Wind Energ. Sci. Discuss., 2020, 1-20, 10.5194/wes-2020-15, 2020.

Revealing system variability of offshore service operations through systemic hazard analysis

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@outlook.com)

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 propose a quantitative, non-probabilistic metric for the preliminary comparison of SOV operational phases. The metric is used as a conditional proxy for the incident likelihood, conditioned upon the presence of similar resources (manpower, time, skills, knowledge, information, etc.) for risk management across compared operational phases. The comparison shows that the three considered phases of SOV operation have rather comparable levels of variability, hence the likelihood for incidents. However, the interface between the SOV and turbine via the gangway system and the manoeuvring between turbines seem to show a higher potential for incidents and performance (work efficiency) shortfalls.

1 Introduction

1.1 Background

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, typically 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) 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. The overall safety management of SOV operations is an amalgamation of individual safety procedures for the SOV, davit, DC, gangway, drone and other sub-systems (Section 3). These safety systems are developed in isolation from a wider operational context and, when integrated, can lead to confusion, surprises and undue pressure on operators (Ahsan et al., 2019). In such conditions, 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, e.g. emergency) modes, 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.

1.2 The challenges

The first challenge for safety of SOV operations comes from the uncertainty as to how the amalgamated systems of safety procedures would actually work, even though the performance of individual systems may be known. This is because safety is an emergent system property, which cannot be asserted or aggregated from properties of individual system components (Leveson, 2011b;Checkland, 1981;Meadows, 2008). This challenge is exacerbated by a high level of automation in SOV operations and complex interactions between technology and operators (Sarter et al., 1997). As highlighted above, some interactions may have not been captured during design and can lead to incidents[1] in practice.

The second challenge is the ability to compare various phases of SOV operation. A quantitative risk-based comparison would be a natural but very precarious choice. This is because the quantification of risks associated with identified hazards is generally invalid, given the prevalence of systematic (unsafe software and human behaviour), as opposed to random (hardware failures), causes in the lead up to hazards. Systems systematically drift, as opposed to probabilistically jump, to failure (Rasmussen, 1997;Dekker, 2016). For instance, non-systematic causal factors (e.g. out-of-range environmental conditions) constituted only

[1] We use the term *incidents* to refer to both incidents and accidents throughout the paper.

some 25% of all incident causes with DP operated support vessels within the Norwegian continental shelf (Chen and Moan, 2005). Although there are still frequent attempts to quantify software failures and human errors in terms of probabilities or alike, this approach have been criticised, e.g. (Rae et al., 2012;Leveson, 2000), and the systematic nature of these hazards is widely recognised and enshrined in international standards and methodologies, e.g. (IEC61508, 1998;DoD, 2012).

1.3 Objectives and organisation

The first challenge can be addressed by applying a systemic hazard analysis (SHA) to an integrated safety management system of operational tasks and procedures within a specific SOV operational phase. In contrast to conventional accident models based on chains of events, systemic models focus on tight couplings and nonlinear interactions between system components (Hollnagel, 2016;Qureshi, 2007). The second challenge can be addressed by proposing some metric that reflects systemic, structural properties of a specific operational phase and then can be used to aid the comparison of various phases. As discussed in Section 4.3, this metric corresponds to the variability within the system in terms of interactions between technical and human components, and it is a by-product of the SHA. The metric is used as a conditional proxy for the incident likelihood, conditioned upon the existence of similar resources (manpower, time, skills, knowledge, information, etc.) for risk management across compared operational phases.

With the above in mind, the objective of this paper is to propose a quantitative metric for the system variability with the purpose to be able to preliminary compare phases of SOV operation. To this end, the SHA was applied to three phases of SOV operation to reveal hazardous scenarios involved in each of them. The considered operational phases were: when transiting and manoeuvring within a windfarm, interfacing with turbines, and launching or recovering daughter crafts. We used the Systems Theoretic Process Analysis (STPA) (Leveson, 2011a;Leveson and Thomas, 2018) as a SHA. The results of SHA were directly used to derive the system variability metric.

The paper is organised as follows. Section 2 explores related work, Section 3 explains the basics behind safety management currently in practice, Section 4 introduces to the research method, specifically addressing the hazard analysis, system description and the concept of system variability. Section 5 outlines and discusses the results. Section 6 highlights the work limitations, whereas Section 7 concludes the paper.

2 Related work

In this section we review academic and industrial literature on hazard, system variability and resilience analysis of servicing windfarms and other offshore installations by SOV-like vessels.

The reviewed literature focuses on collision (ship to ship, shop to turbine), reliability issues with technology (DP, gangway, and other systems) and human factors (Presencia and Shafiee, 2018;Dong et al., 2017;Rollenhagen, 1997;Sklet, 2006), (Rokseth et al., 2017;SgurrEnergy, 2014). The used hazard analysis mainly followed a conventional, non-systemic, approach

where individual hazards or scenarios are considered in isolation. In most cases, statistics or probabilistic analysis is used for decision making. The exception is Rokseth et al. who applied the STPA method to hazard analysis of offshore supply vessels running on the DP system (Rokseth et al., 2017). None of the studies use systemic indicators or measures (e.g., of resilience) to infer the safety level or compare operational phases or other aspects.

When it comes to indicators or measures of system variability and resilience, the general literature is abound, e.g. (Hollnagel et al., 2007;Herrera et al., 2010). The literature specific to the maritime domain is limited but present, e.g. (Praetorius et al., 2015;Patriarca and Bergström, 2017;de Vries, 2017). However, the authors have not come across a work which connects results of a systemic hazard analysis, namely hazardous scenarios, with the system variability or similar systemic indicators.

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, separate 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.

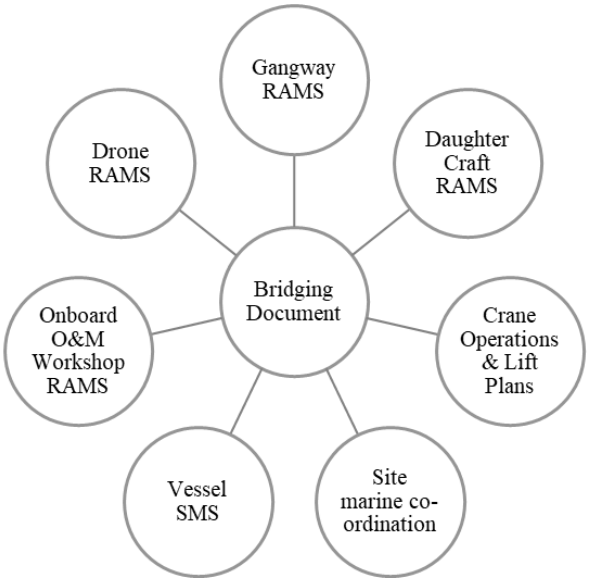

Figure 1: Illustration of current safety governance

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 (cf. 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.

In view of these practices, a systemic, top-down approach to hazard analysis—when multiple systems (e.g., the DP and gangway systems) are engaged at the same time—is required to properly address the system-level hazards. The following section explicates why and how systemic analysis is performed.

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 Hazard analysis

In view of several systemic hazard analysis methods available, we selected the Systems Theoretic Process Analysis (STPA)(Leveson, 2011a;Leveson and Thomas, 2018). The method is based on systemic accident model STAMP (System-Theoretic Accident Model and Processes), which is designed for complex, highly automated, socio-technical systems (Leveson, 2004;Leveson, 2011b). The comparison of STPA and STAMP with other analysis methods and accident models can be found in the literature, e.g.(Salmon et al., 2012;Sulaman et al., 2019;Qureshi, 2007), and it is, hence, disregarded in this paper.

Before explaining the method, it would be helpful to agree on the terminology used. A hazard is a system state that will lead to an incident or accident given specific environmental conditions beyond the control of system designer (Leveson, 2004). 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 or service). An accident is a materialised hazard with significant consequences (significant loss or damage). Accidents would normally interrupt the prime function.

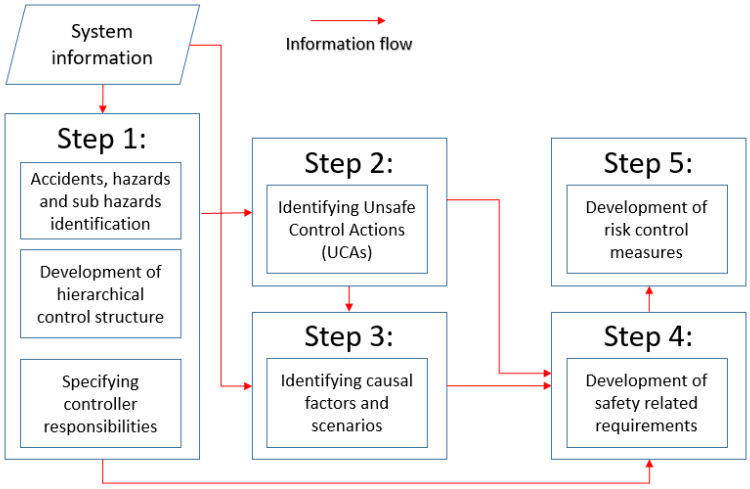

Figure 2: STPA process

A sequential process behind the STPA method is shown in Figure 2. The analysis begins by defining the system and its boundaries. This allow clarifying what accidents (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. However, the reference to accidents is beyond the scope of this paper, as explained earlier.

Sample system-level hazards are:

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 operates on DP class 1, i.e. no redundancy in thrusters, power generation and other safety critical components;
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. 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.

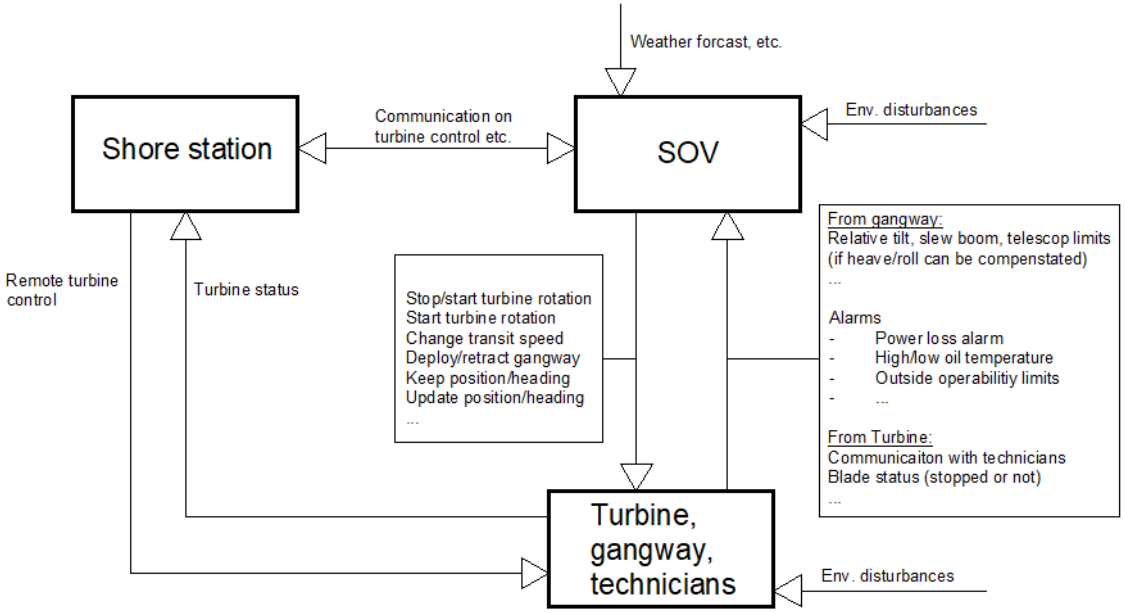

Figure 3: Hierarchical safety control diagram of interface between SOV and turbine (further explained in Section 4.2)

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.

The second and third steps of the hazard analysis generate hazardous scenarios, which are then used to develop safety requirements. 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).

The fourth and fifth steps of the hazard analysis in Figure 2 are outside the scope of this paper. However, we provide an example analysis result which also includes proposed functional requirements. Thus, Table 2 shows sample hazardous scenarios and safety requirements for the control action "stop turbine rotation" by SOV controller. 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.

Table 2: Hazardous scenario with three functional requirements

Hazard ←	**Unsafe control actions** ←	**Causal factors** ←	**Functional requirements**
Vessel does not keep a min safe distance to turbine or its blades	Not stopping turbine prior to approaching it	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.	Effective communication between the site operator and vessel operator shall be established and maintained
			When turbines are to be approached for maintenance, the site and vessel operators shall be able to follow the communication procedures
			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)
		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	…
		Remote stopping of turbine does not work as intended, and there is no feedback of unsuccess. Therefore, vessel operator assumes it is successful.	…
	Turbine rotation is stopped too late, after vessel violates a safe distance to turbine.	…	…

4.2 System overview

The overall system in question is shown in Figure 4. The figure shows the analysed interactions between system components at the system level. These interactions are of physical contact (e.g., SOV and turbine), communication via radio (e.g., SOV and shore, turbine and shore), and sensory (distance, visual, and audio) by installed sensors and people. Other interactions at the system level (e.g., the links between the DC and turbine or other ships) were not analysed.

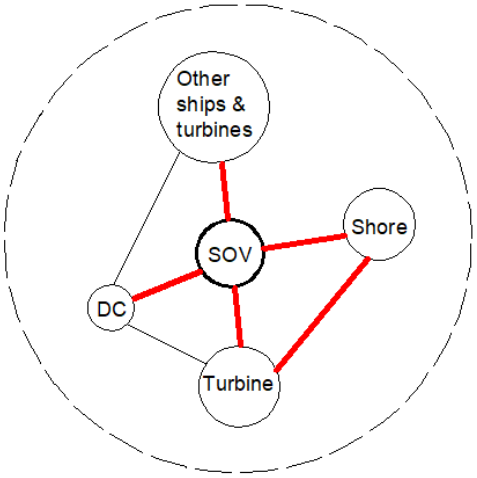

Figure 4: System components and system boundary (SOV – service operation vessel, DC – daughter craft)

The considered interactions corresponded to four operational phases:

- Transit and manoeuvre within a wind farm. The dynamic positioning (DP) system was considered as the main system providing the navigation and station keeping (position and heading) functions. The DP system can be switched into an automatic mode to fully control all three degrees of freedom (DoF): surge, sway, and yaw. The control of DoF can also be shared with a DP operator who can use a joystick or manual thruster levers.
- Interface between a SOV and turbine (approach, station keeping, and departure). The DP and motion-compensated gangway systems were considered to be jointly used. The gangway system is used for technician transfer from SOV to/from a wind turbine. At the time of transfer, the SOV keeps position and heading by means of the DP system. The gangway is controlled by a gangway operator who extends, retracts, and maintains communication with the technicians. There is also a continuous communication between the DP and gangway operators to maintain the gangway operation within its operability limits.
- Interface between a 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. The interface between a SOV and DC was assumed to following sub-phases with corresponding systems

and hazards involved: (1) launch from the SOV and recovery of a DC from water using the davit system, (2) and technician and equipment are transfer when a DC is on water, with technicians claiming up/down the ladder.

These phases 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.

For each phase, a safety control diagram was developed, e.g. Figure 3 shows the one used for the interface between a SOV and a wind turbine. Thus, the safety control diagram in Figure 3 was developed by assuming the SOV to be the main controller, which comprises human controllers on the bridge (e.g., a DP operator), automation, and other ship systems. The shore station as a controller was not analysed, and only the communication with the SOV was considered. The text next to the arrows explain their meaning, i.e. what control and feedback information was assumed. The SOV as a controller is generally responsible for (1) keeping the station (position and heading) until the transfer of technicians via the gangway is complete and (2) providing power to the gangway. Additionally, it was assumed that these responsibilities are only exercised when the SOV, gangway and other systems are fully operational. Based on this information, control actions and feedback can be inferred. Technical publications, such as DP operational manuals, were also used determine control actions and feedback signals (e.g., distance sensors, GPS signals). As Figure 3 shows, the process under control comprised the gangway and turbine, with controlled parameters such as the relative distance, bearing, power supply and others.

This phase of SOV operation additionally included a separate hazard analysis of the gangway control, as shown in Figure 5. The control diagram was developed to reflect industrial safety and other requirements for gangways and technician transfer, i.e. (IMCA, 2014;DNVGL, 2017, 2015a). The continuous lines correspond to control channels, with the text indicating the control actions, and dashed lines corresponding to feedback channels. In this diagram, the human operator corresponded to the gangway operator controlling the gangway position and motions by means of the gangway control system. There is also communication with technicians who walk via the gangway.

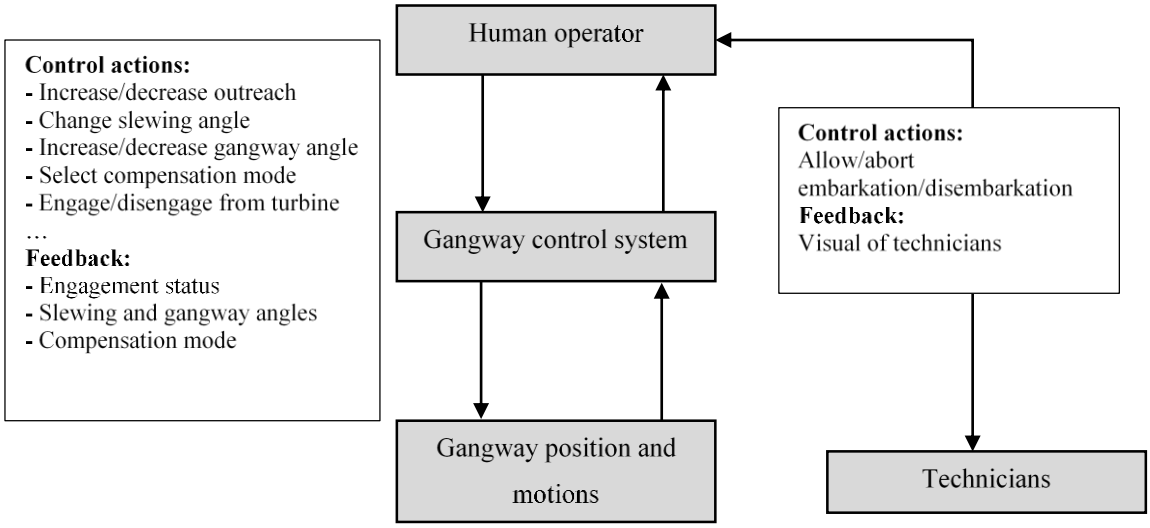

Figure 5 Gangway control diagram with sample control and feedback information

Detailed explanations of other control diagrams corresponding to other phases of SOV operation are outwith the scope of this paper. An interested reader is referred to other authors' publications where, for example, a system description and hazard analysis for the DP system in the above phases of SOV operation can be found (Puisa et al., 2019). We note that the safety control diagrams developed for each operational phase were of the same level of abstraction. This makes them comparable, as done in the following section.

4.3 System variability

As argued in Section 1, quantification of system safety within the probabilistic framework is often unwarranted in modern, highly automated systems. In this section we introduce the notion of system variability and explain its application to a preliminary comparison of SOV phases.

Design and operational errors are frequent and procedures are often underspecified in complex systems (Hollnagel, 2018), meaning that hazardous scenarios and operational uncertainties will likely be present all the time. In other words, operational conditions are not stationary, but are dynamic, variable and sometimes surprising. Then, the inability to adequately adjust to such operational complexity due to meagre resources (time, knowledge, competence, etc.) is a harbinger of untoward events (Woods and Hollnagel, 2017); the reverse is system *resilience* (Hollnagel et al., 2007).

We make the following corollary assumptions derived from the above observations:

- Incidents and accidents happen when hazardous scenarios (i.e. opportunities for safety incidents) are present within the system and existing resources (time, manpower, skill, knowledge, information etc.) are inadequate to effectively manage the associate risks.
- Analogically, underperforming or failing on prime operational objectives (e.g., delivery of technicians and equipment to turbines) happens when operational circumstances are complex and uncertain, and existing resources are inadequate to effectively manage such circumstances.
- Performance and safety, therefore, share a common denominator – the ability to manage surprises in view of limited resources. According to the Rasmussen's boundary of safe behaviour, production pressures push operations towards the safety boundary because the performance is at maximum there (Rasmussen, 1997). In other words, the performance increases as the incident likelihood increases, but up to a point. After this point, frequent incidents inhibit the performance.
- The presence of hazardous scenarios (i.e. opportunities for safety incidents) and operational complexity (i.e. opportunities for performance shortfalls) are germane, and overlapping conditions within the system. The higher likelihood for incidents is, the higher operation complexity might be present in the system, and vice versa.

Although we cannot predict when an untoward event can happen, we can say whether it is likely or not. It can be done "by characterising the variability within the system, specifically the variability of components and subsystems and how they may combine in unwanted ways. This can be done by looking at how functions and subsystems depend on each other." (Hollnagel, 2016, p. 172). This very information is obtainable from a systemic hazard analysis where flawed interactions between system components at various levels of abstraction are revealed.

With this in mind, the first above assumption about the incident likelihood (in a non-probabilistic sense) can be expressed more formally, Eq. (1).

$$\text{Likelihood}_{\text{incident}} \propto \frac{\text{NHS}}{\text{RtA}} \tag{1}$$

where NHS corresponds to the number of hazardous scenarios (pathways to hazards), whereas RtA stands for Resources to Adjust to avoid those scenarios. The actual dependence between the left- and right-hand sides of the equation is unknown, and requires further studies. In this paper we are only interested in an approximate form of this relationship, so we could compare, although preliminary, various systems or operational phases.

On this basis, we propose the following model to capture the incident likelihood, referring to this surrogate metric as the system variability, Eq. (2). It is a ratio of the number of hazardous scenarios per operational phase, NHS_i, to the total number of hazardous scenarios across all *N* phases of operation, Eq. (2).

$$\text{System variabilty}_{\text{i}} = \frac{\text{NHS}_{\text{i}}}{\sum_{i}^{N} \text{NHS}_{\text{i}}} \quad (2)$$

The numerator matches the one in Eq. (1), whereas the denominator is used to normalise the numerator across all operational phases. The RtA figure from Eq. (1) is apparently not included. For this reason, we do not refer to this metric as the likelihood, because it captures only a part of the risk picture. However, if RtA can be assumed to be similar across compared system states (e.g., modes of SOV operation), then Eq. (2) would reflect the incident likelihood. The assumption of similarly can be reasonable if we consider a rather short period of time, say a two-week shift that the SOV crew spends at a windfarm. This is because human resources, skills, work and safety culture etc. will likely remain the same for the shift. For the sake of demonstration of the approach, we assume that RtA is similar across all phases of SOV operation, and Eq. (2) is hence valid to apply.

5 Results and discussion

This section outlines the results of hazard analysis by STPA, covering the three stages of SOV operation (Section 4.2). Table 3 to Table 5 outlines the considered hazards, the number of identified scenarios that can lead to them, along with example scenarios meant to demonstrate the interactions involved. Based on these tables, Figure 6 shows the system variability as described in Section 4.2. The values indicate that the interface between the SOV and gangway has, potentially, the highest variability. Although, the system variability for the transit and manoeuvring phase is almost the same. The lowest variability is of the SOV interface with daughter crafts.

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. This means redundancy against failure of critical components such as thrusters is unavailable.	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.

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 (incl. vessel approaching a rotating turbine or the turbine starts rotating when the vessel is nearby)	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. This means redundancy against failure of critical components such as thrusters is unavailable.	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.

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 develops swing or/and spinning motions during launch/recovery	78	Securing of daughter craft (DC) is inadequately checked before launch/recovery as checking is inconvenient/inhibited due to design features.
2	Davit does not keep the daughter craft secured while launching/recovering	77	Davit 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 develops excessive motions on water when being launched or about to be recovered	42	Davit 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 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, leading to damage caused by impact on water	25	Davit operator 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 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 is significantly misaligned with respect to the lifting hook line.	11	Correctness of DC loading is inadequately checked before launching DC, because davit 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 too slowly.	7	Technician are unaware that crossing should be instant: unfamiliar with safety instructions or the crossing is inadequately coordinated.

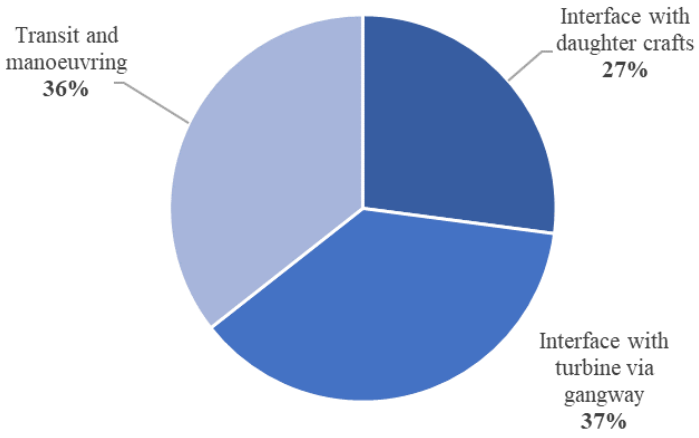

Figure 6: System variability for the three stage of SOV operation

The presented results of the systemic hazard analysis are twofold. First, they bring awareness of system-level hazards involved in various stages of SOV operations, although the existing industrial rules and good practices are likely to cover them. For instance, the sample 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, 2015b). However, these technical publications do not explain how the rules or guidelines can be violated and what the level of complexity involved when following them.

This bring us to the second contribution of the study, namely to the number of scenarios in the lead up to these hazards. These scenarios reflect the system complexity, i.e. the degree of freedom for the system to fail. The proposed metric of system variabilities, which is based on the number of hazardous scenarios shown in Eq. (2), aims to capture the likelihood of system failure. As Figure 6 shows, all three phases of SOV operation have rather comparable levels of system variability and hence likelihood for incidents, given that similar resources for risk management are available in the three phases. However, the interface between the SOV and turbine via the gangway system and the manoeuvring between turbines seem to be more complex phases of operation where the potential for incidents is more likely. The similarity between these two phases may come from the fact that the DP system is used in both of them, and this system is quite complex. At the same time, the gangway system does not seem to add a significant amount of variability in the analysis we have performed.

Given the relationship between performance and safety (see Section 4.3), the phases with higher system variability may also be more complex and exposed to higher time and other production pressures. Hence, these phases need adequate resources to maintain both safety and performance.

6 Limitations

The proposed indicator of the system variability is only suitable for some preliminary analysis. The paper has not validated the indicator by analytical or empirical means. However, the presented theoretical basis and used assumptions therein provide a reasonable support for the indictor. Clearly, further research is needed in this still new area of systemic safety analysis.

We recognise that the proposed indicator is not fully independent from how a hazard analysis is performed. Different analysts will produce different set of results for the same system, and hence the system variability will also be different. Therefore, such indicators should not be used to compare different analyses—unless those analyses used the same assumptions—and should be limited to a comparison of different operational scenarios or phases within a single analysis.

7 Conclusions

The paper has presented the results of systemic hazard analysis of service offshore vessel's (SOV) operations. 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.

The study has made the following contributions and conclusions:

- It has brought awareness of system-level hazards involved in various phases of SOV operation and the number of hazardous scenarios associated with them.
- The paper has introduced the notion of system variability as a conditional proxy to the incident likelihood. It can be used to compare various phases of operation, provided that resources for risk (safety) management are very similar within those phases. The proposed metric can be seen as an alternative to aggregate probabilistic figures (e.g., total risk) which are frequently employed.
- The comparison has shown that all three phases of SOV operation have rather comparable levels of system variability. However, the interface between the SOV and turbine via the gangway system and the manoeuvring between turbines seem to be more complex phases of operation with a higher potential for both incidents and performance (work efficiency) shortfalls. Consequently, continuous management of resources is necessary to maintain both safety and performance there.
- Future studies should incorporate the effect of resources (for risk and performance management) into the comparison, as discussed in Section 4.3.

8 Appendices

NA

9 Code availability

NA

10 Data availability

NA

11 Executable research compendium (ERC)

NA

12 Sample availability

NA

13 Video supplement

NA

14 Supplement link

NA

15 Team list

NA

16 Author contribution

Main author contributions are listed below, based on the CRediT contributor roles taxonomy:

- Romanas Puisa: Funding acquisition, Conceptualization, Methodology, and Writing – review & editing.
- Victor Bolbot: Investigation, Formal analysis, and Methodology.
- Andrew Newman: Validation, Methodology and Writing – original draft preparation.
- Dracos Vassalos: Supervision.

17 Competing interests

The authors declare that they have no conflict of interest.

18 Disclaimer

This paper represents the opinions of the authors, and is the product of professional research. It is not meant to represent the position or opinions of their organisations, nor the official position of any staff members. Any errors are the fault of the authors.

19 Special issue statement

NA

20 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.

21 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.
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.
BS EN 31010:2010: Risk management. Risk assessment techniques.
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.
Chen, H., and Moan, T.: DP incidents on mobile offshore drilling units on the Norwegian Continental Shelf, Advances in Safety and Reliability-Proceedings of the European Safety and Reliability Conference, ESREL, 2005, 337-344,
de Vries, L.: Work as done? Understanding the practice of sociotechnical work in the maritime domain, Journal of Cognitive Engineering and Decision Making, 11, 270-295, 2017.
Dekker, S.: Drift into failure: From hunting broken components to understanding complex systems, CRC Press, 2016.
DNVGL: Certification of offshore gangways for personnel transfer, 2015a.
DNVGL: Dynamic positioning vessel design philosophy guidelines. Recommended practice (DNVGL-RP-E306). 2015b.
DNVGL: Offshore gangways (DNVGL-ST-0358)DNVGL-ST-0358, 2017.
DoD, U. S.: Department of Defense. In: Standard practice. System safety, 2012.
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.
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.
Herrera, I. A., Hollnagel, E., and Håbrekke, S.: Proposing safety performance indicators for helicopter offshore on the Norwegian Continental Shelf, 2010,
Hollnagel, E., Woods, D. D., and Leveson, N.: Resilience engineering: Concepts and precepts, Ashgate Publishing, Ltd., 2007.
Hollnagel, E.: Barriers and accident prevention, Routledge, 2016.
Hollnagel, E.: Safety-I and Safety-II: the past and future of safety management, CRC Press, 2018.
IEC61508: IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems, International Electrotechnical Commission, Geneva, Switzerland, 1998.

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.
IMCA: International Guidelines for The Safe Operation of Dynamically Positioned Offshore Supply Vessels (182 MSF Rev. 2). 2015.
IMO: International Safety Management Code (ISM Code) with guidelines for its implementation. IMO, London, 2018.
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., 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.
Meadows, D. H.: Thinking in systems: A primer, chelsea green publishing, 2008.
Patriarca, R., and Bergström, J.: Modelling complexity in everyday operations: functional resonance in maritime mooring at quay, Cognition, Technology & Work, 19, 711-729, 2017.
Praetorius, G., Hollnagel, E., and Dahlman, J.: Modelling Vessel Traffic Service to understand resilience in everyday operations, Reliability engineering & system safety, 141, 10-21, 2015.
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.
Puisa, R., Bolbot, V., and Ihle, I.: Development of functional safety requirements for DP-driven servicing of wind turbines, The 7th edition of the European STAMP Workshop and Conference (ESWC), Helsinki, 2019.
Qureshi, Z. H.: A review of accident modelling approaches for complex socio-technical systems, Proceedings of the twelfth Australian workshop on Safety critical systems and software and safety-related programmable systems-Volume 86, 2007, 47-59,
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.
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.
Rollenhagen, C.: MTO–an Introduction; the Relationship Between Humans, Technology and Organization, Utbildningshuset, Lund, Sweden, 1997.
Salmon, P. M., Cornelissen, M., and Trotter, M. J.: Systems-based accident analysis methods: A comparison of Accimap, HFACS, and STAMP, Safety Science, 50, 1158-1170, https://doi.org/10.1016/j.ssci.2011.11.009, 2012.
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.
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.
Woods, D. D., and Hollnagel, E.: Prologue: resilience engineering concepts, in: Resilience engineering, CRC Press, 13-18, 2017.