https://doi.org/10.5194/wes-2020-15
Preprint. Discussion started: 12 February 2020

Systemic hazard analysis of offshore service operations

Romanas Puisa[a], Victor Bolbot[a], Andrew Newman[b], Dracos Vassalos[a]

[a]Maritime Safety Research Centre, University of Strathclyde, UK
[b]Global Marine Group, UK

Correspondence to: Romanas Puisa (r.puisa@strath.ac.uk)

Abstract. As windfarms are moving further offshore, logistical concepts increasingly include service operation vessels (SOV) as the prime means of service delivery. However, given the complexity of SOV operations in hostile environments, their safety management is challenging. The objective of this paper is to bring awareness of hazards that may have been overlooked in earlier assessments, and allow for a preliminary comparison of various operational stages. To this end, we use a systems approach to identify and analyse hazards arising during the SOV transit and manoeuvre within a windfarm and interfaces with turbines and daughter crafts. The hazard analysis is performed by systemic method STPA, allowing to explore hazardous scenarios caused by flawed interactions between system components and, to a lesser extent, by component failures. The results comprise 23 operational hazards arising during the three stages of SOV operation and 1,270 hazardous scenarios (pathways) leading to the hazards. The preliminary comparison of SOV operations shows that approaching and departing from turbines in auto and manual modes is potentially the riskiest stage of SOV operation. The lowest risk is of the SOV interface with daughter crafts. The paper discusses the analysis results and explains how they can be used to inform new and existing safety management systems of SOV.

1 Introduction

Offshore wind is becoming a major source of renewable energy in many countries (GWEC, 2019). As wind farms are moving further offshore, significant innovations in the infrastructure and services are required to maintain the judicious trend. One of such innovations is the specialised service vessels, or service operation vessels (SOVs), which are offering new logistical concepts for servicing windfarms further offshore. They enable an extended stay of technicians (typically for two weeks) in the vicinity of a windfarm, thereby replacing the logistical concept of transferring technician from shore by crew transfer vessels (CTVs). The latter becomes unreasonable due to prolonged sailing times and increased risk of seasickness.

SOVs are akin to offshore supply vessels and are typically around 80 meters in length, can endure severe environmental conditions and offer a wide array of services. They are highly automated ships (e.g., position and course can be kept automatically by the Dynamic Positioning (DP) system), hosting dozens of technicians, support (daughter) crafts, and heavy equipment. Daughter crafts (DCs) are medium size boats (under 20 meters) which are carried by the SOV and used to transport lighter equipment to turbines in moderate environmental conditions (< 1.8m significant wave height). DCs are loaded with technicians and launched from a SOV deck by some davit system (typically 3-5 times per day) and then recovered (lift-up)

https://doi.org/10.5194/wes-2020-15
Preprint. Discussion started: 12 February 2020

from the water periodically. SOVs would also have a sophisticated system for transferring technicians and equipment to and from a turbine. It is normally a motion-compensated (3 or 6 DoF) gangway system, which allows for relatively safer (based on experience so far) and time-efficient (within some 5 minutes) transfer.

The multifaceted nature of SOV operations complicates the management of their safety. Accidents can be caused by well-known but inadequately managed scenarios (e.g., loss of power or control), as well as by yet unknown scenarios created by new technology or new ways of operation. In 2018, the offshore supply vessel Vos Stone temporally lost control of thrusters, drifted and struck a wind turbine (BSU, 2019). Amongst the causes, the officers on the bridge did not manage to seamlessly switch between modes of thruster control (from DP to other mode) because they were confused about them. Inadequately controlled transitions between modes of operation, particularly between normal (frequently used) and abnormal (rarely used, i.e. emergency) models, is a classic scenario for accidents (Sarter et al., 1997;Leveson, 2011a, p. 289). Another incident happened in 2013 when the diving support vessel Bibby Topaz drifted off the position (maintained by the DP system) while two divers where exploring the seabed (IMCA, 2013). Amongst the causes, the vessel had had a dormant (unidentified) hazard—a design error—that did not allow to adequately respond to safety critical faults that preceded the incident. These two examples demonstrate how complex the designs and operations have become, so that only a subset of all real hazards can be identified. In complex socio-technical systems design errors are frequent and procedures are often underspecified (Hollnagel, 2018). The design errors constitute hazardous situations when between system components are overlooked (Perrow, 1984, p. 78), because there are simply too many system states to check (Leveson, 2000).

Given the nature of SOV operations today, along with increasing automation and autonomy in the near future (Twomey, 2017), it would not be unreasonable to assume that—in a strict sense—SOV operations constitute a complex, socio-technical system (Johnson, 2006;Perrow, 1984). Such a system can create “interactions in an unexpected sequence” (Perrow, 1984, p. 78), and some of these interactions can be hazardous. These interactions, and their consequences, is difficult to envisage from the purview of an individual system component, because "a system is more than the sum of its elements” (Rasmussen, 1997). Hence, in complex systems incidents are emergent phenomena and safety (like quality, resilience etc.) is a system property, not a component property (Checkland, 1981;Meadows, 2008;Leveson, 2011b). However currently, the overall safety management system of SOV operations is an amalgamation of individual safety procedures for the SOV, davit, DC, gangway, drone and other systems (Section 3). These safety systems are developed in isolation from a wider operational context and, when integrated, can lead to confusion and surprises (Ahsan et al., 2019). The way to deal with this is to build safety management on the *systems approach* (top-down) rather than on reductionism (bottom-up) as commonly done (Leveson, 2015).

The objective of this paper is to bring awareness of hazards that may have not been captured in earlier assessments, and allow for a preliminary comparison of various operational stages of SOV. To this end, we used a systemic approach to identify and analyse hazards arising during the SOV transit and manoeuvre within a windfarm and interfaces with turbines and daughter crafts. The hazard analysis aimed to explore hazardous scenarios caused by flawed interactions between system components and, to a lesser extent, by component failures. The latter was not the prime scope of the analysis, for individual failures are normally captured by conventional methods such as HAZOP and FMEA (Van, 2012;Vamunu et al., 2016). The analysis was based on a novel method of Systems Theoretic Process Analysis (STPA) (Leveson, 2011a;Leveson and Thomas, 2018). The method implements the systemic accident model STAMP (System-Theoretic Accident Model and Processes), which is designed for complex socio-technical systems (Leveson, 2004;Leveson, 2011b). The method contrasts with conventional methods in such a way that it is better suited for socio-technical systems with high level of automation, and it has propensity to identify more hazardous scenarios (Leveson, 2011a;Sulaman et al., 2019).

The paper is organised as follows. Section 2 explores related work, Section 3 explains the basics behind safety management, Section 0 introduces to the method and explains how it was applied, Section 5 outlines the analysis results, and Section 6 discusses the results and their utilisation. Section 7 concludes the paper.

2 Related work

In this section we review the academic and industrial work on safety hazards to servicing windfarms and other offshore installations by SOV-like vessels. The review specifically focuses on the identification of hazards leading to incidents, their causal analysis and ranking.

Presencia and Shafiee performed a quantitative risk analysis of collisions between services ships and offshore turbines (Presencia and Shafiee, 2018). The authors used statistics to, for instance, calculate the average frequency of collisions, then adjusting it to the type of turbine maintenance: reactive or preventive. The authors noted that vessels with personnel transfer systems (gangways and others) have lower chance of colliding with turbines, as opposed to vessels (e.g., crew transfer vessels / CTV) that conduct technician transfer by pushing against the turbine (e.g., by using the rubber bumper system). Other highlighted hazards were: the inadequate ability of personnel to handle severe weather conditions, unreliability of navigation, propulsion and control systems, and maintaining the wind turbines individually can result in high frequency of ship traffic, and hence, increased risk of ship collisions with offshore wind turbine structures. The above are significant hazards, but the authors did not analyse neither their causes nor relative importance of the hazards.

Dong et al. studied collision incidents and accidents between an offshore installation (FPSO vessels) and visiting vessels (shuttle tankers) (Dong et al., 2017). The analysis used the method of Man, Technology and Organisation (MTO) (Rollenhagen, 1997;Sklet, 2006). The main hazards analysed were: drive-off forward (prime concern), drift-off, and excessive surging and yawing events ("failure prone situations" in tandem offloading). The principal immediate cause of drive-off was the untimely detection or ineffective response (primarily by humans) to drive-off precursors. Under causes were related to design errors in software (e.g., wrong specification), human-machine interface, insufficient training and organisational deficiencies. The authors did not perform any ranking of the hazards.

https://doi.org/10.5194/wes-2020-15
Preprint. Discussion started: 12 February 2020

Rokseth et al. applied the STPA method to hazard analysis of marine operations, particularly the operations of offshore supply vessels using the DP system (Rokseth et al., 2017). The authors analysed the following system and sub-system level hazards: vessel motion is not controlled according to the motion-control objectives, the motion-control objectives are not in line with the operational function of the vessel, thrusters are not controlled in a manner that satisfies the control objectives, adequate amount of power is unavailable for thrusters. The study did not consider interactions between the vessel and other systems and was limited to the DP operation—from the design standpoint—only. The authors did not provide any ranking of hazards either.

The guidelines on offshore wind health and safety highlight key activities and safety hazards that are likely to arise over the lifecycle of a turbine (SgurrEnergy, 2014). The guidelines cover, inter alia, such operational stages as the personnel transfer between a SOV and turbine (incl., the use of gangways), vessel to vessel transfers (incl., launch and recovery of daughter crafts), davit or crane operations, marine coordination, vessel navigation (incl., the use of DP and other systems), and vessel selection. Hazards are extracted from various safety rules and regulation. Example hazards: falling from height, entrapment between vessels or vessel and the ladder, failure of lifting equipment (mechanical and software), navigation in close proximity to other vessels, loss of control (e.g., blackout, mishandling), drift-off and drive-off towards turbines or other vessels, collisions of floating turbines, and inadequate vessel's capabilities. The document discussed how the hazards should be assessed (e.g., using the HAZOP method) and managed for specific cases. No causal analysis or ranking of the hazards was addressed.

3 Safety management practice

As any safety critical system, SOVs comply with international and national safety standards during vessel design, construction and operation (Grace and Lee, 2017). The latter is "managed by vessel operators as part of their safety management system" (IMCA, 2015). The key element of safety management is a risk assessment (IMCA, 2014;Bromby, 1995), i.e. the identification of safety hazards to ships, personnel and the environment and establishment of appropriate controls. This also constitutes one of the objectives of the International Safety Management (ISM) Code (IMO, 2018). Risk Assessment Method Statements (RAMS) are documents that OEMs (e.g., of davit system, daughter crafts) create after they conduct individual risk assessments. RAMS contain details on identified hazards as well as a step-by-step safe working guide that crew, contractors (technicians), and others should follow to avoid and adequately respond to hazards. The hazards inform training, briefing notes and operational procedures. Notably, RAMS are used interchangeably with safety procedures and manuals.

As SOV operations use diverse systems (davits, gangways, daughter crafts, drones) that interact, individual RAMS are used for each interaction, with a bridging document to state the overall emergency protocol and document primacy (cf. Figure 1). In other words, the overall safety management system (SMS), or safety governance, onboard of a SOV is comprised of multiple RAMS, depending on the type of systems in interaction.

https://doi.org/10.5194/wes-2020-15
Preprint. Discussion started: 12 February 2020

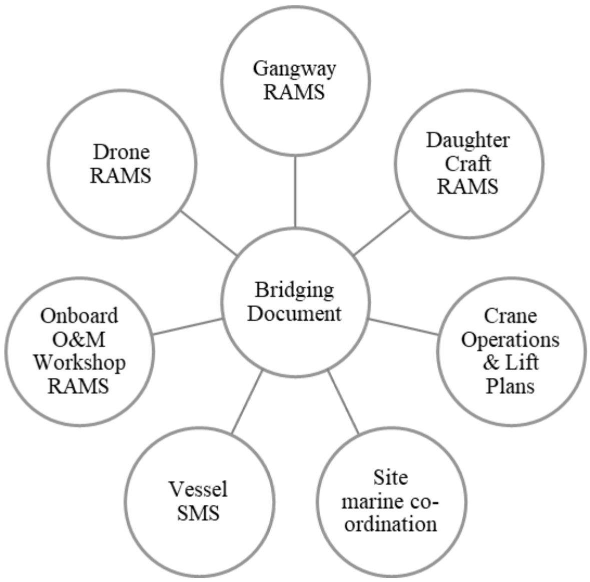

Figure 1: Illustration of current safety governance

For example, for a typical 14-day SOV operation in the UK, the safety governance may involve over five regulators simultaneously when alongside a turbine (Table 1). This ad-hoc or case-by-case safety management, however, happens sufficiently rare is that the developed SMS could often be timed for longer periods. This is a result of evolutionary process where a limited “bolt on” capacity was mobilised to a vessel which did not warrant a rework of the vessel safety systems.

When faced with the multitude of internal RAMS (procedures), the opportunity for confusion and hazardous surprises arises. This is because the knowledge of all individual safety procedures is often outside of what is normally expected of seafarers. Also, RAMS are developed in isolation and their amalgamation into one system can create conflicts between safety procedures or create unintended consequences. Therefore, safety management is heavily reliant on operator’s general competence and familiarity with operations.

Table 1: Safety governance in various stages of operation

Stage of operation	Safety rules, regulations, RAMS
Entering the site	Marine Co-ordination rules (site specific operator rules)
Within exclusion zone of a turbine.	Electrical safety rules, UK MCA for port state, vessel flag state, classification society, marine co-ordination and turbine specific control centre
Transit from turbine to turbine	Special Purpose Ships (SPS) Code (UK MCA, class rules and flag regulations)
Interface with turbine	Vessel operations governed by SPS Code, crane operations by UK HSE Lifting Operations and Lifting Equipment Regulations 1998 (LOLER) regulations, workshop activities by Provision and Use of Work Equipment Regulations 1998 (PUWER), UK HSE regulations, and IMCA guidelines (IMCA, 2014)
Interface with daughter craft	Class rules, site specific rules, company and vessel specific guidelines

4 Method

4.1 Phases of operation

The hazard analysis focuses on several operational phases:

- Transit and manoeuvre within a wind farm. In this case, dynamic positioning (DP) system (in automatic and manual modes) is used.
- Interface between SOV and turbine (approach, station keeping, and departure). In this case the DP and motion-compensated gangway systems (for technician transfer from SOV to/from turbine) are jointly used.
- Interface between SOV and daughter crafts (DC) with a conventional davit system. The DC would be vertically attached to the davit via a lifting line (vertical) and the painter line to keep the DC aligned with SOV. Both lines are typically connected and disconnected manually by DC deck crew. DCs are loaded with technicians and equipment, and launched from a SOV deck by the davit (typically 3-5 times per day) and then recover (lift up) DCs from the water the same way. During the DC launch and recovery, SOV uses the DP system to maintain the position and heading.

These modes of operation are safety critical and there are different safety hazards to watch for (next section). For instance, during a transit or manoeuvring, the vessel might collide with turbines or other vessels, e.g. when the vessel deviates from a correct trajectory or inadequately performs collision avoidance.

4.2 Hazard analysis

The prime focus of system safety is the management of hazards: their identification, evaluation, elimination, and control through analysis, design and management procedures (Roland and Moriarty, 1990;Leveson, 2003). A hazard is a system state that will lead to an incident or accident given certain environmental conditions beyond the control of system designer. The system in question can be a safety management system (SMS) which is designed according to the ISM Code or amalgamated from different RAMS. Incidents and accidents are defined as follows (Rausand, 2013). An incident is a materialised hazard with insignificant consequences. Incidents do not necessary interrupt the prime function (delivery of payload). Accident are incidents with significant consequences (some loss or damage). Accidents would normally interrupt the prime function.

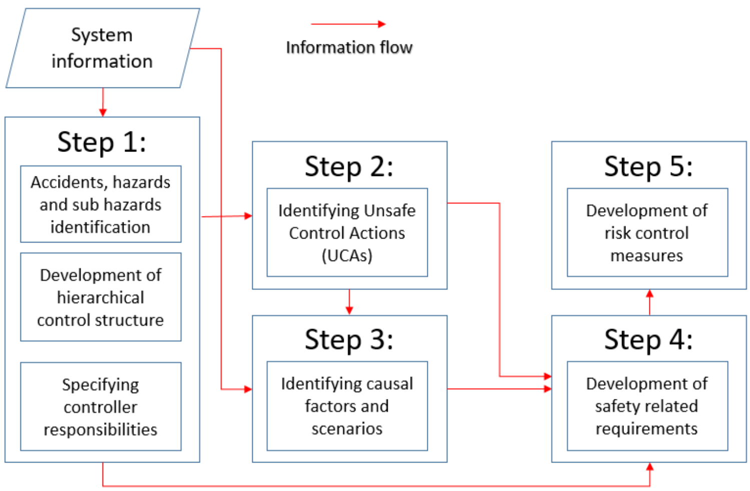

Figure 2: STPA process

There are many methods for hazard analysis (Bahr, 2014). We use the STPA method based the systemic accident model STAMP. The key assumption behind STAMP is that safety is a dynamic control problem and incidents (or accidents) occur when safety constraints are wrong, not enforced, or inadequately enforced (Leveson, 2004). This can happen not only due to technical failures or human errors, but primarily due to dysfunctional interactions between system components. Figure 2 illustrates the STPA process applied in this work.

The analysis begins by defining the system and its boundaries. This allow to clarify what accidents (unwanted losses) and system-level hazards (conditions for incidents) should be considered in the analysis. For instance, during the SOV interface with the turbine via a gangway, the assumed accidents corresponded to the deviation from the interfacing objective, i.e.

occurrence of injuries and life losses, and damages to SOV, gangway, or turbine. Sample system-level hazards—recalling that incidents occur at the system level—that can lead to these incidents were:

1. Vessel does not keep a min safe distance to turbine or its blades (approaching/staying at turbine when it is in motion);
2. SOV does not keep position/heading within target limits for a predefined time;
3. SOV does not operate on DP class 2 or above;
4. SOV transfers technicians when the gangway is disconnected or dysfunctional (e.g., not motion compensated).

The system-level hazards are typically found in safety rules and regulations. The hazards can be further decomposed into (or described through) sub-system and component-level hazards, which are often more helpful during the analysis. The important aspect is that sub-system hazards are linked to system-level hazards. For instance, the second hazard is equivalent to a situation when DP operational requirements do not request a DP operator to enable DP class 2 before starting the transfer.

The system definition further involves its modelling as a hierarchical control diagram. It is a natural way to represent many systems, including safety governance, that involve feedback loops. Figure 3 shows a control diagram for the interface between SOV and a turbine. The control diagram is at higher level of abstraction, where one controller box comprises three other controllers and controlees: turbine, gangway and technicians being transferred. The arrows indicate control and feedback channels with example control actions and feedback signals indicated. The control actions reflect the responsibilities assigned to a controller. The responsibilities, or purpose, are also reflected in the control algorithm and feedback information necessary for adequate control.

The use of control diagram for hazard analysis contrasts with classic analysis methods that instead use failure diagrams such as fault trees and event trees. The key difference between control and failure diagrams is that the latter show imaginary linear chains of causes and effects (BS EN 31010:2010). The chains are typically based on past accidents, assuming that future ones should happen in a similar fashion. The control diagram, on the other hand, does not make such assumptions and shows real interactions in daily operations. This makes the STPA results credible, easier to communicate and generalise.

https://doi.org/10.5194/wes-2020-15
Preprint. Discussion started: 12 February 2020

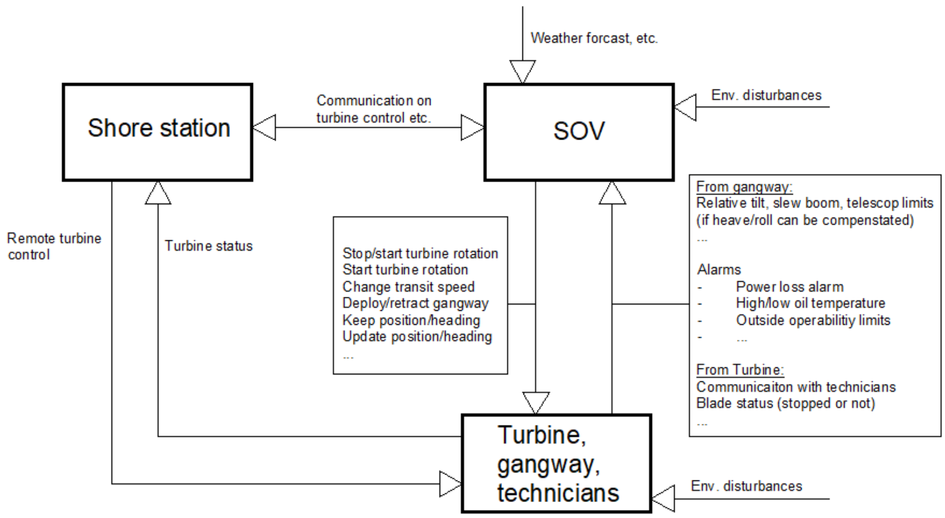

Figure 3: Hierarchical control diagram of interface between SOV and turbine

The second and third steps of the hazard analysis generate hazardous scenarios, which are then used to develop safety requirements (Figure 2). A hazardous scenario explains how control actions—from each controller in the control diagram—can lead to sub-system or system-level hazards, and why this can happen. Scenarios are inferred by searching the operational context (or states of operation), looking for circumstances—within the entire system—under which a given control action would lead to a hazard. The STPA uses specific keywords to guide the search (Leveson and Thomas, 2018). Figure 4 clarifies the input for the analysis.

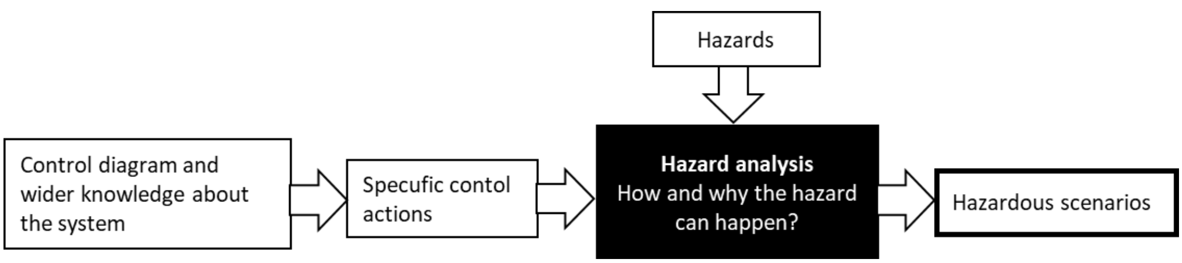

Figure 4: Prerequisites for inferring hazardous scenarios

The fourth and fifth steps of the hazard analysis are outside the scope of this paper. However, we provide an example analysis result which also includes proposed functional requirements. Thus, Table 2 contains sample hazardous scenarios and safety requirements for the control action "stop turbine rotation" by SOV controller (cf. Figure 3). The arrows indicate the scenario as a pathway from basis causal factors to system-level hazards: causal factors cause unsafe control actions, which, in turn, lead to hazards. The shaded cells illustrate a specific scenario, which is preventable by implementing the three functional safety requirements. These requirements are complementary, representing organisational and design controls.

https://doi.org/10.5194/wes-2020-15
Preprint. Discussion started: 12 February 2020

eawe european academy of wind energy
Open Access WIND ENERGY SCIENCE DISCUSSIONS

Table 2: Hazardous scenario with three functional requirements

<table>
<tr><th>Hazard</th><th>Unsafe control actions</th><th>Causal factors</th><th>Functional requirements</th></tr>
<tr><td rowspan="6">Vessel does not keep a min safe distance to turbine or its blades</td><td rowspan="5">Not stopping turbine prior to approaching it</td><td rowspan="3">Inadequate communication with the site manager leads vessel operator to wrongly believe the site manager is in control (in reality vessel operator is) of the nacelle and will stop the turbine in time.</td><td>Effective communication between the site operator and vessel operator shall be established and maintained</td></tr>
<tr><td>When turbines are to be approached for maintenance, the site and vessel operators shall be able to follow the communication procedures</td></tr>
<tr><td>When turbines are to be approached for maintenance, SOV control panel (or other design features) shall indicate who is in control of turbine (site manager or vessel)</td></tr>
<tr><td>Vessel operator wrongly assumes (based on prior experience) the site manager is by default in control of the nacelle and will stop the turbine in time. However, the default situation is opposite - vessel operator is in control unless it is changed</td><td>…</td></tr>
<tr><td>Remote stopping of turbine does not work as intended, and there is no feedback of unsuccess. Therefore, vessel operator assumes it is successful.</td><td>…</td></tr>
<tr><td>Turbine rotation is stopped too late, after vessel violates a safe distance to turbine.</td><td>…</td><td>…</td></tr>
</table>

4.3 Ranking and classification

Hazard analyses can produce hundreds, and even thousands, hazardous scenarios for a handful of hazards. To make use of the results in practice, the prioritisation of hazards is necessary and the availability of hazardous scenarios helps achieve this objective.

Normally, hazards are ranked based on their likelihood and potential consequences. Risk matrices are used to combine these two qualities and decide which hazards are more and less important (Bahr, 2014). The hazard tolerability is often decided ad hoc, based on the end user's (client's) preferences. As incident prevention is the focus on this paper, the likelihood alone can be used to rank the hazards, provided the consequences all considered hazards are similarity intolerable. Hence, the questions are:

Q1: How likely is a hazard to happen?

Q2: How the hazard can lead to an incident and what is the likelihood of that?

https://doi.org/10.5194/wes-2020-15
Preprint. Discussion started: 12 February 2020

As for Q1, we use the number of hazardous scenarios as the *degree of exposure to the hazard* (hazard exposure). The greater the exposure is, the more opportunities for the hazard to materialise. The hazard exposure can be regarded as a proxy for operational risk. Surely, some (or all) such opportunities can be addressed in design or safety procedures, but, as discussed in Section 6, gaps can exist and hazard exposure remains a useful measure of the hazard likelihood.

The answer to question Q2, i.e. the progression from hazardous states to incidents, goes beyond the hazard analysis by STPA. However, we provide a short discussion as a basis for future work. As indicated above, a hazard is a system state that can lead to an incident under certain environmental, external, or worst-case conditions. A joint analysis of such conditions and hazards can provide the degree of certainty about the likelihood of incidents. For instance, a probability distribution of wind speed in the area of SOV operation can be combined with the loss of thrust scenario when the SOV is in a certain proximity to turbine (ref. the Vos Stone incident from Section 1). If prevailing wind forces are too low to push the vessel within the expected time of recovery, this hazard would be unlikely and could be discarded. Knowledge gleaned from incidents and accidents can be also helpful in reducing uncertainty in this analysis, as well as expert judgment available in house.

In addition to ranking the hazards, their scenarios can be classified according to what elements of safety control they involve (Figure 5). The hazardous scenarios can involve inadequacies in:

- Control algorithm
- Control actions
- Feedback and/or process model
- Internal or external communication
- Handling of external disturbances

These elements can be said to be part of causal factors within the hazardous scenarios.

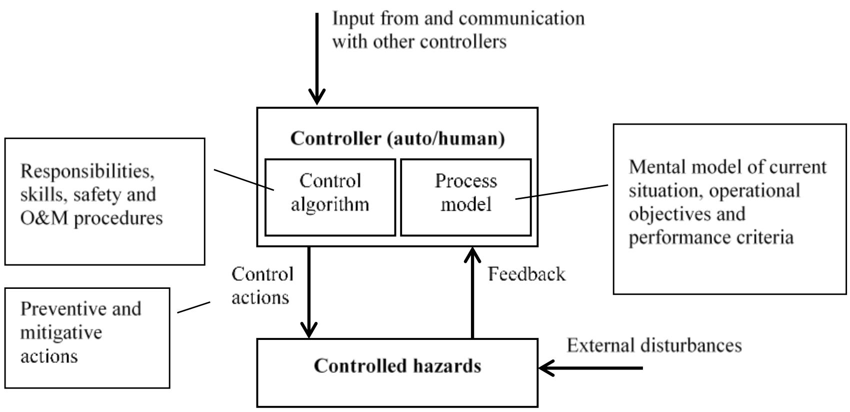

Figure 5: Generalised feedback control

https://doi.org/10.5194/wes-2020-15
Preprint. Discussion started: 12 February 2020

eawe european academy of wind energy
Open Access WIND ENERGY SCIENCE DISCUSSIONS

This classification is well aligned with safety management as a closed-loop process of continuous improvement (plan-do-check-act) (Li and Guldenmund, 2018;Kristiansen, 2005).

4.4 Comparison by relative exposure to hazard

Given hazards and their exposure (the number of scenarios to hazard) for each stage of SOV operation, the stages can be compared in terms of their relative exposure to hazards. The relative exposure to a hazard is the ratio between its exposure to the total exposure across all hazards and operational stages. As hazards can be grouped by operational stage, so can be relative exposures. We use a box plot to show the relative exposures across the three operational stages. Hence, medians, and other quartiles, can be used to guide the comparison. The comparison is, nevertheless, preliminary and should be used as a preface for a more detail, potentially quantitative, comparison.

5 Results

This section outlines the results of hazard analysis by STPA, covering the three stages of SOV operation (Section 4.1). Table 3 to Table 5 outlines the considered hazards, the number of identified scenarios that lead to them, along with example scenarios meant to clarify the meaning of the hazards. Based on this tables, Figure 6 shows the relative exposures to hazards (Section 4.4) per stage of SOV operation in a box plot. The median values indicate that the transit and manoeuvring stage of operation has, potentially, the highest relative exposure to hazards. The lowest exposure is of the SOV interface with daughter crafts. However, when comparing the lower quartiles, the SOV interface with turbine via gangway can be riskiest in some cases.

Table 6 provides a classification of hazardous scenarios, as explained in Section 4.3. The table shows that flaws in communication and control algorithms can be present during all stages of SOV operation.

https://doi.org/10.5194/wes-2020-15
Preprint. Discussion started: 12 February 2020

Table 3: Analysed hazards and their hazard exposure (number of scenarios to hazard) for SOV operational stage: Transit and manoeuvring

#	**Hazards**	**Number of scenarios**	**Example scenarios**
1	Thruster control actions mismatch the current mode of operation (i.e. mode confusion)	259	Setpoint is not updated when vessel position, heading or trajectory exceeds alarm/alert limits. This can happen when the DP system does not accept new joystick setpoints when the previous task is not yet finished (i.e. the old setpoint has not been yet achieved).
2	Vessel control actions are in conflict with operational objectives (e.g., position/heading is kept or selected not according to the plan)	174	New operational objectives (e.g. move to another position, heading, waypoint) are inadequately (clearly, accurately and timely) communicated and the DP operator does not update the setpoints.
3	Operation does not comply with the required IMO DP class	11	When operational objective/circumstances change, operator unwittingly mismatch the DP class to given operational circumstances and does not receive any indicator of the error.
4	Untimely transfer of thruster control between bridge and engine control room (i.e. inadequate internal communication)	8	Because of emergency, crew is distracted or unable to perform a prompt transfer of control.

https://doi.org/10.5194/wes-2020-15
Preprint. Discussion started: 12 February 2020

Table 4: Analysed hazards and their hazard exposure (number of scenarios to hazard) for SOV operational stage: Interface turbine via gangway

#	Hazards	Number of scenarios	Example scenarios
1	Significant gangway motions while personnel (technicians) are on the gangway. Or, gangway structure under increased expansion or compression force as a result of out-of-range gangway/vessel movements.	169	Sluggish compensation of relative vertical motions between the SOV and turbine. This can happen due to inadequate predictions of vessel motions or undetected mechanical malfunctions of the gangway.
2	Vessel does not keep relative position/heading within target limits	80	Distance to turbine is not queried when vessel is settling at or keeping the target position as operator does not switch on the distance querying to turbine.
3	Vessel does not keep a minimum safe distance to the turbine or its blades	70	When the DP/auto mode of approach to turbine is used, manually entered position/heading at the turbine violates the safe distance: typo, wrongly communicated or determined, etc.
4	Technicians are transferred when the gangway is improperly connected or dysfunctional (e.g., motion compensation is faulty or cannot compensate)	53	Deployment of gangway when gangway alarms are active (high oil temp, low oil level, etc.). Given previous experience and management/time pressure, the vessel or gangway operator wrongly assumes that gangway limits are too conservative and alarms are false and it is possible to safely perform the transfer in given env. conditions.
5	Personnel hands or legs caught between gangway moving parts or between gangway and wind turbine	50	The gangway transfer is carried out during bad visibility or external disturbances (e.g., sudden wind, rain, snow).
6	Gangway is retracted when technicians are being transferred	26	Gangway operator reacts mechanically when gangway alarms unexpectedly go off (gangway suddenly reaches the operability limits).
7	Vessel does not supply required power to gangway continuously	17	The vessel operator (and gangway operator) does not check the available power before deploying the gangway. This can happen due to time pressure or inadequate training.
8	Vessel does not operate on DP class 2 or above	9	Vessel operator switches on DP2/3 and assumes it is on. However, DP2/3 is not activated due graceful faults or unavailable redundancy (e.g., insufficient power). Meanwhile, operator is busy with other tasks and does not notice.

https://doi.org/10.5194/wes-2020-15
Preprint. Discussion started: 12 February 2020

Table 5: Analysed hazards and their hazard exposure (number of scenarios to hazard) for SOV operational stage: Interface with daughter crafts

#	Hazards	Number of scenarios	Example scenarios
1	Daughter craft (DC) develops swing or/and spinning motions during launch/recovery	78	Securing of DC is inadequately checked before launch/recovery as checking is inconvenient/inhibited due to design features.
2	Davit does not keep the daughter craft (DC) secured while launching/recovering	77	David operator (DO) mechanically switches off davit while launching/recovering DC (only relevant if DC securing can be lost upon switching off davit) as DO receives "abort" order from the bridge / other crew members.
3	Daughter craft (DC) develops excessive motions on water when being launched or about to be recovered	42	David operator (DO) starts launch of DC during excessive waves/current. This can happen when DO mechanically follows orders from an uninformed coordinating officer.
4	SOV interfaces with the daughter craft (DC) when SOV is unable to maintain position/heading (either automatically or manually)	38	SOV bridge operator does not wait until the DP settles before the DC launch can proceed. This can be because of time pressure, lack of training, or lack of feedback on the DP settlement status.
5	Davit violates the maximum launching speed of the daughter craft (DC), leading to damage caused by impact on water	25	David operator (DO) starts launch of DC when SOV is at speed or the SOV speed increases during the time of DC launch.
6	Technicians moving on the SOV ladder are unsecured (unprotected from falls, trips, and slips).	21	Despite significant motions (accelerations) of SOV, technician wrongly assumes it is ok to use just one hand while climbing the ladder.
7	While on the SOV or water, daughter craft (DC) abruptly shifts when technicians getting in/out DC or when DC crew is working on deck	17	Davit Operator (DO) retracts davit lines when DC is still being detached by DC crew. DO underestimates the time needed to detach DC and communicates it to DO before completing the task. This scenario can happen due to time pressure, or ignorance of environmental conditions that can prolong the task.
8	SOV interfaces with the daughter craft (DC) when either of ships experience excessive motions	16	Due to delayed forecast of env. conditions, the SOV bridge permits the DC launch in environmental conditions which quickly deteriorate during the launch.
9	Technicians are crossing from SOV ladder to/from the daughter craft (DC) when a gap between SOV and DC is too big or increasing (DC is not pushing against SOV).	12	Technician steps over without waiting (immediately) until DC starts pushing against SOV. This can happen because the crossing process is not coordinated by a safety officer or coordinated inadequately.
10	Horizontal centre-of-gravity of the daughter craft (DC) is significantly misaligned with respect to the lifting hook line.	11	Correctness of DC loading is inadequately checked before launching DC, because david operator (or other crew) does not have adequate skills/knowledge or checking was impeded.
11	Technicians are crossing from the SOV ladder to the daughter craft (DC) too slowly	7	Technician are unaware that crossing should be instant: unfamiliar with safety instructions or the crossing is inadequately coordinated.

https://doi.org/10.5194/wes-2020-15
Preprint. Discussion started: 12 February 2020

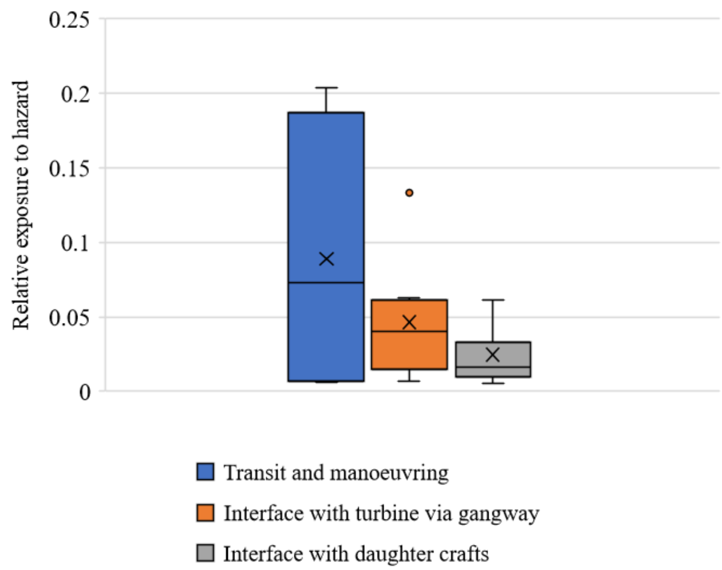

Figure 6: Box plot of relative exposures to hazards for the three stage of SOV operation

Table 6: Causal factors within hazardous scenarios across the stages of SOV operation

Stage of SOV operation: / Inadequacies in:	Transit and manoeuvring	Interface with turbine via gangway	Interface with daughter craft
Control algorithm (responsibilities, skills, safety and O&M procedures)	X	X	X
Control actions (preventive and mitigative actions)		X	X
Feedback and/or process model (feedback signals, mental model of current situation, operational objectives and performance criteria)		X	X
Handing of external disturbances	X		
Internal and external communication	X	X	X

6 Discussion

The results of the hazard analysis bring awareness of what hazards can materialise during various stages of SOV operations, and which one of them are potentially more likely—judging by exposure to hazard—than others. The exposure is controlled by safety measures applied to hazardous scenarios (by eliminating or isolating the opportunities to hazards) or hazards

https://doi.org/10.5194/wes-2020-15
Preprint. Discussion started: 12 February 2020

themselves (by restoring the system into a safe state). Safety measures are imposed by safety rules and regulations, as well as safety practices.

We expect that the majority of the analysed hazards should be already covered, partly or completely, by existing safety rules or regulations. For instance, the example scenario for the hazard in Table 4 "Vessel does not keep a minimum safe distance to the turbine or its blades" is addressed by class rules which require the DP system to perform self-check routines and bring the system to a stop if necessary (DNVGL, 2015). However, the presence of safety requirements does not automatically guarantee they will be or can be followed in practice. Even for highly constrained task situations such as nuclear power operation, modification of instructions is repeatedly found (Fujita, 1991) and the operators' violations of rules appear to be quite rational, given the actual work load and timing constraints (Rasmussen and Suedung, 2000). Thus, the violation of safety requirements and O&M procedures when running and maintaining equipment is often necessary for maintaining safety per se, given continuous changes to equipment (e.g., aging) and its operational context (Besnard and Hollnagel, 2014).

The partial coverage of hazards means that some hazardous scenarios, which are perfectly plausible, are not addressed by regulations. This could be because they were not revealed during hazard analysis at the time, or were identified but considered unlikely by expert opinion or calculations. It is known that expert opinions can be skewed by cognitive biases (Kahneman and Klein, 2009;Skjong and Wentworth, 2001), whereas the probabilistic risk assessment is prone to precarious assumptions and oversimplifications that can discard risky scenarios (Rae et al., 2012). Hence, the partial coverage should be expected, meaning that the pertinent hazards can materialise via overlooked and discarded pathways.

There is also a historical perspective to the analysed hazards. Some of the hazardous scenarios have been featured in past incidents and accidents. Thus, one can assume that appropriate measures were taken to avoid them in the future. However, looking at the earlier discussed accident with Vos Stone (BSU, 2019), improving only operational procedures to avoid similar scenario in the future may not be enough. Essentially, the investigation recommended to increase reliability of the operational procedures. However, wider causal factors behind the deviation from these procedures were not analysed, given that people do not err purposely but do their best and success most of the time (Dekker, 2014). The ignorance of underlying causes creates the possibility for the new procedures to be equally violated and incidents to happen (Perrow, 1984). Additionally, recalling the hierarchy of hazard control, organisational measures are less reliable than engineering controls (NASA, 1993;Books, 1997). Therefore, to avoid this and similar scenario in the future, changes in vessel design could also be considered. For instance, a notification (or interlock) on the control panel that would alarm against (or not allow) certain actions when the vessel is too close to a turbine or any other object. The combined data from already used proximity sensors, measurements of environmental forces and thrust could be used to trigger the safety function. This was actually one of the safety requirements that came out of the hazard analysis of which results are presented in this paper.

Notably, the analysis focused only on hazards that can lead to incidents, i.e. unwanted and expected events. That is, we did not consider the subsequent events that, if not adequately controlled, would lead to losses or accidents. The focus on incident

https://doi.org/10.5194/wes-2020-15
Preprint. Discussion started: 12 February 2020

prevention well aligns with the business objective of keeping operation uninterrupted. If this can be achieved cost-effectively, that would be the best investment in safety. A similar reasoning is used in other safety critical industries like rail, where collision avoidance is the main safety focus (Holmberg, 2017, p. 49).

The question is how to apply the analysis results in practice? The following can be considered:

- The results can be used to update risk assessments, RAMS (or hazard logs) and training. The hazards should be compared against the RAMS (or hazard logs) to verify if they are already prevented, or mitigated, by specific risk controls (safety barriers). Regardless if the controls are in place, the hazards of high priority (high degree of exposure) should be subjected to detailed risk assessments which considers specifics of the operations. Such specifics were obviously not captured in this study.
- The results can be used to improve awareness of hazards through training. The hazards should be discussed with technicians and SOV crew as part of safety briefings and other risk awareness activities.

7 Conclusions

The paper has presented the results of systemic hazard analysis of service offshore vessel's (SOV) operations. The work is predicated on the premise that SOV operations are complex, while risk assessments are done piecemeal and potentially lacking completeness when integrated into one system. This means that various hazards and their scenarios may have been overlooked in earlier risk assessments. Therefore, this work aims to bring awareness about potentially overlooked hazards. The analysis also offers a preliminary comparison of the analysed stages of SOV operation.

We have specifically analysed 23 operational hazards arising during the three stages of SOV operation: (1) transit and manoeuvre within a windfarm and interfaces with (2) turbines and (3) daughter crafts. The hazards are mostly related to flawed interactions between people and technology, as opposed to individual failures (e.g., human errors, random failures of equipment) that are addressed conventionally. During the hazard analysis, we identified 1,270 hazardous scenarios that explain how hazards can materialise. We used the hazardous scenarios to prioritise the hazards, assuming that the number of scenarios reflects the degree of exposure to the hazard, indicating its likelihood.

In addition to the description and ranking of hazards for each stage of SOV operation, the study has found that all analysed stages of operation are exposed to a similar number of hazardous scenarios, with the interface between SOV and turbine having the largest exposure. The common causal factors behind these scenarios were flaws in communication and control (responsibilities, skills, and procedures). However, when comparing median values of relative hazard exposures, the transit and manoeuvring stage of operation has, potentially, the highest relative exposure to hazards. That is, approaching and departing from turbines in auto and manual modes is potentially the riskiest stage of SOV operation (recall the case of Vos Stone from Section 1). The lowest exposure is of the SOV interface with daughter crafts.

The paper has also discussed how the results can be used to update risk assessments, RAMS (or hazard logs) and training of new and existing operations. Notably, the paper has pointed that many (but not all) of the analysed hazards and their scenarios are likely already covered by existing rules and regulations. However, we did not investigate the actual degree of coverage, leaving this task for future work.

8 Acknowledgement

The work described in this paper was produced in research project NEXUS (https://www.nexus-project.eu). The project has received funding from the European Union's Horizon 2020 research and innovation programme under agreement No 774519. The authors are thankful to their colleagues and project partners who directly and indirectly contributed to the presented work. Particular thanks go to Kongsberg Maritime (former Rolls Royce Marine) for sharing design information and providing valuable feedback. The sponsorship of the Maritime Research Centre by DNV GL and Royal Caribbean Cruises Ltd is also much appreciated.

9 References

Ahsan, D., Pedersen, S., Bang Nielsen, M. R., and Ovesen, J.: Why does the offshore wind industry need standardized HSE management systems? An evidence from Denmark, Renewable Energy, 136, 691-700, https://doi.org/10.1016/j.renene.2019.01.034, 2019.
Bahr, N. J.: System safety engineering and risk assessment: a practical approach, CRC Press, 2014.
Besnard, D., and Hollnagel, E.: I want to believe: some myths about the management of industrial safety, Cognition, Technology & Work, 16, 13-23, 10.1007/s10111-012-0237-4, 2014.
Books, H.: Successful health and safety management, HS (G), 1997.
Bromby, M.: Ensuring compliance with the IMO's Code and its place within quality management systems, Conference on Quality Management Systems in Shipping, London, 27-28 March, 1995.
BSU: Allision between VOS STONE and a wind turbine on 10 April 2018 in the Baltic Sea. Investigation report 118/18, Bundesstelle fuer Seeunfalluntersuchung, 2019.
Checkland, P.: Systems thinking, systems practice, J. Wiley, 1981.
Dekker, S.: The field guide to understanding'human error', Ashgate Publishing, Ltd., 2014.
Dong, Y., Vinnem, J. E., and Utne, I. B.: Improving safety of DP operations: learning from accidents and incidents during offshore loading operations, EURO Journal on Decision Processes, 5, 5-40, 10.1007/s40070-017-0072-1, 2017.
Fujita, Y.: What shapes operator performance, JAERI Human Factors Meeting, Tokyo, 1991,
Grace, L., and Lee, W.-H.: Cost Effective Offshore Concepts-Compact Semi-Submersible-A New Concept of Windfarm Service Operations Vessel, Offshore Technology Conference, 2017,
GWEC: Global Wind Report 2018, Global Wind Energy Council (GWEC) Brussels, 2019.
Hollnagel, E.: Safety-I and Safety-II: the past and future of safety management, CRC Press, 2018.
Holmberg, J. E.: Defense-in-Depth, Handbook of Safety Principles, 42-62, 2017.
IMCA: Serioius DP diving incident. IMCA Safety Flash 02/13, 2013.
IMCA: Guidance on the Transfer of Personnel to and from Offshore Vessels and Structures (IMCA SEL 025 Rev. 1, IMCA M 202 Rev. 1), 2014.
Johnson, C. W.: What are emergent properties and how do they affect the engineering of complex systems?, Reliability Engineering and System Safety, 91, 1475-1481, 2006.
Kahneman, D., and Klein, G.: Conditions for intuitive expertise: a failure to disagree, American psychologist, 64, 515, 2009.
Kristiansen, S.: Maritime transportation: safety management and risk analysis, 2005.
Leveson, N.: White paper on approaches to safety engineering, Disponible en ligne sur le site de l'auteur (sunnyday. mit. edu/caib/concepts. pdf), 2003.

https://doi.org/10.5194/wes-2020-15
Preprint. Discussion started: 12 February 2020

eawe european academy of wind energy
Open Access WIND ENERGY SCIENCE DISCUSSIONS

Leveson, N.: A new accident model for engineering safer systems, Safety science, 42, 237-270, 2004.
Leveson, N.: Engineering a safer world: Systems thinking applied to safety, MIT press, 2011a.
Leveson, N.: A systems approach to risk management through leading safety indicators, Reliability Engineering & System Safety, 136, 17-34, 2015.
Leveson, N., and Thomas, J.: STPA Handbook, MIT, 2018.
Leveson, N. G.: System safety in computer-controlled automotive systems, SAE Technical Paper0148-7191, 2000.
Leveson, N. G.: Applying systems thinking to analyze and learn from events, Safety science, 49, 55-64, 2011b.
Li, Y., and Guldenmund, F. W.: Safety management systems: A broad overview of the literature, Safety Science, 103, 94-123, 2018.
Meadows, D. H.: Thinking in systems: A primer, chelsea green publishing, 2008.
NASA: Safety Policy and Requirements Document. NHB 1700.1 (V1-B), NASA, Washington, DC, 1993.
Presencia, C. E., and Shafiee, M.: Risk analysis of maintenance ship collisions with offshore wind turbines, International Journal of Sustainable Energy, 37, 576-596, 2018.
Rae, A., McDermid, J., and Alexander, R.: The science and superstition of quantitative risk assessment, Journal of Systems Safety, 48, 28, 2012.
Rasmussen, J.: Risk management in a dynamic society: a modelling problem, Safety science, 27, 183-213, 1997.
Rasmussen, J., and Suedung, I.: Proactive risk management in a dynamic society, Swedish Rescue Services Agency, 2000.
Rausand, M.: Risk assessment: theory, methods, and applications, John Wiley & Sons, 2013.
Rokseth, B., Utne, I. B., and Vinnem, J. E.: A systems approach to risk analysis of maritime operations, Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 231, 53-68, 2017.
Roland, H. E., and Moriarty, B.: System safety engineering and management, John Wiley & Sons, 1990.
Rollenhagen, C.: MTO–an Introduction; the Relationship Between Humans, Technology and Organization, Utbildningshuset, Lund, Sweden, 1997.
Sarter, N. B., Woods, D. D., and Billings, C. E.: Automation surprises, Handbook of human factors and ergonomics, 2, 1926-1943, 1997.
SgurrEnergy: Offshore Wind and Marine Energy Health and Safety Guidelines, RenewableUK, 2014.
Skjong, R., and Wentworth, B. H.: Expert judgment and risk perception, The Eleventh International Offshore and Polar Engineering Conference, 2001,
Sklet, S.: Safety barriers: Definition, classification, and performance, Journal of Loss Prevention in the Process Industries, 19, 494-506, https://doi.org/10.1016/j.jlp.2005.12.004, 2006.
Sulaman, S. M., Beer, A., Felderer, M., and Höst, M.: Comparison of the FMEA and STPA safety analysis methods–a case study, Software Quality Journal, 27, 349-387, 2019.
Twomey, B.: Making the case for safe autonomous marine cyber physical systems, Marine Electrical and Control Sytems Safety Conference (MECSS), Glasgow, 23-23 November, 2017.
Vamunu, B., Necci, A., Tarantola, S., and Krausmann, E.: Offshore Risk Assessment. An overview of methods and tools, European Commission, 2016.
Van, L. U.: Risk analysis methods within offshore wind energy, Institutt for produksjons-og kvalitetsteknikk, 2012.