collisions with other ships and to prevent excessive maneuvers that may jeopardize the ship's intact stability. Therefore, the accidents of investigation are collision with an obstacle and stability failure. The issues of cybersecurity and intentional attacks (i.e., arson or vandalism) are presently excluded to reduce the scope of the analysis. The losses (L) are therefore:

- L-1: The ship collides with an obstacle.
- L-2: The ship capsizes.

System level hazards that may lead to the losses are listed below. The parenthesis indicate the loss to which the hazard (H) may lead.

- H-1: The ship violates the CADCA for the obstacle (L-1).
- H-2: The ship violates the minimum stability requirement (L-2).

The hazards were refined to consider two causal scenarios of each failure type. First, we consider hazards in which faulty or invalid commands are provided. These lead to a violation of CADCA or the minimum stability requirement. Next, we consider hazards in which the correct commands are not provided.

- H-1.1: Motion control commands that result in violation of the CADCA for an obstacle are provided (L-1).
- H-1.2: Motion control commands that result in preservation of the CADCA for an obstacle are not provided (L-1).
- H-2.1: Motion control commands that result in violation of the minimum stability requirement are provided (L-2).
- H-2.2: Motion control commands that result in preservation of the minimum stability requirement are not provided (L-2).

4.1.3 *Step 1.2: Hierarchical control structure*

Figure 2 presents the hierarchical control structure for the system of study. Each box indicates a controller. Control actions are shown in red. Feedback is shown in blue.

The hierarchical control structure displays the relationships between various controllers of the system. As an example of the control hierarchy, we describe the flow of commands for a typical evasive maneuver: The AIS transceiver provides target ship (TS) information to the motion predictor. Based on an analysis of the OS and TS trajectories, CADCAs are retrieved for evasive maneuvers at the ship's current speed and for various rudder angles (e.g. 5°, 10°, 35°). These are restricted by the maximum allowable rudder angle provided by the stability computer. The CADCAs are then provided to the DSS and displayed to the OOW. To perform the evasive action, the OOW provides the rudder command signal to the ship's rudder. The rudder then imparts a turning force on the ship.

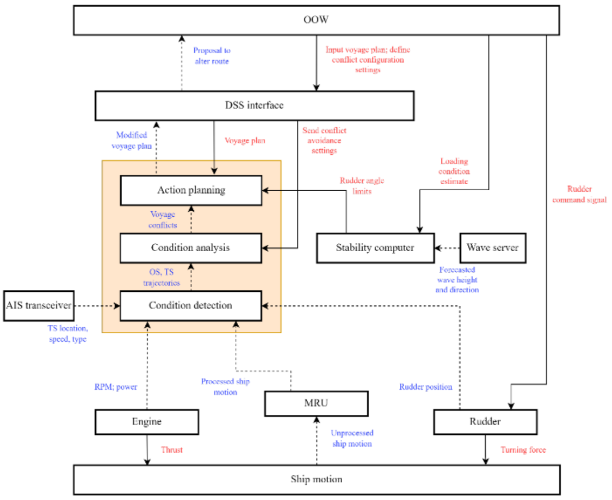

Figure 2. Hierarchical control structure of the DSS.

4.1.4 *Step 1.3: Identify Unsafe Control Actions (UCAs)*

The subsystem of focus for the next two steps of the STPA is the stability computer and its singular control action: "provide rudder angle limits to the conflict resolver". Rudder angle limits are determined by considering the intact stability estimate provided by the OOW at the beginning of the voyage, and dynamic estimates of wave forecast and direction retrieved from the GFS server at periodic intervals. One variable that cannot be measured by the system is the true value of the ship's intact stability. Instead, the system relies upon the estimate of the loading condition provided by the OOW.

Table 1 presents the identified unsafe control actions for the stability computer. Based on the estimate of intact stability and the environmental conditions received, the stability computer decides the maximum possible rudder angles for an evasive maneuver. Evasive maneuvers with higher rudder angles will be considered for high intact stability and low wave height. Conversely, the range of rudder angles decreases for estimates of low intact instability and forecasts with high wave height.

Table 1. Identified UCAs of the stability computer

Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
UCA-1: Stability computer does not provide rudder angle limits [H-2.2].	UCA-2: Stability computer provides excessively lenient rudder angle limits [H-1.1, H-2.2].	UCA-3: Stability computer provides proper rudder angle limits after evasive maneuver is initiated [H-1.1, H-2.1].	UCA-4: Stability computer removes rudder angle limits during evasive maneuver [H-2.1].
	UCA-5: Stability computer provides excessively strict rudder angle limits [H-1.2, H-2.1].		UCA-6: Stability computer maintains rudder angle limits after execution of evasive maneuver [H-1.1].

4.1.5 *Step 1.4: Identify Loss Scenarios (LSs)*

Loss scenarios (LS) are generated to determine causal failures that can lead to unsafe control actions. For conciseness, we focus on UCA-2: "Stability computer provides excessively lenient rudder angle limits [H-1.1, H-2.2]." Two example loss scenarios are presented below.

LS-2-1: Wave forecast information underpredicts the significant wave height. For the predicted wave height, the stability computer underpredicts the expected roll motion of the ship, and provides lenient rudder angles limits. This allows for performing an evasive maneuver at a rudder angle that leads to excessive roll motion of the vessel. [H-2.2].

LS-2-2: At the beginning of the voyage, the OOW provides the weight and location estimate which results in an overpredicted measure of intact stability. For the estimated ship stability condition, the stability computer provides lenient rudder angle limits for the given wave forecast information. This leads to excessive roll motion of the vessel [H-2.2].

Loss scenarios provide context for developing performance tests of system's functions. For LS-2-1, we identify that the accuracy of forecast information impacts the ability of the controller to provide adequate rudder angle limits. LS-2-2 identifies the presence of an unmeasured PV within the system: the ship's actual stability. The difference between the ship's actual and predicted intact stability may contribute to a loss of the vessel.

4.2 *Step 2: Integration Testing*

4.2.1 *Step 2.1: Functional Testing*

The first step is the identification of the PVs that contribute to the unsafe control action. For UCA-2: "Stability computer provides excessively lenient rudder angle limits [H-1.1, H-2.2]", the variables of interest are the target ship presence (PV-1), rudder angle limits (PV-2), predicted ship intact stability (PV-3), and forecasted wave height (PV-4). Furthermore, two variables exist but are unobserved by the system: the observed intact stability and wave height. Therefore, PVs-3 and -4 are revised: these are instead presented as the differences between the observed and predicted intact stability (PV-3) and wave height (PV-4).

The functional test is developed for the requirement of the system to provide adequate rudder angle limits.

Functional Test: Adequate rudder angle limits are correctly provided during operation.

- Objective: To assess the provision of rudder angle limits during system operation.
- Setup: Utilize simulation test-bed. The test-bed should include a six degree-of-freedom hydrodynamic model of the ship with its actuators in addition to a world model that can consider waves and wind forces. Review code for generating rudder angle limits from lookup tables.
- Execution: Initiate sailing with a given forward speed, given sea-state, and a planned obstacle conflict. Evaluate rudder angle provision for all expected stability conditions (PV-3) and wave heights (PV-4). Repeat for various obstacle configurations (PV-1).
- Evaluation: Review the provided rudder angle limits by the stability computer. Ensure that rudder angle limits are updated when new forecast information is retrieved by the system. System should recognize latent information and display information through DSS that wave forecast information is delayed. Observe failure tolerant behavior and appropriate display information on the DSS interface.

4.2.2 *Step 2.2: Performance Testing*

The performance test is developed for LS-2-2. The evaluation of performance is derived from the assessment of PVs that contribute to the LS. The PV of primary interest is the difference in predicted and actual ship stability (PV-3).

Performance Test: Analyze rudder angle limit provision behavior for over- and under-predicted ship intact stability (LS-2-2).

- Objective: Quantify the behavior of the system for under estimates and over-estimates of the ship's intact stability.
- Setup: Utilize simulation test-bed. As before, the test-bed should include the hydrodynamic model of the ship and actuators. The fidelity of the world model should be reduced to allow for faster computation. Review code for generating rudder angle limits from lookup tables.
- Execution: Initiate sailing with a given forward speed, planned obstacle conflict, and ratio of estimated to actual ship intact stability (i.e., ratios greater than one indicate over-prediction). Repeat for range of ratios. Repeat for various sea-states, forward speeds, and time delays.
- Evaluation: Quantify the ratio of rudder angle limits for the estimated and actual intact stability. Investigate the necessity of safety margins to increase the rudder angle limits for various forward sailing speeds.

4.2.3 *Use of integration tests*

The test cases presented here reflect an application of the methodology to a section of the system of study. A larger scale analysis would identify a larger number of tests to assess system functionality and performance.

5 DISCUSSION

5.1 *Methodological implications*

The approach demonstrates the development of integration testing for system verification. The development of the hierarchical control structure allows for the visualization of control and feedback for system behavior analysis. Modeling the system as a control system ensures a focus on system behavior, and the results of STPA steps 3 and 4 reveal interactions among components that are not immediately apparent. Furthermore, the interactions are modeled across human, hardware, and software aspects of system design. The method allows for determining key variables that should be investigated and tested during integration testing.

Performing STPA at an early stage of system development can identify key aspects of integration well in advance of the verification process. The traditional V-model delays verification until after the coding has been finalized. However, design changes towards the beginning of a project are often less costly than those implemented towards the end.

The use of digital testing requires additional considerations that are not explored here in detail. The use of a hydrodynamic model requires extensive development, and validation of the model should be achieved using full-scale data for the vessel, if possible [25].

5.2 *Limitations of the study*

The approach requires background knowledge on the system's purpose, structure, and operation. Furthermore, STPA is a labor intensive methodology. New research has studied the synthesis of STPA with systematic methods for test generation. These include automatic scenario generation [26] and conformance and fault injection (CoFI) [27]. For the purpose of integration, such methods could be directed towards the result of an input/output analysis for a controller.

5.3 *Recommendations for future research*

The approach complements simulation as a method of verification for autonomous systems. Future work could describe the test-bed and setup of the simulation test-bed. The research can be further extended to include an analysis of the testing results. Additional work would focus on how the results of the simulations impact the system's operation, and describe any modifications to the system structure. If the results of testing are found to improve system design, the methodology should be iterative to incorporate changes to system structure and behavior. For example, the introduction of a system to estimate the vessel's intact stability [28] would have to be modeled in the revised control hierarchy. The analysis should be modified to include the effects of any design changes, as they could potentially introduce emergent behavior to the system.

6 CONCLUSION

This paper has demonstrated the use of STPA to analyze system behavior and identify test cases for system operation. Requirements for verification of critical systems fall into two categories: failure handling and integration testing. The method was applied to a decision support system for collision avoidance focusing specifically on stability monitoring for collision avoidance. The hierarchical control structure demonstrates the relationships between controllers, and the UCAs and LSs were used to suggest functional and performance integration tests for the stability computer as a case study.

STPA is uniquely positioned to analyze the hazards related to integration of complex systems of systems. Modeling the system as a control structure presents a structured approach to identify interactions among controllers. Furthermore, due to its flexibility, it can be used at early stages of system development. The use of the method can lead to more robust design of safety critical systems.

ACKNOWLEDGMENTS

The work has been performed as part of the Detection, prediction, and solutions for safe operations of MASS (ENDURE) project (number NOR/POLNOR/ENDURE/0019/2019–00), supported by the Polish National centre for Research and Development and financed by Research Council of Norway. Research supported in part by the Research Council of Norway through SFI Autoship (RCN 309230).

REFERENCES

[1] M. Gil, K. Wrobel, J. Montewka, F. Goerlandt, A bibliometric analysis ´ and systematic review of shipboard Decision Support Systems for accident prevention, Safety Science 128 (2020) 104717. doi:10.1016/j.ssci.2020.104717.

[2] IEEE, IEEE Standard for System, Software, and Hardware Verification and Validation, Technical Report, 2017. Conference Name: IEEE Std 1012-2016 (Revision of IEEE Std 1012-2012/ Incorporates IEEE Std 1012-2016/Cor1-2017).

[3] DNV, Rules for Classification: Ships, Technical Report DNV-RU-SHIP, 2022.

[4] DNV, Class Guideline: Autonomous and remotely operated ships, Technical Report DNV-CG-0264, DNV, 2021.

[5] R. Skjetne, O. Egeland, Hardware-in-the-loop testing of marine control system, Modeling, Identification and Control: A Norwegian Research Bulletin 27 (2006) 239–258. doi:10.4173/mic.2006.4.3.

[6] O. Smogeli, J. E. Skogdalen, Third Party HIL Testing of Safety Critical Control System Software on Ships and Rigs, OnePetro, 2011. doi:10. 4043/22018-MS.

[7] T. A. Pedersen, J. A. Glomsrud, E.-L. Ruud, A. Simonsen, J. Sandrib, B.-O. H. Eriksen, Towards simulation-based verification of autonomous navigation systems, Safety Science 129 (2020) 104799. doi:10.1016/j. ssci.2020.104799.

[8] K. Wrobel, J. Montewka, P. Kujala, Towards the development of a system-theoretic model for safety assessment of autonomous merchant vessels, Reliability Engineering & System Safety 178 (2018) 209–224. doi:10.1016/j.ress.2018.05.019.

[9] N. Leveson, J. Thomas, STPA Handbook, https://psas.scripts.mit.edu/home/get file.php?name=STPA handbook.pdf, 2018.

[10] R. Patriarca, M. Chatzimichailidou, N. Karanikas, G. Di Gravio, The past and present of System-Theoretic Accident Model And Processes (STAMP) and its associated techniques: A scoping review, Safety Science 146 (2022) 105566. doi:10.1016/j.ssci.2021.105566.

[11] N. A. Zikrullah, H. Kim, M. J. van der Meulen, G. Skofteland, M. A. Lundteigen, A comparison of hazard analysis methods capability for safety requirements generation, Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability 235 (2021) 1132–1153. doi:10.1177/1748006X211003463, publisher: SAGE Publications.

[12] R. Yang, I. B. Utne, Towards an online risk model for autonomous marine systems (AMS), Ocean Engineering 251 (2022) 111100. doi:10.1016/ j.oceaneng.2022.111100.

[13] B. Rokseth, I. B. Utne, J. E. Vinnem, A systems approach to risk analysis of maritime operations, Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability 231 (2017) 53–68. doi:10.1177/1748006X16682606.

[14] B. Rokseth, I. B. Utne, J. E. Vinnem, Deriving verification objectives and scenarios for maritime systems using the systems-theoretic process analysis, Reliability Engineering & System Safety 169 (2018) 18–31. doi:10.1016/j.ress.2017.07.015.

[15] B. Rokseth, O. I. Haugen, I. B. Utne, Safety Verification for Autonomous Ships, MATEC Web of Conferences 273 (2019) 02002. doi:10.1051/ matecconf/201927302002, publisher: EDP Sciences.

[16] N. Leveson, Engineering a Safer World: Systems Thinking Applied to Safety, Engineering systems, MIT Press, Cambridge, Mass, 2011.

[17] NTSB, Capsizing of Roll-on/Roll-off Vehicle Carrier Golden Ray, St. Simons Sound, Brunswick River, near Brunswick, Georgia, September 8, 2019 (2020).

[18] H. Kim, S. Haugen, I. B. Utne, Assessment of accident theories for major accidents focusing on the MV SEWOL disaster: Similarities, differences, and discussion for a combined approach, Safety Science 82 (2016) 410– 420. doi:10.1016/j.ssci.2015.10.009.

[19] E. V. Lewis, Principles of naval architecture, 2nd revision (3rd ed.) ed., Society of Naval Architects and Marine Engineers, Jersey City, 1988. OCLC: ocm37002765.

[20] P. Krata, T. Hinz, S. A. Dugan, M. Marley, J. Montewka, Prediction and Evaluation of an Angle of Heel due to Turning Maneuver of Small Training Ships: Comparison of Dynamic Analysis and Static Design Criteria, in: Proceedings of the 15th International Symposium on Practical Design of Ships and Other Floating Structures, 2022.

[21] J. Montewka, P. Krata, T. Hinz, M. Gil, K. Wrobel, Probabilistic model estimating the expected maximum roll angle for a vessel in the turn (2022) 10.

[22] K. Wrobel, M. Gil, P. Krata, K. Olszewski, J. Montewka, On the use ′ of leading safety indicators in maritime and their feasibility for Maritime Autonomous Surface Ships, Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability (2021) 1748006X211027689. doi:10.1177/1748006X211027689, publisher: SAGE Publications.

[23] M. Gil, J. Montewka, P. Krata, T. Hinz, S. Hirdaris, Determination of the dynamic critical maneuvering area in an encounter between two vessels: Operation with negligible environmental disruption, Ocean Engineering 213 (2020) 107709. doi:10.1016/j.oceaneng.2020.107709.

[24] M. Gil, A concept of critical safety area applicable for an obstacleavoidance process for manned and autonomous ships, Reliability Engineering & System Safety 214 (2021) 107806. doi:10.1016/j.ress. 2021.107806.

[25] K. H. Chua, S. Coutinho, A. Norahim, D. Konovessis, Development of Recommendations for Digital Testing of MASS Navigation Safety prior to Sea Trials, Journal of Physics: Conference Series 2311 (2022) 012025. doi:10.1088/1742-6596/2311/1/012025.

[26] T. A. Pedersen, A. Neverlien, J. A. Glomsrud, I. Ibrahim, S. M. Mo, M. Rindarøy, T. Torben, B. Rokseth, Evolution of Safety in Marine Systems: From System-Theoretic Process Analysis to Automated Test Scenario Generation, Journal of Physics: Conference Series 2311 (2022) 012016. doi:10.1088/1742-6596/2311/1/012016.

[27] C. M. Hirata, A. M. Ambrosio, Combining STPA With CoFI to Generate Requirements and Test Cases for Safety-Critical System, IEEE Systems Journal 16 (2022) 6635–6646. doi:10.1109/JSYST.2022.3200586, conference Name: IEEE Systems Journal.

[28] L. Santiago Caamano, M. Miguez Gonzalez, S. Allegue Garcia, V. Diaz Casas, Evaluation of onboard stability assessment techniques under real operational conditions, Ocean Engineering 258 (2022) 111841. doi:10.1016/j.oceaneng.2022.111841.