Methods

Christian Neurohr*, Marcel Saager, Lina Putze, Jan-Patrick Osterloh, Karina Rothemann, Hilko Wiards, Eckard Böde and Axel Hahn

Towards efficient certification of maritime remote operation centers

Ansatz zur effizienten Zertifizierung von maritimen Fernsteuerungszentren

https://doi.org/10.1515/auto-2025-0074
Received July 31, 2025; accepted December 1, 2025

Abstract: Additional automation being built into ships implies a shift of crew from ship to shore. However, automated ships still have to be monitored and, in some situations, controlled remotely. These tasks are carried out by human operators located in shore-based remote operation centers. In this work, we present a concept for a hazard database that supports the safeguarding and certification of such remote operation centers. The concept is based on a categorization of hazard sources which we derive from a generic functional architecture. A subsequent preliminary suitability analysis unveils which methods for hazard analysis and risk assessment can adequately fill this hazard database.

Keywords: remote operation center; autonomous surface ships; hazard analysis & risk assessment; safety; certification; human factors

Zusammenfassung: Die zunehmende Automatisierung von Schiffen führt zu einer Verlagerung der Besatzung vaom Schiff ans Land. Automatisierte Schiffe müssen jedoch weiterhin überwacht und in bestimmten Situationen ferngesteuert werden. Diese Aufgaben werden von menschlichen Operateuren in landgestützten Fernsteuerungszentren ausgeführt. In dieser Arbeit stellen wir ein Konzept für eine Gefährdungsdatenbank vor, welche die Sicherung und Zertifizierung solcher Fernsteuerungszentren unterstützt. Das Konzept basiert auf einer Kategorisierung von Gefährdungsquellen, abgeleitet aus einer generischen Funktionsarchitektur. Eine anschließende vorläufige Eignungsanalyse zeigt, welche Methoden zur Gefährdungsanalyse und Risikobewertung diese Gefährdungsdatenbank füllen können.

Schlagwörter: Fernsteuerungszentrum; autonome Überwasserschiffe; Gefährdungsanalyse und Risikobewertung; Sicherheit; Zertifizierung; menschliche Faktoren

1 Introduction

Increasing levels of automation is being built into vessels, leading to the advent of Maritime Autonomous Surface Ships (MASS), as defined by the International Maritime Organization (IMO) [1]. Shore-based Remote Operation Centers (ROCs) are emerging as a supplemental technology alongside MASS to monitor or remote-control such ships in harbors, in coastal waters, or for inland waterways [2], [3]. There exist various novel approaches adapted for the Hazard Analysis and Risk Assessment (HARA) of MASS to cope with the complexity that is introduced by automation technology [4]. For example, the Risk-based Assessment Tool commissioned by the European Maritime Safety Agengy (EMSA) [5]. Regarding classification of MASS, there exists class guidelines such as the DNV-CG-0264 on *Autonomous and Remotely Operated Ships*. These safeguarding approaches are centered around MASS and possible remote control components are considered as MASS functionality. Therefore, the safety of ROCs is considered as part of the MASS HARA. In this concept paper, we put forth the idea to collect safety-relevant artifacts for a generic ROC in a database to enable their reuse. Hence, to facilitate more efficient certification of MASS-ROC pairs, we tackle the research question.

How can we build a hazard database that integrates technical as well as human hazards and facilitates the

***Corresponding author: Christian Neurohr**, German Aerospace Center (DLR e.V.), Institute of Systems Engineering for Future Mobility, Oldenburg, Germany, E-mail: christian.neurohr@dlr.de
Marcel Saager, Lina Putze, Jan-Patrick Osterloh, Karina Rothemann, Hilko Wiards, Eckard Böde and Axel Hahn, German Aerospace Center (DLR e.V.), Institute of Systems Engineering for Future Mobility, Oldenburg, Germany, E-mail: marcel.saager@dlr.de (M. Saager), lina.putze@dlr.de (L. Putze), jan-patrick.osterloh@dlr.de (J. Osterloh), karina.rothemann@dlr.de (K. Rothemann), hilko.wiards@dlr.de (H. Wiards), eckard.boede@dlr.de (E. Böde), axel.hahn@dlr.de (A. Hahn)

efficient certification of generic ROC-MASS pairs with well-defined interfaces?

In this regard, we contribute.

- a review of standards, regulations, and HARA methods in the maritime domain in Section 2,
- a generic ROC-MASS functional architecture as a starting point for a hazard database in Section 3,
- a categorization of hazard sources for ROCs, a suitability analysis for methods to adequately cover these categories, and potential benefits of a hazard database in Section 4.

2 Related work

In this section, with a distinct focus on ROCs, we briefly review relevant standards and regulations in the maritime domain in Subsection 2.1 and relevant HARA methods in Subsection 2.2.

2.1 Relevant standards and regulations

IMO MASS Code: Within the IMO, the Maritime Safety Committee (MSC) developed the *Interim Guidelines for MASS Trials* in 2019 [6]. These interim guidelines seek to assist authorities and stakeholders to conduct trials for MASS and related systems safely, securely, and under environment protection. These guidelines were specifically formulated for experimental trials over limited periods. The MASS Code is on track to be finalized in its non-mandatory form in 2026 [7]. The code uses a goal-based approach, focusing on performance standards rather than prescriptive rules.

DNV-RU-SHIP(Pt.6,Ch.12): The classification society DNV updated their rules for classification document in 2024 to introduce the Autonomous and Remotely Operated Ships (AROS) class notation [8]. AROS as a framework wants MASS to be at least as safe as conventional vessels. Therein, the term *autoremote* refers to operations, tasks, functions, or systems that enhance decision support, remote control, or autonomy compared to traditional crewed ships. There are four AROS notations – navigation, engineering, operations, safety – each with one qualifier for operation mode and one describing the control location.

DNV-CG-0264: The Class Guideline DNV-CG-0264 [9], developed by DNV, aims to provide guidance for the safe implementation of novel technologies in the context of autoremote vessel functions. Further, it formulates a recommended work process to obtain the approval of novel concepts. Overall, the framework is designed to ensure that the implementation of innovative concepts and technologies meets or exceeds the safety standards of traditional vessel operations. It also outlines the specific class notations applicable to autonomous and remotely operated ships (AROS), cf [8].

DNV-ST-0324: The DNV-ST-0324 standard provides a set of required competences for humans operating ROCs, i.e., operators tasked with supporting, monitoring, or controlling MASS from a remote, shore-based location [10]. The standard makes suggestions on the necessary skills and knowledge for human ROC-operators regarding communication, navigation, machinery, and cargo. As such the standard is highly relevant to the identification of hazards (and their causes) related to human factors – due to ROC-operator potentially lacking basic skills or knowledge. The DNV-ST-0324 is complemented by the recommended practice DNV-RP-0323 regarding certification schemes for ROC-operators [11].

ISO 23860: The technical specification ISO/TS 23860 covers vocabulary for highly automated or autonomous ships [1]. It introduces terms ranging from related to autonomous ship systems, e.g., *autonomy* and *control*. In this work, we will follow the ISO/TS 23860s definition for terms such as ROC or MASS. Furthermore, the standard addresses the interrelations of terms for autonomous ships such as the relations between of ROC, MASS, and support services.

CMOROC: Based on the ISO/TS 23860, the EMSA study 'CMOROC – Identification of Competences for MASS Operators in Remote Operation Centres' analyses the requirements for future operators of MASS from ROC. It is based on three representative ship types (feeder, RoPax ferry, bulk carrier) and examines which tasks are required in a ROC and which competences are necessary for this. The study identifies different levels of automation and develops a structured model for the operation and distribution of roles within a ROC. A key result is a catalogue of skills based on the STCW (Standards of Training, Certification and Watchkeeping for Seafarers), which is used as the basis for training. Building on this, a basic and an advanced curriculum is being developed [12].

ISO 26262 & ISO 21448: The ISO 26262 [13] and ISO 21448 [14] are safety standards from the automotive domain that complement each other. While the ISO 26262 focuses on functional safety – addressing risks arising from system failures, ISO 21448 is concerned with the safety of the intended functionality (SOTIF). SOTIF addresses risks that arise not from system failures, but from insufficiencies in the specification, performance limitations or the inability to detect or prevent reasonably foreseeable misuses. ISO 21448 provides a structured framework that offers guidance on managing SOTIF for road vehicles equipped with automated driving systems. The standard organizes the main SOTIF activities and defines high-level objectives to support a systematic development and validation process [15]. Although the

ISO 21448 specifically targets driving automation, the concept of SOTIF is also highly relevant for automated systems in other domains.

2.2 Relevant methods for hazard analysis and risk assessment

For conventional vessels, there exists a wide range of well-established HARA methods which are commonly applied in practice, e.g., Failure Mode and Effect Analysis (FMEA) or Fault Tree Analysis (FTA). To address the specific challenges posed by automated maritime systems, such as their reliance on sensor perception and the complexity of system interactions, adaptions of established methods as well as new approaches have been explored in recent research [4], [16], [17]. However, only a limited number of studies explicitly consider ROCs. A literature review provided by Zhou et al. [18], which evaluates the suitability of commonly used HARA methods for automated maritime system, highlights this gap. Notably, the authors observe that among the evaluated studies, so far only System-Theoretic Process Analysis (STPA) was applied with explicit consideration of the communication between vessel and ROC [19]–[22]. Similarly, another literature review on risk models for automated maritime systems by Thieme et al. [16] reports that only two of the investigated studies explicitly address the communication with a ROC – one employing STPA, and the other a combination of brainstorming and Bayesian Networks [19], [23]. Furthermore, Li et al. emphasize the importance of incorporating human factors into the HARA of automated maritime systems, noting that these systems constitute highly complex socio-technical systems in which the role of the remote operator is significantly more complex than that of a traditional onboard operator [17].

In the following, we briefly introduce common HARA methods that may be applicable for ROCs, as well as some emerging approaches specifically developed for highly automated systems. As the human operator is of particular relevance for remote operation, we consider not only HARA methods focusing on technical system safety but also methods that explicitly address human factors.

2.2.1 Technical system safety

There exists a variety of methods for identifying and analyzing hazards arising from faults or insufficiencies within the system, each with a slightly different focus. Some approaches emphasize the identification of component failures, while others concentrate on the analysis of causal chains or the evaluation of the associated risks. The methods employ either inductive or deductive reasoning strategies and can be tailored for specific stages of the system development process. Moreover, HARA techniques can be roughly classified as qualitative or quantitative, depending on whether they primarily rely on expert judgment or derive probabilistic statements from data.

A broadly applied hazard analysis method is the **Failure mode and effects analysis (FMEA)** [24]. FMEA follows a seven-stage procedure, that focuses on identifying failure modes, their causes and effects on the overall system. The method relies on inductive reasoning and emphasizes systematic documentation throughout the analysis process. Typically, FMEA is conducted by an interdisciplinary team ensuring comprehensive consideration of system interactions. FMEA provides a semi-quantitative method, supporting risk assessment by the calculation of a risk priority number (RPN), which is derived from the estimated probability of occurrence, significance, and the error's detectability. The implementation of FMEA at an early stage in the development process has been shown to result in a substantial and quantifiable reduction in the likelihood of potential errors [25]. Originally developed by the US military, FMEA has become a widely adopted tool across various domains including the maritime sector [26], [27].

Another common method is the **Hazard and Operability study (HAZOP)** which provides a systematic approach to identify potential hazards in systems of all kinds [28]. The method was developed in the 1970s in the chemical industry and is now employed in numerous domains. HAZOP is qualitative method that employs a systematic brainstorming approach utilizing keywords to investigate deviations from specified behavior. An interdisciplinary team examines the system under consideration from different perspectives to identify potential causes of errors, their consequences, and countermeasures.

A method that is designed to analyze causal chains leading to harm is the **Fault Tree Analysis (FTA)**. FTA is a deductive top-down hazard analysis method which aims at identifying and evaluating combinations of faults and failures that can lead to a predefined undesired event, commonly referred to as 'top level event'. Using Boolean logic and a hierarchical structure of logical gates (e.g. AND, OR), FTA systematically decomposes system-level failures into basic events at component level. This approach enables both qualitative understanding and quantitative risk assessment, including the calculation of failure probabilities. Initially developed in the aerospace and nuclear industries [29], FTA has been widely adopted in various sectors. It is particularly valued for its structured reasoning, and

ability to support quantitative risk assessment. FTA is especially effective when applied to hardware-dominated systems. However, extensions have been developed to address human-related hazards and SOTIF, such as provided by Birch et al. [30] or Kramer et al. [31].

Similar to FTA, **Event tree analysis (ETA)** employs a logic tree structure to model potential progression of accidents capturing system responses and failure chains. In contrast to FTA, however, ETA relies on inductive reasoning determining possible outcomes that may result from a specific initiating event [32]. ETA supports both qualitative and quantitative risk evaluation.

Bayesian Networks (BNs), also known as belief networks, provide another method to investigate causal chains. BNs are probabilistic graphical models that represent variables and their conditional dependencies using directed acyclic graphs [33], [34]. In BNs, each node corresponds to a system variable, while the edges represent statistical or causal dependencies, quantified through conditional probability tables. BNs enable reasoning under uncertainty by relying on principles of probability theory, making them highly suitable for complex systems that are employed in uncertain environments. BNs were originally developed for decision support and diagnostics and have been adapted for use in various safety-critical domains. Their ability to integrate both expert judgment and empirical data makes them particularly valuable for probabilistic risk assessment of dynamic and complex systems.

System-Theoretic Process Analysis (STPA) developed by Leveson and Thomas [35] is a relatively novel hazard analysis method grounded in system theory. It conceptualizes safety as a control problem emphasizing inadequate control actions within socio-technical systems rather than isolated component failures. This perspective makes STPA especially well-suited for systems with complex interactions and software components. STPA employs a top-down approach consisting of four main steps: First, the goals of the analysis are defined in form of losses. In the second step, the system is modeled in form of a hierarchic control structure. Based on this model, unsafe control actions are identified using a keyword-based technique. Finally, so called loss scenarios are derived containing causal factors that may lead to the unsafe control actions. Originally developed for aerospace, STPA has since been adapted across various industries. In the maritime domain, STPA has gained relevance in the context of autonomous vessels [17], [18].

A framework that has been developed by EMSA particularly for the hazard analysis of MASS is the **Risk-based Assessment Tool (RBAT)**. RBAT provides a structured methodology to compare automation and remote operations safety with conventional shipping [5]. The methodology consists of five main parts and a total of 19 steps, encompassing the description of automation usage, hazard identification, mitigation analysis, to risk assessment and risk control. Central to RBAT is the modeling of vessel missions, control functions and the qualitative assessment of risks. Risk levels for each scenarios are derived from a combination of worst-case outcome severity, the effectiveness of mitigation measures and the vessels exposure to enabling conditions. Rather than focusing on the probability of systematic failures, the method integrates technical and operational aspects and emphasizes minimizing the consequences of functional failures. A key feature of RBAT is the explicit integration of Remote Operation Centers (ROC) as supervisory unit within the safety analysis. The methodology enables the systematic identification of scenarios, in which the ROC is required to intervene, the information it must receive to perform this role, and the system architecture necessary to support interventions – particularly in relation to mitigation strategies. Supervisory control agents located within the ROC operate in either an active or passive monitoring capacity, typically involving human operators. The effectiveness of mitigation measures attributed to the ROC is thus evaluated not only on the technical basis, but also with regard to human performance factors, such as operator response time or workload.

Another method specifically developed for automated systems has been proposed by Kramer et al. [31], [36]. The **Automation Risk** method has initially been designed for automotive applications, but has also been transferred to the maritime domain [37], [38]. It aims to identify and evaluate hazardous scenarios, thereby supporting a scenario-based safety assessment. Conceptually, the method draws upon HAZOP and FTA, adapting and integrating elements of both to address the specific challenges that arise for highly automated systems.

2.2.2 Human factors

Human factors risk analysis methods have become essential for understanding and mitigating the impact of human error in complex systems. These methods recognize that performance is shaped by a combination of individual capabilities, organizational culture, environmental influences, and system design. Traditional engineering risk assessment techniques often fall short in capturing these human and organizational dimensions, prompting the development of dedicated methodologies. Broadly speaking, human factors analysis approaches can be classified into predictive methods, which aim to anticipate potential errors during

system design, and retrospective methods – like HFAC [39] or HFACS-MA [40] – that analyze incidents after they occur. This paper focuses on predictive methods suitable for integration into early system development phases.

One such predictive methodology is the **Systematic Human Error Reduction and Prediction Approach (SHERPA)**, which provides a structured framework for anticipating human errors during task performance. Introduced by Embrey [41], SHERPA employs hierarchical task analysis to decompose complex operations into subtasks and applies error mode identification to foresee potential failure modes. Its strength lies in its proactive application during system design, helping to prevent errors by addressing both internal human factors and external, error-promoting conditions.

THERP, or the **Technique for Human Error Rate Prediction**, offers a quantitative means of evaluating human reliability, especially in high-risk settings like nuclear power. Developed by Swain and Guttmann [42], this method integrates task analysis with human error probabilities and performance-shaping factors to deliver probabilistic risk estimates. While modeling human variability remains a challenge, THERP's primary value is in supplying numerical data to broader system reliability assessments.

The **Functional Resonance Analysis Method (FRAM)** is presented by Hollnagel [43] as a paradigm shift from traditional accident analysis methods toward understanding complex socio-technical systems. Resilience engineering has consistently argued that safety is more than the absence of failures, and FRAM builds on this foundation. FRAM is based on four principles: the equivalence of failures and successes, the central role of approximate adjustments, the reality of emergence, and functional resonance as a complement to causality. Unlike conventional methods that focus on what went wrong, FRAM is used to model the functions that are needed for everyday performance to succeed, and this model can then be used to explain specific events by showing how functions can be coupled. Over the past two decades, systemic-based risk assessment methods have garnered more attention, and FRAM is one of the most widely used systemic methods for risk assessment and accident analysis. The method represents Hollnagel's evolution from the more traditional CREAM approach [44] toward understanding how normal performance variability can lead to both successful and unsuccessful outcomes in complex systems.

In the medical domain, human error analysis has evolved to include integrated techniques like the **Human Factors Failure Mode and Effects Analysis (HF-FMEA)**. Song et al. [45] demonstrate how combining traditional FMEA with human factors considerations enhances safety in medical device usage. Their approach allows for systematic identification of possible user-related errors, risk evaluation, and prioritization of preventive measures, adapting a well-established reliability tool to address human contributions more directly.

Another valuable technique, the **Success Likelihood Index Method (SLIM)**, is used to assess human reliability in specialized maritime operations such as pilot transfers. Aydin and colleagues [46] show how SLIM, when integrated with the HFACS-PV framework, enables both qualitative and quantitative analysis of performance-shaping factors. This combination helps to clarify mechanisms behind human error while also estimating error probabilities, contributing to comprehensive maritime safety assessments.

In the petroleum sector, **Petro-HRA (Petroleum Human Reliability Assessment)** has been developed as an industry-specific method tailored to offshore operations. As outlined by Blackett et al. [47], this approach enables both qualitative and quantitative evaluation of tasks affecting major accident risk. Its emphasis on post-initiating event scenarios, complex technical systems, and harsh operational environments underscores the limitations of generic HRA tools and the value of specialized adaptations.

The **Analysis of Pre-Accident Operator Actions (APOA)** offers another perspective by focusing on human actions occurring prior to accident events. Øie and Fernander [48] introduce APOA as a structured method for tracing the sequence of decisions and actions that influence accident development. By examining the timing and context of human involvement, this approach enhances understanding of how specific actions may either exacerbate or mitigate incident outcomes, particularly in petroleum and maritime contexts.

The **CRIOP (Crisis Intervention and Operability Analysis)** framework is adopted by Hoem, Rødseth, and Johnsen [49] as an interdisciplinary risk analysis method specifically applied to the design of remote control centers for maritime autonomous systems. The authors demonstrate how CRIOP can be effectively utilized to identify and analyze human factors risks in the emerging field of autonomous maritime operations, where traditional shipboard crew operations are replaced by shore-based remote monitoring and control. Their work shows how the CRIOP framework addresses the unique challenges of designing human-machine interfaces and operational procedures for remote maritime operations, considering both technical system capabilities and human operator competency requirements. The paper illustrates the framework's value in bridging the gap between human factors analysis and system

design in advanced maritime technologies, providing a structured approach to ensure that remote control centers are designed with appropriate consideration of human performance limitations and requirements.

Taken together, these methodologies illustrate the expanding toolkit available for human factors analysis. Their diverse strategies – from structured task analysis to probabilistic modeling and cognitive frameworks – highlight the critical importance of anticipating human error during system design. By integrating these predictive methods early in the development process, industries can better manage safety risks and improve system resilience across a range of high-hazard domains.

3 Maritime remote operation centers

Following the literature review of Section 2, we now move to our modeling activities. In Subsection 3.1, we introduce maritime ROCs as preparation for the conceptual description of the hazard database. As an illustrating use-case we describe berthing in a port in Subsection 3.2. This leads to a generic MASS-ROC functional architecture described in Subsection 3.3.

3.1 Introduction to maritime ROCs

A ROC is a shore-based control center required for monitoring, controlling and supporting MASS. Depending on the level of automation, MASS can be highly automated or autonomous surface ships that can be remotely monitored and controlled by a ROC. Although the ROC operators are physically separated from the ship, they perform important tasks during regular operations, in extreme situations, and when making critical decisions [1]. The main features of a ROC are:

- there is a human operator (HO)
- it centralizes the monitoring and remote control of MASS
- its operating modes range from passive monitoring to active remote control of the ship
- it offers a high degree of automation on board with minimal human intervention if required,
- it has technical interfaces to navigation systems, sensors, communication, emergency management.

Importantly, the ISO/TS 23860 specifies four different operation modes for ROCs [1]:

Strategic Control: In this mode, the operator provides instructions to the entire fleet. This covers planning and organisational tasks. For example, a strategy for saving fuel under certain conditions may be communicated.

Tactical Control: We are now moving to the individual MASS level. Tactical control is used to influence the decision making of an automation system. In contrast to the long-term approach of strategic control, tactical control takes a more short-term view. For example, decisions on routing or adjusting speeds in cooperation with the automated system (which directly controls the MASS).

Direct Control: Direct control means interacting directly with the functions of the MASS. This would directly override the decisions of an automation system. The operator literally controls the MASS. This includes all parameters and processes that can be manipulated and controlled. For example direct remote control of the MASS. It would be possible to take over the control directly in difficult situations, such as lock passages or at berthing places where the limits of the automation have been reached. In order to take over direct control from automation to operator, coordination must be carried out within the context of Human-Automation cooperation.

Monitoring: Monitoring includes the observation and evaluation of the MASS (the ship and the automation) and the environment or situation in which the MASS is located. The aim is therefore to recognise deviations or anomalies in order to be able to react to them. Operators in the ROC monitor by receiving information about relevant processes via displays and control panels. Alarms also help them to quickly draw attention to a deviation or anomaly.

Figure 1 shows the ROC from a human factors perspective. The different control modes are represented as potential actors. Although the crew on board and the automation of the MASS are located outside the ROC, they are important actors to the overall concept. Depending on the degree of automation, a crew on board may be optional.

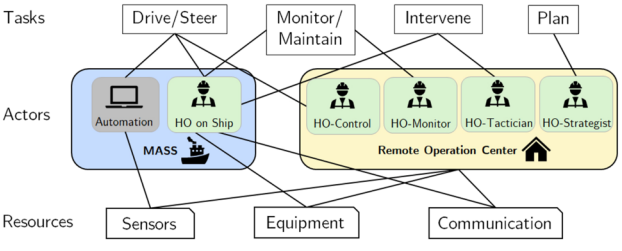

Figure 1: Tasks, actors, and resources derived from ISO/TS 23860.

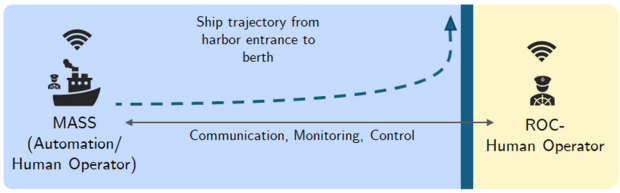

Figure 2: Use case: MASS maneuvering from harbor entrance to berth, adapted from Saager et al. [50].

3.2 Use case example: takeover request during port entrance

To substantiate our approach, we sketch a use case for which a MASS-ROC certification may be required. Consider a shore-based ROC controlling a MASS in a harbor where berthing is generally difficult due to its geometry. For our use case we assume that a MASS – controlled by the automation – approaches the harbor area and wants to dock at the berth. In addition, there is a crew on board that can take over some nautical or technical tasks if required. The ROC operator assists the ship in safely entering the port and during the berthing maneuver. Here, support is provided either tactically by intervening in the automation, or – if necessary – by directly controlling individual ship functions remotely. Figure 2 depicts this use case which is considered a typical process occurring in daily ship operations. The goal is to certify this MASS-ROC pair for this use case efficiently.

Next, we want to model a functional architecture for this use case. This forms the basis for a subsequent HARA and also for a potential database scheme. The results can therefore fill the hazard database with content for that use case. This, in turn, aids the certification process for other ROC-MASS pair in this use case.

3.3 Functional architecture

We start by modeling the functional architecture of a generic MASS-ROC pair at a high level of abstraction with a focus on the flow of information. This functional architecture, shown in Figure 3, serves as a starting point for building a hazard database as it defines generic interfaces between the involved entities. Note that the abstraction level needs to be detailed enough to enable the identification and analysis of hazards and abstract enough to keep HARA efforts manageable. Inside the ROC itself, we model exactly one control station with three components:

Data Communication Middleware (DCM): This component is responsible for managing the exchange of data between the ROC and the MASS. As indicated by the blue color coding, this component is present in the MASS as well. However, for brevity, we abstain from explicitly modeling it within the MASS here. Crucially, the DCM defines the interfaces between the ROC and the MASS. As input to the ROC we have the transfer of all relevant data from the MASS. This inncludes the MASS's data model and environment model.

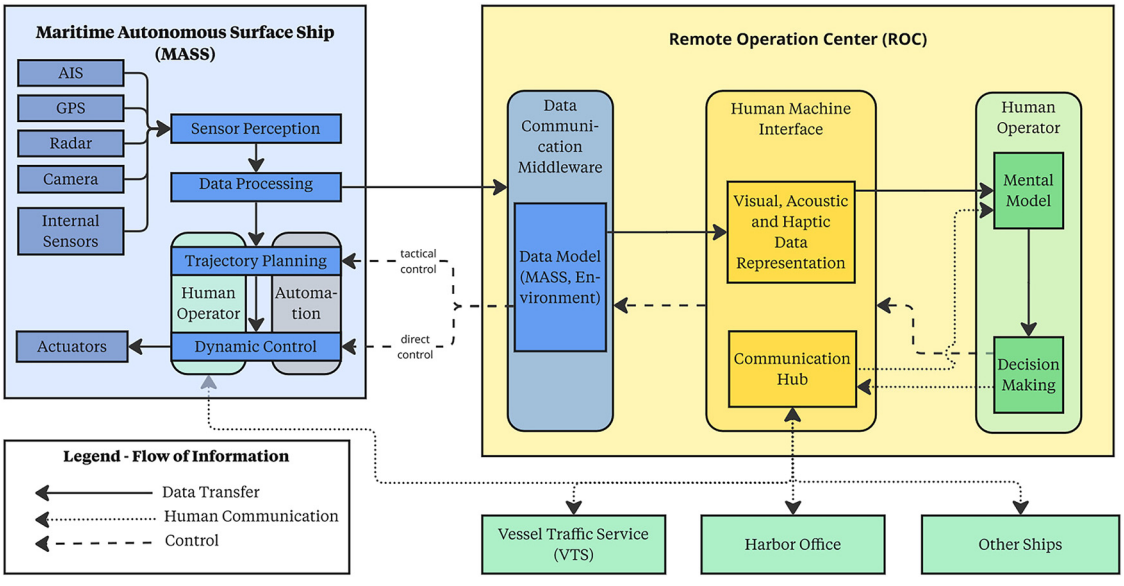

Figure 3: Functional architecture for a single control station inside a shore-based ROC and a generic MASS. The flow of information in encoded by three different types of arrows.

On the side of the ROC's output, the DCM facilitates remote control (direct or tactical) of the MASS by the ROC's human operator.

Human Machine Interface (HMI): The HMI bridges the gap between all inputs to the ROC and its outputs by interacting with the ROC's human operator. In particular, the HMI feeds the human operator's mental model with a visual, acoustic and haptic representation of data as well as human communication from external entities such as the MASS's human operator (if present), vessel traffic service (VTS), the harbor office, and other ships. His mental model infuses the decision making which directly leads to the human operator's output in form of either taking control of the MASS or communication with other humans – both of which are managed by the HMI's communication hub.

Human Operator: The final component of the ROC is the human operator. All his actions within the ROC are through the HMI. His output is the HMI's input and vice versa as described before in Section 3.1.

The functional architecture of Figure 3 can now be used with various HARA methods. For example, it supports keyword-based approaches to hazard identification such as HAZOP – which are also suggested by RBAT [[34], § 4.2]. Note that for a concrete ROC, the level of detail should be expanded locally when conductive for hazard identification and analysis. e.g., applying the keyword *not provided* to *visual, acoustic, and haptic representation of data*, a more detailed modeling of the HMI's data representation functionality becomes necessary. If one wants to use STPA, a corresponding control loop can easily be derived from the architecture of Figure 3. Moreover, methods for causal analysis such as FTA/ETA or causal Bayesian [51] networks profit greatly from a functional architecture, because it supports the modeling of the system's internal dependencies.

4 Building a hazard database for remote operation centers

Similar to the database of criticality phenomena for automated driving systems suggested in previous work, cf. Neurohr et al. [[38], § 4.2.1] and Babisch et al. [52], we propose to collect generic safety artifacts for maritime ROCs in a *Hazard-DB*. This Hazard-DB can include suitable abstractions of.

- hazards and their potential sources,
- the corresponding causal relations [53],
- risks and harms associated with these hazards, and
- strategies and mechanisms for risk mitigation.

When such safety-relevant artifacts have been identified and analyzed during a HARA for a concrete MASS-ROC pair, they can be integrated into the Hazard-DB, cf. Figure 4. This includes an appropriate abstraction step, as the goal is to reuse these artifacts for future HARAs.

4.1 Categorization of hazard sources

In order to gain an initial structure for HARA artifacts within a hazard database, we derive the following categorization of sources of hazard directly from the functional architecture of Figure 3:

Data Communication: This category includes technical hazards sources in the data communication between the ROC and the MASS on a technical level. Examples would be a disturbed and non-redundant communication channel, software failures in the DCM, but also include erroneous sensor data due to perception failures on the MASS.

Human Machine Interface: This category contains technical hazards sources originating in the HMI located in

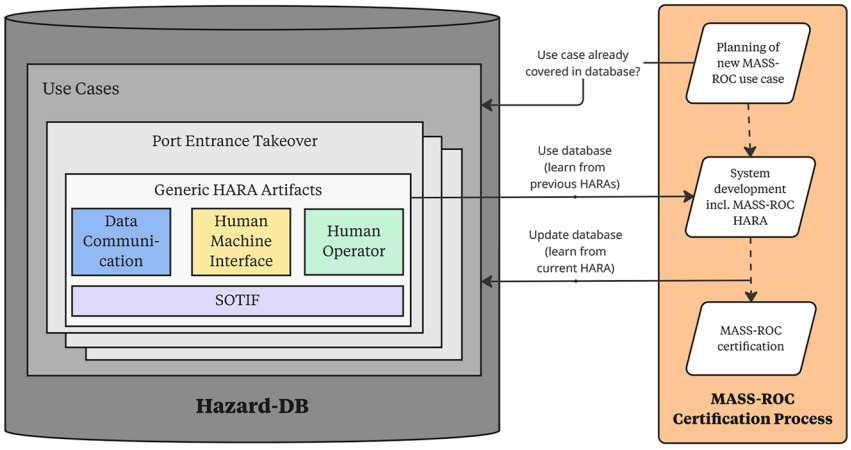

Figure 4: Concept for a hazard database supporting the certification process of a MASS-ROC pair.

the ROC. Examples include the malfunctioning of displays, software failures related to the user interface, or alarm system failures.

Human Operator: This category consists of hazards originating from the behavior of the human operating the ROC. Included here are errors of commission, errors of omission, lack in skills (e.g. remote operating via a joystick, lacking knowledge of vessel), erroneous interpretation of data, and misuse of the HMI.

Additionally, we argue that the **Safety of the Intended Functionality** (SOTIF) is relevant for ROC safety and, as a category, complementary to the above. SOTIF covers hazards that are caused by so called functional insufficiencies, i.e. limitations of the technical capabilities and insufficiencies of the specification, including the inability to handle reasonably foreseeable misuse, as well as overall insufficiencies in the HMI design (e.g., too small fonts, too low contrast, cluttering, and information overload). Depending on the type of remote operation, the human operator is responsible for monitoring, direct, strategic or tactical control. As the operator is not on the vessel, all decisions must be derived based on data acquired through some kind of sensor input. Thus, similar to automated drivings systems governed by the ISO 21448 standard [14], it is imperative to ensure that the sensor data and their subsequent processing deliver sufficient information to enable, in this case the human operator, to effectively execute their designated tasks.

Viewing our categorization of hazard sources for maritime ROCs through the ISO 21448's lens, we spot several potential connections. Both, the technical data communication as well as the HMI are considered to be within the scope of SOTIF. Functional insufficiencies concerning the technical communication may include, for example, an inadequate handling of signal dead zones or inference caused by signal jamming. For the HMI, functional insufficiencies may concern the information presented to the HO, e.g., an inadequate warning presented data are outdated. Moreover, in the SOTIF context, the human operator's behavior is analyzed in terms of direct and indirect misuse. We remark that all these considerations are applicable for maritime ROC safety.

4.2 Concept for a hazard database

Based on the categorization of hazard sources we provide a first sketch of how a hazard database could support the certification process of a MASS-ROC pair, cf. Figure 4.

The Hazard-DB contains use cases, exemplified by 'Port Entrance Takeover', which encompasses generic HARA artifacts rooted in the categories from the functional architecture of Figure 3: Data Communication, Human Machine Interface, Human Operator, and SOTIF. The certification workflow demonstrates a cyclical process beginning with the planning of new MASS-ROC use cases, progressing through system development with an integrated HARA, and culminating in the MASS-ROC certification.

The concept employs a bidirectional knowledge transfer mechanism: it leverages existing database knowledge from previous HARAs to inform current analyses while simultaneously updating the database with insights from ongoing HARA processes, thereby creating a continuous learning framework that enhances the accuracy and comprehensiveness of future risk assessments for MASS-ROC pairs. Once the Hazard-DB underwent the inital set up for a given use case, we can subsequently expect an efficiency increase regarding the future certification processes.

4.3 Preliminary suitability analysis

In order to grasp which of the HARA methods of Section 2 have the potential to support the build-up of a hazard database, cf. Figure 4, we performed a preliminary, expert-based evaluation of their applicability to the three categories of hazard sources plus SOTIF. For each method, we evaluated whether it is applicable for technical hazard sources (i.e., data communication and human machine interface), human hazard sources, and whether SOTIF aspects are addressed appropriately.

Table 1 shows the results of this preliminary suitability analysis. A green check mark means that the method supports the category by design, a orange check mark means the method has been extended to this category, and a red cross encodes that the method has not been applied yet. Note that we did not evaluate to what degree the methods (or their extensions) cover these categories.

Summarizing Subsection 4.3, we see an expected divide between methods that natively cover technical hazard and those that were designed for human factors. Therefore, to generate results that densely fill the Hazard-DB, we want to either.

(i) choose a universal method with adequate extensions to all categories such as STPA, or
(ii) combine a technical method with a human factors method, e.g., RBAT and FRAM.

Finally, we want to emphasize the integration of SOTIF aspects for all three categories. Neglecting functional insufficiencies or foreseeable misuse, e.g., in the HMI design, can easily lead to accidents during operations.

Table 1: Overview which HARA methods address the introduced categories of hazard sources. A green check mark means “supported”, an orange check mark means “could be extended to”, and a red cross means “not supported”.

	Data communication	Human machine interface	Human operator	SOTIF aspects
STPA [35]	✓	✓	✓ [54]	✓ [14]
FMEA [24]	✓	✓	✓ [45]	✗
FTA [29]	✓	✓	✓ [30]	✓ [31]
ETA [32]	✓	✓	✓ [30]	✗
HAZOP [28]	✓	✓	✓ [55]	✓ [31]
RBAT [5]	✓	✓	✗	✓
Bayesian networks [33]	✓	✓	✓ [56]	✓ [51]
Automation risks [31]	✓	✓	✗	✓
FRAM [43]	✓	✓	✓	✗
SHERPA [41]	✗	✗	✓	✗
THERP [42]	✗	✗	✓	✗
SLIM [46]	✗	✗	✓	✗
Petro-HRA [47]	✗	✗	✓	✗
APOA [48]	✗	✗	✓	✗
CRIOP [49]	✗	✗	✓	✓

5 Conclusions

In this paper, we laid first steps towards building a hazard database for certification of shore-based ROCs. Based on a generic MASS-ROC functional architecture we derived three different categories of hazard sources while identifying SOTIF as a relevant, complementary category. Moreover, we performed a preliminary suitability analysis of HARA methods which may cover these categories.

Regarding future work, conducting a HARA for a concrete shore-based ROC by combining adequate techniques will enable the initial build-up of safety artifacts for the envisioned Hazard-DB.

Research ethics: Not applicable.
Informed consent: Not applicable.
Author contributions: All authors have accepted responsibility for the entire content of this manuscript and approved its submission.
Use of Large Language Models, AI and Machine Learning Tools: None declared.
Conflict of interest: The authors state no conflict of interest.
Research funding: None declared.
Data availability: Not applicable.

References

[1] International Organization for Standardization, “ISO/TS 23860: Ships and marine technology — vocabulary related to autonomous ship systems,” 2022.

[2] C. G. Debouche *et al.*, *Remote Operation Centers for Autonomous Ships*, Barcelona, Universitat Politècnica de Catalunya, 2024.

[3] K. Bratić, I. Pavić, S. Vukša, and L. Stazić, “A review of autonomous and remotely controlled ships in maritime sector,” *Trans. Marit. Sci.*, vol. 8, no. 02, pp. 253—265, 2019.

[4] M. Wylie and E. Rajabally, “Safety assurance of maritime autonomous surface ships,” *J. Phys.: Conf. Ser.*, vol. 2867, no. 1, p. 012045, 2024.

[5] K. Kvinnesland, A. Snilstveit Hoem, S. Øie, and R. Brensdal Pederson, “RBAT — method description,” European Maritime Safety Agency (EMSA), Lisbon, Tech. Rep., 2024.

[6] International Maritime Organization (IMO), “Interim guidelines for MASS trials,” 2019.

[7] International Maritime Organization (IMO), “Maritime safety committee — 110th session (MSC 110), 18-27 June 2025,” 2025 [Accessed: July. 30, 2025].

[8] DNV, “Part 6 additional class notations, chapter 12 autonomy and remote operation. Rules for classification,” 2024.

[9] DNV, “Autonomous and remotely operated ships. Class guideline DNV-CG-264,” 2024.

[10] DNV, “Competence of remote control centre operators. *Standard DNV-ST-0324*,” 2022.

[11] DNV, *Certification Scheme for Remote Control Centre Operators*, Recommended Practice DNV-RP-0323, 2021.

[12] T. Jung, M. C. Harre, N. Rousselle, A. Lüedtke, and M. Saager, “CMOROC Identification of Competences for MASS Operators in Remote Operation Centre,” European Maritime Safety Agency (EMSA), Lisbon, Tech. Rep., 2023.

[13] International Organization for Standardization, “ISO 26262: Road vehicles — functional safety,” 2018.

[14] International Organization for Standardization, “ISO 21448: Road vehicles — safety of the intended functionality,” 2022.

[15] L. Putze, L. Westhofen, T. Koopmann, E. Böde, and C. Neurohr, “On quantification for SOTIF validation of automated driving systems,” in, *2023 IEEE Intelligent Vehicles Symposium (IV)*, Anchorage, AK, USA, 2023, pp. 1—8.

[16] C. Alexander Thieme, I. Bouwer Utne, and S. Haugen, "Assessing ship risk model applicability to marine autonomous surface ships," *Ocean. Eng.*, vol. 165, pp. 140—154, 2018.
[17] Z. Li, D. Zhang, B. Han, and C. Wan, "Risk and reliability analysis for maritime autonomous surface ship: A bibliometric review of literature from 2015 to 2022," *Accid. Anal. Prev.*, vol. 187, p. 107090, 2023.
[18] X. Y Zhou, Z. J. Liu, F. W Wang, Z. L. Wu, and R. D Cui, "Towards applicability evaluation of hazard analysis methods for autonomous ships," *Ocean. Eng.*, vol. 214, p. 107773, 2020.
[19] K. Wróbel, J. Montewka, and P. Kujala, "System-theoretic approach to safety of remotely-controlled merchant vessel," *Ocean. Eng.*, vol. 152, pp. 334—345, 2018.
[20] K. Wróbel, J. Montewka, and P. Kujala, "Towards the development of a system-theoretic model for safety assessment of autonomous merchant vessels," *Reliab. Eng. Syst. Saf.*, vol. 178, pp. 209—224, 2018.
[21] O. A. Valdez Banda, S. Kannos, F. Goerlandt, P. H. A. J. M. van Gelder, M. Bergström, and P. Kujala, "A systemic hazard analysis and management process for the concept design phase of an autonomous vessel," *Reliab. Eng. Syst. Saf.*, vol. 191, p. 106584, 2019.
[22] I. Schjølberg, ASME (American Society of Mechanical Engineers), "Risk management of autonomous marine systems and operationAs," in *Structures, Safety and Reliability of International Conference on Offshore Mechanics and Arctic Engineering, Volume 3B*, Trondheim, Norway, ASME, 2017. https://doi.org/10.1115/omae2017-61645.
[23] K. Wrobel, P. Krata, J. Montewka, and T. Hinz, "Towards the development of a risk model for unmanned vessels design and operations," *TransNav Int. J. Mar. Navig. Saf. Sea Transport.*, vol. 10, no. 2, pp. 267—274, 2016.
[24] SAE International, "SAE J 1739-2021 - potential failure mode and effects analysis (FMEA)," in *Supplemental FMEA-MSR, and Process FMEA*, Warrendale, Pennsylvania, USA, SAE International, 2021.
[25] N. Kök and M. S. Yıldız, "New generation fmea method in automotive industry: An application," *J. Turk. Oper. Manag.*, vol. 7, no. 1, pp. 1630—1643, 2023.
[26] S. Narayanagounder and K. Gurusami, "A new approach for prioritization of failure modes in design fmea using anova," *World Acad. Sci. Eng. Technol.*, vol. 49, nos. 524-31, 2009.
[27] S. M. M. El-Awady, "Overview of failure mode and effects analysis (fmea): A patient safety tool," *Glob. J. Qual. Saf. Healthc.*, vol. 6, no. 1, pp. 24—26, 2023.
[28] International Electrotechnical Commission *et al*., *IEC 61882: Hazard and Operability Studies (HAZOP studies)—Application Guide*, Geneva, Switzerland, International Electrotechnical Commission, 2001.
[29] W. E. Vesely, F. F. Goldberg, N. H. Roberts, and D. F. Haasl, *Fault Tree Handbook*. Technical report, Washington DC, Nuclear Regulatory Commission, 1981.
[30] D. Birch, E. Miller, and T. Bradley, "Human reliability analysis using a human factors hazard model," *J. Syst. Saf.*, vol. 58, no. 2, pp. 7—29, 2023.
[31] B. Kramer, C. Neurohr, M. Büker, E. Böde, M. Fränzle, and W. Damm, "Identification and quantification of hazardous scenarios for automated driving," in *Model-Based Safety and Assessment*, M. Zeller and K. Höfig, Eds., Cham, Springer International Publishing, 2020, pp. 163—178.
[32] C. A. Ericson, "Event tree analysis (chapter 12)," in *Hazard Analysis Techniques for System Safety*, Hoboken, New Jersey, John Wiley & Sons, Ltd, 2005, pp. 223—234.
[33] J. Pearl, *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*, San Francisco, CA, USA, Morgan Kaufmann Publishers Inc., 1988.
[34] J. Pearl, *Causality*, 2nd ed. Cambridge, Cambridge University Press, 2009.
[35] N. G. Leveson and J. P. Thomas, *STPA Handbook*, MIT — Massachusetts Institute of Technology, 2018.
[36] E. Böde *et al*., "Identifikation und Quantifizierung von Automationsrisiken für hochautomatisierte Fahrfunktionen," Institute for Information Technology (OFFIS e.V.), Oldenburg, Germany, Tech. Rep., 2019.
[37] S. Vander Maelen *et al*., "An approach for safety assessment of highly automated systems applied to a maritime traffic alert and collision avoidance system," in *2019 4th International Conference on System Reliability and Safety (ICSRS),* Rome, Italy, 2019, pp. 494—503.
[38] G. Hake, J. S. Becker, A. Austel, L. Putze, and N. Wetzig, "Safety assessment of maritime autonomous surface ships: A scenario-based approach," *J. Phys.: Conf. Ser.*, vol. 3123, p. 012022, 2025. in press, https://doi.org/10.1088/1742-6596/3123/1/012022.
[39] A. W. Douglas and S. A. Shappell, "A human error approach to aviation accident analysis: The human factors analysis and classification system," *Aviat. Space Environ. Med.*, vol. 74, no. 11, pp. 1006—1016, 2003.
[40] S. T. Chen, A. Wall, P. Davies, Z. Yang, J. Wang, and Y. H. Chou, "A human and organisational factors analysis method for marine casualties using HFACS-maritime accidents," *Saf. Sci.*, vol. 60, pp. 105—114, 2013.
[41] D. Embrey, "SHERPA: A systematic human error reduction and prediction approach," in *Proceedings of the International Topical Meeting on Advances in Human Factors in Nuclear Power Systems*, Knoxville, TN, USA, American Nuclear Society, 1986, pp. 184—193.
[42] A. David Swain and H. E. Guttmann, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*. Technical report, Albuquerque, NM (USA), Sandia National Labs., 1983.
[43] E. Hollnagel, *FRAM: The Functional Resonance Analysis Method: Modelling Complex Socio-Technical Systems*, Farnham, UK, Ashgate Publishing, 2012.
[44] E. Hollnagel, *Cognitive Reliability and Error Analysis Method (CREAM)*, Amsterdam, Elsevier, 1998.
[45] W. Song, J. Li, H. Li, and X. Ming, "Human factors risk assessment: an integrated method for improving safety in clinical use of medical devices," *Appl. Soft Comput.*, vol. 86, p. 105918, 2020.
[46] M. Aydin, Ö. Uğurlu, and M. Boran, "Assessment of human error contribution to maritime pilot transfer operation under HFACS-PV and SLIM approach," *Ocean. Eng.*, vol. 266, p. 112830, 2022.
[47] C. Blackett, J. E. Farbrot, S. Øie, and M. Fernander, "The petro-HRA guideline Rev. 1 vol. 1.," *IFE — Institute for Energy Technology, Kjeller, Norway, Tech. Rep.*, 2022.
[48] S. Øie and M. Fernander, *Analysis of Pre-accident Operator Actions (APOA)*, DNV, 2023.
[49] Å. S. Hoem, Ø. J. Rødseth, and S. O. Johnsen, "Adopting the CRIOP framework as an interdisciplinary risk analysis method in the design of remote control centre for maritime autonomous systems," in *Advances in Safety Management and Human*

Performance, P. M. Arezes and R. L. Boring, Eds., Cham, Springer International Publishing, 2021, pp. 219—227.
[50] M. Saager, M. C. Harre, and A. Hahn, "Towards modelling cooperation in future maritime remote-control center," in *Design for Equality and Justice. INTERACT 2023*, Springer, Cham, Lecture Notes in Computer Science, 2024.
[51] R. Gansch, L. Putze, T. Koopmann, J. Reich, and C. Neurohr, "Causal bayesian networks for data-driven safety analysis of complex systems," in *Model-Based Safety and Assessment*, Cham, Springer Nature Switzerland, 2026, pp. 222—237.
[52] S. Babisch, C. Neurohr, L. Westhofen, S. Schoenawa, and H. Liers, "Leveraging the GIDAS database for the criticality analysis of automated driving systems," *J. Adv. Transp.*, vol. 2023, no. 1, pp. 1349269—25, 2023.
[53] T. Koopmann, L. Putze, L. Westhofen, R. Gansch, A. Adee, and C. Neurohr, "Grasping causality for the explanation of criticality for automated driving," *IEEE Access*, vol. 13, pp. 54739—54756, 2025.
[54] Megan Elizabeth France, *Engineering for Humans: A New Extension to STPA, PhD thesis*, Massachusetts Institute of Technology, Cambridge, 2017.
[55] J. Dunjó, V. Fthenakis, J. A. Vílchez, and J. Arnaldos, "Hazard and operability (HAZOP) analysis. A literature review," *J. Hazard. Mater.*, vol. 173, pp. 19—32, 2010.
[56] P. Trucco, E. Cagno, F. Ruggeri, and O. Grande, "A bayesian belief network modelling of organisational factors in risk analysis: A case study in maritime transportation," *Reliab. Eng. Syst. Saf.*, vol. 93, no. 6, pp. 845—856, 2008.

Bionotes

Christian Neurohr
German Aerospace Center (DLR e.V.), Institute of Systems Engineering for Future Mobility, Oldenburg, Germany
christian.neurohr@dlr.de

Christian Neurohr received the B.Sc. and M.Sc. in Mathematics in 2011 and 2013 from RPTU Kaiserslautern, Germany and his pH.D. (Dr. rer. nat.) from Carl von Ossietzky Universität Oldenburg, Germany in 2018. After a short period as a visiting researcher at the University of Sydney, he started his occupation as a postdoctoral researcher at the German Aerospace Center (DLR e.V.) Institute of Systems Engineering for Future Mobility where he is working in the area of scenario-based verification and validation of automated vehicles. Since 2023 he has lead the 'Criticality Analysis' team within the division 'Theory and Design'.

Marcel Saager
German Aerospace Center (DLR e.V.), Institute of Systems Engineering for Future Mobility, Oldenburg, Germany
marcel.saager@dlr.de

Marcel Saager received the B.A. in Business and Economics and M.Sc. in Business Information Systems in 2016 and 2019 from Carl von Ossietzky Universität Oldenburg, Germany. After two years as a Modelling- and Software Engineer at Humatects, a company specialized in Human Machine Interaction Solutions, he started his occupation as a doctoral researcher at the German Aerospace Center (DLR e.V.) Institute of Systems Engineering for Future Mobility where he is working in the area of human factors and human centered engineering of highly automated vessels and trains. Furthermore he works and worked as a Lecturer at University of Oldenburg, Private University of Applied Sciences Vechta and University of Applied Sciences in Nuertingen-Geißlingen.

Lina Putze
German Aerospace Center (DLR e.V.), Institute of Systems Engineering for Future Mobility, Oldenburg, Germany
lina.putze@dlr.de

Lina Putze received the B.Sc. and M.Sc. degrees in Mathematics from the University of Münster in 2016 and 2019, specializing on the topics of stochastic processes, probability theory and its applications. She is currently working as a researcher at the group System Concepts and Design Methods at the German Aerospace Center (DLR e.V.) Institute of Systems Engineering for Future Mobility. The focus of her research is on methods to ensure trustworthiness of highly automated transport systems in different domains, including the identification and analysis of hazards and risk triggering scenario properties, causal analysis and risk assessment.

Eckard Böde
German Aerospace Center (DLR e.V.), Institute of Systems Engineering for Future Mobility, Oldenburg, Germany
eckard.boede@dlr.de

Eckard Böde received his Dipl.-Inform. degree in Computer Science from the Carl von Ossietzky University, Oldenburg, Germany, in 2001. He subsequently joined OFFIS e.V., where he focused on safety assessment and model-based safety analysis for aerospace and automotive applications. In 2012, he was appointed Group Leader for Safety Analysis and Verification. He currently leads the R&D group System Concepts and Design Methods at the German Aerospace Center (DLR e.V.), Institute of Systems Engineering for Future Mobility. His research interests include methods and tools for the design and verification of trustworthy cyber-physical systems, with a particular emphasis on safety assessment of automated systems and the integration of functional safety with SOTIF in safety cases.

Axel Hahn
German Aerospace Center (DLR e.V.), Institute of Systems Engineering for Future Mobility, Oldenburg, Germany
axel.hahn@dlr.de

Axel Hahn holds a Doctorate in Mechanical Engineering from the University of Paderborn. He currently serves as the Director of the German Aerospace Center (DLR e.V.) Institute of Systems Engineering for Future Mobility, which emerged from the former Transportation Division of OFFIS. In addition, he has a professorship at the Carl von Ossietzky University Oldenburg. His work centers on dependable and intelligent systems in mobility and transport, with a focus on software engineering, system architecture, and safety-critical applications across the automotive, maritime, and aeronautics domains. With a strong interdisciplinary orientation, he bridges research and practical innovation in digitization, automation, and systems engineering. He has led numerous national and European research projects and actively contributes to shaping future mobility concepts through both technical leadership and strategic guidance.