Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P232-cd

Identifying Test Scenarios for Simulated Safety Demonstration using STPA and CAST

Raffael Wallner[1,*], Bjørn Axel Gran[2,†], Tom Arne Pedersen[3,‡], Tor Arne Johansen[4,*], Mary Ann Lundteigen[5,*]

[*] *Department of Engineering Cybernetics, Norwegian University of Science and Technology, Norway.*
[†] *Risk, Security and Physical Science, Institute for Energy Technology (IFE), Norway.*
[‡] *Group Research and Development, Det Norske Veritas (DNV), Norway.*
E-mail: [1] *raffael.wallner@ntnu.no,* [2] *bjorn.axel.gran@ife.no,* [3] *tom.arne.pedersen@dnv.com,*
[4] *tor.arne.johansen@ntnu.no,* [5] *mary.a.lundteigen@ntnu.no*

Assuring safety for new technologies like a Maritime Autonomous Surface Ship (MASS) or an Uncrewed Surface Vessel (USV) is challenging due to their complexity and varying operational environments. Safety demonstrations in simulations may be used to verify operational safety, but it is impossible to test all possible scenarios. The paper proposes an approach to identify critical scenarios for scenario-based safety demonstrations based on System Theoretic Process Analysis (STPA). STPA studies the whole system including interactions between components in the hazard analysis and is, therefore, well-suited for systems like MASS or USV, involving interactions of multiple components, sub-systems, the environment, and humans. The presented approach identifies critical scenarios using STPA and generates simulation scenarios from the identified critical, as well as presumably safe, scenario spaces. In case of incidents or unexpected critical scenarios that have been uncovered during the simulated tests, a Causal Analysis using System Theory (CAST) is conducted. Thus, it is possible to improve safety in new design iterations based on the results of the evaluation. The proposed approach is demonstrated in a simplified example of a USV during remote operations.

Keywords: Safety Demonstration, STPA, CAST, Scenario Identification, Automation, Autonomous System, Autonomous Ship, MASS, Test and Verification

1. Introduction

Generally, demonstrating and assuring safety is important both for simple systems with few components and dedicated functionality as well as for large, complex, and versatile systems like a Maritime Autonomous Surface Ship (MASS), or an Uncrewed Surface Vessel (USV), featuring a high degree of automation or autonomy. While for simple, comprehensible systems it might be straightforward to evaluate the risk of component failures or usage errors, systems like MASS or USV pose particularly difficult challenges in the process of safety assurance. That is due to a large number of involved components, subsystems, and software as well as due to complex interactions; considering intended and unintended interactions among the system components or subsystems as well as with humans and the environment. Additionally, the desired operational environments may vary significantly in several aspects and the system needs to meet the safety standards in a huge number of possible operational scenarios (Koopman and Wagner, 2016; Wallner and Lundteigen, 2022). Moreover, it may be impossible to ensure that mechanisms have no side effects without testing a large number of scenarios. This is illustrated in a case where one sub-system will shut down in case of a failure and another sub-system will restart the system to maintain operation. Assessed individually both failures are handled well, but when run in operation or simulations it will lead to a never-ending loop.

Those challenges in assessing and demonstrating safety cannot, or only insufficiently, be solved by purely conventional approaches, as pointed out in Leveson et al. (2016) and Rokseth et al. (2017). Approaches demonstrating and verifying the safety of such systems include, e.g., running scenario-based tests with the system and evaluating the performance in terms of safety. Depending on the design and production state, scenario-based testing of MASS or USV may be per-

formed physically, with the real ship in the real-world or dedicated closed test facilities as well as in simulated or hybrid environments, either of the environments having certain advantages and shortcomings (Pedersen et al., 2020; Wallner and Lundteigen, 2022). The approaches in this paper focus on testing USV in simulations. One of the key benefits of simulations is the eliminated risk of harming humans, facilities, or the environment during testing. This is particularly important given the potential safety hazards that can arise when testing critical scenarios with such new and not yet well-tested technologies. In addition, simulation testing is less costly than physical testing since it does not require expensive test facilities or the actual ship and it can be done faster than real-time. This can result in significant cost savings for ship designers and manufacturers. Moreover, simulation testing allows for the testing of MASS or USV at an early stage of the design process, making it possible to identify and address potential issues before the ship is built.

Identifying the right scenarios for scenario-based testing is crucial to ensure that, e.g., a USV is capable of handling any situation it may face during operation. While simulations can provide a safe environment for testing even faster than in real-time, it is still impossible to simulate every possible scenario. It must be shown that the USV is able to handle a wide variety of scenarios, ranging from planned operations in calm waters to emergencies in extreme sea states, to ensure safety and reliability. Therefore, it is important to choose scenarios that are representative of the types of situations that a USV is likely to encounter.

This paper presents an approach to the identification of test scenarios for safety demonstrations utilizing Systems-Theoretic Process Analysis (STPA) and Causal Analysis using System Theory (CAST) based on System-Theoretic Accident Model and Processes (STAMP) (Leveson, 2016). Section 2 presents related research projects supporting the interest in and significance of the research field. In Section 3 STPA and CAST are described. Their use for the identification of test scenarios is presented in Section 4 for the example of a USV in operations involving a Remotely Operated Vehicle (ROV) and a Remote Operation Center (ROC). Section 5 concludes and proposes future steps.

2. Related Work

In Wallner and Lundteigen (2022) challenges in the process of safety assurance of autonomous systems are pointed out. Accordingly, they propose simulated safety demonstrations including the utilization of digital twins to approach some of these challenges. A prototype for simulation-based testing of autonomous navigation systems of ships including the use of digital twins, dynamic test scenario generation, and test scenario evaluation is presented in Pedersen et al. (2020). Both works mention the importance of sophisticated approaches for identifying simulation scenarios to achieve confidence about the safety of the system. Zhang et al. (2022) introduced a taxonomy for critical scenario identification for scenario-based verification processes in automated driving based on a comprehensive literature review. In Rokseth et al. (2017) an insufficiency in the risk assessment of complex systems like autonomous ships with conventional methods has been pointed out and the benefit of a systems approach like STPA has been shown. Abrecht (2016) showed the suitability and advantages of STPA and CAST in applying them on marine vessels. Rokseth et al. (2019) presented the use of STPA for the identification of critical scenarios and regarding safety requirements for autonomous ships as well as a safety verification program. In a case study, the presented methodology is shown to be feasible for the intended purpose. A methodology for automated testing by using Signal Temporal Logic (STL) for formulating simulation requirements and automated evaluation along with the use of Gaussian Process (GP) to estimate robustness and uncertainties is presented in Torben et al. (2022). This methodology using STL and GP was applied in Pedersen et al. (2022) after safety constraints and requirements for automated maritime systems have been identified by using STPA. Moreover, also Johansen et al. (2023) applied the automated testing approach for a risk-based control system for autonomous ships.

3. Methods

Traditional and widely used methods for risk analysis are Fault Tree Analysis (FTA) or Failure Mode, Effects, and Criticality Analysis (FMECA) (Pilot, 2002; Borgovini et al., 1993). They use the principle of undesired events being traced down to component failures and vice versa analyzing the consequences of erroneous modes of components through chains of failures. Thoroughly applying those methods has worked well for a majority of analyzed systems in the last decades. However, in recent years, systems are increasingly more complex, involving software-intensive processes, featuring increasing automation or autonomy, and, at the same time, still need to take human factors into account. The interplay of so many different influencing factors, components, and sub-systems places a whole new challenge in terms of risk and hazard analysis. Hence, conventional methods are no longer able to always provide a comprehensive analysis (Leveson et al., 2016; Rokseth et al., 2017).

3.1. *STAMP based approaches*

A recent and holistic approach for analyzing such complex and diverse systems is provided by methods based on STAMP introduced by Nancy Leveson (Leveson, 2016) as a model to analyze hazards and accident causation based on system theory. STAMP provides an approach treating the prevention of undesired scenarios as a control problem rather than a problem of reliability of components. STAMP also covers accidents occurring even though there are no failing components, i.e. also accidents that might have been caused by design errors, flawed requirements, human interactions, and so-called emerging properties, which are a result of interactions between different systems. Hence, STAMP-based approaches are well suited for the application of large and complex systems like MASS or USV.

STPA and CAST are STAMP-based methods. STPA is used for the analysis of the safety of a system to uncover possible hazards and hazardous events, whereas CAST is a method for the analysis of accidents that have occurred and to identify causal events.

3.2. *STPA & CAST workflow*

In Leveson (2016) and Leveson and Thomas (2018) the following definitions are used:

Accident: An undesired and unplanned event that results in a loss.

Loss: A loss involves something of value to stakeholders. Losses may include a loss of human life or human injury, property damage, environmental pollution, loss of mission, loss of reputation, loss or leak of sensitive information, or any other loss that is unacceptable to the stakeholders.

Hazard: A system state or set of conditions that, together with a particular set of worst-case environment conditions, will lead to an accident (loss).

The workflow of an STPA analysis as described in Leveson and Thomas (2018) is split up into four steps as follows: (1) Define the purpose of the analysis; (2) Model the control structure; (3) Identify unsafe control actions; and (4) Identify loss scenarios.

The workflow of a CAST analysis consists of the five following steps, see Leveson (2019): (1) Assemble basic information; (2) Model the control structure; (3) Analyze each component in loss; (4) Identify control structure flaws; and (5) Create an improvement program.

Preparation: For an STPA it is necessary to define the purpose, declaring the system boundaries, goals, losses, and hazards that should be taken into account. For a CAST analysis, the investigated accident implicitly defines the loss. Consequently, all information about the accident needs to be collected to reconstruct the accident.

Modelling: The modeling of the control structure is the same for both methods and is based on prior collected information and declarations of the investigated system to be modeled. Interactions between components and sub-systems are generally represented by control actions (CA) and feedback (FB). Relevant external information or data flows (DF) may be included as well.

Analysis: In an STPA analysis, the aim is to identify loss scenarios, caused by so-called unsafe control actions (UCA) or generic systematic flaws. UCAs are interactions in the control struc-

ture that potentially lead to one of the considered losses. Generic design flaws in the hierarchy may cause losses even without failing components or UCAs. A CAST analysis aims to analyze each component of the modeled control structure in the loss scenario. Therefore, the role of each component is determined and undesired behavior is identified and explained. The fourth step during a CAST analysis is to identify flaws in the control structure itself in case generic systemic factors contributed to the accident. In the final step, an improvement program is created as an output of the CAST analysis that may contain recommendations for structural changes to prevent similar accidents in the future.

4. Identification of Test Scenarios using STPA and CAST

In order to identify a feasible but comprehensive subset from an infinitely large set of possible operational scenarios for scenario-based testing and safety demonstrations, a holistic view of the system is necessary. The approach presented in this work is to (1) identify critical scenarios using STPA to (2) evaluate the safety of identified critical scenarios in simulations. Complementing the evaluation, (3) additionally, samples from the presumably less critical scenario space are simulated to allow uncovering hazards not considered in the prior analysis. In the case of unexpected incidents in the simulations, (4) a CAST analysis is conducted. For the application during the design phase of a USV or during mission planning of operations, the results of the CAST analysis can propose (5) design improvements or updates of the mission strategy, respectively.

The investigated system in this work is a USV with autonomous features in remote operations. To start analyzing the safety of a system, it is crucial to first define the system of interest and its scope. In this work, a representative example of a USV has been selected. Fig. 1 shows a simplified visualization of the operation setup. The USV is capable of transporting, launching, and recovering a tethered ROV, and can operate in both remotely controlled and autonomous modes. During autonomous operations, when the autonomous control system (ACS) is generating motion Control Actions (CA), the USV can receive destinations or specific waypoints from the ROC or follow the ROV during a mission. During the manual modes, the human operators in the ROC send the motion CAs. For this demonstration, the scope is focused on evaluating the USV's ability to autonomously follow the ROV and maintain a safe distance based on the current conditions. Specifically, the evaluation aims to ensure that the USV maintains a distance leaving adequate safety margins to the maximum range of the tether or umbilical cable during the ROV survey task. Additionally, the USV needs to be able to limit or abort the mission if safety margins cannot be met.

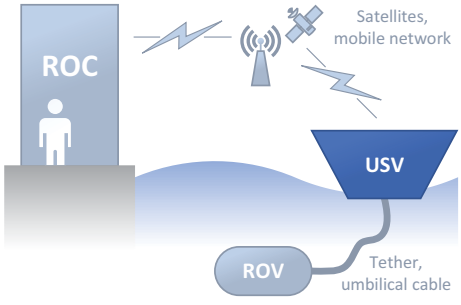

Fig. 1. A USV following an ROV that is controlled from a ROC.

4.1. *Safety analysis using STPA*

A full STPA would include a large number of possible losses, and inherent analysis paths to investigate. Therefore, only selected paths are pursued. The focused scope and selective STPA allow a brief but effective demonstration of the proposed approach for evaluating the safety of autonomous USVs.

Purpose of analysis: The possible scenario space is limited to the ability of a USV to follow the ROV, i.e., the goal is to stay within a range of the ROV that leaves a sufficient safety margin adequate for the currently unwound length of the tether or umbilical cable under the prevailing conditions. Possible losses are formulated as follows:

L-1 Damage to the tether/umbilical cable

L-2 Damage to the USV
L-3 Interruption of mission

A few of the system-level hazards that may lead to one or more of the losses (in parenthesis) are:

H-1 The USV does not follow the ROV with the required safety margin to the maximum range of the tether (L-1,L-3)
H-2 The USV moves away from the ROV violating the required safety margin to the maximum range of the tether (L-1,L-3)
H-3 The tether is wound up violating the required safety margin to the maximum range of the tether w.r.t. the current distance to the ROV (L-1,L-3)

To each hazard, a system-level safety constraint is assigned:

SC-1 The USV must follow the ROV leaving enough safety margin to the maximum range of the tether
SC-2 The safety margin for the current distance to the ROV must be maintained when winding up the tether

Modelling of control structure: A simple structure of the control hierarchy for the considered USV in an operation deploying an ROV that is controlled from a ROC is shown in Fig. 2. The actual USV (USV hull) is moving based on applied thruster forces and influence from disturbances and interactions with the ROV. The Propulsion System (PS) is controlling the thrusters based on motion CAs. The motion control happens in a feedback loop with either the ROC in the manual operation mode or the ACS in one of the autonomous operation modes. CAs in those feedback loops include desired directions and velocities and the Feedback data (FB) provides information about the thruster load and reserve, as well as the feasibility of the CA from the PS. The Situational Awareness System (SITAW) collects internal states like system health or energy levels, the measured movement of the USV, as well as external states based on the environmental perception via sensors. The collected and preprocessed information is forwarded to the ACS and the ROC as higher-level FB. The ACS is responsible for deciding on CAs based on internal and external states received from the SITAW and waypoints or mission goals from the ROC during autonomous operation modes. For example, when following the ROV, the ACS has to generate CAs, for the USV to stay within a safe range of the ROV. Therefore, the current conditions and the health and energy state of the USV determine the mobility capabilities of the USV and the necessary safety margin before reaching the maximum range of the tether/umbilical cable. In case the safety requirements cannot be met, the ACS needs to limit the ROV's speed and inform the ROV operator in the ROC about the limiting conditions. During manual modes with remote motion control from the ROC, the ACS operates as an assistant, updating the human operator in the ROC with useful information and intervening in emergency situations. Human operators in the ROC control the USV in manual mode, the ROV, and the mission. The human operators are provided with real-time or low-latency FB including camera pictures and movement data in order to decide on CAs for the USV and ROV. Moreover, high-resolution data and higher-level FB with system states are sent to the ROC for operational decisions and data collection. In case of critical situations, the ROC receives warnings and information about limited conditions from the USV. The communication and data transfer happens via the tether to the USV and the communication link of the USV to the ROC. Further optional automated functions of the ROV include following predefined paths or survey targets like deep-sea cables or pipelines. The maximum speed and the mobility range of the ROV need to be adapted to the mobility of the USV and vice versa, which is communicated between the USV and the ROV.

Identifying unsafe control actions: The third step of an STPA is to identify UCAs. Therefore, the CAs in the modeled system are investigated w.r.t. the four modes of unsafe control mentioned in Leveson and Thomas (2018): (1) Not providing the CA leads to a hazard. (2) Providing the CA leads to a hazard. (3) Providing a potentially safe CA but too early, too late, or in the wrong

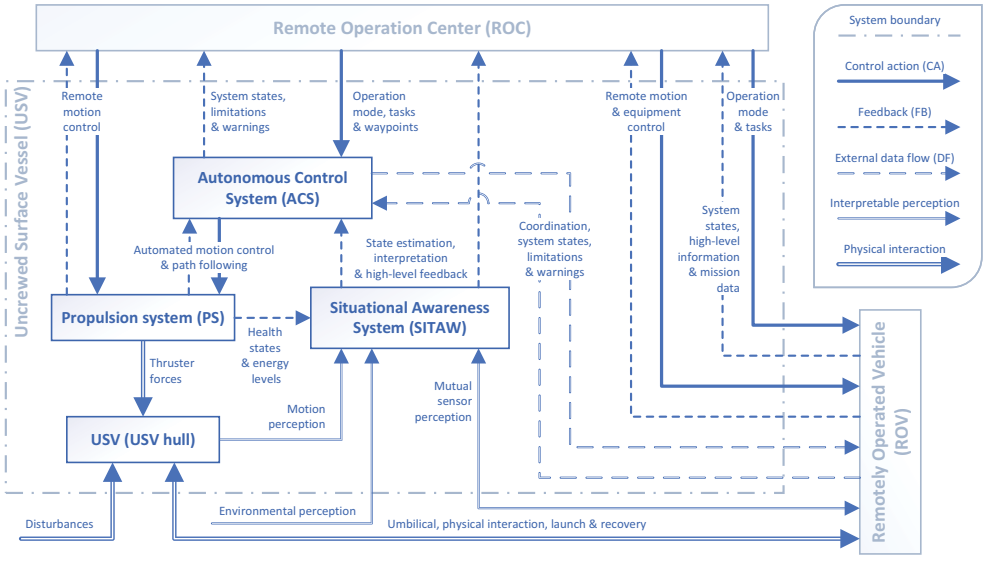

Fig. 2. A simple control structure for a USV in operation.

order. (4) The CA lasts too long or is stopped too soon. To analyze the *Automated motion control & path following* CAs between the ACS and the PS in Fig. 2, they first need to be defined more concretely. The PS receives commands/CAs about the desired movement of the USV from the ACS including, e.g., desired course and velocity along with limits for several control variables and states. In case the USV is autonomously following the ROV which is accelerating within its allowed boundaries, the ACS needs to provide an acceleration CA to the PS increasing the desired velocity, such that the USV keeps up with the ROV. Considering this interaction, the following UCAs might occur:

UCA-1 ACS does not provide an acceleration CA when the ROV is faster and ahead of the USV (H-1)

UCA-2 ACS provides an acceleration CA even though the ROV is neither faster nor ahead of the USV (H-2)

UCA-3 ACS provides a too-high acceleration CA while the ROV is accelerating (H-2)

UCA-4 ACS provides an acceleration CA while the ROV is heading in a different direction than the USV (H-2)

UCA-5 ACS provides an acceleration CA too late after the ROV has already been faster and ahead of the USV (H-1)

Identifying loss scenarios: In the last step of an STPA, the actual loss scenarios are identified. According to Leveson and Thomas (2018) two questions may be considered to retrieve different types of loss scenarios: (1) Why would UCAs occur? and (2) Why would CAs be improperly or not executed, leading to hazards? Further investigating UCA-1, some possible loss scenarios are:

LS-1 The hardware of the ACS fails while the ROV is accelerating (UCA-1, H-1)

LS-2 The ACS does not issue an acceleration CA due to a missing notification about the ROV accelerating (UCA-1, H-1)

LS-3 A late recognized collision hazard forced the USV to perform a sudden emergency maneuver while the ROV is accelerating (H-1, H-2)

LS-1 and LS-2 are examples of UCAs occurring, while LS-3 is caused by missing mitigation of emergency maneuvers with the ROV at the range limit or missing adaption to areas with collision hazards such sea ice.

4.2. *Identification of test scenarios*

The identified loss scenarios are then used as the source for test scenarios for scenario-based safety demonstrations. The derived test scenarios need to challenge the associated loss scenario to test the actual behavior, the consequences, or if the problem has been mitigated. As an example, based on LS-3, a series of test cases with sudden emergency maneuvers of the USV can be implemented to determine if the ACS properly adapts the safety margins for the maximum range of the tether, such that at any time it is possible to perform those maneuvers. The test scenarios need to cover limit cases with the ROV at the boundary of the safety margin to test the worst-case conditions. Moreover, they may cover situations with the ROV outside its desired range to determine the robustness of the safety margins w.r.t. uncertainties in the position or violations of the operational boundaries. Additionally, e.g., a naive search method from Zhang et al. (2022) may be used to sample from the safe scenario space.

4.3. *Incident analysis using CAST*

Ideally, there are no severe or unexpected incidents in the simulation of chosen scenarios. Expected incidents may occur in scenarios outside the operational limits when testing boundary conditions. In any incident case, to rule out overlooked hazards, a brief investigation w.r.t. the causes is required. A thorough investigation is needed for unexpected incidents or causes. CAST (Leveson, 2019) is proposed as a suitable tool for that analysis.

As an example for the chosen case study, the following test scenario and discovered loss scenario are assumed: In order to challenge the handling emergency maneuvers, which was identified as critical in loss scenario LS-3, several test scenarios with situations with emergency maneuvers are tested. Design updates mitigated the problems identified in the prior analysis. However, in a test scenario including an induced connection problem delaying the warning about the speed limit. That caused an accident with the human operator not being able to react in time and the ROV being pulled off track, hence resulting in L-3.

Assemble basic information: In the first step of CAST, the analyzed system, its scope, losses, hazards, and preventive system-level safety constraints must be defined and all information about the accident must be collected, including, e.g., simulation logs and human operator interviews. Using the definition of the STPA analysis, the occurred loss can be defined as L-3, the hazard as H-2, and the safety constraint as SC-1.

Model the control structure: In the second step, the investigated system has to be modeled. It is possible to reuse the modeled control hierarchy in Fig. 2 and described in Section 4.1.

Analyze each component in loss: Next, each involved component is investigated during the accident. A brief description of the components' roles is: *SITAW* informs ACS about obstacles and is aware of current maneuverability and data connection; *ACS* issues an emergency break and sends the required speed limit to ROC and ROV; *ROC* does not receive the speed limit in time and the human operator cannot react; *ROV* follows the instructed speed from the ROC but does not automatically follow the speed limit from ACS. Hence, an uncovered undesired behavior is that the ROV prioritizes the command of the ROC over the speed limit of the ACS.

Identify control structure flaws: A structural flaw that the CAST analysis may point out in addition is, that the SITAW should warn about the bad connection, forcing lower operation speeds.

Create an improvement program: Based on the CAST results, the problem of the neglected speed limit must be mitigated. It may also be considered to force lower speeds due to bad connections.

4.4. *Discussion and evaluation*

The results of the brief analysis show, how the approach can contribute to increasing confidence about safety in critical scenarios by being able to uncover even unconsidered hazards. For a demonstration of compliance with certain safety requirements, relevant industry standards, and class rules or guidelines, those have to be considered in the

STPA as well as in the generation of scenarios. For example, losses may be defined as failed safety shutdown or lost operability in case of single-point failures, when testing resilient maritime systems. Further considerable factors for test cases are, e.g., metocean conditions and weather windows. For the validation of simulation results, representative test cases may be identified for real-world tests.

5. Conclusion

The proposed STPA-based approach allows identifying critical scenarios for safety demonstrations for complex systems. The condensed case study on a USV demonstrates how to generate simulation scenarios from identified critical and presumably safe scenario spaces to demonstrate safety or challenge the system and uncover overlooked hazards. By conducting a CAST analysis, possible safety improvements are identified.

In further work, sampling test scenarios from certain scenario spaces may be refined, e.g., by using STL. Additionally, previous accidents from other vessels may be analyzed using CAST in order to incorporate those loss scenarios in design improvements. Furthermore, the approach is to be applied to an actual vessel conducting a more comprehensive analysis.

Acknowledgement

This work and the related research project are part of SFI AutoShip, an 8-year research-driven innovation center focusing on safe and sustainable autonomous ship operations. We would like to thank our partners, including the Research Council of Norway under Project number 309230.

References

Abrecht, B. R. (2016). *Systems Theoretic Process Analysis applied to an Offshore Supply Vessel dynamic positioning system*. Thesis, Massachusetts Institute of Technology.

Borgovini, R., S. Pemberton, and M. Rossi (1993, April). Failure Mode, Effects, and Criticality Analysis (FMECA). Technical Report ADA278508, Reliability Analysis Center. Section: Technical Reports.

Johansen, T., S. Blindheim, T. R. Torben, I. B. Utne, T. A. Johansen, and A. J. Sørensen (2023, June). Development and testing of a risk-based control system for autonomous ships. *Reliability Engineering & System Safety 234*, 109195.

Koopman, P. and M. Wagner (2016, April). Challenges in Autonomous Vehicle Testing and Validation. *SAE International Journal of Transportation Safety 4*(1), 15–24.

Leveson, N., C. Wilkinson, C. Fleming, J. Thomas, and I. Tracy (2016, April). A Comparison of STPA and the ARP 4761 Safety Assessment Process. Technical Report, MIT PSAS.

Leveson, N. G. (2016). *Engineering a Safer World: Systems Thinking Applied to Safety*. The MIT Press.

Leveson, N. G. (2019). *CAST handbook*. Cambridge, MA, USA.

Leveson, N. G. and J. P. Thomas (2018). *STPA handbook*. Cambridge, MA, USA.

Pedersen, T. A., J. A. Glomsrud, E.-L. Ruud, A. Simonsen, J. Sandrib, and B.-O. H. Eriksen (2020). Towards simulation-based verification of autonomous navigation systems. *Safety Science 129*, 104799.

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

Pilot, S. (2002, March). What is fault tree analysis? *Quality Progress 35*(3), 120. Num Pages: 1 Place: Milwaukee, United States Publisher: American Society for Quality.

Rokseth, B., O. I. Haugen, and I. B. Utne (2019). Safety Verification for Autonomous Ships. *MATEC Web of Conferences 273*, 02002.

Rokseth, B., I. B. Utne, and J. E. Vinnem (2017, February). A systems approach to risk analysis of maritime operations. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability 231*(1), 53–68.

Torben, T. R., J. A. Glomsrud, T. A. Pedersen, I. B. Utne, and A. J. Sørensen (2022). Automatic simulation-based testing of autonomous ships using Gaussian processes and temporal logic. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability 0*(0), 1–21.

Wallner, R. and M. A. Lundteigen (2022, August). Approaches to Utilize Digital Twins in Safety Demonstration and Verification of Automated and Autonomously Controlled Systems. In *32nd European Safety and Reliability Conference (ESREL 2022)*, Volume 32, pp. 2262–2270.

Zhang, X., J. Tao, K. Tan, M. Torngren, J. Gaspar Sanchez, M. Ramli, X. Tao, M. Gyllenhammar, F. Wotawa, N. Mohan, M. Nica, and H. Felbinger (2022). Finding Critical Scenarios for Automated Driving Systems: A Systematic Mapping Study. *IEEE Transactions on Software Engineering 49*(3), 991–1026.