Advances in Reliability, Safety and Security, Part 2 – Kołowrocki, Magryta-Mut (eds.)
 ISBN 978-83-68136-14-2 (printed), ISBN 978-83-68136-01-2 (electronic)

Advances in Reliability, Safety and Security

ESREL 2024
Monograph Book Series

Risk Based Analysis Of Autonomous System Guidance Of Inland Waterway Vessels

Olena Shyshova, Waldemar Boschmann, Dirk Söffker

Chair of Dynamics and Control, University of Duisburg-Essen, Duisburg, 47057, Germany

Abstract

The ability of vehicles on land, in the air, or on water to behave autonomously/unmanned (without support from outside the vehicle) or automated (with support from outside the vehicle, e.g. by providing behavioral predictions) is one of the central current research and development goals of the related industries. Progress in automotive vehicles, particularly in specific driving tasks, is evident. In inland waterway vehicles, development follows a progression of assistance, automation, and autonomy. Central functionalities like self-localization and behavior prediction are integral at each automation level. Reliability and safety considerations, crucial in a commercial context, differ significantly from maritime seashipping rules. Inland shipping faces distinct challenges, including hazard potential in industrial/residential areas, waterway-related challenges, and the need for precise maneuvering in complex situations like fast-flowing rivers due to the underpowered nature of inland vessels.
The focus of the paper is is mainly related to the FMEA (Failure Mode and Effects Analysis)/FTA (Fault Tree Analysis)-based functional analysis of an example architecture of an autonomous vehicle guidance system but also for the remotely-operated assisted guidance case. Here, modules for vessel localization, object recognition, object trajectory generation, ego vehicle path planning, action option generation, decision making/decision support systems, system integrity checking, diagnosis and prognosis including sensor and actuator monitoring, advanced sensing based on fused approaches are interactively cooperating and therefore considered. The introduced novel risk approach links risks with specific driving scenarios considering hardware and software failures and limitations regarding environmental variables. This facilitates the formulation of requirements for fallback levels, functional limitations, and reliability. The proposed approach aims to replace rigid reliability requirements with dynamic, situation-based requirements that promote both reliability and function-oriented realization. In this contribution, the new approach is presented in detail and illustrated using an example.

Keywords: Autonomous inland vessel, Safe autonomous system, Functional analysis, Situated risk assessment, Perception reliability

1. Introduction

Increasing automation up to a targeted full autonomy system receives rising interest in the shipping industry due to assumed potential to improve efficiency, safety, and environmental protection. The use of autonomous or automated systems in inland navigation has been the subject of several recent studies (Bakhshande et al., 2020; Bolbot et al., 2020; Koschorrek, 2022). Despite the many potential benefits that full automation of inland waterway vessels brings, it also poses several safety-related risks that need to be analyzed and solved. In addition to the usual technical failures and malfunctions, whether due to software errors, hardware failures or communication problems between the various components of the system, this paper focuses primarily on unpredictable or rare situations. Failures/events in these critical situations are characterized by quick decision-making and require special attention. Therefore, a new approach is required that combines existing rigid safety methods with new considerations to generate a situational approach.

In this context, the consideration of the reliability of the system itself and related components or functionalities is essential. The authors in (Lee et al., 2021) investigated the safety of autonomous navigation using FTA (Fault Tree Analysis). A reference system was proposed and MTBF (Mean Time Between Failures) data for key components were collected. A fault tree was developed for the reference system under optimal conditions. Failure probabilities and criticality measures were calculated. Critical components were identified and based on the analysis, design recommendations were given. The key findings of (Lee et al., 2021) are: ANS (Autonomous

Navigation System) and its systems to generate technical situation awareness are responsible for navigation failures. Conventional navigation systems and sensors were deemed noncritical in good weather and daylight conditions. In (Luo et al., 2022), FMECA (Failure Mode and Effects and Criticality Analysis) is combined with DEMATEL (Decision-Making Trial and Evaluation Laboratory) to analyze ship positioning system failures. The authors state specific components like the high-accuracy attitude sensor are highly unreliable mainly caused by environmental factors and other influences which cannot be detailed. The conclusions are integrated into the safety design for ship positioning systems. In (Chang et al., 2021), FMEA (Failure Mode and Effects Analysis) is combined with ER (Evidential Reasoning) and RBN (Rule-based Bayesian Network) using fuzzy-rule-based Bayesian reasoning. The assumed hazard categories contributing to overall risk are: i) interaction with manned vessels and detection of objects, ii) cyber-attacks, iii) human errors, and iv) equipment failures. These highest risks result from i) failure in detection of semi-submerged objects followed by ii) failure to determine correct action with vessels, as well as iii) collision due to poor interaction with manned vessels.

In (Abaei et al., 2021), a systematic approach is presented to evaluate and estimate the failure rate of an autonomous system. It offers a quantitative method using a Dynamic Reliability Model. In (Zhang and Zhang, 2023), an Entropy-TOPSIS-Coupling Coordination Model is used to assess navigation risks of autonomous ships introducing a comprehensive navigation risk evaluation index system. In (Basnet et al., 2023), a methodology is presented based on an integrating system theoretic process analysis, a Bayesian network, noisy-OR gates, parent-separation techniques etc.

Comparisons were made between different reliability evaluation approaches applied to an autonomous vessel. While FTA and FMEA assess component-level failures, STPA (System Theoretic Process Analysis) addresses unsafe scenarios resulting from both component-level interactions and systemic factors. However, STPA focuses on hazard identification and does not evaluate risk levels.

Also, STPA and BBN (Bayesian Belief Networks) are integrated in (Johansen and Utne, 2022) applied to control systems for autonomous ships to enable supervisory risk control. As next step the authors intend to develop an online risk model based on the STPA results and BBN. The BBN risk model considers consequences categorized as high, medium, low, or no consequences assuming resulting varying cost as utility variable. The paper includes a sensitivity analysis and a case study but lack of direct relevance to the central question of the underlying reliability evaluation. A risk matrix is developed within a specific operational concept in (Bolbot et al., 2022). The authors propose a novel methodology for developing risk matrices and ratings based on individual and societal risk acceptance criteria and realize risk assessment for autonomous and conventional ships during the early design stage. In (Zhou et al., 2020) the authors discuss six methods out of 28 for evaluating the reliability of autonomous vessels.

Safety requirements are classified into three categories: navigation functions, auxiliary functions, and engineering functions. The clustering results demonstrate which methods are applied to different types of ships.

As the requirements for automation continue to grow, so does the scope of risk consideration. In addition to the usual focus considering physically realized processes and hardware failures, the evaluation of software (with respect to the realized algorithms and functionalities with respect signal to information conversion), as well the human-software interactions are becoming increasingly important. The approach presented here, is not only based on reliability statistics (metrics, values) as common in reliability engineering. The globally accepted methods target the reliability of components as well as systems in order to weight the failure probabilities against the risks in case of failure. This results in numerous advantages based on the diverse, broad, and detailed analysis methods applied to the different fields as well as to the controllability of statistical failure risks, e.g. through generating redundancy. Although the use of this kind of methods in the hardware domain is usual and legitimate, the related approaches aim with selected methods (Rakowsky, 2002; Verma and Karanki, 2016; Stapelberg, 2009; DIN EN IEC 61508, 2011) the (systematic) reliability-technically evaluated controllability of critical components for design situations occurring in the period under consideration with a design probability, but not at the reliability-oriented operational management of safety-relevant systems, which, based on the same basic knowledge, evaluate and address the controllability of a failure situation occurring from a reliability-oriented view. First approaches for such kind of reliability control-oriented approaches are developed in (Söffker, 2000; Söffker and Rakowsky, 1997; Wolters and Söffker, 2005; Bejaoui et al., 2022). Further, the degradation of the functionality with respect to the related increase of the reliabity-related features is allowed for the failure moment. The limited usefulness or correctness of algorithms due to variable operating situations or environmental conditions can be integrated. This requires new approaches, which consider risks that arise in the specific domain due to automation. These risks can be of technical (system failures, sensor errors, and communication errors) or operational (errors in the guidance of the autonomous system, unexpected environmental conditions, or failures in the communication network) nature and - as mentioned - are considered with regard to the reliable controllability of specific critical situations, e.g. can be specified through the application of classical methods of risk-based analysis.

The development of new risk analysis methods will help to analyze and manage situated risks associated with autonomous system guidance and develop strategies to minimize them and therefore represents a step forward to understand and solve the risks related to autonomous systems. The approach is based on an operational scenario from inland vessels. The newly developed strategy in this contribution is briefly introduce and explained using a specific scenario.

The paper is structured as follows: The challenges of the autonomous inland vessel application field and the background of the underlying methods applied, and the adapted concept of dependent functionality are described in Sections 1 and 2. In Section 3.1 first example case of two encountering inland vessels (canal situation) is presented, to which the new method is partially applied. The system architecture necessary for the realization of the highly automated/autonomous behavior concludes the Section 3. In Section 4 the example of failure within the sensory system is used to illustrate how automation reaches its functional limits due to failure (component/module/function) and what are the situational resulting risks. To this end, a classical functional analysis approach for considering cause and consequences of failure, as well as the limits of its application, is applied and presented. The background for the introduction of the new principle is prepared and discussed. Risk-based synthesis of the autonomously guided vessel in case of deterministic malfunction of key components and degraded take-over of redundant reserve components is shown in Section 5. Summary and conclusions are finalizing the paper.

2. Background of the underlying methods

2.1. Functional analysis

Classical approaches such as FTA, Reliability Block Diagram (RBD), Event Tree Analysis (ETA), or FMEA can be used to identify critical components as the cause of failures or faults. This is useful to determine the topology of functional dependencies and the associated quantitative values. Assuming a fixed and given architecture of functional and physical dependencies here FTA Method is used for both quantitative and qualitative evaluation of the system's probability of failure, unreliability, or unavailability. The classical fault tree analysis is a static approach dependent on an initial condition for performing reliability assessment (Lee et al., 2021). An important task of the FTA is related to the representation of events leading to the top event and their causal relationships using logical connections, denoted as gates and easy to be used for illustration. Two types of gates are typical:

AND gate: This gate represents the requirement of simultaneous fulfillment of several conditions as a necessary condition. It indicates that all input events must occur to cause the parent event.

OR gate: This gate represents an 'OR' fulfillment of conditions. It indicates that at least one of the input events must occur to cause the parent event.

In this way, cause-effect relationships between different events can be represented in a structured way as fault tree. This helps to visualize and also identify potential sources of errors and to develop appropriate measures for risk assessment and error prevention. The approach FMEA is widely used for the systematic evaluation of the severity of potential failure modes and is one of the most popular safety and reliability analysis tools (Yang et al., 2008).

In the context of this work, the two classical approaches are used to show the effects of sensor failures for the behavior of the autonomous ship. It is investigated what can cause the failures and what consequences the occurrence of these failures has for the entire system.

2.2. Dependent functionality

In addition to methods that analyze topologies in terms of their overall dependencies, this approach additionally assumes that component functionality is constrained or limited with respect to operational or environmental parameters.

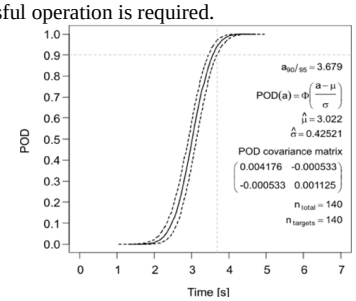
Reliability and safety criteria are always related to specific operational limits. An example of this are adverse weather conditions, which affect the technical physical limits and, in combination with algorithms, also the technical perception capability and hence the performance of state-of-the-art sensor systems, as discussed in (Zhang et al., 2021). It is assumed that (apart from low thresholds) no fixed operating limits (or operating specifications) can be determined. However, this is an important requirement for safe autonomous or highly automated operations. In contrast to the previous consideration with the above-mentioned fixed operating limits, the dependency of the operating limits on further variables is discussed and used in this paper.

In this sense the evaluated operating range could be included in the consideration as a variable dependent on operating conditions, so that the safety-oriented consideration allows to include that. The recently presented

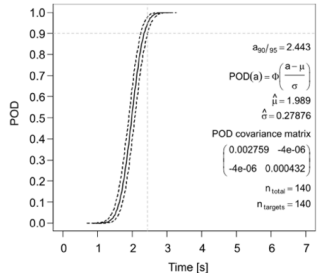
modified POD (Probability Of Detection)-based methodology (Ameyaw and Söffker, 2022) for the evaluation of machine learning methods as a function of process parameters represents a possible reliability-based evaluation to be used as a reliability-oriented measure connecting reliability (in a statistic sense), the functionality, and the dynamic operation/environmental variables leading to this dependency.

The POD is a probabilistic method allowing to compare the performance of different monitoring techniques by evaluating the sensitivity and reliability of inspection methods or sensors, taking into account statistical variability. In a recent study (Ameyaw et al., 2022), the POD approach was extended to evaluate the ability of classifiers to predict human driver intent based on the time remaining to a known event. Classifier performance was evaluated using the detection rate (DR) and false alarm rate (FAR). Here also a newly extended POD approach was introduced as a measure of the limitations of the ROC curve and accuracy in classifier evaluation. Several POD curves are constructed for different approaches to be compared, two example applications are shown in Figure 1.

Following this approach, in the present situation the POD is evaluated as a function of the distance between the two vessels. Related to the case study, it means that the reliability for successful realization of the task is assumed as a causal chain between the detection of an object and the repositioning of the ship and therefore does not only depend on the failure rate of the actuator and sensor systems, but also on the control in between. In the current contribution it is assumed that depending on the distance of the object to be detected, the reliability and the application area of the sensors is different, leading to specific consequences if a minimum reliability of the successful operation is required.



(a) Improved ANN POD for right lane change of driver 1.



(b) SVM POD for right lane change of driver 1.

Fig. 1. POD curves for different ML approaches applied to the same scenario data (Ameyaw, 2022). Symbols as follows: $a_{90/95}$: Maximum flaw size that could be missed with 90 % POD at 95 % confidence level. Φ: Cumulative distribution function. $n_{targets}$: Number of observations considered in the POD evaluation. n_{total}: Total number of observations.

3. Case study

The proposed method for functional analysis and risk assessment of the command and navigation system focuses, as mentioned at the beginning, on rare critical situations. For this purpose, an operating scenario is proposed in this section in which failures in the system could lead to serious consequences. Furthermore, an example architecture for an autonomous inland vessel is presented. The combination of the architecture and the defined scenario provides a basis for the following investigations.

3.1. General scenario

The presented operating scenario is based on the frequently occurring situation of two ships passing each other. In this example, two (large inland cargo vessel / large Rhine ship) inland vessels meet each other in a channel. Navigation on open stretches usually is conducted at a speed permitted in the "BinSchStrO (Binnenschifffahrtsstraßenordnung)" [Regulations for Navigation on Inland Waterways] or at a technically feasible ship speed. On many waterways, the ship speed is limited upwards due to the engine power and the hydraulic boundary conditions. The permissible ship speeds can vary greatly depending on the waterway. Based on the maximum permissible speed of both ships for draught T > 1.3 m and v_zul = 10 km/h (Abromeit et al., 2010).

Vessels sailing alone usually travel either along the center of the waterway or eccentrically at the edge of a single lane along the canal axis. As a general rule, a value of 0.97 v_zul is recommended in (Abromeit et al., 2010) for the design ship speed of vessels sailing in the center of a waterway. When a vessel is preparing to pass or overtake another ship, it can also sail along the outermost edge of the existing double lane specified according to the Guidelines for Standard Canal Cross-Sections (Abromeit et al., 2010).

For the encounter takes place in the channel case, it is assumed that the flow velocity *v_flow* is less than 0.5 m/s and the design of the shore has a rectangular profile (R-profile) - perpendicular on both sides. From these assumptions it follows that the distance between two lanes (minimum safety distance) is 2 m for encountering traffic (BMVBS, 2011).

Table 1. System state and boundary conditions.

Initial state	
Draught	2.5 m
Wide	11 m
Length	100 m
Initial speed v_0	9.7 km/h
Initial turning speed r_0	0 °/min
Initial rudder angle δ_0	0 °
Boundary conditions	
Max. time for execution t_{end} (CESNI, 2023)	110 s
Min. distance at the side	2 m

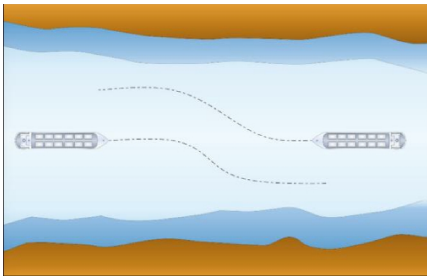


Figure 2. Driving scenario 'Passing-maneuver': Ego-vessel (left), Oncoming-vessel (right).

According to the general navigation rules, in this case both vessels would switch to their right side and pass each other port to port (cf. Figure 2.). The distance of 2 m between the two vessels must be maintained. To perform this, the following steps must be carried out in the following order

- move rudder (steer to the right),
- move rudder (steer to the left until zero position) and
- accelerate.

The following assumptions for the calculation represent a rough approximation of the minimum frontal distance necessary to safely perform the evasive maneuver. According to (CESNI, 2023) the execution of an evasive maneuver is described with the applicable requirements and boundary conditions. The time *t_end* set in (CESNI, 2023) for the considered ship executing the entire evasive maneuver must not be exceeded. Given an initial state as defined in Table 1 for the ego and the encountering vessel, as well as the stated boundary conditions, the necessary minimum frontal distance of the two ships is about 600 m without safety factor.

3.2. Architecture of the autonomously-guided system

A general system architecture consists of components to enable the system to plan and execute safe maneuvers. The main parts are the sensing of the environment, perception of the obtained information, maneuver planning and decision-making, the executing system platform as well as actuators for communication and motion control. A possible architecture is shown in Figure 3. Different sensors are providing information of the environment.

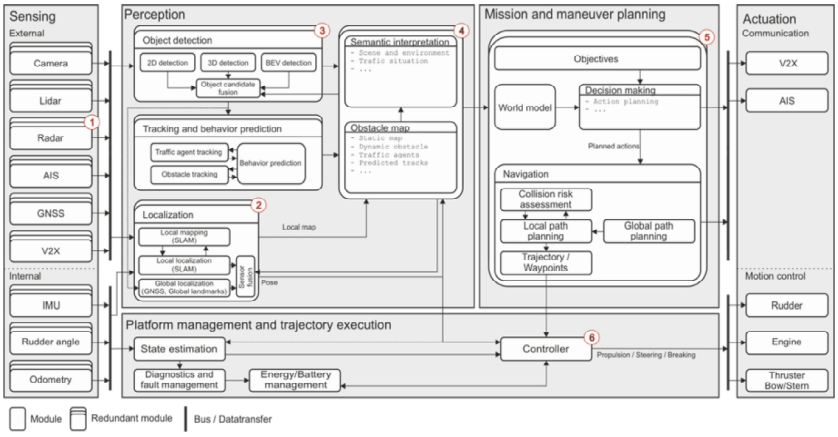


Fig. 3. Example architecture for an autonomous vessel. Different system components and their submodules are shown. Exchange of information is indicated with arrows. The numbering indicates error propagation in case of a failure of the radar system, compare Section 5.

Cameras capture textural information, while Lidar and Radar sense sparse depth details in the environment. Global Navigation Satellite Systems (GNSS) provide system pose information, and the Automatic Identification System (AIS) relays data on the position, speed, and course of other vessels. Internal sensors, such as the inertial measurement unit (IMU), offer estimated insights into the system for diagnozing or localization purposes. Environmental object perception includes modalities like AIS, presenting information in 2D, 3D, or Bird's Eye View (BEV) representations. An object candidate fusion module integrates predictions from various approaches, considering different modalities, representations, or situational factors. Detected objects, classified as traffic agents or obstacles, can be vessels or static elements like shorelines and buoys. Object movement is tracked, and potential actions are predicted. Ego system location is obtained from GPS, and Simultaneous Localization and Mapping (SLAM) facilitates localization and map generation using available sensor data. The information is processed into higher-level data like an obstacle map and semantic situation description, supporting system decision-making. Defined actions are executed by the control system for trajectory adjustments, with information communicated through AIS or other Vehicle-to-Everything (V2X) systems. Each of the components of the architecture can be implemented in a redundant manner. This can be realized via redundant sensors and actuators, redundant processing units for different software modules, or redundant software modules.

4. Application of functional analysis

The proposed investigation method is based on the failure of a key component, in the case considered the radar system. In the first step, this failure is analyzed using traditional methods such as Fault Tree Analysis (FTA) and Failure Mode and Effects Analysis (FMEA). In the next step, a method for evaluating the (still existing) functionality is proposed using the POD approach. In addition, the failure of the component is evaluated quantitatively using hardware and software. An adaptive solution is then provided to adapt to the given and specified requirements with adjustment of the operating parameters.

4.1. Classical approach

Considering the encounter situation described above, the following scenario should be considered: Assuming good weather conditions for distant vision tasks, two vessels (one automated) come towards each other as described in Section 3.1. The sensor system of the ego ship provides necessary information on the other vessel (as obstacle) as well as the localization and decision-making takes place on the basis of these information. The maneuver is initiated. In the next moment, the radar fails completely so the position information about the other vessel as obstacle get loss. Other sensors and other hardware components of the system architecture are not affected. As consequence, the subsequent localization and object recognition measures are based on the information provided by the other sensors able to realize the same task (object localization) but with other constraints. To further investigate the effects of the failure of the radar information system, classical approaches of reliability engineering are first applied. The analysis is only carried out from the perspective of the ego vessel.

4.2. FTA

The first step is to investigate those events and conditions leading to a collision between the two vessels. For this purpose, failure causalities of the system described can be analyzed developing the related FT (Fault Tree). The FTA is used to model different combinations of fault events which might lead to undesired top events. Once a top event is defined, the associated undesired events are systematically identified and classified in the top fault tree layer. In this contribution the main focus of the approach is on the identification and development of fault trees for the top event "Collision with Encountering Vessel", which can lead to, among other things, personal injury, machine damage, and mission failure. The logical relationships between each event are thoroughly examined, taking into account the types of gates and their specific inputs. For this contribution the focus is on examining the relationships with the failure of the radar system based on (Swarup and Rao, 2014) as required for the scenario considered.

4.3. FMEA

Radar-based object detection plays a critical role in detecting, locating, and tracking objects using radio waves. To evaluate the reliability and performance of radar systems, it is important to understand the failure modes and their effects. By performing an FMEA, the critical failure modes, their occurrence, and their detection capabilities can be defined. Furthermore, the assessments can be used to derive measures to mitigate risks and improve the robustness of the overall system. It should be noted that FMEA is usually a collaborative process involving a team of professionals. To identify many possible defects, the FMEA of this work (cf. Table 2) also includes results of

other works (Swarup and Rao, 2014; Luo et al., 2022). For reasons of clarity, only selected examples are shown here.

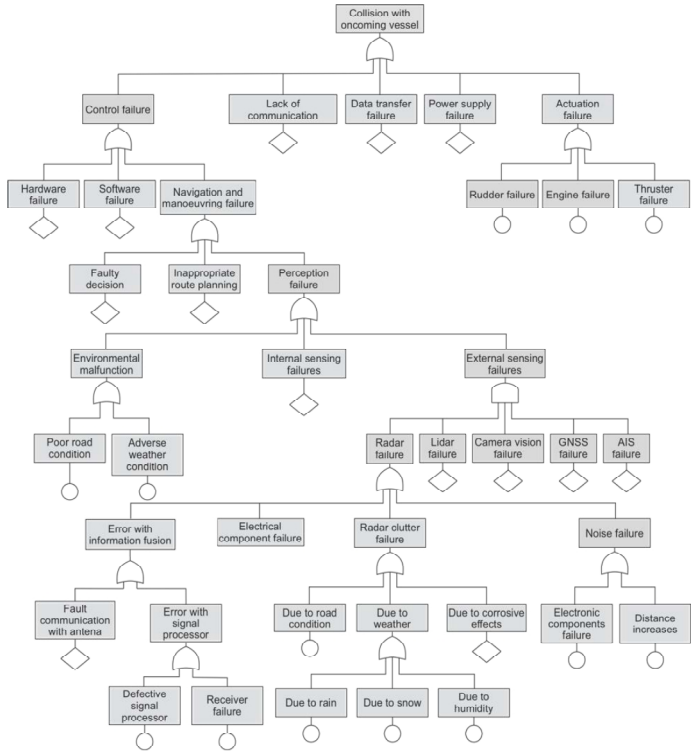


Fig. 4. Fault tree of collision with oncoming vessel

Table 2. FMEA of the system element radar.

Function / Component	Failure mode	Failure effects	Cause of failure	Current controls
Radar transmitter	No signal output	Loss of bases / system situational awareness	Hardware failure	Regular maintenance and calibration
Radar receiver	No signal input	Signal distortion or complete signal loss/ Inability to detect objects	Weather conditions Road conditions Antenna malfunction (mechanical/electrical)	Regular maintenance and calibration
Power supply	Voltage drop	System shutdown	Power outage	Backup power supply
Signal processing	Data loss corruption	Incorrect object identification	Software failure	Validation and verification

4.4. POD-based evaluation of reduced functionality

The scenario described in Section 3.2 relies on the assumption that the sensor suite will be able to realize the prediction of an encountering object at a certain distance with a sufficient, but configuration and situation dependend reliability. A schematic overview of the relation between the quality of the detection horizon with respect to the reliability of the statement with respect to the correctness, the related achievable detection horizon, and the related velocity, is visualized in Figure 4. The figure can be read following the numbering:

1. Intersection of the reliability profile for case 1 with the reliability threshold indicating the maximum safe detection range.
2. The maximum safe detection range defining the guaranteed (safe) detection horizon. The intersection with different velocity profiles is determined.

3. The resulting maximum velocity for safe navigation of the ego system, based on case 1 and the medium velocity of the encountering object.

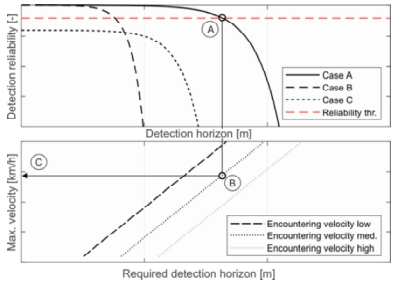


Fig. 5. Top) Detection reliability over distance. Different possible cases, examples as follows:
Case A: Good weather conditions, all sensors available;
Case B: Good weather conditions, all sensors except radar available;
Case C: Bad weather conditions, all sensors available;
Bottom) Maximum velocity based on the given safe detection horizon, assuming different velocities of the encountering object.

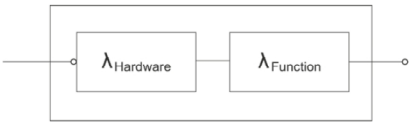


Fig. 6. Series circuit model of radar system failure rate.

5. Risk-based synthesis of autonomously guided vessel in case of deterministic malfunction of key components and degraded take-over of redundant reserve components

Statistical reliability figures are often used to estimate the reliability or probability of fault-free operation over a period of time. One such metric is the failure rate; this quantifies the frequency of malfunctions and failures. To estimate the unusability of the radar functionality considered, the failure rate of the radar hardware (classical case) and the reliability of a correct functionality (from the algorithmic function of the displayed information) are considered together. Both the hardware and the software function must be fully functional to provide a correct indication. This means that the failure of one of the two parts (hardware, software) leads to the failure of the whole system or the concrete functionality, which is understood here as a correct statement.

The statement is non-correct if there is no statement (hardware failure) or the statement is wrong (software failure). Both (hardware/software) are therefore considered as a series connection Figure 6. To calculate the total failure rate λ_{sys} of a series connection, the individual failure rates λ_i of the components has to be summed up. Here, no particular radar sensor type is assumed in this example, so the usual parameters for electronic components are assumed. These are in the range of 10E-4/a for hardware. For the software functionality, it is assumed that the algorithm works correctly with a probability of 95 %, so that the functionality is as follows

$$\lambda_{sys} = 0.0001 + 0.05 = 0.0501 \text{ res} \quad (1)$$

$$\text{p. sucess rate}_{sys} = 1 - \lambda_{sys} = 0.9499 \quad (2)$$

holds. Thus, it can be assumed for the case that the described radar failure occurs in combination with a loss of function or misrepresentation (1 time in 175200 operating hours). This approach shows how important the probability is, but does not take into account the external influences (such as the weather conditions described) that can affect the radar. Accordingly, it is first assumed that the radar is operated in the range of usual operation parameters.

Regardless of the probability of failure or the probability of obtaining a correct statement about the position of objects at all, it is assumed in the following that the radar or the functionality is not available or not available as correct information. To guarantee the required correctness of the functionality, the related requirements must be specified. As described in Section 3.3, radar-based environmental detection provides the central information for the vessel's behavior. If the Radar sensor fails, a redundant system has to provide the required depth information about the encountering object. If no fall-back system is available or both systems fail as a result of the environmental conditions, no radar information would be available. In this situation, the available sensing range reduces significantly. Object detection would be limited to the range of the Lidar and camera system, while camera-based systems provide worse depth information. Information about traffic participants beyond a certain distance might be available via AIS, but without guaranteed update frequency. A potential error propagation is indicated following the numbering in Figure 3. Following the mentioned example, the error propagation could be described as follows:

1. The radar fails to provide usable long range depth information of the environment due to hardware failure or environmental conditions.
2. Radar-based localization approaches are no longer available but can be covered by other systems.

3. Radar-based object detection is no longer available, sensing range is limited to options of the remaining systems.
4. Semantic interpretation and obstacle map are limited to the available and reduced sensing range.
5. Decision-making has to be done based on information with limited range, reducing the reaction time etc.
6. Control actions have to be executed within less time resulting into increased actuation or an impossible maneuver due to dynamic limitations of the system.

To counteract these uncertainties, in this contribution for the first time in this context the following core idea is proposed: A degradation of the functionality, e.g. in the presented case of speed is used for adaption with respect to ensure safety and reliability requirements (cf. Figure 7).

To ensure the required safety level (red), the situated overall safety and reliability level must be guaranteed as above the required level. If the radar fails, the redundant systems will ensure the functionality but not with the required safety level (pink). If the speed of the Ego vessel as proposed in Figure 7 (black) is reduced, the functional and safety requirements can still be met. This is due to the fact that now the required safety and reliability standards are met (but with reduced speed). The previously defined safety threshold is defined in a classical manner, so that with the expected regular functionality, the autonomous ship fits the safety standards. With the loss of functionality (here: use of other sensors) the operating variables (here: speed) has to be adapted (not as functionality degradation but as an operating degradation), to operate the complete system on the required safety level.

The likelihood of an autonomous vessel performing a maneuver reliable depends on various factors, including the technology and systems used, the level of development of the autonomous system and the prevailing conditions under which the maneuver is performed. In the presented example these are not specified.

6. Conclusion

The use of autonomous systems on inland vessels has the potential to improve the efficiency, safety, and

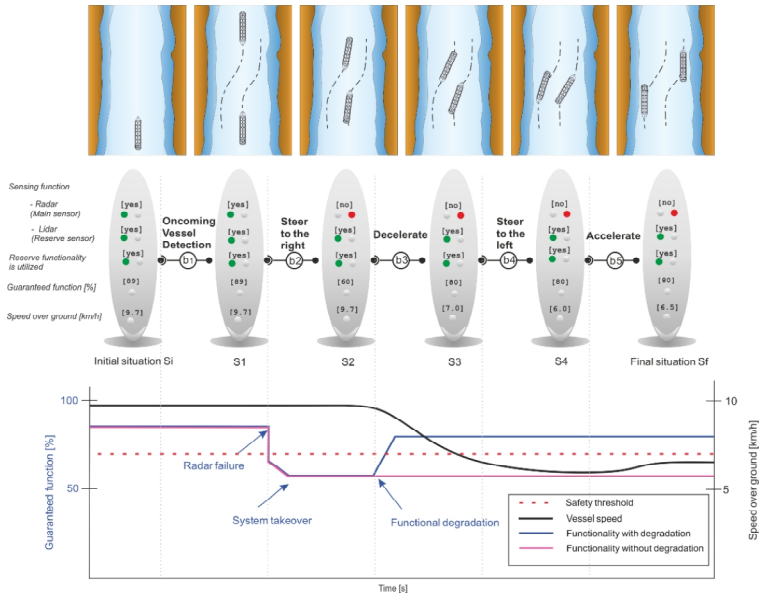


Fig. 7. Chronological stages of the scenario's development.

environmental compatibility of maritime transport. However, the use of autonomous systems also entails various risks that need to be analyzed and managed. This paper presents a risk-based analysis of the governance of autonomous systems on inland vessels. This paper focuses on the functional analysis and risk assessment of the command and navigation system and provides as adaptive solution to fit the given and fixed requirements with adaption of operating parameters. An example architecture of an autonomous inland vessel is presented. Based on a defined scenario, a component failure, in this case the radar system, is analyzed using classical methods such as Failure Mode and Effects Analysis (FMEA) and Fault Tree Analysis (FTA). Furthermore, the example also shows

the approach proposed linking risks associated with specific driving scenarios and the failure of required hardware components with the formulation of an operating parameter-depending reliability formulation so that the function-oriented realization in combination with operating parameters overcomes the static and therefore rigid reliability setting to find risk-oriented solutions for vehicle guidance systems.

Acknowledgements

This research is partly supported by the AutoBin project (Grant No. EFRE-0801714) supported by the European Regional Development Fund (ERDF) and SafeBin project (Grant No. 45DTW2V05) supported by the Federal Ministry for Digital and Transport of Germany.

References

Abaei, M. M., Hekkenberg, R., and BahooToroody, A. 2021. A multinomial process tree for reliability assessment of machinery in. Reliability Engineering and System Safety, Vol. 210, 107484.

Abromeit, U., Alberts, D., Bartnik, W., Fischer, U., Fleischer, P., and Fuehrer, M. 2010. Principles for the Design of Bank and Bottom Protection for Inland Waterways (GBB). Bundesanstalt für Wasserbau (BAW).

Ameyaw, D. A., Deng, Q., and Söffker, D. 2022. Evaluating Machine Learning-Based Classification Approaches: A New Method for Comparing Classifiers Applied to Human Driver Prediction Intentions. IEEE Access, Vol. 10, pp. 62429-62439.

Bakhshande, F. et al. 2020. The AutoBin project – Key concepts, status, and intended outcomes. Autonomous Inland and Short Sea Shipping Conference - AISS2020, Duisburg, Germany.

Basnet, S., BahooToroody, A., Chaal, M., Lahtinen, J., Bolbot, V., and Valdez Banda, O. A. 2023. Risk analysis methodology using STPA-based Bayesian network- applied to. Ocean Engineering, Vol. 270, 113569.

Bejaoui, A., He, C., and Söffker, D. 2022. Novel model-based decision support. Annual Conference of the PHM Society 2022, Nashville, Tennessee, USA.

Ben Swarup, M., and Srinivasa Rao, M. 2014. Safety Analysis of Adaptive Cruise Control System Using FMEA and FTA. International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4 (6),pp. 330-337.

BMVBS. 2011. Richtlinien für Regelquerschnitte von Binnenschifffahrtskanälen. Bundesministerium für Verkehr, Bau und Stadtentwicklung.

Bolbot, V., Theotokatos, G., Boulougouris, E., Wennersberg, L. A. L., Nordahl, H., Rødseth, Ø. J., Faivre, J., and Colella, M. Molica 2020. Paving the way toward autonomous shipping development for European Waters – The AUTOSHIP project. Conference: Autonomous ships 2020, London,UK.

Bolbot, V., Theotokatos, G., McCloskey, J., Vassalos, D., Boulougouris, E., and Twomey, B. (2022). A methodology to define risk matrices e Application to inland water. International Journal of Naval Architecture and Ocean Engineering, Vol. 14, 100457.

CESNI. 2023. Europäischer Standard der technischen Vorschriften für Binnenschiffe (ES-TRIN). Europäischer Ausschuss zur Ausarbeitung von Standards im Bereich der Binnenschifffahrt.

Chang, C., Kontovas, C., Yu, Q., and Yang, Z. 2021. Risk assessment of the operations of maritime autonomous surface ships. Reliability Engineering and System Safety, Vol. 207, 107324.

DIN EN IEC 61508. 2011. Functional safety of electrical/electronic/programmable electronic safety-related systems.

Johansen, T. and Utne, I. B. 2022. Supervisory risk control of autonomous surface ships. Ocean Engineering, Vol. 251, 111045.

Koschorrek, P., Kosch, M., Nitsch, M., Abel, D., and Jürgens, D. 2022. Towards semi-autonomous operation of an over-actuated river ferry. at – Automatisierungstechnik, 70, 433 – 443.

Lee, P., Bolbot, V., Theotokatos, G., Boulougouris, E., and Vassalos, D. 2021. Fault Tree Analysis of the Autonomous Navigation for Maritime Autonomous Surface Ships. Proceedings of the 1st International Conference on the Stability and Safety of Ships and Ocean Vehicles, Glasgow, Scotland, UK.

Luo, X., He, H., Zhang, X., Ma, Y., and Bai, X. 2022. Failure Mode Analysis of Intelligent Ship Positioning System. Processes 2022, Vol. 10, 2677.

Rakowsky, U. K. 2002. Systemzuverlässigkeit. Reliability of Systems (in German). Hagen: Life-Long Learning.

Stapelberg, R. F. 2009. Handbook of Reliability, Availability, Maintainability and Safety in Engineering Design. London: Springer.

Söffker, D. 2000. Online determination of reliability characteristics as a module of the SRCE-concept (in German). at-Automatisierungstechnik, 48, pp. 671-682.

Söffker, D. and Rakowsky, U. K. 1997. Perspectives of Monitoring and Control of Vibrating Structures by Combining New Methods of Fault Detection with New Approaches of Reliability Engineering. A publication of the Society for Machinery Failure Prevention Technology, pp. 671-682.

Verma, A. K., Ajit, S., and Karanki, D. R. 2016. Reliability and Safety Engineering. London: Springer.

Wolters, K. and Söffker, D. 2005. The potential of the Safety and Reliability Control Engineering concept as framework for reliability-based utilization strategies. Structural Health Monitoring 2005, Proc. of the 5th Int. Workshop on Structural Health Monitoring, Stanford, CA, pp. 1353-1360.

Yang, Z., Bonsall, S., and Wang, J. 2008. Fuzzy Rule-Based Bayesian Reasoning Approach. IEEE Transactions on Reliability, Vol. 57 (3), pp. 517-528.

Zhang, W. and Zhang, Y 2023. Navigation Risk Assessment of Autonomous Ships Based on entropy-topsis-coupling coordination model. Journal of Marine Science and Engineering, Vol. 11, 422.

Zhang, Y., Carballo, A., Yang, H., and Takeda, K. 2021. Perception and sensing for autonomous vehicles under adverse weather conditions: A survey. ISPRS Journal of Photogrammetry and Remote Sensing.

Zhou, X., Liu, Z., Wang, F., Wu, Z., and Cui, R. 2020. Towards applicability evaluation of hazard analysis methods for. Ocean Engineering, Vol. 214, 107773.