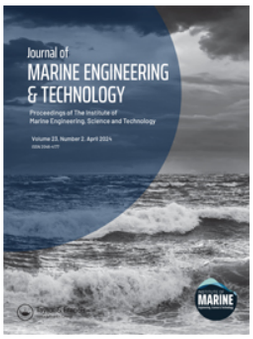

Taylor & Francis
Taylor & Francis Group

Journal of Marine Engineering & Technology

ISSN: 2046-4177 (Print) 2056-8487 (Online) Journal homepage: www.tandfonline.com/journals/tmar20

A systems approach to hazard identification for solar-powered and wave-propelled unmanned surface vehicle

S. D. Kristensen, A. Dallolio & I. B. Utne

To cite this article: S. D. Kristensen, A. Dallolio & I. B. Utne (2024) A systems approach to hazard identification for solar-powered and wave-propelled unmanned surface vehicle, Journal of Marine Engineering & Technology, 23:2, 122-134, DOI: 10.1080/20464177.2024.2315646

To link to this article: https://doi.org/10.1080/20464177.2024.2315646

© 2024 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group.

View supplementary material

Published online: 12 Feb 2024.

Submit your article to this journal

Article views: 1450

View related articles

View Crossmark data

Citing articles: 10 View citing articles

Full Terms & Conditions of access and use can be found at
https://www.tandfonline.com/action/journalInformation?journalCode=tmar20

JOURNAL OF MARINE ENGINEERING & TECHNOLOGY
2024, VOL. 23, NO. 2, 122–134
https://doi.org/10.1080/20464177.2024.2315646

Taylor & Francis
Taylor & Francis Group

OPEN ACCESS Check for updates

A systems approach to hazard identification for solar-powered and wave-propelled unmanned surface vehicle

S. D. Kristensen[a], A. Dallolio[b] and I. B. Utne[a]

[a]Department of Marine Technology, NTNU Norwegian University of Science and Technology, Trondheim, Norway; [b]Department of Engineering Cybernetics, NTNU Norwegian University of Science and Technology, Trondheim, Norway

ABSTRACT

Decarbonization is a trend in the maritime industry and may include the use of alternative energy sources on ships. At the same time, autonomous ships are under development. In the future, the two technologies may be combined. The objective of this study is to identify possible hazards related to the operation of autonomous vessels using green energy sources. An extended and holistic Systems-Theoretic Process Analysis (STPA) based approach is proposed, where both safety and security is considered. Changes in level of autonomy during operation are considered, and an extension of the STPA method is proposed to highlight the interaction between the system and external energy source. A solar-powered and wave-propelled unmanned surface vehicle is analysed. The results show that mission performance may be affected by both safety and security issues, and that considering influences from the environment and the autonomous functionalities of the system together, contributes to identifying hazards. The results are compared to operational experience from multiple field campaigns. The case study focuses on a relatively simple autonomous vehicle, but some functionalities may be shared with Maritime Autonomous Surface Ships (MASS). Hence, implications for utilisation of alternative energy sources on MASS, and effects on risks, are discussed.

ARTICLE HISTORY
Received 31 August 2023
Accepted 4 February 2024

KEYWORDS
STPA; hazard identification; unmanned surface vehicle (USV); renewable energy sources; maritime autonomous surface ship (MASS)

1. Introduction

Maritime autonomous surface ships (MASS) are currently under development, and prototypes are being tested (IMO 2023). With the advancements in information and communication technology, ships with automated and autonomous functionalities can be developed, and they may in the future operate independently from human operators. The development towards an increased level of autonomy (LOA) for ships is motivated by a possible increase in safety, cost-efficiency, and environmental performance (DNV 2018). However, more research is required before the safety performance of future MASS can be determined (Wróbel et al. 2017).

The risks related to the operation of MASS are being investigated. Hazard identification is the first element of risk analysis and can be defined as 'The process of identifying and listing the hazards and accidents associated with a system' (DEF STAN 00-56 2007). The objective is to identify all relevant hazards for the system (Rausand and Haugen 2020). The hazards related to MASS must be identified before they can be put into operation. Zhou et al. (2020) investigate 29 different approaches to hazard analysis of conventional ships and evaluate their applicability to autonomous ships. Systems-Theoretic Process Analysis (STPA) is the only method that fulfils all the derived evaluation criteria and is found to be a promising method for hazard analysis for autonomous ships. The usefulness of STPA for hazard analysis of autonomous marine systems is supported by other studies (Thieme et al. 2018; Yang and Utne 2022).

Requirements to hazard identification methods for MASS have been developed, and include identification of hazards on the system level, relating to both safety and security, covering software, hardware, and interactions between humans and the technical system (Zhou et al. 2020). Hence, a hazard identification method for MASS must be holistic. STPA has been applied to MASS (Wróbel et al. 2018; Chaal et al. 2020). Yang et al. (2020) uses STPA to identify hazards for autonomous marine systems as a function of their LOA. STPA has also been used for both safety and security analysis. Young and Leveson (2013) present Systems-Theoretic Process Analysis for Security (STPA-Sec), an extension of STPA for safety and security analysis. STPA-Sec has been extended with the use of STRIDE (spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege) to classify attacks and develop security-related scenarios (Kaneko et al. 2018; Souza et al. 2020).

Different autonomous marine systems are under development, and their operation may be associated with different risks (Utne et al. 2017). Hence, the terminology used to describe the systems may be important to define. With respect to surface vehicles, it may be separated between unmanned surface vehicles (USVs) and autonomous surface vehicles (ASVs), where an USV operates without the presence of human operators onboard the vehicle, while an ASV operates independently of human operators, and may be unmanned (Vagale et al. 2021). In the context of the regulatory scoping exercise for autonomous ships, a MASS was defined as 'a ship which, to a varying degree, can operate independent of human interaction' by the International Maritime Organization (IMO) (IMO 2021). Separating between a MASS and a USV or ASV may be done by investigating the definition of a ship (as in MASS), and a vehicle (as in USV and ASV). A ship may be defined as 'any large floating vessel capable of crossing open waters' (Davies et al. 2023). In addition, it is stated that the term, in modern times, is used for vessels with a displacement of over 500 tons. Based on these

CONTACT S. D. Kristensen susanna.d.kristensen@ntnu.no Department of Marine Technology, NTNU, 7491, Trondheim, Norway

Supplemental data for this article can be accessed online at https://doi.org/10.1080/20464177.2024.2315646.

© 2024 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group.
This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

references, it may be observed that USVs, ASVs, and MASS refer to different types of vehicles, and that differences may be related to the presence of crew on the vehicle, ability to operate independently from human operators, and size of the vehicle.

In addition to the development of different autonomous marine systems with increasing LOA, decarbonisation is an important trend in the maritime industry. Transportation at sea is considered to be an energy efficient option, compared to other modes of transportation (Bouman et al. 2017). However, when it comes to emissions to air, shipping was responsible for 2.2% percent the total CO_2 emissions globally in 2012, and the IMO has defined a target of reducing the greenhouse gas emissions from the maritime industry with 50% percent compared to the 2008 level within 2050 (IMO 2018). Local requirements are also being developed, such as zero emission from ships operating in world heritage fjords in Norway within 2026 (Norwegian Maritime Authority 2023). Hence, there is a pressure on the maritime industry to reduce emissions (DNV 2022). Alternative fuels and alternative energy sources must be a part of the solution, together with other measures related to ship design and operation (Bouman et al. 2017).

The effect of the use of green energy sources on the safety of ships is under investigation. Alternative fuels and energy sources may be used to reduce the emissions from ship operations (DNV 2022). However, the effect on the operational risk must also be considered. The IMO has provided guidelines on the use of alternative fuels. Extensive risk assessment is required to show that the alternative systems are equally safe as conventional fuel systems (DNV 2022).

The use of green energy on ships, together with the trend of digitalisation, for example with increased use of advanced control systems, may be seen as two important parallel developments (DNV 2022; Joung et al. 2020). This implies that the technologies can be combined and integrated in ships in the future. Potentially, this may lead to safer and more environmentally friendly ship operations. A prerequisite for this would be a thorough investigation of the risks related to the operation of systems that utilise these functionalities together, starting with identification of possible hazards.

The objective of this study is to identify the hazards related to the combination of green energy and autonomous functionalities on ships. From the reviewed literature, it can be seen that previous research has been focussed on hazard identification for ships using renewable energy, and for ships with increasing LOA, but only to a limited extent on the hazards associated with the combination of these technologies. Because decarbonisation of the shipping fleet and increasing levels of autonomy are two developments in the industry today, an investigation of the hazards related to the combination of the technologies is relevant.

A holistic method for hazard identification is proposed, where the focus is on the interactions between the autonomous system and the environment, with the purpose of identifying hazards related to the combination of the use of renewable energy and autonomy. The method is based on STPA, and includes previously developed extensions for security analysis, and analysis of systems with dynamic LOA. An addition to the existing methodology is described, which includes a focus on the interaction between the system and the environment, as this interaction is increasingly important with the use of alternative energy sources. There are two novel contributions with respect to the method. The first is an addition to the existing STPA method that includes a focus on the interaction between the system and possible alternative energy sources from the environment. The second contribution is the combination of existing methodologies to a holistic STPA method that considers relevant elements for a hazard identification for an autonomous vehicle. The method is applied to a solar-powered and wave-propelled USV in a case study.

This paper is structured as follows: in Section 2, the proposed hazard identification method is presented. In Section 3, a case study is described, and the results of the case study are presented. The results are discussed in Section 4. In Section 5, a conclusion is given, and indications for further work are described.

2. Method

For hazard identification for MASS, STPA has been found to be a suitable method. This is because it is applicable for conceptual systems as well as existing systems, and because it has been proven to handle complex and software-intensive systems well (Leveson 2011). It is also because the method has been found to be an applicable hazard identification technique for MASS in previous studies (Thieme et al. 2018; Yang and Utne 2022). The STPA method is applicable for complex, socio-technical systems, and has been applied to many different domains, at different points in the system life cycle (Leveson and Thomas 2018). An advantage of STPA is that it is applicable in the early phases of the system life cycle before the detailed design is finished. STPA is based on systems theory, and views safety as a control problem. Because of this, it is possible to include hazardous scenarios not only related to component failures, but also related to unsafe system interactions (Rausand and Haugen 2020; Leveson and Thomas 2018). In addition, STPA makes it possible to include different aspects of the system, including software, human, and organisational elements (Leveson and Thomas 2018). This is an advantage over other hazard identification methods that focus on only the technical system, as some causal factors can be ignored if the broader socio-technical system is not considered. As MASS are complex systems, that are a part of a larger socio-technical context, the advantages of applying the STPA method may lead to a more comprehensive analysis than other hazard identification methods.

For a hazard identification of an autonomous ship to be holistic and identify relevant hazards, safety and security must be included. For the security analysis, STPA-Sec is a relevant method because it builds on STPA and is meant to be used for cyber-physical systems (Young and Leveson 2013). STPA plus STPA-Sec has also been described as a comprehensive method that can identify more hazards compared to other methods for safety and security co-analysis, specifically for highly autonomous systems (Torkildson et al. 2018). Because the method has been found to produce comprehensive results, and because it builds on STPA, which has been found to be an applicable hazard identification method for MASS, STPA plus STPA-Sec is found to be an applicable method for this analysis. To support the identification of security-related scenarios, STRIDE is used. A STRIDE-enforced STPA-Sec analysis is therefore applied to incorporate the security aspect into the hazard identification.

A MASS may potentially use renewable energy sources. In that case, the method must facilitate the identification of hazards related to the interactions between the system and the external energy source. In systems theory, a division is often made between the system and the environment, where a boundary is drawn between that which can be controlled, and that which cannot be controlled (Leveson and Thomas 2018). The first is then defined as the system, and the latter is defined as the environment. The environment may still influence MASS. An additional step is added to focus on the influence of the environment as input to the system, and the effect on the system safety.

Autonomous ships may operate with varying LOA during one operation (Yang et al. 2020). To capture hazards related to switching between operational modes, selected additional steps from the STPA-based approach presented by Yang et al. (2020), are used.

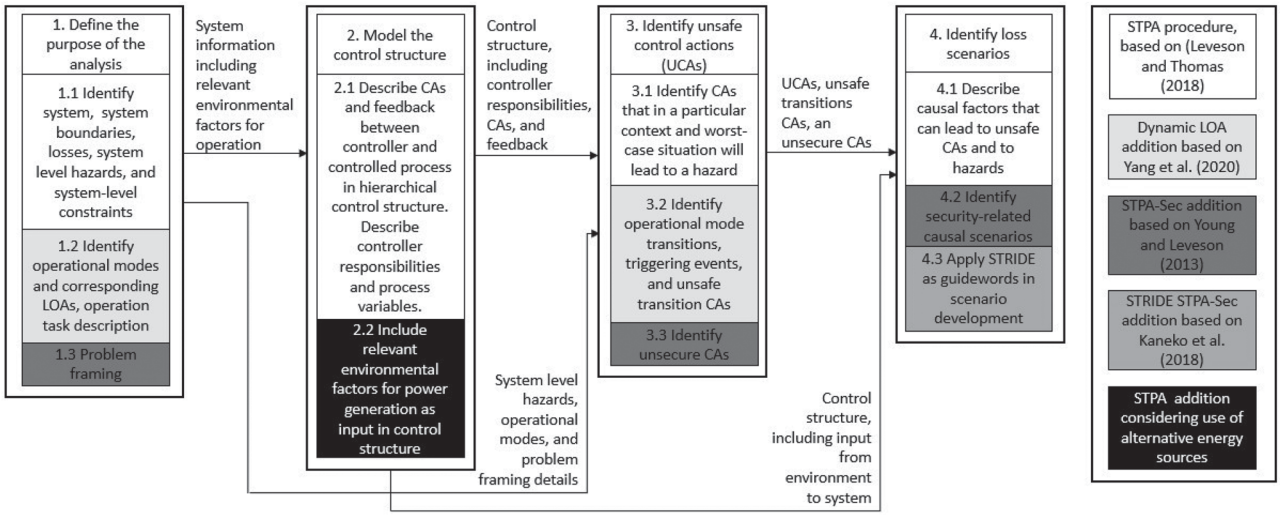

Figure 1. Illustration of the extended methodology. STPA procedure description (white) based on Leveson and Thomas (2018), STPA-Sec procedure description (dark grey) based on Young and Leveson (2013), STPA method considering dynamic STPA addition (light grey) based on Yang et al. (2020), and STRIDE STPA-Sec addition (medium grey) based on Kaneko et al. (2018). Additions related to inclusion of green energy aspects are illustrated in black.

2.1. Proposed method

The method used in this paper builds on STPA, and the four main phases of the method, with additional steps in each phase, are illustrated in Figure 1. STPA is a hazard identification method where safety is viewed as a control problem. To reduce risks, new or different safety constraints must be implemented in the system through control actions (CAs) (Leveson and Thomas 2018). The description of the four main phases of STPA are based on the descriptions by Leveson and Thomas (2018). STPA-Sec is an extension of the STPA process, and the additional steps of the method are described by Young (2020). STRIDE is used in the development of scenarios, based on the approach by Kaneko et al. (2018). Analysing hazards related to autonomous systems operation, including transitions between operational modes, is described in Yang et al. (2020). Further, a step is added to the method to include the effect of the use of green energy on the system.

2.1.1. Define the purpose of the analysis

Step 1.1 has five main objectives. Firstly, the system must be described and the system boundaries determined. Secondly, losses are identified. A loss is defined as an unacceptable loss of something that is valued by stakeholders, which might include human life and health, assets, efficiency, and product quality, and should be identified at a system level (Leveson and Thomas 2018). Next, system-level hazards are identified. A hazard is described as a 'system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss' (Leveson and Thomas 2018). System-level hazards can be states or events. The fourth objective is to define system-level constraints corresponding to the hazards. Lastly, the system-level hazards can be refined, and more detailed hazards defined.

According to Yang et al. (2020), the first phase of the analysis should include a description of the operational modes of the autonomous system under analysis, and corresponding LOAs. This is added as step 1.2 in the methodology.

The first phase includes a STPA-Sec addition, namely problem framing, which is step 1.3. This includes clearly stating the purpose of the system or activity, and is meant to help prevent misunderstandings, and ensure that the assets valued by stakeholders are protected (Young 2020). Problem framing includes describing the problem, the method, the goal, and the constraints.

2.1.2. Model the control structure

The second phase includes modelling the control structure. A hierarchical control structure is defined as 'a system model that is composed of feedback control loops' (Leveson and Thomas 2018). Step 2.1 is to develop a structure that consists of controllers and controlled systems. CAs are used to enforce constraints on the behaviour of the controlled system, and feedback is used to update the execution of the CAs. The control structure is hierarchical, meaning that the controllers are placed according to their authority in the system. The term *control* must be interpreted in a broad sense, and controllers can be everything from governmental agencies to single technical components in the system (Leveson and Thomas 2018). The control structure is developed based on the system description and boundary definition defined in step 1.1. In addition to defining the control structure, controller responsibilities and associated process variables are defined for all controllers in the system.

As the focus of the analysis is on hazards related to the use of renewable energy sources, a step 2.2 is added in the method to emphasise the interaction between the system and the energy sources that are part of the environment. The focus area of step 2.2 is illustrated in Figure 2. This step includes adding relevant environmental factors for power generation in the control structure, as input to the affected part of the control structure. This is done to clarify the dependency between the power generation in the system and the environment. An explicit illustration of the interaction between the environment and the generation of power in the system is necessary and will contribute to the identification of interactions that may lead to losses in later stages of the hazard identification.

2.1.3. Identify unsafe control actions

Identifying unsafe control actions (UCAs) is the third phase of the STPA process. A UCA is a 'control action that, in a particular context and worst-case environment, will lead to a hazard' (Leveson and Thomas 2018). In step 3.1, UCAs are identified. CAs can be unsafe in four different ways; by not providing the CA, by providing the CA, by providing a CA too early, too late, or in the wrong order, or by

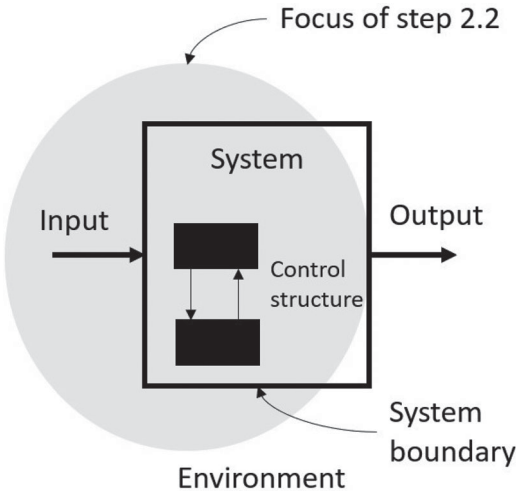

Figure 2. The purpose of step 2.2 in the method is to identify and add the relevant input from the environment to the system, and allocate the input to the element in the control structure that is influenced.

Figure 3. The AutoNaut USV.

Table 1. AutoNaut: vehicle specifications.

System aspect	Description
Length	5 m
Weight	230 kg (max 360 kg with payload)
Source of power	Solar power
Source of propulsion	Wave energy
Speed	2 knots

applying the CA too long or not long enough. The context of the UCA should describe why the CA is unsafe, which may include operational modes identified in step 1.2.

To incorporate hazards related to transitions between operational modes, transition diagrams and descriptions of triggering events should be included in the third phase of the analysis (Yang et al. 2020), and this is added as step 3.2. This should give input to the identification of UCAs and be included in the description of the context of the UCA in step 3.1 and 3.3.

Step 3.3 is related to security. According to STPA-Sec, identifying UCAs must also include identifying unsecure CAs (Young and Leveson 2013).

2.1.4. Identify loss scenarios

The fourth and last phase is divided into three steps. The first, step 4.1, consists of identifying loss scenarios. A loss scenario includes the causal factors that can lead to CAs being unsafe, and to hazards. These scenarios can lead to UCAs, and to CAs not being executed or not being executed correctly (Leveson and Thomas 2018). The development of scenarios build on the already identified UCAs in phase 3 of the method, and may involve interactions with the environment, as described in the extended hierarchical control structure, defined in step 2.2.

In step 4.2, security-related causal scenarios are assessed, according to Young and Leveson (2013). In this phase, step 4.3 is added to use STRIDE as guide words for the identification of security-related scenarios, according to the method presented by Kaneko et al. (2018). The following description of the STRIDE elements is based on the classification given by Microsoft (2022). The first element of STRIDE is spoofing. This refers to a situation where an attacker uses another user's authentication information to access the system. An example can be to use the username and password of another user. The second element is tampering, which means modification of data. The data can be either stored, or in transit between computers. Repudiation is when a user denies having performed an action, and that there is no approach to confirming if this is true or not. An example can be that a user has bought a service but denies having received this service. Information disclosure is when information is exposed to unauthorised users. This is relevant for data that is stored and data that is transferred. Denial of service is when authorised users cannot access a service, either because the service is out of order or because it is not available. The last element of STRIDE is elevation of privilege. This means that an unauthorised user gains access to the system in the same way as a normal user. In other words, the attacker becomes a part of the trusted system. In combination with STPA-Sec, STRIDE may be used to identify scenarios and causal factors relating to cybersecurity.

3. Case study

The AutoNaut USV (see Figure 3) is used as a case study. The vehicle operates without human presence on board and under normal operation, the vehicle operates autonomously. The vehicle can be operated by a human operator at a remote location, for example in emergency situations or for navigation in enclosed areas. Vehicle specifications are mentioned in Table 1. The descriptions given in this section are based on the system design and control architecture presented by Agdal (2018), Dallolio (2022), and Dallolio et al. (2019).

The forward propulsion of the vehicle is ensured by using wave foil technology. Two foils attached to the hull transform wave motions to forward propulsion, independently of the wave and vehicle directions. The vehicle is also equipped with a thruster for use in emergency situations or in flat sea. Photovoltaic (PV) panels are used to power the electric thruster, and all other electric systems on board the vehicle.

Three distinct levels are used to describe the vehicle control architecture. Level 1 is named *system monitoring and fallback autopilot*. The level is responsible for monitoring the health of the system, distributing power to other modules, and handling navigation if the main navigation system is unable to perform this function. Level 2 is *navigation and collision avoidance*, consisting of both necessary sensors and computational units. Level 3 is the *scientific system*, and has sensors for performing the missions specified by the operator, and a computational unit for handling the gathered data.

An on-board power management system (PMS) is used to handle the generation, storage, and distribution of power on the vehicle,

and is a part of level 1. This system consists of three PV panels for harvesting energy and four batteries for storing the power. Two Maximum Power Point Tracker (MPPT) controllers are used to handle the uneven generation of power from PV panels. This ensures that the charger input will be higher than the minimum voltage requirements. A computer determines the distribution of power in the system, and level 2 and 3 can be disconnected to save power.

The USV has several communication channels. Channels for communication between the USV and the human operator at the shore control centre (SCC) includes VHF radio, internet connection, and Iridium satellite communication. When internet communication is used, new mission plans can be uploaded for local storage on the vehicle. If internet connection is lost, the operator has limited control of the different functionalities of the vehicle. Communication between the USV and other vehicles is through the AIS system. In this way, other vehicles can detect the position of the USV, and obtain information about the speed and heading of the vehicle. Communication between sub-systems consist of Ethernet communication between level 3 and level 2. Communication between Level 1 and level 2 is also wired and performed according to NMAE0183 protocol.

Results from the hazard identification, including the results of the four phases and associated steps of the method, is presented in this section. The full hazard identification result can be seen in the appendix. Hazard identification of technical systems depend on expert knowledge for accuracy and relevance. In addition to the expertise on risk analysis involved in this analysis, three system experts have been consulted in two workshops, one in 2021 and one in 2022, to verify the hierarchical control structure, to identify and verify UCAs, and to give input to the development of scenarios for the UCAs in the extended STPA-based analysis. The system experts have experience with the planning, preparation, and operation of the AutoNaut in different geographical areas in Norway.

3.1. Define the purpose of the analysis

Step 1.1 starts with defining the system, and system boundaries. The USV and the USV operator are the two main elements considered as part of the system under analysis. The defined system and system boundaries are shown in Figure 4.

Secondly, accidents were identified. Several potential accidents are relevant for the AutoNaut vehicle. However, the accidents used here are related to the objectives of this study, based on identified stakeholder values and corresponding unacceptable losses. From the system accidents, system hazards and losses were identified. Three potential safety-related losses were considered in this study:

(1) loss of life or injury to people;
(2) loss of or damage to USV;
(3) loss of scientific mission.

In step 1.3, problem framing and identification of security-specific losses and accidents was performed, to compliment the already specified accidents relating to safety. The results from the problem framing are shown in Table 2. One additional potential loss was specified, namely *4. loss of collected information*. Further, *loss of maneuverability control* was identified to have relevance both for safety and security. System hazards and safety constraints are given in Table 3. Hazard and safety constraint no. seven are related to the security-specific losses.

In step 1.2 the operational modes of the vehicle were identified. The vehicle has three possible operational modes, and transitions between the three modes are determined either by the human operator or by the autonomous system on board the vehicle. The three operational modes, namely normal, manual, and fallback, are described in Table 4.

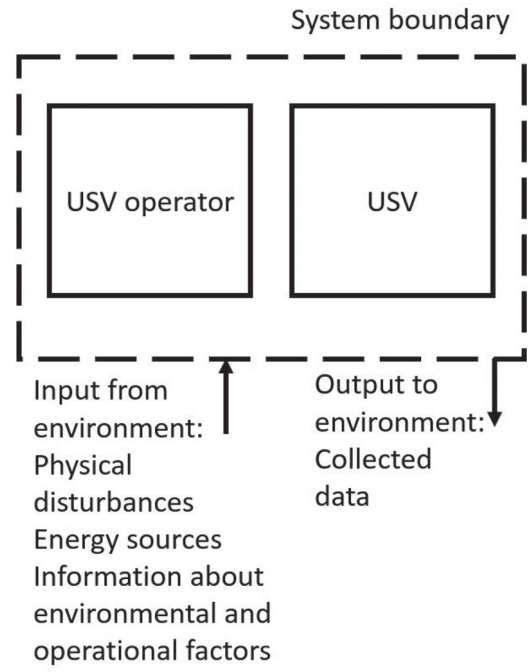

Figure 4. Step 1.1 system and system boundaries.

Table 2. STPA-Sec: problem framing.

Topic	Description
Problem	A vehicle for performing long-lasting scientific missions autonomously
Method	By using renewable energy sources and autonomous functionalities
Goal	Reduce costs and enable continuous monitoring of relevant factors in the sea
Constraints	Maximise system autonomy and measurement performance quality while maintaining an acceptable level of risk

In manual control, the human operator has direct control of the thruster speed and rudder angle on the vehicle. In normal mode, these values are determined by the navigation system module on board the vehicle, based on waypoints determined by the human operator. In fallback mode, pre-determined settings for use of thruster and rudder are enabled, or a fallback autopilot is used. The LOA description in Table 4 is based on Utne et al. (2017).

The typical tasks and related operational modes were described to present the dynamics of the operation. The AutoNaut is used for scientific missions whose objectives concern the upper water column, as described in Dallolio et al. (2019). The vehicle may be deployed from shore by use of a crane or slip, or it can be deployed from a support vehicle. When in the ocean, the vehicle may be controlled by the operator, in manual mode, until the USV is in the desired area of operation. Then, the USV operates in normal mode, meaning without human intervention. The use of renewable energy sources allows the vehicle to perform long-endurance missions, from days to months in duration. The scientific objectives are achieved using sensors to gather specified data, in a route preplanned by the human operator. The vehicle will alter its route to avoid collision and grounding, based on AIS information and electronic navigation charts. When faced with specific pre-defined conditions, such as loss

Table 3. System hazards/threats and safety constraints.

System hazards		Safety constraints	
H1	USV violates minimum safe distance to another moving obstacle in ocean [L1, L2]	SC1	USV must keep safe distance to other vehicles in the ocean
H2	USV manoeuvrability control lost [L1, L2 L3]	SC2	USV must not loose manoeuvrability control
H3	USV does not maintain safe distance to seabed [L2]	SC3	USV must maintain safe distance to seabed
H4	USV does not maintain safe distance to static obstacle [L2]	SC4	USV must maintain safe distance to static obstacle
H5	USV is unable to collect the requested data [L3]	SC5	USV must collect the requested data
H6	USV does not operate in defined area [L3]	SC6	USV must operate in defined area
H7	Collected information lost to unauthorised person [L4]	SC7	Information must not be exposed to unauthorised sources

Table 4. Operational modes of AutoNaut.

Operational mode	Description	LOA
Manual	Operator controls USV.	LOA 1
Normal	Autonomous system executes mission based on specifications (waypoints) from operator.	LOA 2
Fallback	USV uses defined rudder angle and thruster intensity, or activates autopilot to keep defined course.	LOA 2

of communication when in manual mode, the USV can enter fallback mode. Updates to the pre-planned route can be communicated from the operator to the vehicle during operation, by use of internet or satellite communication.

3.2. Control structure model

In step 2.1, the hierarchical control structure was developed based on the system description and boundaries defined in phase 1. Because the focus of the analysis was on production and use of power, power management, PV panels, and batteries are added as separate units in the control hierarchy. Supply of power is added in the diagram, to illustrate the distribution of power through the system. In the hierarchy, red arrows indicate control actions and blue arrows indicate feedback. The control hierarchy can be seen in Figure 5. Certain components were left out of the control hierarchy, including for example bilge pumps and signal lights. The reason for this is that they were considered to not be of primary importance for this analysis.

The responsibilities and associated process variables were described for all controllers. The controller responsibility and process variables are used in the development of UCAs and causal scenarios. For the power management module, responsibilities include providing power settings to other modules on the vehicle during all operational modes. The controller responsibility has the following related process variables:

PV 1 possible power settings (scientific module/advanced navigation module on/off);
PV 2 critical battery level threshold;
PV 3 estimated power consumption;
PV 4 estimated power generation;
PV 5 estimated battery storage level;
PV 6 component error status.

The human operator provides control actions related to many of the aspects of the operation of the USV. With respect to power management, the operator has the responsibility to provide power settings to other modules on the vehicle during manual operation. The controller responsibility has the following related process variables:

PV 1 possible power settings (scientific module/advanced navigation module on/off);
PV 2 mission specifications;
PV 3 power status for vehicle;
PV 4 weather forecast for area of operation;
PV 5 bathymetry and obstacles in area of operation.

In step 2.2, the relevant inputs from the environment of the vehicle were added in the hierarchy. The environment is not a part of the system, according to systems theory, as it cannot be changed or controlled by the system designers. However, a vehicle using green energy sources, such as the AutoNaut, is strongly dependent on environmental factors, and the relationship between the vehicle and the environment is therefore added to clarify the dependency. The result of step 2.2 can be seen in Figure 5, where arrows are pointing from the Environment box to different elements in the control structure. Sun exposure affects the generation of power in the PV panels, and wave, currents, and wind affect the propulsion and steering.

3.3. Unsafe control actions

In step 3.1, UCAs were identified for all control actions in the hierarchy, based on the guide words mentioned in Section 2.1. The identified operational modes from step 1.2 were used to specify the context of the UCAs.

In step 3.2, transitions between the different modes of operation were identified, to assist the identification of possible unsafe transitions. The transitions and triggering events are described in Figure 6. The illustration of the triggering events shows how the system can change between different operational modes during operation. This may happen due to active commands or based on the technical condition of the components of the vehicle. The human operator can give commands to change mode of operation. If the communication between the operator and the vehicle fails, or if communication between the modules in the vehicle fail, the vehicle will automatically enter fallback mode. If communication is restored, the operation mode changes back to the original mode of operation before the loss of communication connection. The different operational modes are described in Table 4.

In total, 56 UCAs were identified. Because the focus of the analysis was on the power management, and effects on risk, the UCAs identified for two control actions related to power management, one from the power management module, and one from the operator, are focussed on, and presented in Table 5.

Because the control actions chosen for this example are discrete control actions, no UCAs could be identified in the *stopped too soon/applied too long* category. Some CAs may be related to both safety and security, as the version of the CA is hazardous regardless of if it happens due to intentional or unintentional actions. In step 3.3 of the analysis, no unsecure CAs were identified in addition to the ones that were already found in the STPA.

3.4. Loss scenarios

In step 4.1, causal scenarios were identified for all UCAs. In accordance with the focus of this analysis, scenarios that were developed

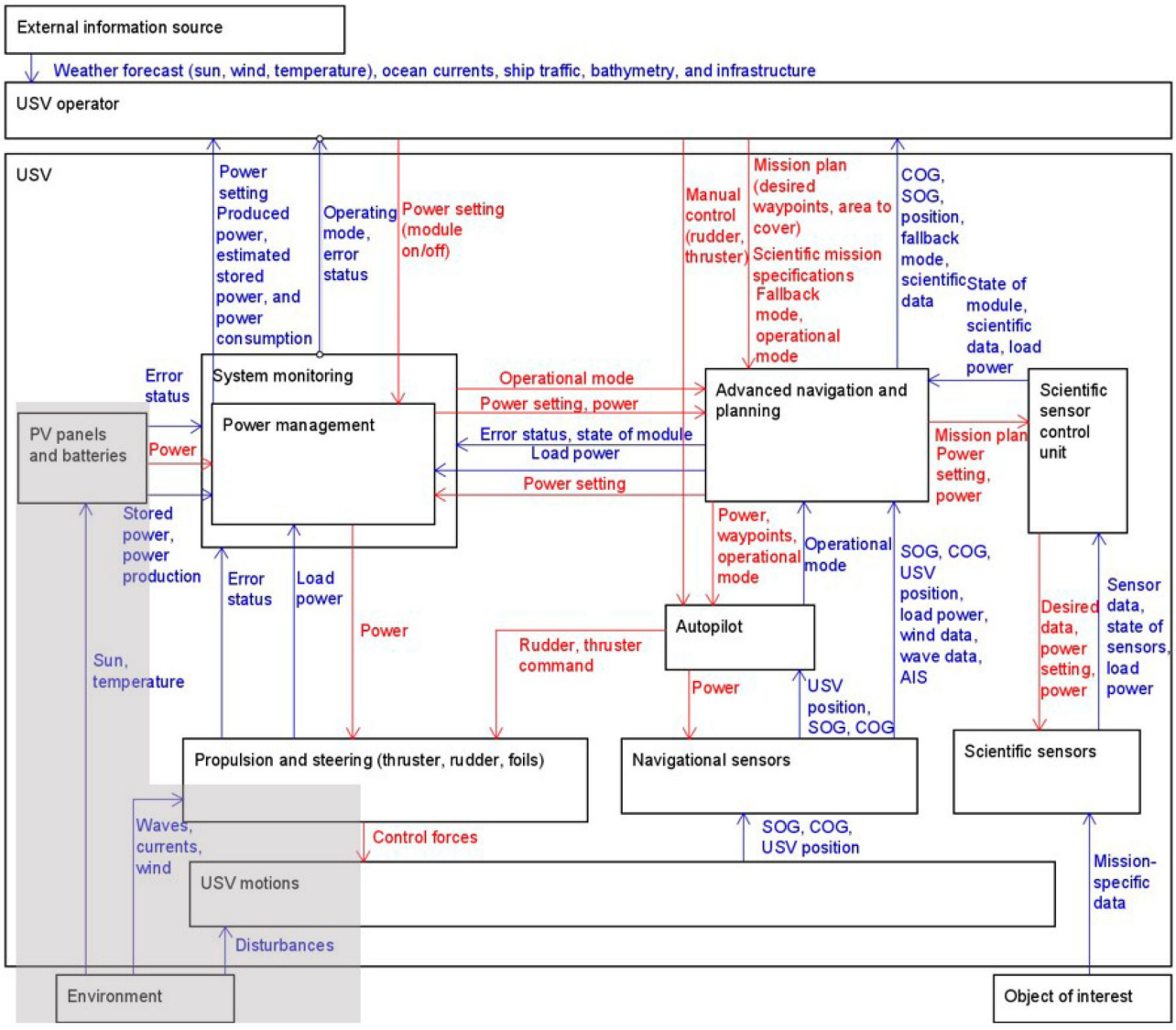

Figure 5. Safety control hierarchy for the AutoNaut. Diagram made in the software by Information-Technology Promotion Agency, Japan (2018). The grey area is added as a result of step 2.2.

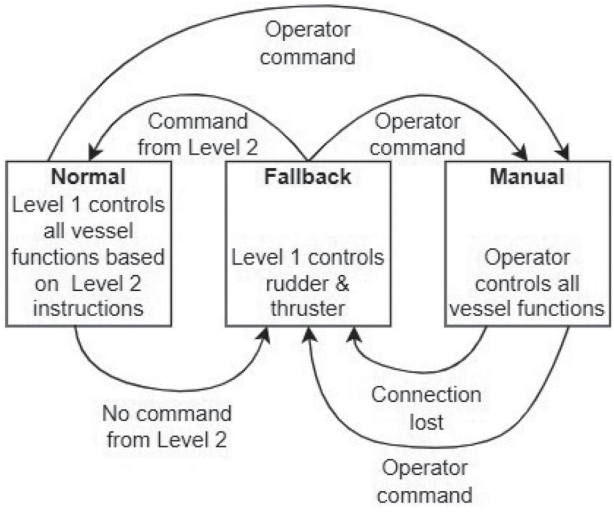

Figure 6. Transitions and triggering events for the three operation modes for AutoNaut, adapted from Agdal (2018).

for the UCAs related to the power management in the system were highlighted. The elements included in the extended control structure presented in Figure 5, are considered in the identification of scenarios and causal factors. The CAs from the power management module are related to controlling the use of the advanced navigation system and the scientific data collection system, Level 2 and Level 3 in the system, respectively. The CAs from the operator are related to controlling the use of all power-consuming equipment, including Level 2 and Level 3, thrusters, and rudders.

The detailed analysis for one UCA related to each of these controllers is presented. The scenarios, and corresponding causal factors for *[UCA5-N-1] PMS does not provide command 'Turn off advanced navigation module' when there is insufficient power during normal operation*, are shown in Table 6. The example shows both how scenarios can lead to UCAs (S-1), and how CAs can be executed incorrectly or not executed at all (S-2, S-3). Scenarios and causal factors for a UCA related to the power setting commands from the operator were also included, namely for *[UCA2-N-1] Operator does not provide command 'Turn off advanced navigation module' when there is insufficient power during manual operation*, as shown in Table 7.

Table 5. Example of identified unsafe control actions related to power management for the AutoNaut.

Control action	Not providing	Providing causes hazards	Too early/too late	Stop too soon/applied too long
Power setting from power management system to advanced navigation system module	PMS does not provide command 'Turn off advanced navigation module' when there is insufficient power available during normal operation [SC2] PMS does not provide command 'Turn on advanced navigation module' when there is sufficient power during normal operation [SC6]	PMS provides command 'Turn off advanced navigation module' when there is sufficient power during normal operation [SC1][SC3][SC4][SC6] PMS provides command 'Turn on advanced navigation module' when there is insufficient power available during normal operation [SC2]	PMS provides command 'Turn off advanced navigation module' too late after insufficient power is available during normal operation [SC2] PMS provides command 'Turn off advanced navigation module' too early before insufficient power is available during normal operation[SC6] PMS provides command 'Turn on advanced navigation module' too late after sufficient power is available during normal operation [SC6] PMS provides command 'Turn on advanced navigation module' too early before sufficient power is available during normal operation [SC2]	Not applicable
Power setting from operator to power management system	Operator does not provide command 'Turn off advanced navigation module' when there is insufficient power during manual operation [SC2]	Operator provides command 'Turn off advanced navigation module' when there is sufficient power during manual operation [SC6]	Operator provides command 'Turn off advanced navigation module' too late after insufficient power is available during manual operation [SC2] Operator provides command 'Turn off advanced navigation module' too early before insufficient power is available during manual operation [SC6]	Not applicable

Table 6. Loss scenarios for [UCA5-N-1] PMS does not provide command 'Turn off advanced navigation module' when there is insufficient power during normal operation [SC2].

	Causal scenario	Causal factors
S-1	PMS is not notified of power shortage when power level is critical, and does not turn off module, which might lead to loss of power	Feedback of current power consumption is delayed/not received by PMS because of failure in communication line (physical failure) Feedback of current power consumption is incorrect because of sensor failure Message of generated/stored power is delayed/not received by PMS because of failure in communication line Feedback of generated/stored power is incorrect because of sensor failure
S-2	PMS does not consider power level to be critical and does not turn off module, which might lead to a loss of power	Correct feedback is received but process model is flawed, and operator can not correct it due to failure of communication line PMS believes power generation capabilities are higher than they are, because equipment has failed but PMS is not notified PMS does not believe that equipment that uses power is online (scientific system, thruster), when it is online and consuming power Storage capacity of batteries is degraded due to low temperatures, making power level more critical than anticipated Power level is critical considering future weather states, but this information is not available to the PMS
S-3	PMS provides the command, but the message is not received by the advanced navigation module, which might result in loss of power	The connection between the modules is broken Software updates to the computers lead to incompatible communication between the modules

In step 4.2 and 4.3, security-related causal scenarios were developed for each of the unsecure CAs. In the same way as for safety-related causal scenarios, hazardous scenarios can happen due to unsecure CAs and CAs not being performed correctly. Scenarios can include inadequate feedback, problems with the control path, controlled processes or unsafe controller behaviour. However, for security-related scenarios, the search focus is on system vulnerabilities to external sources of hazard. Security-related causal scenarios were investigated for the same UCAs that were investigated in the STPA. The additional security-related scenarios and causal factors are presented. The causal factors are labelled with the associated STRIDE element. Security-related scenarios for the unsecure CA [UCA5-N-1] are given in Table 8. Security-related scenarios for the unsecure CA [UCA2-N-1] are given in Table 9. As can be seen in the table, no security-related causal factors could be found for scenario S-3.

4. Discussion

The results of the hazard identification for the AutoNaut USV points to several safety and security issues for a USV using renewable energy sources. The focus of the analysis is on hazards related to the use of green energy sources and autonomous functionalities on surface vehicles, as this is a combination of functionalities that may be expected in the future. The following topics are discussed:

Table 7. Loss scenarios for [UCA2-N-1] Operator does not provide command 'Turn off advanced navigation module' when there is insufficient power during manual operation [SC2].

	Causal scenario	Causal factors
S-1	Operator does not consider the power level to be critical, and does not provide command to turn off module, which might lead to loss of power	Vehicle is outside internet and satellite coverage, restricting the communication of detailed information about the power status on the vehicle One or more PV panels are not producing electricity, and the failure is not known to the operator who believes the power generation capacity is higher than it is Battery capacity is degraded due to low temperatures, but this is not known to the operator who believes the capacity is higher than it is Future weather/sea state is more critical than anticipated, resulting in lower power generation and/or higher power consumption than anticipated The operator believes that the system is capable of performing power management, and that manual commands are not necessary Inference between satellite and internet communication restricts communication of detailed information about the power status of the vehicle
S-2	Operator sends message to turn off module but the message is not transmitted/not transmitted correctly, which causes the equipment to continue to consume power, which might lead to loss of power	Vehicle is capsized and not able to self-correct its stability due to environmental loads, causing antennas to stay under water, restricting communication Software updates have been implemented, and control action messages are not formulated according to updates communication channel standards There is no communication connection between the operator and the vehicle, because the vehicle is outside internet and satellite communication coverage
S-3	Operator considers the use of the advanced navigation module to be necessary considering the environment, and does not turn off module, which might lead to loss off power	The vehicle is in the middle of an evasive maneuver, and the advanced navigation system is necessary to avoid violating safe distance to obstacle

Table 8. Security-related loss scenarios for [UCA5-N-1] PMS does not provide command 'Turn off advanced navigation module' when there is insufficient power during normal operation [SC2][SC7].

	Security-related Causal scenario	Classification	Causal factors
S-1	PM system is not notified of power shortage when power level is critical and does not turn of module, which might lead to loss of power	Denial of service	PM module is denied access to power status for components, because attacker has gained access to communication channel
		Physical security	Vandalism against computers/communication lines on vehicle
S-2	PM system does not consider power level to be critical, and does not turn of module, which might lead to loss of power	Spoofing	Attacker accesses control system through operator username and password and changes PM battery level threshold
		Tampering	Feedback of battery power level has been altered by intervention from attacker
S-3	PM provides the command, but the intended message is not received by the advanced navigation module, which might lead to loss of power	Spoofing	Attacker accesses control system through operator username and password and implements control command

Table 9. Security-related loss scenarios for [UCA2-N-1] Operator does not provide command 'Turn off advanced navigation module' when there is insufficient power during manual operation [SC2][SC7].

	Security-related Causal scenario	Classification	Causal factors
S-1	Operator does not consider the power level to be critical, and does not provide command to turn off module, which might lead to loss of power	Spoofing	Unauthorised user accesses control system through operator username and password and inserts incorrect information
		Tampering	Feedback messages from USV components have been altered by intervention from unauthorised source, and this is not detected by operator
		Physical security	Antenna on vehicle is damaged by attacker, making system unable to convey information
S-2	Operator sends message to turn off module, but the message is not transmitted/ not transmitted correctly, which causes the equipment to continue to consume power, which might lead to loss of power	Physical security	Antenna on board vehicle has been broken by attacker
		Physical security	Message is not received because the vehicle has been completely submerged in water, due to intervention by attacker, causing damages to the communication system
S-3	–	–	–

(1) hazard identification results;
(2) use of hazard identification results for improved design and risk-awareness for the AutoNaut;
(3) the application of the extended STPA method for including external energy sources;
(4) case study result implications for use of renewable energy for MASS;
(5) limitations and uncertainties.

4.1. Hazard identification results

The AutoNaut has been used for several missions, where hazards have been encountered and detected. The identified safety and security issues from the hazard identification can be compared with the operational experience described by Dallolio (2022).

Several safety issues identified in the hazard identification are related to the functionality of the power management process model, where results show that the choice to power down modules on the

USV is important for the risks in the system. This corresponds to the operational experience from a real mission, where it was necessary to retrieve the USV due to lack of power. Incorrect estimation of consumed power can lead to misjudgements in the distribution of power, like shutting down modules too late when it is necessary to save power. Evaluating the availability of power is dependent on the process model, and the available feedback related to the energy source.

The operational experience shows that the operator plays an important role in the operation of the USV. The operator develops the initial operation plan, based on the scientific mission requirements and information about the area of operation. The results from the hazard identification show that the properties of the planned mission are important. If the mission is specified so that the USV encounters hazardous situations, such as not being able to produce enough power, the USV has limited abilities to mitigate the risks without intervention from the human operator. The hazard identification results indicate that the communication between the operator and the USV is important for the safe operation of the vehicle. Missing, delayed, or corrupted messages between the USV and the operator can cause hazardous situations.

Hazards related to security have not been met in the documented operational experience. This means that the available literature and existing hazard identifications of similar systems must be used to verify the results. The results from these analysis may be used for comparison.

Kavallieratos et al. (2019) identified the SCC as one of the more vulnerable elements of a general MASS system. This agrees with the results in the hazard identification, as security scenarios related to the SCC and the communication between the operator and the vehicle, were identified in the analysis. Further, the authors identified the security related to the engine automated system to be less critical than the other elements of the autonomous ship, based on the likelihood and impact of potential attacks. Several scenarios identified in the hazard identification, were related to attacks against the power management of the AutoNaut. In this way, the results from the literature differ from the hazard identification results.

Thieme et al. (2019) identified physical security as an issue in the analysis of the security of an autonomous ferry. Scenarios including vandalism against the vessel and control centre were identified in the STPA-based hazard identification for the AutoNaut. In this way, the results from the analysis are in line with the results presented in the literature.

Situations where the operator receives wrong or missing data from the USV due to attacks, were also identified in the hazard identification. Considering the operational profile of the USV, where the operator plays an important role in operation, the information received about the state of the system may have large implications for the operational decisions. If these decisions are made based on wrongful or missing data, accidents may happen.

4.2. Use of hazard identification results for improved design and risk-awareness for the AutoNaut

The STPA-based hazard identification results obtained in Section 3 show the high correlation between the on-board architecture design and the operational hazards. The main driver that characterises the hardware and software architectures design is the scientific objectives to which the vehicle is dedicated. At the design stage, scientific objectives translate to technological constraints that concern endurance, manoeuvrability and capability of the vehicle to successfully accomplish field campaigns. The technological limitations are considered when the on-board system is designed and implemented. An extensive hazard evaluation, as performed above, plays an essential role in this context and provides valuable insights that help the engineers improve and correct the architecture during the design stage. This analysis can be executed offline and support the design phase prior to field exercise, or it may provide a foundation for an online risk model, i.e. a risk model that supports the decision-making by the MASS during operation, by providing frequently updated estimates of risk based on different sources of data (Utne et al. 2020).

Increasing the autonomy of the USV is of primary interest. The STPA-based hazard identification could be a basis for changing a platform designed for human-in-the-loop control for surface observations, to a vehicle which can take high level human intent, and break it down into actionable tasks, while being critically aware of operational risks related to technological failures, shallow bathymetry, surface traffic, low solar irradiance or overly calm waters. Doing so will require the ability to autonomously monitor itself to prevent future failures, by tasking itself with new goals without human intervention. Capabilities of this kind are hindered by a number of factors due to the variation and unpredictability of the environments. For example, while the vehicle has a well-defined situational awareness of the environment, the onboard goal-driven autonomy must trade operational risk in the 'here and now' with the desire and intent shaped by humans on shore who might not have full situational awareness. This is crucial for the AutoNaut that operates in the open ocean, where the communication can be very limited and the on-board system cannot rely on directives from shore.

4.3. Application of the extended STPA method for including external energy sources

The operation of the AutoNaut includes transitions between different operational modes during the execution of a mission. Considerations with respect to dynamic LOA were included in the analysis, by using certain aspects of the methodology presented by Yang et al. (2020). From the results, it can be seen that the operational mode may be included in the context of the unsafe/unsecure CA. An example is CA5, where the USV should shut down the advanced navigation module when the power level reaches a critical level. If it does not do this, while in normal operation, this can lead to a hazard. If the vehicle is in manual operation, then this decision is made by the operator, and a failure from the PMS is less critical. The extended STPA method shows that the division of responsibility between the different controllers in the hierarchical control structure is important to consider, to avoid hazardous situations. However, UCAs related to the operational modes and unsafe transitions between operational modes have not been the main focus in the analysis. A more detailed analysis of this aspect may be a subject for further work, for example by developing control structures for every operational mode, as suggested by Yang et al. (2020). Nevertheless, the method proposed in this work includes an identification of operational modes, so these can be considered when describing the context of the UCAs. This makes it possible to include the effect of the operational mode on the safety of the system during operation.

An additional step was added to the original STPA procedure for the purpose of identifying hazards for systems using green energy sources. Here, focus was placed on the input from the environment to the defined system. This additional step can give a better foundation for assessing the effect of the interaction with the environment on the system-level risk. This can help when developing loss scenarios. Future MASS may be more reliant on environmental factors if renewable energy sources will be used, and the effect of this must be incorporated in hazard identifications. Even if the environment cannot be controlled by the system designers and is therefore

not normally considered a part of the system according to systems theory, it can still have an extensive influence on the operation of the system. An extended hierarchical control structure including the environmental factors ensures that these are considered in the hazard identification.

The extended methodology made it possible to identify and describe relevant loss scenarios and causal factors. From the results shown in Tables 6 and 7 it can be seen that the temperature in the area of operation and the predicted weather conditions and sea state are identified as causal factors. The two UCAs are based on the same CA, which is to turn off the advanced navigation module. During normal operation, this is the responsibility of the power management module (as in UCA5-N1, Table 6), and during manual operation this is the responsibility of the operator (as in UCA2-N-1, Table 7). In scenario 2 (S-2) related to UCA5-N-1, where the PMS does not decide to reduce the power consumption in the system, because it does not consider the power level to be critical, a causal factor was described to be the lack of feedback available to the PMS. It does not have information about the future weather states, and therefore only a limited ability to evaluate the criticality of the power level. In scenario 1 (S-1) related to UCA2-N-1, where the operator does not decide to reduce the power consumption, other causal factors were identified, as the information about the current and future environmental conditions is meant to be available to the operator. Here, the causal factors are related to how this information can be wrong, not used correctly, or not received by the operator. The scenarios build on the consideration of relevant environmental factors, as shown in the extended control structure. In the examples, the context of the UCA included the operational mode of the system. This shows that the extended methodology may contribute to identifying relevant UCAs, loss scenarios, and causal factors that capture the interaction between the autonomous functionalities and the use of renewable energy from the environment.

An extension of the STPA was added to include security considerations. One example is the identification of the security-related hazard, *H7 Collected information lost to unauthorised sources*. As the gathered information is communicated to the on-shore operator via internet communication and a server, unauthorised sources affecting the communication was identified as a causal factor. Depending on the consequence of loosing information or being restricted from transmitting information between the USV and the operator, this can lead to unacceptable risk levels. Loss of control of the vehicle was defined to have relevance for both safety and security. This may be critical for the AutoNaut because the vehicle can be damaged. However, because of its limited size and speed capacity, the risk of damaging other people or assets might be limited. Nevertheless, the same hazard can exist for larger vehicles with the potential for obtaining a larger kinetic energy. This can potentially lead to risks for people and infrastructure.

The proposed method may have advantages and disadvantages compared to applications of other hazard identification techniques. For the case study, where a small USV was analysed, the use of an extended STPA may be too time and resource demanding. However, for a MASS, there may be a need for a comprehensive method to identify relevant hazards related to both safety and security, and the interactions inside the system, and between the system and the environment. Applying the method to a small USV may have a value, both in identifying system-specific hazards for use in further development of the system, and for testing and demonstration of the proposed method.

The method is focussed on identifying hazards for autonomous vehicles using green energy, but may be applied to vehicles with different LOAs, and energy and propulsion systems. The extension of the method requires a higher workload, as operational modes have to be identified, security scenarios evaluated, and potential influences from the environment included. For conventional ships or MASS with conventional energy and propulsion systems, the method may be applicable, but may not produce any additional results, compared to already existing STPA extensions proposed in the literature.

4.4. Case study result implications for use of renewable energy for MASS

Some of the results from the case study may be relevant not only to the study object, but also to general MASS. With respect to power management, the results from the analysis point to the importance of the choice of the operator and PMS to reduce the navigation capabilities of the vehicle to save power or continue to operate as efficiently as possible with respect to the mission it is performing. The choice of route was also found to be important, as this affects the opportunity to harvest the necessary energy to operate safely, when it is reliant on environmental conditions for propulsion and to power all on-board systems. The ability to incorporate information about the future environmental conditions on the specified route in mission planning and re-planning, is important for safe operation. If the operation is to have a high degree of autonomy, such capabilities must be integrated in the autonomous system itself, and not only be left to the operators. This may be relevant for autonomous vehicles using green energy.

Similarly to the case study USV, future MASS may be unmanned, which may increase the requirement to the robustness of the system design. The hazard identification results, specifically for the analysis of the power setting sent from the power management system and the navigation system, identified a scenario where after a complete loss of power, the vehicle could not re-start the navigation system automatically (See UCA5-N-3 in Appendix A). Loss of power is a critical situation for any vehicle. However, for vehicles using green energy sources, the availability of energy may change during operation, and handling fluctuating energy levels (even including complete loss of power) may be of particular importance. This is because loss of power may result in loss of control of the vehicle. Even for unmanned vehicles, this can lead to great risks to humans, being third parties to the operation of the vehicle. To achieve an acceptable level of risk to people, redundancy in the power generation for the vehicle may be necessary.

The hazard identification results indicate that there is a potential to increase safety by developing an online risk model. This model could provide information to the PMS, and in this way give the PMS the ability to consider risk in its decision making, and consequently improve its operational capabilities. This is illustrated for example in the identified scenarios shown in Table 6; unsafe decisions made in the PMS can lead to loss of control of the vehicle. The online risk model would provide an estimate of the risk that could be considered in the decision-making. However, the risk cannot be the only factor considered when making decisions, and it would have to be balanced with the rewards related to performing a mission with the specifications of the stakeholders. An example is determining if the advanced navigation module should be turned off to save power, which would depend on the associated risks, such as the risk of collision or grounding, and the potential rewards, such as saving power and potentially operating longer, without intervention from the human operator.

4.5. Limitations and uncertainties

The focus of this analysis is on balancing power consumption and generation on the vehicle, and its effect on risk. Consequently, UCAs

relating to other functionalities have not been presented in detail. Examples of these include functionalities related to handling capsizing or full submersion. However, these functions are important for safe operation.

A second limitation is related to the security-related results. As no security-related hazards had been met during the operation of the AutoNaut, developing and verifying the security-related scenarios was challenging. However, the results were compared to, and discussed considering the results from other security analysis of similar systems presented in the literature. This may reduce the uncertainty related to the results.

The transition from the case study results, to more general comments about the relevance for MASS is a source of uncertainty. This is because the analysed USV is a relatively simple system, compared to MASS. However, some functionalities, such as the need for power management may be common between the systems. Nevertheless, the relevance of the results from the case study to MASS will depend on the system design and operational profile for that specific MASS.

5. Conclusion

In this paper, an extended STPA-based approach to hazard identification for autonomous vehicles using renewable energy has been presented. This is based on the need for a holistic hazard identification method for future MASS. Hazards with respect to both safety and security are included in the approach, by using STPA, and its extension, STPA-Sec combined with STRIDE, respectively. Further, an addition to the STPA has been included to cover potential hazards related to the generation and use of green energy sources for autonomous vehicles. This is because the introduction of autonomous vehicles and use of green energy are two important developments in the maritime industry. In the future, the two technologies may be combined, and relevant hazards must be investigated.

The proposed STPA-based approach has been applied to a wave-propelled and solar-powered USV. The analysis identified several important issues with respect to safety and security. The decisions made by the power management module and the human operators related to the prioritisation of power onboard the USV are highlighted as important. When the objective is to perform safe and efficient operation, the results from the analysis show that it is important to balance the risks related to not performing a mission, and the risks related to potential hazardous situations arising if the available power level is becoming critically low. The extended STPA-based approach made it possible to focus on hazards related to the interaction between the system and the environment, when this is necessary for power generation.

Both safety and security aspects have been included in the analysis, and it was found that robust communication links between the operators onshore and the USV is important, but that the risks depend on the consequences of losing information or control of the USV, or being denied access to information from the USV. This is highly mission and context specific. It is also dependent on the ability of the vehicle to operate independently of the operator.

The results from the analysis have been verified by comparing the identified hazards with real operational experience for the USV. The results from the analysis presented in this paper show that accidents during the operation of a USV using green energy can happen because of unsafe control actions from the PMS and the human operator. Causal factors, such as communication failure between the human operator and the vessel and inadequate information for decision-making, were identified. This highlights the value of performing a detailed hazard identification, as it can identify hazards and causal factors in advance, and in this way contribute to design changes and improved operational procedures. Using the hazard identification to develop an online risk model was also discussed. Potentially, this could allow the system itself to make better priorities regarding power expenditure during operation, and consequently, reduce risk. This may also be useful for MASS using green energy.

Further work may include applying the defined method to different systems with different LOAs, and different energy and propulsion systems, to evaluate the usefulness of the method. It may also include developing an online risk model based on the hazard identification results, including defining requirements for the risk model, data collection, and integration with decision support systems or control systems.

Acknowledgments

The authors are very grateful to Professor Tor Arne Johansen, from the Department of Engineering Cybernetics, at the Norwegian University of Science and Technology, and to another system expert, for their participation in workshops, and for sharing their knowledge about the AutoNaut USV. The authors also highly appreciate the valuable comments from the reviewers to an earlier version of the paper.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

The work by Kristensen and Utne was supported by the Research Council of Norway (RCN) (Norges Forskningsråd) through the SFI Autoship project [grant number 309230]. The work by Dallolio was supported by the RCN through the MASSIVE project [grant number 270959], and AMOS [grant number 223254].

References

Agdal BO. 2018. Design and implementation of control system for green unmanned surface vehicle [master's thesis]. Trondheim: Norwegian University of Science and Technology.

Bouman EA, Lindstad E, Rialland AI, Strømman AH. 2017. State-of-the-art technologies, measures, and potential for reducing GHG emissions from shipping—a review. Transp Res D: Transp Environ. 52:408–421. doi: 10.1016/j.trd.2017.03.022

Chaal M, Banda O, Glomsrud J, Basnet S, Hirdaris S, Kujala P. 2020. A framework to model the STPA hierarchical control structure of an autonomous ship. Saf Sci. 132:104939. doi: 10.1016/j.ssci.2020.104939

Dallolio A. 2022. Design and experimental validation of a control architecture for wave-propelled USV: from system design to ocean studies [dissertation]. Trondheim: Norwegian University of Science and Technology.

Dallolio A, Agdal B, Zolich A, Alfredsen JA, Johansen TA. 2019. Long-endurance green energy autonomous surface vehicle control architecture. In: OCEANS 2019 MTS/IEEE SEATTLE.

Davies EAJ, Woodward JB, Stilwell JJ, Vance JE. 2023. ship. Encyclopedia Britannica. [accessed 2023 Aug 23]. https://www.britannica.com/technology/ship.

DEF STAN 00-56. 2007. Safety management requirements for defence systems part 1 requirments. Glasgow: Defence equipment & support, UK defence standardization

DNV. 2018. Group technology and research, position paper 2018: remote-controlled and autonomous ships in the maritime industry. Hamburg: DNV

DNV. 2022. Energy transition outlook—a global and regional forecast to 2050. Høvik: DNV AS. https://www.dnv.com/energy-transition-outlook/.

IMO. 2018. Resolution MEPC.304(72) initial IMO strategy on reduction of GHG emissions from ships. London: IMO

IMO. 2021. Outcome of the regulatory scoping exercise for the use of maritime autonomous surface ships (MASS) msc.1/circ.1638. London: IMO

IMO. 2023. In focus: autonomous shipping. [accessed 2023 Aug 23]. https://www.imo.org/en/MediaCentre/HotTopics/Pages/Autonomous-shipping.aspx.

Information-Technology Promotion Agency, Japan. 2018. STAMP workbench. https://www.ipa.go.jp/en/digital/complex_systems/stamp_wb/manual_en/index.html.

Joung TH, Kang SG, Lee JK, Ahn J. 2020. The IMO initial strategy for reducing greenhouse gas (GHG) emissions, and its follow-up actions towards 2050. J Int Marit Saf Environ Aff Shipp. 4:1–7.

Kaneko T, Takahasaki Y, Okubo T, Sasaki R. 2018. Threat analysis using STRIDE with STAMP/STPA. In: The international workshop on evidence-based security and privacy in the wild. p. 10–17.

Kavallieratos G, Katsikas S, Gkioulos V. 2019. Cyber-attacks against the autonomous ship. In: Computer security: ESORICS 2018 international workshops, CyberICPS 2018 and SECPRE 2018, Barcelona, Spain, September 6–7, 2018, Revised Selected Papers 2. Springer. p. 20–36.

Leveson N. 2011. Engineering a safer world. Cambridge (MA): The MIT Press

Leveson N, Thomas J. 2018. STPA handbook. https://psas.scripts.mit.edu/home/get_file.php?name = STPA_handbook.pdf.

Microsoft. 2022. Microsoft threat modeling tool threats. [accessed 2023 Aug 23]. https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats.

Norwegian Maritime Authority. 2023. Zero emissions in the world heritage fjords by 2026. [accessed 2023 Aug 23]. https://www.sdir.no/en/shipping/vessels/environment/prevention-of-pollution-from-ships/zero-emissions-in-the-world-heritage-fjords-by-2026/.

Rausand M, Haugen S. 2020. Risk assessment: theory, methods, and applications. 2nd ed. Newark (NJ): Wiley. (Wiley series in statistics in practice).

Souza NP, César DAC, Bezerra JM, Hirata CM. 2020. Extending STPA with STRIDE to identify cybersecurity loss scenarios. J Inf Secur Appl. 55:102620.

Thieme CA, Guo C, Utne IB, Haugen S. 2019. Preliminary hazard analysis of a small harbor passenger ferry–results, challenges and further work. J Phys Conf Seri. 1357:012024.

Thieme CA, Utne IB, Haugen S. 2018. Assessing ship risk model applicability to marine autonomous surface ships. Ocean Eng. 165:140–154. doi: 10.1016/j.oceaneng.2018.07.040

Torkildson EN, Li J, Johnsen SO, Glomsrud JA. 2018. ESREL 2018. In: Haugen S, Barros A, Gulijk C, Kongsvik T, Vinnem JE, editors. Proceedings of the 28th European Safety and Reliability Conference; Jun 17-21; Trondheim. London: Taylor & Francis; p. 2949–2957.

Utne IB, Rokseth B, Sørensen AJ, Vinnem JE. 2020. Towards supervisory risk control of autonomous ships. Reliab Eng Syst Saf. 196:106757. doi: 10.1016/j.ress.2019.106757

Utne IB, Sørensen AJ, Schjølberg I. 2017. Risk management of autonomous marine systems and operations. In: Proceedings of the International Conference on Offshore Mechanics and Arctic Engineering. Vol. 57663. American Society of Mechanical Engineers. p. 1–10.

Vagale A, Oucheikh R, Bye RT, Osen OL, Fossen TI. 2021. Path planning and collision avoidance for autonomous surface vehicles I: a review. J Mar Sci Technol. 26:1292–1306. doi: 10.1007/s00773-020-00787-6

Wróbel K, Montewka J, Kujala P. 2017. Towards the assessment of potential impact of unmanned vessels on maritime transportation safety. Reliab Eng Syst Saf. 165:155–169. doi: 10.1016/j.ress.2017.03.029

Wróbel K, Montewka J, Kujala P. 2018. System-theoretic approach to safety of remotely-controlled merchant vessel. Ocean Eng. 152:334–345. doi: 10.1016/j.oceaneng.2018.01.020

Yang R, Utne IB. 2022. Towards an online risk model for autonomous marine systems (AMS). Ocean Eng. 251:111100. doi: 10.1016/j.oceaneng.2022.111100

Yang X, Utne IB, Sandøy SS, Ramos MA, Rokseth B. 2020. A systems-theoretic approach to hazard identification of marine systems with dynamic autonomy. Ocean Eng. 217:107930. doi: 10.1016/j.oceaneng.2020.107930

Young W. 2020. Basic introduction to STPA for security (STPA-Sec). Boston (MA): 2020 STAMP Conference.

Young W, Leveson N. 2013. Systems thinking for safety and security. In: Proceedings of the 29th Annual Computer Security Applications Conference.

Zhou X, Liu Z, Wang F, Wu Z, Cui R. 2020. Towards applicability evaluation of hazard analysis methods for autonomous ships. Ocean Eng. 214:107773. doi: 10.1016/j.oceaneng.2020.107773