

1 **Anonymous Referee #1,**

2 Received 16 Apr 2020

3 Referee comments:

4 Comment1: Line 210 - it is not clear to what specific steps of hazards analysis the authors are
5 referring. Some graphical representation of this process would be helpful.

6 Comment2: Tables 3-5 Since one hazard may results in numerous scenarios (e.g. hazard #1 creates 259 scenarios), please
7 elaborate more on the process of transition from a hazard
8 to a scenario. It is not clear at this stage.

9 Comment3: Figure 6 Please explain the meaning of relative exposure to hazards and the way this
10 index is calculated.

Author response:

All comments are valid and the manuscript has been updated appropriately.

Comment1: A cross-reference to Fig.2 has been inserted where the steps of hazard analysis are given.

Comment2: Section 5 now contains explanation about the transition between hazards and their scenarios.

Comment3: The concept of the relative exposue was removed in the revised manuscript. The major revision was done

11

12

13

14

15

16

17

18

19

Anonymous Referee #2

20

Received and published: 10 July 2020

21

22 General comments:

23 The authors points out that SOV operations constitute a complex socio-technical system, consisting of several subsystems.
24 Each subsystem has specified safety procedures, but the authors argue that potential hazards resulting from the interaction of
25 subsystems might not be properly accounted for with the existing approach, which focus on potential hazards for each
26 subsystem. Instead, they propose to use the systemic method STPA, where the starting point is to identify hazards on the
27 system level. The topic of the paper is relevant, and it is generally well structured. However, I see some issues in the quantitative
28 outcome of the analysis, as given below.

29 The authors make conclusions about the risk in the abstract, however, they do not actually do a risk analysis, as they do not
30 consider the consequences/potential losses, and also not directly the likelihood.

1. Author's response to the preceding paragraph

Indeed, risks associated with the identified hazards, in terms of likelihood and consequences, are not presented in the paper. The scope of the paper is limited to hazard prevention/control, i.e. hazard mitigation is outside the scope. To make sure the message is unambiguous, appropriate changes will be made in the abstract and elsewhere in the paper.

However, based on other review comments, the paper has updated and doesn't not use the hazard likelihoods either. Instead, the comparison is done by using a systemic indicator – system variability.

31

32 They write in line 224-225: "As incident prevention is the focus on this paper, the likelihood alone can be used to rank the
33 hazards, provided the consequences all considered hazards are similarity intolerable." However, there is no justification that
34 the hazards are similarly intolerable. In fact, according to the reference for the applied STPA analysis (Leveson and Thomas
35 2018), the first step of the analysis should be to identify losses (before hazards are identified). However, the authors seem to
36 omit this part of the analysis. I suggest the authors to either modify the analysis to include the losses, or to clearly state in the
37 paper and abstract that this part of the analysis is omitted, and not to make conclusions on the risk.

2. Author's response to the preceding paragraph

The quotation from the paper refers to worst-case consequences of the hazards, and they are quite certain. As stated in the paper (Section 4.2, lines 176-177), all analysed hazards will lead to the same accidents /consequences: injuries and life losses, and damages to SOV, gangway, or turbine. Because consequences are the same for all hazards, we only rank hazards based on their degree of exposure – the proxy for likelihood. We agree it should be stated more clearer what accidents/consequences are considered and that all analysed hazards are assumed to lead to them.

However, based on other review comments, the paper has updated and doesn't not use the hazard likelihoods either. Instead, the comparison is done by using a systemic indicator – system variability.

38

39 The hazard exposure is quantified through the number of scenarios leading to each hazard, and results are presented in tables
40 3-5. It is not clear to me, whether this is this the number of different scenarios, or if it is some frequency of exposure. It is also
41 not clear to me how these scenarios were actually found – e.g. were they found using some documents, in dialog with
42 Kongsberg Maritime, using incident reports, or other? If the number of scenarios is to be understood as the number of different
43 scenarios that can potentially lead to a hazard, I do not follow the argument, that it can be seen as a measure of exposure. The
44 exposure would depend on the probability/frequency and duration of the “scenarios”.

3. Author's response to the preceding paragraph

In this paper, the exposure refers to the number of scenarios in the lead up to a hazard (see Section 4.4). In other words, it is the number of pathways to a hazardous state. Some of these pathways are addressed by design and management measures, while others may be overlooked or intentionally discounted as being unlikely. Thus, the exposure is not time related in the context of this paper, and the dictionary definition of exposure does not imply the link to time. The dictionary definition of exposure is “the state of being in a place or situation where there is no protection from something harmful or unpleasant” (ref. Oxford English Dictionary).

However, based on other review comments, the paper has updated and doesn't not use neither the hazard likelihood or exposure to hazard anymore.

45

46 The number of scenarios seem to depend mainly on how things are defined, and how exhaustive/imaginative the analyst is.

4. Author's response to the preceding paragraph

That is correct. The analysis was performed based on the technical documentations available, and discussions with designers and operators. There is indeed a real possibility that some scenarios were overlooked. However, it is a common practice in safety engineering when the analysis is done manually. Unfortunately, automated analysis that could exhaustively explore all scenarios is unavailable.

As indicated in responses above, we adopted a systemic indicator to be less sensitive to this problem.

47

48 The assumption that the hazard exposure can be quantified through the number of scenarios leading to each hazard seems to be
 49 made, in order to come up with a quantitative outcome of the analysis, but I cannot see the need (or justification) for coming
 50 up with a quantitative outcome. In the abstract, it is written: “The objective of this paper is to bring awareness of hazards that
 51 may have been overlooked in earlier assessments, and allow for a preliminary comparison of various operational stages.”
 52 Specifically, they wish to “explore hazardous scenarios caused by flawed interactions between system components”. Based on
 53 this, I believe that the main outcome of the analysis, and the main result to be presented in the paper, should be the identified
 54 “hazardous scenarios caused by flawed interactions between system components” If such scenarios were not found, the abstract
 55 and conclusion should reflect this.

5. Author’s response to the preceding paragraph

All hazardous scenarios in Tables 3-5 are of interaction nature. The quantification in terms of number of scenarios is not actually done, and it is never claimed that it has been. The exposure (vulnerability) to hazards is used only to give guidance as to what priority of the follow-up, more detailed and potentially quantitative analysis should follow. This is stated on Line 258-259: “ The comparison is, nevertheless, preliminary and should be used as a preface for a more detail, potentially quantitative, comparison.”

Thus, the paper delivers system level hazards and associated information.

56

57 Specific comments:

58 Line 32-33: “It is normally a motion-compensated (3 or 6 DoF) gangway system, which allows for relatively safer (based on
 59 experience so far) and time-efficient (within some 5 minutes) transfer.” I believe that the bump-and-jump method is
 60 significantly more time-efficient, if conditions allow for transfer this way - this could be mentioned. (see e.g. Nikki Twigt,
 61 Access Systems for Offshore Turbines - A review of conventional and walk-to-work transfer methods, 2020)

6. Author’s response to the preceding paragraph

It is indeed can be more time efficient, but less safer, based on our opinion. We’ll familiarise with the publication and cite it if relevant.

62

63 Technical corrections:

64 Line 72: Reference to Section 0

65 The paper needs a language check.

66

7. Author's response to the preceding paragraph

The corrections will be made. Thank you.

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

Anonymous Referee #3

88

Received on 27 July 2020

89

Major comments:

90

1. About the objective, as stated in abstract and line 60, the objective of the paper is 1)

91

to bring awareness of hazards that may have not been captured in earlier assessments,

92

and 2) allow for a preliminary comparison of various operational stages of SOV. The

93

second objective is clearly addressed in the paper. However, the first one: capturing

94

hazards that may have been overlooked by earlier assessments, the so-called earlier

95

assessments are not specific enough in the paper. There is no way to judge whether

96

those identified hazards were overlooked in earlier assessments. The only place that

97

mentioned earlier assessments is part 2 related work. However, the review work does

98

not seem to be complete or provide enough evidence that identified hazards in this

99

work is more complete than others. My arguments are 1) defined scope of hazard analysis are different, therefore resulting

100

different hazards identified, for example, both

101

Presencia and Shafiee, Dong et al. focused on collision, Rokseth et al. focused on DP

102

system. 2) The depths of hazard analysis are different. The definition of hazards is

103

relative, for example, the occurrence of an event can be considered as an accident in

104

one analysis however can be defined as a hazard in another analysis. We can always

105

find root causes after root cause if we dive deeper. If the authors want to compare with

106

earlier assessments, you need to compare with the assessment which considered the

107

same system or scope of analysis.

108

I suggest the authors delete “that may have not been captured in earlier assessments”

109

from your objective.

110

1. Author’s response to the preceding paragraph

Indeed, the paper doesn’t provide an explicit, systematic comparison with the state of the art. And so is not claimed in the paper. Such a comparison is only possible if, as rightly pointed by the reviewer, there a hazard analysis conducted in similar settings to compare with. The authors have not come across such an analysis.

This and other comments by the reviewer, prompted us to revise the paper and introduce significant changes in to the objectives/scope as well.

111

112

113

2. System description. There is no description about the system to be analyzed in the

114

work. To conduct hazard analysis by STPA, the first step is to define system. However,

115

the author did not clearly specify the system boundaries and components included,

116

even though the authors described the different phases of operation in 4.1.

117

2. Author’s response to the preceding paragraph

We agree with the comment concerning the insufficient of system description in terms of boundaries and components. The revised version will have more detail on this. However, the paper will be limited to a high-

level description, given that hazardous scenarios are outwith this paper. We also limit the description to one of the operational phases only.

118
119 In Figure 3, shore station is included, however the control loops between shore station
120 and SOV, and shore station and turbine are not part of your analysis. This is fine. It
121 could be better to mark that shore station is not within your defined system scope.
122
123

3. Author's response to the preceding paragraph

Actually it was a part of the analysis. The analysis was under Hazard 3 in Table 4. We had scenarios of miscommunication between shore and SOV, leading to this hazard. We've added extra text for this hazard.

124
125
126 The authors did not specify what accident (unwanted losses) were considered in the
127 analysis either. This is the very important part when applying STPA method. Using
128 "For instance. . ." in Line 176 may not be enough to specify targeted accidents (Loss).
129 Especially the authors wanted to focus on "to bring awareness of hazards that may
130 have not been captured in earlier assessments". Without being specific, readers need
131 to assume that your work covered all accidents and incidents, such as a heart attack of
132 a personnel during operation. The example I gave here is bit too extreme but is within
133 the definition of accident (unexpected and unwanted loss of life).
134

4. Author's response to the preceding paragraph

We agree. However, as the revised manuscript shows, this become irrelevant. The study focusing on hazards and their scenarios only. There is no ranking based on risk.

135
136
137 3. Comparison of different operational phases. There are several issues here. First, the authors chose median value for
138 comparison without providing argument to support that the median value is a proper choice.

5. Author's response to the preceding paragraph

The revised manuscript proposes a systemic indicator for this comparison. The median is not used anymore.

139
140 Second, the authors assumed that 1) all hazards are equally intolerable, and 2) number of hazardous scenarios present the
141 occurrence probability. These two assumptions are not widely accepted. This is fine since the authors clearly stated that those
142 are assumptions. However, the authors did not discuss the inaccuracy of the conclusion due to these assumptions.

6. Author's response to the preceding paragraph

The revised manuscript (thanks to the comments by this reviewer) has significant changes and does not refer to probabilities and provides a different interpretation of hazardous scenarios.

143
144

145 Third, obviously, there are other quantities that can be used for ranking as well. The ultimate objective is to compare different
146 operation phases. If we median value, then the rank (high to low risk) is transit and maneuvering > Interface turbine via
147 gangway > interface with daughter craft. If we use the total number of hazardous scenarios of each phase, then the rank (high
148 to low risk) is Interface turbine via gangway (474 hazardous scenarios) > transit and maneuvering (452) > interface with
149 daughter craft (344). However, if we use the total number of hazards of each phase, then the rank (high to low risk) is interface
150 with daughter craft (11)> Interface turbine via gangway (8) >transit and maneuvering (4). Different quantities can provide
151 different results, and I can make reasonable assumptions to support the rationality of all these quantities. Since ranking is a
152 focus of the paper as stated in the objective, the authors need to provide enough supportive arguments for their choice and
153 discuss other opposite possibilities as well.

154

7. Author's response to the preceding paragraph

This is a very good observations. This comment is the main cause for substantial changes the paper has undergone. We now use a different measure and provide a detailed rationale why it makes sense.

155

156 4. Limitations of the method. The authors did not specify the limitations of using STPA methods for hazard analysis. A method
157 is not almighty, limitations of the method applied should be specified as well besides the biases and knowledge limitation from
158 the analyzers.

8. Author's response to the preceding paragraph

References to other publications which address the STPA limitations will be added.

159

160 5. Language check is required. There are many misspellings in the paper, for example, "Specufic control actions" in Figure 4,
161 Line 72 "Section 0".

9. Author's response to the preceding paragraph

The language will checked and improved.

162

163 Minor comments:

164 1. Line 164-166, about the definition of incident and accident. 1) Even though the authors referred Rausand's differentiation
165 between incidents and accidents, this differentiation is not used anywhere in the paper at all. From my point of view, authors

166 focused on possible accidents. However, incident is the terms showed up in many places in the paper which actually means
 167 accidents (if I understand it correctly). 2) If the authors defined incident is a materialized hazard with insignificant
 168 consequences, how accident can be incidents with significant consequences? I suggest the authors either delete this
 169 differentiation or be more precise when using these two terms if such a differentiation is made in the paper. In addition, a
 170 thorough check of where accident and incident are used is necessary.

10. Author's response to the preceding paragraph

The used understanding is that depending on consequences of an untoward event, it is called a near-miss, incident or accident. Near-misses would not have consequences at all, incidents will have insignificant ones, whereas accidents will have significant consequences. The term incident is also used to refer all untoward events when consequences are assumed unknown, but this is indeed confusing and a stricter definition should be used. Corrections will be made.

172
 173 2. Line 181, Line 269 Table 3, Line 282, Table 4. "3. SOV does not operate on DP class 2 or above" etc. Therefore, I do not
 174 think this can be considered as an operational hazard. Or at least, the way the authors phrased it does not seem right. DP failure
 175 sounds more like a hazard.

11. Author's response to the preceding paragraph

DP class 2 or higher introduces redundancy against thruster and other component/sub-system failures. It is a safety procedure that has to be followed when the ship is engaged in safety critical tasks. Therefore, operating without redundancy on, represents a hazard. Text will be added to explain all this.

176
 177 3. Line 208, Figure 4. The author did not explain why there are black box and white box in the figure. I think Figure 4 can be
 178 deleted. The information from Figure 4 is already covered by Figure 4. Figure 4 does not provide any new information from
 179 my point of view.

12. Author's response to the preceding paragraph

Figure 4 clarifies the input for the analysis, as indicated on Line 206. But it is indeed redundant and will be removed.

180
 181 4. Line 293, Table 6. It is a bit strange that during transit and maneuvering phrase, there is no inadequacy in control actions &
 182 feedback and/or process model. A simple scenario can be the collision accident between installed turbine (if there are some
 183 other turbines which have been installed in the field) and vessel, or vessel and ice. A possible hazard is "the vessel does not
 184 keep a min safe distance to turbine or its blades. Possible hazardous scenario can be that the vessel stops too slowly (especially

185 in manual navigation), turbine(blade) is not noticed etc. The same applies to that there is no inadequacy in handling external
186 disturbances during interface with turbine via gangway and interface with daughter craft.

13. Author's response to the preceding paragraph

The hazard "the vessel does not keep a min safe distance to turbine or its blades" was assigned to the phase when the vessel is interfaced with the turbine. During transit and manoeuvring, other hazards were considered (Table 3) and amongst them, credible causal factors were not related to control and feedback channels. This clarification will be added into the text.

187

188 5. The second and third paragraph in the discussion part. Well, the appearance of these two paragraphs is a bit abrupt. In
189 addition, it does not highlight the necessary/advantage of conducting such a hazard analysis as the authors did. The authors
190 first argued that analyzed hazards should be already covered by existing safety rules or regulations, however it is not guaranteed
191 those rules can be followed in practice. Well, this can be true that rules may not be followed in practice, therefore there is still
192 residual risk during the operation. However, residual risk also exists after a hazard analysis (risk analysis) is conducted.
193 Hazards are identified does not mean that hazards are eliminated. The authors also judged that some hazardous scenarios are
194 not addressed by regulations for certain reasons. However, in my opinion, those reasons also apply to the hazard analysis that
195 the author conducted. Rule/regulations are not perfect, so is your hazard analysis. If you want to compare the hazards you
196 identified with those stated by rules/regulations, at least you should start with the same defined scope of analysis, the same
197 type of accident (loss), the same hazards. I suggest that the authors rephrase these two paragraphs or can simply delete them.

14. Author's response to the preceding paragraph

The issues of imperfect analysis and comparison is correct. However, the paper doesn't attempt to provide comparisons with the rules or other analyses. As discussed in the earlier response, such comparison is indeed not possible because the input used for drafting the rules is unavailable for public use.

However, this becomes irrelevant in the revised paper, which has slightly different scope.

198

199 6. The first paragraph in the conclusion part. I already stated my argument in the first comment about the objective. There is
200 not enough evidence showing that risk assessments are done piecemeal and potentially lacking completeness. . . . It may sound
201 better if you simply say that no such risk assessment has been conducted in the industry (only if experts from industry told you
202 so). The value of academic work is not to conduct a specific risk assessment, sure you cannot find such from published papers.
203 Conducting hazard analysis/risk assessment is an industrial practice which do not necessary provide enough academia value.

204

15. Author's response to the preceding paragraph

Agreed, the academic value from a hazard analysis is limited, if any. The response #7 alludes to the academic value of this work. The text throughout the paper will be updated accordingly.

205

206 7. The detailed intermediate results and final results from the STPA can be added in the appendix. For example, the control
207 diagrams, identified unsafe control actions.

16. Author's response to the preceding paragraph

We have reduced the amount of graphics and the paper itself. Other results than those published cannot be shared due to PR constraints.

208

209

210

211

212

213

214

215

216

217

218

219

220

221

222

223

Revealing system variability of offshore service operations through systemic hazard analysis

Romanas Puisa^a, Victor Bolbot^a, Andrew Newman^b, Dracos Vassalos^a

^aMaritime Safety Research Centre, University of Strathclyde, UK

^bGlobal 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 twofold. First, we perform a systemic hazard analysis by the STPA method for three phases of SOV operation: when transiting and manoeuvring within a windfarm, interfacing with turbines, and launching or recovering daughter crafts. This gives us sets of scenarios containing potentially hazardous interactions between various system components. Such scenarios reflect the complexity and potential for necessary and unwanted variability in the system. Second, we use these results to compare the three operational phases in terms of a proposed systemic indicator—the system variability. The comparison shows that all three phases of SOV operation have rather comparable levels of variability. However, the interface between the SOV and turbine via the gangway system and the manoeuvring between turbines seem to show a higher potential for uncontrolled variability. We have broadly discussed what resources and capabilities should be added to improve the control. The study has also shown how results of a systemic hazard can be linked to systemic indicators or measures of system safety, namely to the system variability.

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

252 equipment. Daughter crafts (DCs) are medium size boats, typically under 20 meters, which are carried by the SOV and used
253 to transport lighter equipment to turbines in moderate environmental conditions ($< 1.8\text{m}$ significant wave height). DCs are
254 loaded with technicians and launched from a SOV deck by some davit system, typically 3-5 times per day, and then recovered
255 (lift-up) from the water periodically. SOVs would also have a sophisticated system for transferring technicians and equipment
256 to and from a turbine. It is normally a motion-compensated (3 or 6 DoF) gangway system, which allows for relatively safer
257 (based on experience so far) and time-efficient (within some 5 minutes) transfer.

258 The multifaceted nature of SOV operations complicates the management of their safety. The overall safety management of
259 SOV operations is an amalgamation of individual safety procedures for the SOV, davit, DC, gangway, drone and other systems
260 (Section 2). These safety systems are developed in isolation from a wider operational context and, when integrated, can lead
261 to confusion, surprises and undue pressure on operators (Ahsan et al., 2019). In such conditions, accidents can be caused by
262 well-known but inadequately managed scenarios (e.g., loss of power or control), as well as by yet unknown scenarios created
263 by new technology or new ways of operation. In 2018, the offshore supply vessel Vos Stone temporarily lost control of thrusters,
264 drifted and struck a wind turbine (BSU, 2019). Amongst the causes, the officers on the bridge did not manage to seamlessly
265 switch between modes of thruster control (from DP to other mode) because they were confused about them. Inadequately
266 controlled transitions between modes of operation, particularly between normal (frequently used) and abnormal (rarely used,
267 e.g. emergency) modes, is a classic scenario for accidents (Sarter et al., 1997;Leveson, 2011a, p. 289). Another incident
268 happened in 2013 when the diving support vessel Bibby Topaz drifted off the position (maintained by the DP system) while
269 two divers were exploring the seabed (IMCA, 2013). Amongst the causes, the vessel had had a dormant (unidentified)
270 hazard—a design error—that did not allow to adequately respond to safety critical faults that preceded the incident.

271 As the cost-efficiency of marine operations is being increased by more automation and autonomy (Twomey, 2017), systems
272 become more tightly coupled, nonlinear and more difficult to understand, design, analyse and operate (Perrow, 1984). Such
273 complex systems tend to create “interactions in an unexpected sequence” (Perrow, 1984, p. 78), and some of these interactions
274 can be hazardous. These interactions, and their consequences, is difficult to envisage during design of individual system
275 components or sub-assemblies, because they manifest themselves at the system level and under specific circumstances or
276 scenarios. System properties and events such as safety, or absence thereof, are emergent (Checkland, 1981;Meadows,
277 2008;Leveson, 2011b), or as Rasmussen put it "a system is more than the sum of its elements" (Rasmussen, 1997). We,
278 therefore, cannot predict when untoward events (near-misses, incidents, and accidents) will occur, as we used to do with
279 electromechanical systems with well-defined probability distributions of failures.

280 This means that focusing on individual hazardous scenarios or hazards is oversimplification and is unhelpful. Safety is a system
281 property, which cannot be inferred from properties of individual components or scenarios (Leveson, 2011b). By making this
282 assumption we follow the systemic view (systems thinking) on safety as highlighted above and acknowledge the danger of the

283 reification fallacy, i.e. “the tendency to convert a complex process or abstract concept into a single entity or thing in itself”
284 (Gould and Gold, 1996;Hollnagel and Woods, 2006). One, therefore, should regard hazards and related events are symptoms
285 of wider, structural issues within safety control. They are symptoms that the safety control structure in place is inadequately
286 designed, because it should not lead to hazards otherwise (Leveson, 2011a, p. 100).

287 Consequently, instead of trying to infer safety or some risk level from individual hazards and scenarios, a systemic measure
288 should be used. As discussed in Section 4.1, this measure should reflect the variability within the system where technical and
289 human components interact. This variability can then combine with other sources of variability such as latent conditions (e.g.,
290 negligent safety culture, inadequate feedback on system performance) and impaired or missing safety barriers to lead to unsafe
291 system states or hazards (Hollnagel, 2016). By knowing where and when the system variability is highest, changes to the
292 design and operation can be made to control it better and, subsequently, prevent incidents and accidents.

293 With the above in mind, the objective of this paper is twofold. First, we perform a systemic hazard analysis for three phases
294 of SOV operation: when transiting and manoeuvring within a windfarm, interfacing with turbines, and launching or recovering
295 daughter crafts. Second, we use the analysis results to estimate and then compare the system variability within the system
296 during three operational phases. For the systemic hazard analysis, we use the Systems Theoretic Process Analysis (STPA)
297 (Leveson, 2011a;Leveson and Thomas, 2018). This is method is based on a systemic accident model and allows to explore
298 hazardous scenarios caused by flawed interactions between system components and, to a lesser extent, by component failures.

299 The paper is organised as follows. Section 2 explores related work, Section 3 explains the basics behind safety management
300 currently in practice, Section 4 introduces to the concept of system variability and describes its adopted indicator, Section 5
301 outlines the analysis results, which are subsequently discussed in Section 6. Section 8 concludes the paper.

302 **2 Related work**

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

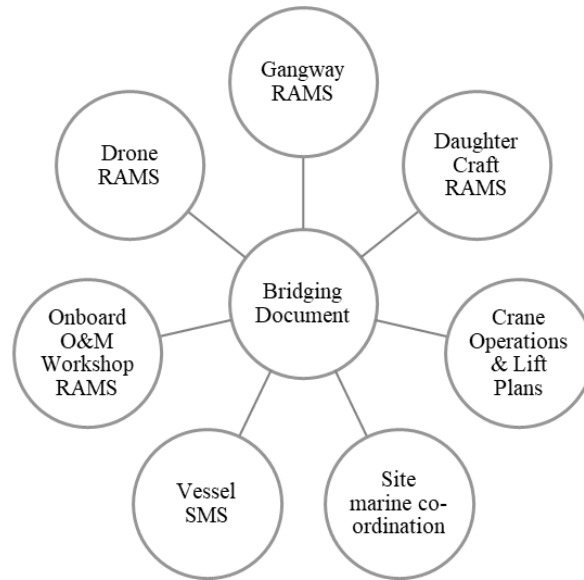
305 The reviewed literature focuses on collision (ship to ship, ship to turbine), reliability issues with technology (DP, gangway,
306 and other systems) and human factors (Presencia and Shafiee, 2018), (Dong et al., 2017), (Rollenhagen, 1997;Sklet, 2006),
307 (Rokseth et al., 2017), and (SgurrEnergy, 2014). The used hazard analysis mainly followed a conventional, non-systemic,
308 approach where individual hazards or scenarios are considered in isolation. In most cases, statistics or probabilistic analysis is
309 used for decision making. The exception is Rokseth et al. who applied the STPA method to hazard analysis of offshore supply
310 vessels running on the DP system (Rokseth et al., 2017). None of the studies use systemic indicators or measures (e.g., of
311 resilience) to infer the safety level or compare operational phases or other aspects.

312 When it comes to indicators or measures of system variability and resilience, the general literature is abundant, e.g. (Hollnagel
313 et al., 2007; Herrera et al., 2010). The literature specific to the maritime domain is limited but present, e.g. (Praetorius et al.,
314 2015; Patriarca and Bergström, 2017; de Vries, 2017). However, the authors have not come across a work which connects
315 results of a systemic hazard analysis, namely hazardous scenarios, with the system variability or similar systemic indicators.

316 **3 Safety management practice**

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

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



330
331 *Figure 1: Illustration of current safety governance*

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

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

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

347

348

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

349

350 **4 Method**

351 **4.1 System variability**

352 As argued in Section 1, a top-down, systemic approach to safety analysis should be used for complex systems. In this section
353 we highlight further characteristics of such systems and introduce the notion of system variability.

354 First, it is helpful to resume our discussion on how untoward events happen in complex, socio-technical systems. The presence
355 of a systematic, as opposed to random, drift to failure is characteristic for all socio-technical systems (Rasmussen,
356 1997;Dekker, 2016). People, and organisations, are constantly looking for trade-offs between production pressures, individual
357 preferences and safety expectations. Sometimes, production pressures, in particular, can outweigh the other ones, with small
358 deviations from earlier established norms being systematically normalised—confusing the absence of risk evidence with the
359 absence of risk. Hollnagel refers to this constant optimisation of performance as the ETTO principle, Efficiency-Thoroughness
360 Trade-Off (Hollnagel, 2017). An important element of the performance optimisation is the need to adjust to irregularities and
361 deviations in the expected performance of other system components and the environment. This can lead to repeated and quite
362 rational violations of procedures to maintain safety (Besnard and Hollnagel, 2014;Fujita, 1991;Rasmussen and Suedung, 2000).
363 As design errors are frequent and procedures are often underspecified in complex systems, such performance adjustments

364 become vital for safety and other system objectives. Hence, inability to adequately adjust to operational complexity due to
365 meagre resources (time, knowledge, competence, etc.) is a harbinger of untoward events (Woods and Hollnagel, 2017). By
366 contrast, the ability to anticipate, adjust and adapt to various irregularities is referred to as system *resilience* (Hollnagel et al.,
367 2007).

368 Under certain conditions the system variability can get out of control, putting safety, or performance alike, in jeopardy. This
369 happens when various sources of variability combine in a nonlinear fashion (i.e., when a cause is disproportional to an effect),
370 exploding the operational complexity and creating opportunities for hazards and, if not mitigated, for incidents and accidents.
371 Hollnagel defines the following sources of variability that may combine (Hollnagel, 2016, p. 170):

- 372 • Human performance variability, as explained by the ETTO principle above.
- 373 • Technological glitches, gradual and outright failures, caused by design or maintenance errors.
- 374 • Inadequate or missing safety barriers due to design or maintenance errors.
- 375 • Latent conditions such a deficient safety culture (i.e. “how things are done here”) and inadequate feedback (e.g.,
376 reporting of incidents) on safety critical processes.

377 Although we cannot predict when an untoward event can happen, we can say whether it is likely or not. It can be done “by
378 characterising the variability within the system, specifically the variability of components and subsystems and how they may
379 combine in unwanted ways. This can be done by looking at how functions and subsystems depend on each other.” (Hollnagel,
380 2016, p. 172). This very information is obtainable from a systemic hazard analysis (Section 4.2) where flawed interactions
381 between system components at various levels of abstraction are revealed.

382 These flawed interactions show how safety control can be lost due to inability to adequately deal with operational complexity,
383 i.e. the inability to anticipate and adjust. The presence of such interactions, or hazardous scenarios, reflects the presence of
384 variability in the system, and this variability is both necessary and unwanted. The more scenarios to a system hazard, the higher
385 potential for the unwanted (uncontrolled) variability and also for the needed flexibility to maximise the performance. As
386 Hollnagel stated “The adaptability and flexibility of human work is the reason for its efficiency. At the same time it is also the
387 reason for the failures that occur, although it is never the cause of the failures.” (Hollnagel, 2016, p. 150). In other words,
388 “failures are the flip side of success, meaning that there is no need to evoke special failure mechanisms to explain the former.
389 Instead, they both have their origin in system variability on the individual and systemic levels, the difference being how well
390 the system was controlled.” (Hollnagel et al., 2007, p. xi). Thus, the system variability revealed via a systemic hazard analysis
391 will lead to hazards if uncontrolled and to successes otherwise.

392 Thus, the presence of potentially unwanted variability (i.e. found through a hazard analysis) should be regarded as invaluable
393 information for improving both safety and performance. That is, such system variability indicates the need for better or more
394 of (Hollnagel and Woods, 2005):

- 395 • Foresight so hazardous situations can be better anticipated that require speedy adjustments or extra resources (people,
396 knowledge, competence, time, speed, power, etc.).
- 397 • Feedback on physical processes with potential for hazards.
- 398 • Flexibility (ability to adjust and adapt) on the part of operational procedures, along with corresponding training of
399 people;
- 400 • Timely availability of safety resources (time, knowledge, competence, etc.) to support adequate adjustment;

401

402 Thus, once we have results from a systemic hazard analysis in the form of hazardous scenarios, how do we use them to discern
403 the existing variability within the system? We propose to use a simple indicator of system variability for a preliminary
404 comparison of various phases of operation. It is a ratio of the number of hazardous scenarios per operational phase, NHS_i , to
405 the total number of hazardous scenarios across all N phases of operation, Eq. (1).

$$\text{System variability}_i = \frac{NHS_i}{\sum_i^N NHS_i} \quad (1)$$

406 Inspired by the Rasmussen's the boundary of safe behaviour (Rasmussen, 1997) and production pressures pushing towards
407 this boundary, Figure 2 illustrate the rationale behind this indicator of system variability. As discussed above, a systemic hazard
408 analysis delivers scenarios of interaction between various system components, the interactions that can lead to hazards. These
409 paths are reflective of the physical design and the majority of them would be constrained by operational procedures in place.
410 However, under production pressures and performance optimisation, the constraints can get violated and loopholes exploited,
411 unwittingly drifting to hazardous states as discussed earlier. Figure 2 shows that if hazard 1 and 2 were to belong to different
412 phases of operation, the first phase would engage more complex operations (because of more complex functions and them
413 implementing systems) than the second phase, leading to higher variability as a result.

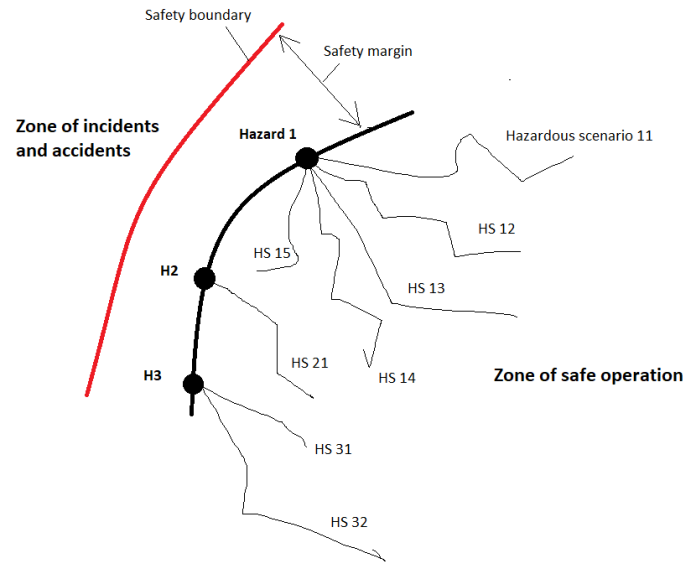


Figure 2: Graphical interpretation of system variability in the context of safety boundary

We note that the proposed indicator of system variability does not include the number of hazards the scenarios led to. This is because we are more concerned about the underlying system structure than the events it can produce. This is a more systemic view on the problem; fundamental discussions on this are found in (Meadows, 2008). This also makes the variability indicator less reflective of the number and type of hazards analysed, which can significantly vary from analysis to analysis.

Nevertheless, 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.

The following section introduces to a systemic hazard analysis and its results which are then use compare the operational phases in terms of system variability.

4.2 Hazard analysis

4.2.1 Systemic accident model

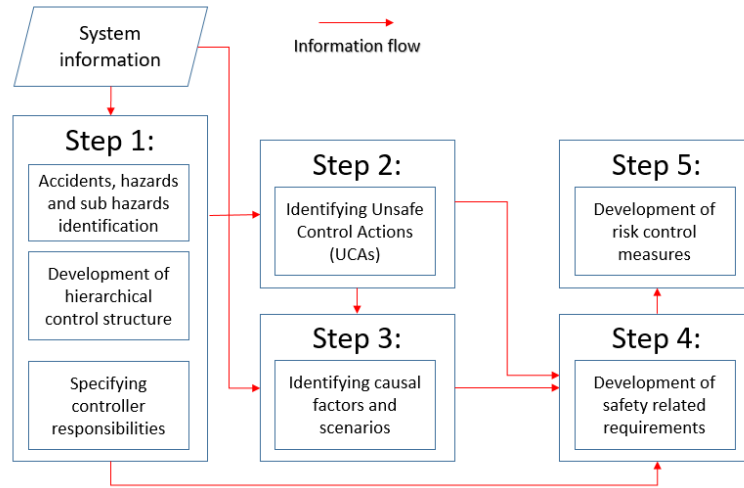
Depending on an accident model assumed, the search principles and analysis goals will be different. Three types accident models can be considered (Hollnagel, 2016): sequential, epidemiological, and systemic. Systemic accident models focus on tight couplings and complex interactions between system components, with the ultimate objective to control the system variability (Hollnagel, 2016). Such accident models are called systemic because the models require to analyse the system as a

432 whole, as oppose to analysing its individual components with the purpose to understand the system's behaviour. The explicit
433 assumption behind systemic accident models is that interactions between system components are more important than
434 component themselves (Meadows, 2008). Individual components can fail, but if interactions remain adequate, the system will
435 heal itself, i.e. such failures would be timely detected and mitigated. Notably, system components change all the time (e.g.,
436 physical components age and get replaced, people come and go), but as long as interactions between them remain the same,
437 the system fulfils its original purpose.

438 4.2.2 STPA

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

445 Before explaining the method, it would be helpful to agree on the terminology used. A hazard is a system state that will lead
446 to an incident or accident given specific environmental conditions beyond the control of system designer (Leveson, 2004). The
447 system in question can be a safety management system (SMS) which is designed according to the ISM Code or amalgamated
448 from different RAMS. Incidents and accidents are defined as follows (Rausand, 2013). An incident is a materialised hazard
449 with insignificant consequences. Incidents do not necessary interrupt the prime function (delivery of payload or service). An
450 accident is a materialised hazard with significant consequences (significant loss or damage). Accidents would normally
451 interrupt the prime function.



452
453 *Figure 3: STPA process*

454 A sequential process behind the STPA method is shown in Figure 3. The analysis begins by defining the system and its
455 boundaries. This allow clarifying what accidents (losses) and system-level hazards (conditions for incidents) should be
456 considered in the analysis. For instance, during the SOV interface with the turbine via a gangway, the assumed accidents
457 corresponded to the deviation from the interfacing objective, i.e. occurrence of injuries and life losses, and damages to SOV,
458 gangway, or turbine. However, the reference to accidents is beyond the scope of this paper, as explained earlier.

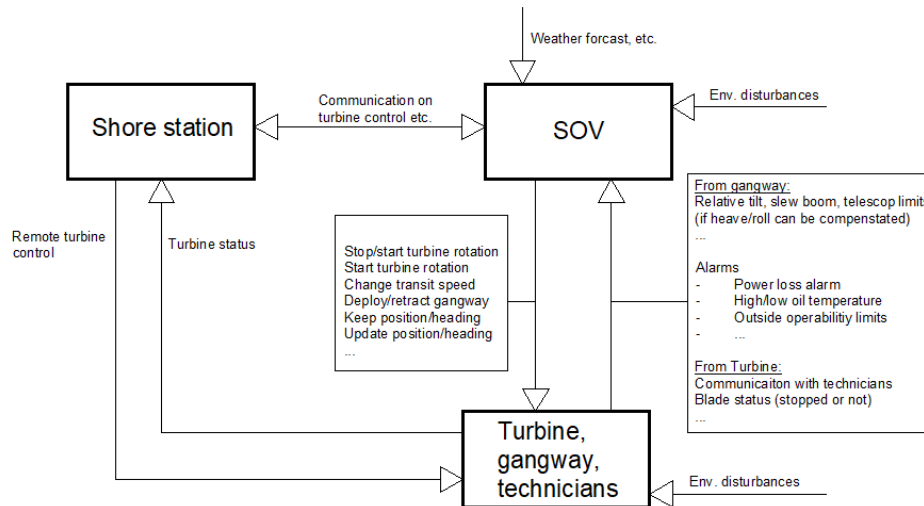
459 Sample system-level hazards are:

- 460 1. Vessel does not keep a min safe distance to turbine or its blades (approaching/staying at turbine when it is in motion);
- 461 2. SOV does not keep position/heading within target limits for a predefined time;
- 462 3. SOV operates on DP class 1, i.e. no redundancy in thrusters, power generation and other safety critical components;
- 463 4. SOV transfers technicians when the gangway is disconnected or dysfunctional (e.g., not motion compensated).

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

468 The system definition further involves its modelling as a hierarchical control diagram. It is a natural way to represent many
469 systems, including safety governance, that involve feedback loops. Figure 4 shows a control diagram for the interface between
470 SOV and a turbine. The control diagram is at higher level of abstraction, where one controller box comprises three other

471 controllers and controlees: turbine, gangway and technicians being transferred. The arrows indicate control and feedback
 472 channels with example control actions and feedback signals indicated. The control actions reflect the responsibilities assigned
 473 to a controller. The responsibilities, or purpose, are also reflected in the control algorithm and feedback information necessary
 474 for adequate control.



475

476 *Figure 4: Hierarchical safety control diagram of interface between SOV and turbine (further explained in Section 4.3)*

477

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

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

488 The fourth and fifth steps of the hazard analysis in Figure 3 are outside the scope of this paper. However, we provide an
 489 example analysis result which also includes proposed functional requirements. Thus, Figure 5 shows sample hazardous
 490 scenarios and safety requirements for the control action “stop turbine rotation” by SOV controller. The arrows indicate the
 491 scenario as a pathway from basis causal factors to system-level hazards: causal factors cause unsafe control actions, which, in
 492 turn, lead to hazards. The shaded cells illustrate a specific scenario, which is preventable by implementing the three functional
 493 safety requirements. These requirements are complementary, representing organisational and design controls.
 494

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.

495

496

Figure 5: Hazardous scenario with three functional requirements

497

4.3 System description

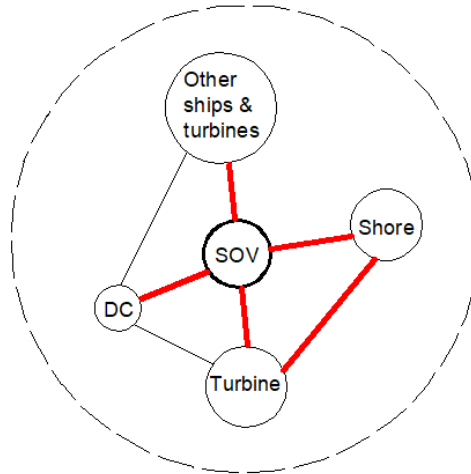
498

The overall system in question is shown in Figure 6. 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

499

500 and shore, turbine and shore), and sensory (distance, visual, and audio) by installed sensors and people. Other interactions at
 501 the system level (e.g., the links between the DC and turbine or other ships) were not analysed.

502



503

504 *Figure 6: System components and system boundary (SOV – service operation vessel, DC – daughter craft)*

504

505 The considered interactions corresponded to four operational phases:

505

- 506 • Transit and manoeuvre within a wind farm. The dynamic positioning (DP) system was considered as the main system
 507 providing the navigation and station keeping (position and heading) functions. The DP system can be switched into
 508 an automatic mode to fully control all three degrees of freedom (DoF): surge, sway, and yaw. The control of DoF can
 509 also be shared with a DP operator who can use a joystick or manual thruster levers.
- 510 • Interface between a SOV and turbine (approach, station keeping, and departure). The DP and motion-compensated
 511 gangway systems were considered to be jointly used. The gangway system is used for technician transfer from SOV
 512 to/from a wind turbine. At the time of transfer, the SOV keeps position and heading by means of the DP system. The
 513 gangway is controlled by a gangway operator who extends, retracts, and maintains communication with the
 514 technicians. There is also a continuous communication between the DP and gangway operators to maintain the
 515 gangway operation within its operability limits.
- 516 • Interface between a SOV and daughter crafts (DC) with a conventional davit system. The DC would be vertically
 517 attached to the davit via a lifting line (vertical) and the painter line to keep the DC aligned with SOV. Both lines are
 518 typically connected and disconnected manually by DC deck crew. DCs are loaded with technicians and equipment,
 519 and launched from a SOV deck by the davit (typically 3-5 times per day) and then recover (lift up) DCs from the
 520 water the same way. During the DC launch and recovery, SOV uses the DP system to maintain the position and

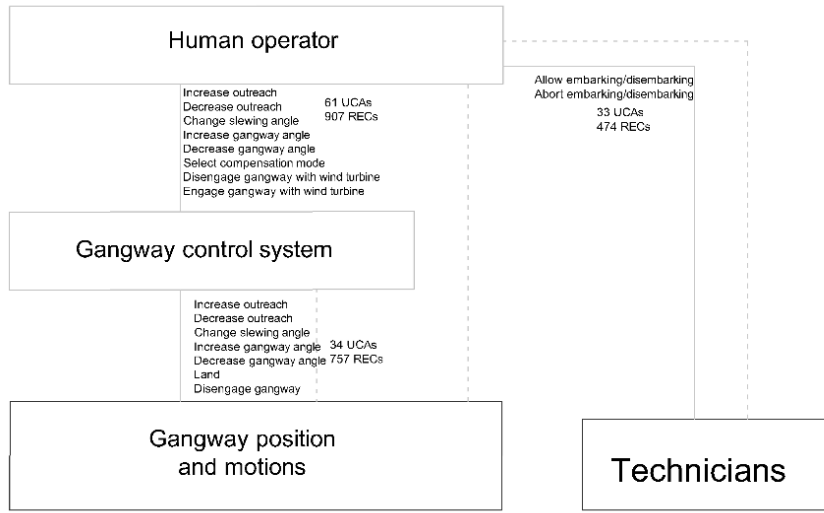
520

521 heading. The interface between a SOV and DC was assumed to following sub-phases with corresponding systems
522 and hazards involved: (1) launch from the SOV and recovery of a DC from water using the davit system, (2) and
523 technician and equipment are transfer when a DC is on water, with technicians claiming up/down the ladder.

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

527 For each phase, a safety control diagram was developed, e.g. Figure 4 shows the one used for the interface between a SOV
528 and a wind turbine. Thus, the safety control diagram in Figure 4 was developed by assuming the SOV to be the main controller,
529 which comprises human controllers on the bridge (e.g., a DP operator), automation, and other ship systems. The shore station
530 as a controller was not analysed, and only the communication with the SOV was considered. The text next to the arrows explain
531 their meaning, i.e. what control and feedback information was assumed. The SOV as a controller is generally responsible for
532 (1) keeping the station (position and heading) until the transfer of technicians via the gangway is complete and (2) providing
533 power to the gangway. Additionally, it was assumed that these responsibilities are only exercised when the SOV, gangway
534 and other systems are fully operational. Based on this information, control actions and feedback can be inferred. Technical
535 publications, such as DP operational manuals, were also used determine control actions and feedback signals (e.g., distance
536 sensors, GPS signals). As Figure 4 shows, the process under control comprised the gangway and turbine, with controlled
537 parameters such as the relative distance, bearing, power supply and others.

538 This phase of SOV operation additionally included a separate hazard analysis of the gangway control, as shown in Figure 7.
539 The control diagram was developed to reflect industrial safety and other requirements for gangways and technician transfer,
540 i.e. (IMCA, 2014;DNVGL, 2017, 2015a). The continuous lines correspond to control channels, with the text indicating the
541 control actions, and dashed lines corresponding to feedback channels. In this diagram, the human operator corresponded to the
542 gangway operator controlling the gangway position and motions by means of the gangway control system. There is also
543 communication with technicians who walk via the gangway.



544

545

Figure 7 Gangway control diagram

546

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.

550

551 **5 Results**

552

This section outlines the results of hazard analysis by STPA, covering the three stages of SOV operation (Section 4.3). Table 2 to Table 4 outlines the considered hazards, the number of identified scenarios that can lead to them, along with example scenarios meant to demonstrate the interactions involved. As discussed earlier, the number of hazardous scenarios behind a hazard does not automatically mean a higher likelihood for that hazard. Instead, it means that there is a higher system variability, i.e. complexity, in connection with this hazard. If this variability is uncontrolled, it can lead to the hazard.

556

557

Based on this tables, Figure 8 shows the system variability as described in Section 4.1. 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.

558

559

560

Table 2: 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.

561

562

563

564

565

566

567

568

569

570

571

572

573

Table 3: 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.

574

575

576

577

578

579

580

Table 4: 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	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 (DC) 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 (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	Davit 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 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 (DC) too slowly.	7	Technician are unaware that crossing should be instant: unfamiliar with safety instructions or the crossing is inadequately coordinated.

581

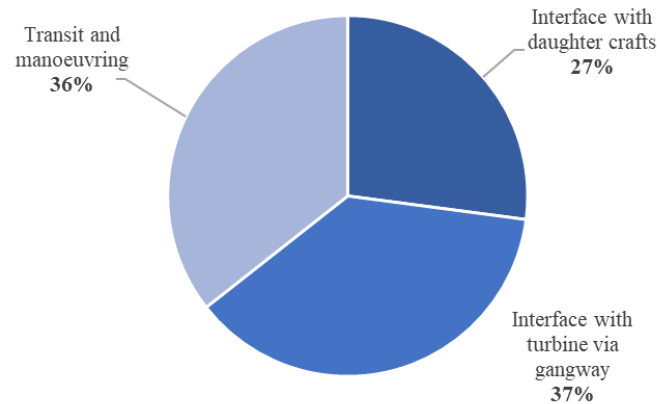


Figure 8: System variability for the three stage of SOV operation

6 Discussion

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 3 “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 brings us to the second contribution of the study, namely the exposure of the variability in the system when in various phases of operation. 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 where the potentially uncontrolled variability 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.

As argued in Section 4.1, the variability in the system is inevitable and necessary to achieve its goals in view of internal deficiencies and external disturbances. However, the variability should be controlled. Uncontrolled variability means that necessary adjustments to keep the system healthy are not performed or performed inadequately due to lack of resources, capabilities, or other reasons. The results of the systemic hazard analysis can be used to locate where such uncontrolled variability is more likely—the likelihood arguably increases with the number of hazardous scenarios—and where resources and capabilities should be added to facilitate performance adjustments. Section 4.1 has already highlighted what general

603 resources and capabilities should be considered to improve the ability to anticipate, adjust and better control the system
604 variability.

605 A detailed discussion on what specific resources and capabilities should be added to each phase of SOV operation is outside
606 the scope of this paper. The presented study only shows that such changes should begin with the SOV interface with turbines,
607 including the approach and departure. The improvements will aim to avoid untoward events such as the earlier highlighted
608 accident with Vos Stone in Section 1.

609 **7 Limitations**

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

613 **8 Conclusions**

614 The paper has presented the results of systemic hazard analysis of service offshore vessel's (SOV) operations. We have
615 specifically analysed 23 operational hazards arising during the three stages of SOV operation: (1) transit and manoeuvre within
616 a windfarm and interfaces with (2) turbines and (3) daughter crafts. The hazards are mostly related to flawed interactions
617 between people and technology, as opposed to individual failures (e.g., human errors, random failures of equipment) that are
618 addressed conventionally. During the hazard analysis, we identified 1,270 hazardous scenarios that explain how hazards can
619 materialise.

620 The study has made the following contributions:

- 621 • It has brought awareness of system-level hazards involved in various phases of SOV operation and the number of
622 hazardous scenarios associated with them. In this study, the number of hazardous scenarios is not interpreted as being
623 proportional to the hazard likelihood (i.e., probability or frequency). Instead, it is interpreted as the degree of system
624 variability which, on the one hand, is necessary for normal performance and, on the other hand, is indicative of system
625 complexity and the potential for uncontrolled variability. We broadly discussed what resources and capabilities should
626 be added to improve the control. Knowledge where the system variability is highest, gives an opportunity to improve
627 both performance (efficiency) and safety. In the latter case, improvements can be introduced to risk assessments (e.g.,
628 by updating assumptions), RAMS (or hazard logs), safety procedures, and training of new and existing operations.
- 629 • The paper has compared the operational phases in terms of a systemic indicator—the system variability—across three
630 phases of SOV operation. All three phases of SOV operation have rather comparable levels of system variability.
631 However, the interface between the SOV and turbine via the gangway system and the manoeuvring between turbines
632 seem to be more complex, exhibiting higher variability within the system. The comparison can be seen as an
633 alternative to conventional comparisons where qualitative or quantitative, typically aggregative, figures are used. As

argued in the paper, the aggregation of hazards or hazardous scenarios into system-level indices is an oversimplification.

- The study has also shown how results of a systemic hazard analysis can be linked to systemic indicators or measures of system safety, namely to the system variability.

9 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.

10 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.
- 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.
- 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.
- 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.
- 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,
- Gould, S. J., and Gold, S. J.: *The mismeasure of man*, WW Norton & company, 1996.
- 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., and Woods, D. D.: *Joint cognitive systems: Foundations of cognitive systems engineering*, CRC press, 2005.
- Hollnagel, E., and Woods, D. D.: Epilogue: Resilience engineering precepts, *Resilience engineering: Concepts and precepts*, 347-358, 2006.

- 675 Hollnagel, E., Woods, D. D., and Leveson, N.: Resilience engineering: Concepts and precepts, Ashgate Publishing, Ltd., 2007.
- 676 Hollnagel, E.: Barriers and accident prevention, Routledge, 2016.
- 677 Hollnagel, E.: The ETTO principle: efficiency-thoroughness trade-off: why things that go right sometimes go wrong, CRC
678 Press, 2017.
- 679 IMCA: Serious DP diving incident. IMCA Safety Flash 02/13, 2013.
- 680 IMCA: Guidance on the Transfer of Personnel to and from Offshore Vessels and Structures (IMCA SEL 025 Rev. 1, IMCA
681 M 202 Rev. 1), 2014.
- 682 IMCA: International Guidelines for The Safe Operation of Dynamically Positioned Offshore Supply Vessels (182 MSF Rev.
683 2). 2015.
- 684 IMO: International Safety Management Code (ISM Code) with guidelines for its implementation. IMO, London, 2018.
- 685 Leveson, N.: A new accident model for engineering safer systems, *Safety science*, 42, 237-270, 2004.
- 686 Leveson, N.: Engineering a safer world: Systems thinking applied to safety, MIT press, 2011a.
- 687 Leveson, N., and Thomas, J.: STPA Handbook, MIT, 2018.
- 688 Leveson, N. G.: Applying systems thinking to analyze and learn from events, *Safety science*, 49, 55-64, 2011b.
- 689 Meadows, D. H.: Thinking in systems: A primer, Chelsea green publishing, 2008.
- 690 Patriarca, R., and Bergström, J.: Modelling complexity in everyday operations: functional resonance in maritime mooring at
691 quay, *Cognition, Technology & Work*, 19, 711-729, 2017.
- 692 Perrow, C.: Normal accidents: Living with high risk systems. New York: Basic Books, 1984.
- 693 Praetorius, G., Hollnagel, E., and Dahlman, J.: Modelling Vessel Traffic Service to understand resilience in everyday
694 operations, *Reliability engineering & system safety*, 141, 10-21, 2015.
- 695 Presencia, C. E., and Shafiee, M.: Risk analysis of maintenance ship collisions with offshore wind turbines, *International
696 Journal of Sustainable Energy*, 37, 576-596, 2018.
- 697 Puisa, R., Bolbot, V., and Ihle, I.: Development of functional safety requirements for DP-driven servicing of wind turbines,
698 The 7th edition of the European STAMP Workshop and Conference (ESWC), Helsinki, 2019.
- 699 Qureshi, Z. H.: A review of accident modelling approaches for complex socio-technical systems, *Proceedings of the twelfth
700 Australian workshop on Safety critical systems and software and safety-related programmable systems-Volume 86*, 2007, 47-
701 59,
- 702 Rasmussen, J.: Risk management in a dynamic society: a modelling problem, *Safety science*, 27, 183-213, 1997.
- 703 Rasmussen, J., and Suedung, I.: Proactive risk management in a dynamic society, Swedish Rescue Services Agency, 2000.
- 704 Rausand, M.: Risk assessment: theory, methods, and applications, John Wiley & Sons, 2013.
- 705 Rokseth, B., Utne, I. B., and Vinnem, J. E.: A systems approach to risk analysis of maritime operations, *Proceedings of the
706 Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, 231, 53-68, 2017.
- 707 Rollenhagen, C.: MTO—an Introduction; the Relationship Between Humans, Technology and Organization, Utbildningshuset,
708 Lund, Sweden, 1997.
- 709 Salmon, P. M., Cornelissen, M., and Trotter, M. J.: Systems-based accident analysis methods: A comparison of Accimap,
710 HFACS, and STAMP, *Safety Science*, 50, 1158-1170, <https://doi.org/10.1016/j.ssci.2011.11.009>, 2012.
- 711 Sarter, N. B., Woods, D. D., and Billings, C. E.: Automation surprises, *Handbook of human factors and ergonomics*, 2, 1926-
712 1943, 1997.
- 713 SgurrEnergy: Offshore Wind and Marine Energy Health and Safety Guidelines, RenewableUK, 2014.
- 714 Sklet, S.: Safety barriers: Definition, classification, and performance, *Journal of Loss Prevention in the Process Industries*, 19,
715 494-506, <https://doi.org/10.1016/j.jlp.2005.12.004>, 2006.
- 716 Sulaman, S. M., Beer, A., Felderer, M., and Höst, M.: Comparison of the FMEA and STPA safety analysis methods—a case
717 study, *Software Quality Journal*, 27, 349-387, 2019.
- 718 Twomey, B.: Making the case for safe autonomous marine cyber physical systems, Marine Electrical and Control Systems
719 Safety Conference (MECSS), Glasgow, 23-23 November, 2017.
- 720 Woods, D. D., and Hollnagel, E.: Prologue: resilience engineering concepts, in: Resilience engineering, CRC Press, 13-18,
721 2017.

