Risk and Reliability Modelling for Multi-Vehicle Marine Domains

Catherine A. Harris and
Alexander B. Phillips
National Oceanography Centre
European Way, Southampton, SO14 3ZH
Email: {cathh, abp}@noc.ac.uk

Carolina Dopico-Gonzalez
Autonomous Surface Vehicles Ltd
Unit 12 Murrills Estate,
Southampton Road,
Portchester, PO16 9RD
Email: carolina.dg@asvglobal.com

Mario P. Brito
Southampton Business School
University of Southampton,
Southampton, SO17 1BJ
Email: m.p.brito@soton.ac.uk

***Abstract*—It is well-known that autonomous underwater vehicle (AUV) missions are a challenging, high-risk robotics application. With many parallels to Mars rovers, AUV missions involve operating a vehicle in an inherently uncertain environment of which our prior knowledge is often sparse or low-resolution. The lack of an accurate prior, coupled with poor situational awareness and potentially significant sensor noise, presents substantial engineering challenges in navigation, localisation, state estimation and control. When constructing missions and operating AUVs, it is important to consider the risks involved. Stakeholders need to be reassured that risks of vehicle loss or damage have been minimised where possible, and scientists need to be confident that the mission is likely to produce sufficient high-quality data to meet the aims of the deployment. In this paper, we consider the challenges associated with risk analysis methods and representations for multi-vehicle missions, reviewing the relevant literature and proposing a methodology.**

I. Introduction

Traditionally, autonomous underwater vehicle (AUV) missions have consisted of a simple sequence of instructions, such as travelling between multiple waypoints, pre-defined by an operator to be within safe-working constraints [1], e.g. ensuring the vehicle maintains a safe distance from the sea floor. Consequently, previous applications of risk and reliability techniques to AUV operations has primarily focussed on attempting to quantify the general reliability of the physical vehicle and its component sub-systems, e.g. the propulsion or manoeuvring systems, through the use of mean-time between failures, fault-trees [2], [3] and expert elicitation [4].

In this paper, we present a review of existing risk and reliability techniques, both within the marine autonomy literature and other related fields. The suitability of each approach is evaluated in the context of our multi-vehicle application and we discuss our proposed risk and reliability methodology.

II. Motivating problem: Multi-vehicle marine domains

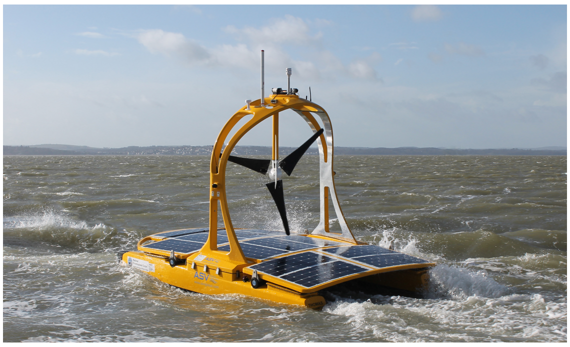

Fig. 1. C-Enduro [7] (Photo: Autonomous Surface Vehicles Ltd.)

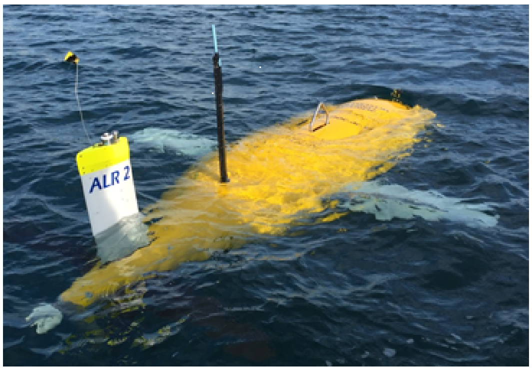

Fig. 2. Autosub Long-Range [8]

Multi-vehicle mission formats are becoming increasingly popular for a variety of applications [5], [6]. Multiple AUVs can survey larger areas, whilst autonomous surface vessels (ASVs) may act as communication hubs or provide navigational updates for AUVs. Whilst some of the traditional challenges associated with AUV operations may be reduced by the presence of a second vehicle, this multi-vehicle marine domain brings new behaviour requirements and thus risks, which need to be further analysed and mitigated where possible.

As part of an Innovate UK funded project (Autonomous Surface / Sub-surface Survey System - ASSS) [9] with industry partners[1], we are researching the use of the C-Enduro [7] ASV (see Figure 1) as a navigation aid and communication link to the long-endurance AUV Autosub Long-Range (ALR) [8] (see Figure 2). As a long-endurance platform, ALR sacrifices power available to sensors to maximise vehicle range. Consequently,

[1] Autonomous Surface Vehicles Ltd, Sonardyne International Ltd and SeeByte Ltd.

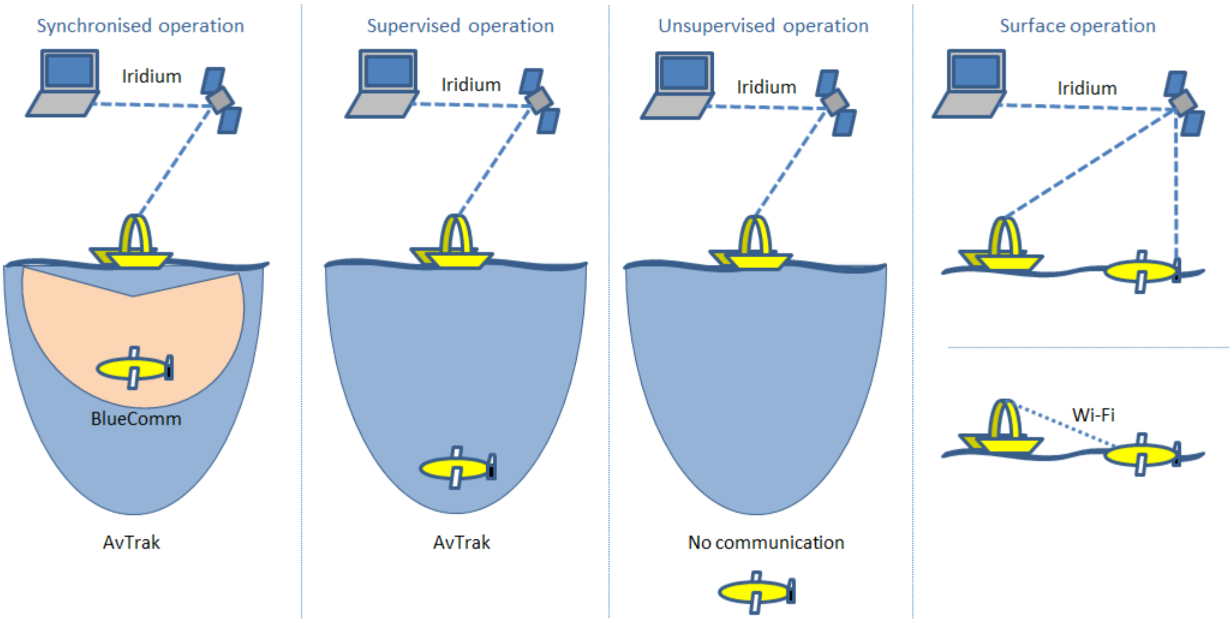

Fig. 3. Schematic showing the various operating modes considered within the ASSS Innovate UK project. *Synchronised operation* requires that the behaviour of the vehicles is closely coupled to permit communication via Sonardyne's BlueComm system; *Supervised operation* requires the vehicles to be in range of Sonardyne's USBL/AvTrak acoustic system; *Unsupervised operation* implies the vehicles are out of range of communication and are operating independently from each other; *Surface operation* allows the vehicles to communicate either directly via Wi-Fi or indirectly via Iridium.

ALR does not have an accurate inertial navigation system (INS) and experiences significant position drift, requiring the vehicle to periodically surface to obtain a GPS fix. With the aim of greatly increasing the positional accuracy of the ALR, we are developing a co-operative mission format in which the C-Enduro provides ALR with position updates during the mission using a USBL system, removing the need for the ALR to surface [10]. The ALR may also send scientific and engineering data to C-Enduro using an acoustic modem, while the C-Enduro may send the ALR new commands (either autonomously or from a remote operator) mid-mission.

Facilitating interaction between the two vehicles inevitably requires more flexible and dynamic behaviours than traditional AUV operations with a single vehicle. For example, if two vehicles are to successfully rendezvous to transmit data, temporal and spatial constraints need to be introduced to both vehicle plans, enabling data transmission whilst preventing collisions. The risks and benefits associated with multi-vehicle interaction are expected to vary throughout the deployment. While both vehicles may interact closely during some tasks, enabling regular navigation updates and data transfer, there may be times in which independent operation is necessary, for example due to weather conditions or a need to collect data in different locations. An overview of the operating modes considered within the ASSS project is given in Figure 3. During independent operation, the navigation error of the ALR will experience unbounded growth, increasing the uncertainty associated with successfully re-establishing contact with the C-Enduro. Consequently, the risk to both the vehicles and the success of the mission is increased.

III. Key Risk and Reliability Considerations

When first approaching the task of risk and reliability management for a system, a preliminary study of the system design specification is needed to highlight elements of the system that may compromise its ideal function. These elements are referred to as the critical items list. A set of safety/reliability functions will be assigned to each of these elements to ensure that the risk is at an acceptable level. For example, two critical items could be defined for C-Enduro and the ALR as follows:

CI1: C-Enduro battery pack voltage
CI2: ALR ability to surface

A description of CI1 would be that 'it is necessary to avoid a drop in the battery voltage of C-Enduro', and for CI2 would be 'to ensure that the ALR always surfaces following a dive'. The safety function for CI1 may encompass human-based monitoring of battery voltage and a set of actions triggered manually, or software-based monitoring and recording of voltage and a set of automated actions. For the CI2, the safety function may be to automatically drop the ALR's abort weight, causing the vehicle to float to the surface. Any further changes in the system will need to be checked against the critical items list before being accepted. For marine vehicles, this list increases with the level of autonomy of the vehicle, and with the number of interacting vehicles. To decide on the safety/reliability functions to implement to ensure an acceptable risk level, and to enable reliability analysis, a number of elements need to be considered. These are discussed in the remainder of this section.

A. Predictive analysis methods

When planning a mission, we need methods for performing qualitative/quantitative reliability analyses to estimate the probability of undesirable events. The most widely used methods are Fault Tree Analysis (FTA), Event Tree Analysis (ETA), Failure Modes and Effects Analysis (FMEA) [11], or a predictive survival plot that combines data with expert judgement. Failure Mode and Effect Analysis (FMEA) is a recommended approach within the marine and unmanned submersible industry [12], [13] for identifying the effect of component-level failures on the successful operation of a system. To perform FMEA, a team of engineers consider the components of the system and determine the causality between component-level faults and system-level failures. In many implementations of FMEA, a risk score is determined using a measure of the severity of a failure and the likelihood of a failure occurring. This score is typically determined informally from expert knowledge and any available fault data - e.g. mean time between failures (MTBF).

In a 2009 paper, Brito and Griffiths [4, p. 2] state that 'in the absence of objective data, a risk analysis exercise is most efficiently carried out using expert subjective judgement'. In a 2010 paper, Brito *et al.* [14] adopted this methodology to predict the survival of the Autosub3 AUV under 4 different environments (Open water, Coastal, Sea ice and Ice shelf) as a function of distance from the departure point. However, the authors highlighted the difficulties associated with using expert judgement, stating that a panel of experts provided probabilities of a fault leading to vehicle loss that spanned three orders of magnitude. To address this large variability, Brito *et al.* combined the collection of expert opinion with the identification of optimistic and pessimistic opinions, leaving the decision of whether to use the optimistic or pessimistic opinion with the human decision maker.

To overcome the lack of data and the large variability introduced by expert judgement, typical analysis methods may be combined with a simulation approach to analyse risk. Bian *et al.* [15] implemented a fault tree analysis within a Monte-Carlo simulation for the analysis of AUVs. The method was shown to be a good predictor of risk and reliability, enabling analysis into how the reliability of each subsystem impacts the reliability of the AUV system as a whole.

Current applications of predictive analysis methods within AUV science have concentrated on conventional mission formats and thus do not represent the risks associated with more dynamic behaviours, such as those required to facilitate interaction between multiple platforms. With a focus on the wider risks associated with traditional AUV deployments, for example those encountered prior or during launch, Brito and Griffiths [16] represent the probabilities of loss or successful recovery during key stages of a deployment as a Markov chain. However, as they consider conventional mission formats, the execution of the mission itself is represented using a single 'Underway' state, where the probability of loss is a function of distance travelled. When considering the dynamic format of multi-vehicle missions, this is likely to be an overly simplistic assumption and thus an extension of the approach is required.

B. Data collection procedures

Data collection may form part of a safety function to inform instant trend analysis, for example to record a number of generator cycles before applying maintenance. Data collection is also necessary for verification purposes, i.e. to verify that the safety function is working correctly, reducing the risk of faults. Additionally, as stated above, data collection is essential for quantitative analysis of mission risk, as well as for long-term ongoing reliability trend analysis to inform subsequent missions. Therefore, it is necessary to formally define a list of data collection processes, describing the required data and its purpose. This may include the need to form an expert panel to gather opinions and build a predictive survival plot of the mission.

C. Short and long-term reliability analysis tools and methods

After each mission, provided that the data collection has been performed properly, a series of analysis tools or methods should be used to monitor the overall efficiency of the vehicle. This may also be included as a predictive method for subsequent missions. The most typical analyses are: root cause of fault plots, which represent the frequency of fault causes; sensitivity analyses, which represent the influence of specific factors on the outcome; and survival plots, which represent the probability of survival vs abort or loss as a function of distance or time.

Survival analysis methods are classified into parametric and non-parametric methods. Among the latter, the most popular is the Kaplan-Meier estimator, also known as product-limit estimator. Brito *et al.* [14] utilised it to estimate the probability of survival of the Autosub3 AUV, as discussed above. This survival plot could also be obtained as a function of time or time/distance ratio, which would likely be the most suitable approach in the present multi-vehicle scenario. Other non-parametric methods that have been used in other fields for survival plots are the Actuarial-Simple and Actuarial-Standard methods for multiple censored data that are arranged in intervals, or the use of Confidence-Bounds [17], [18]. Typical parametric methods used in statistics use a continuous function as the survival plot of a series of data. Brito *et al.* [14] also used a Weibull distribution to calculate the effect of mitigation, which consisted of monitoring the AUV for a distance away from the departure point, which happened to be when most of the losses took place. It was seen that it improved the AUV survival significantly. Other parametric statistical models widely used in statistics for survival analysis are the lognormal, loglogistic and exponential [19], [20].

In their 2004 paper, Podder *et al.* [21] describe their reliability growth analysis in relation to MBARI's Dorado AUV. The authors performed trend analysis to determine whether the failure rate increases or decreases over time, representing failures occurring during AUV operations as stochastic point processes. The trend analysis showed a statistically significant positive reliability growth trend. However, they report a large variation between the lower and upper bounds of MTBF for different types of failure. The largest variation in MTBF, calculated for the extremely critical class of failures, varied from 52.4 hours to 997.9 hours. To increase the consistency in MTBF and reliability estimates, they state that more data needs to be collected.

Unlike traditional expert judgement, where the experts assess the risks individually, Brito *et al's* [22] behavioural probabilistic risk assessment approach requires the experts to discuss and agree the a priori distribution of risks to the vehicle during an upcoming deployment as a group. Following the completion of the deployment, the experts meet for a second time and review the mission performance, updating their prior estimate using Bayes' rule to produce an estimate of the a posteriori probability of risk.

D. Verification methods

For each of the safety/reliability functions implemented for the critical items, a verification method should be placed to verify its correct function. They can range from manually checking some parameters such as temperature or voltage, to automatic data analysis. The verification methods should be part of the safety function's validation test. For example, Tadjine *et al.* [23] verified the pedestrian collision avoidance of cars by scene simulations. Nemet and Bartha [24] used model checking techniques to formally verify the block diagram leakage safety function in a nuclear plant.

E. Rules and protocols to adhere to from an organisational and human factors perspective

Together with the expanded use of AUVs, as technology becomes increasingly costly, it is necessary to enforce risk targets through the implementation of organisational management procedures. Ideally, these procedures should adhere to reliability industry standards. Thieme *et al.* [25] proposed a risk management framework focusing on human and organisational factors (HOFs), including elements of the ISO 31000. A general document is followed as guidance for all phases. It shows an application using Fault Tree Analysis and Event Tree Analysis. This is a very simplified case compared to our combined multi-vehicle mission, but the framework can be used as a good protocol example.

F. Agreed risk level

From a company perspective, the target risk level for each vehicle/mission needs to be agreed so that safety functions can be implemented to meet the target and their effectiveness verified against it.

IV. Risk and reliability representations

In this paper, we focus on the specific problem of selecting suitable models and quantitative analysis methods for our multi-vehicle marine domain. To determine a suitable representation to model our multi-vehicle scenario, we first need to identify the key aspects of the domain that influence mission and vehicle reliability.

A. Definition of mission success criteria

The majority of AUVs are typically deployed with the primary purpose of collecting high-quality data. In the previous section, we identified that current applications of risk and reliability techniques to AUV science have mostly focussed on the risk or loss of damage to the vehicle itself, rather than the risk to the vehicle's data collection capability or the on-board data itself. Whilst the safe return of the vehicle is paramount, it is far from the only factor in quantifying the success of the mission. To evaluate the effect of the mission plan on the probability of successfully meeting the data collection objectives, we need a way to represent data quality.

B. Temporal and spatial representation

A temporal representation is especially important when considering multi-vehicle robotics domains as the interaction (or lack-of) between two vehicles has a significant impact on the likelihood of a failure. For instance, while a component failure in the navigation system of one vehicle may increase the probability of a collision with a second vehicle, a collision is only likely if the two vehicles are in a similar location at the same time. Conversely, in order to successfully complete a mission in which multiple vehicles must interact, representing the spatial and temporal separation of the vehicles is crucial to establishing the probability of successfully completing the mission.

C. Representation of operating environment

Marine autonomous vehicles operate in extreme environments, where the conditions are often harsh and unpredictable. The majority of existing risk and reliability work for AUV missions do not explicitly represent the impact of the environmental conditions, instead focussing on the specific mission or the general reliability case, represented using techniques such as fault trees. In work by Brito *et al.* [22] the panel of experts was asked about a specific mission, implicitly factoring the environment into the analysis process.

D. Heterogeneous vehicles

Our multi-vehicle marine domain involves multiple vehicles of different types (AUV and ASV) with different risks and probabilities of failures. To model multi-vehicle missions, we need to reconcile and combine different vehicle models in a meaningful way.

V. Review of representations and quantitative analysis methods from related fields

In a 2007 paper, Grunske *et al.* [26] state that traditional applications of FMEA are labour-intensive and the calculation of the likelihood of system failures occurring is prone to errors. To this end, they extend FMEA with probabilistic model checking techniques, presenting an approach they call probabilistic FMEA (pFMEA). By including component-level failure rates and probabilistic analysis, pFMEA calculates the probability of system level failures, allowing engineers to formally identify and evaluate whether a failure mode occurs more frequently than is deemed acceptable in the system specification. Model checking tools may then be used to validate the system against the safety specification as well as to experiment with adjusting the component-level probabilities. For example, evaluating how the reliability of the system changes if the failure rate of a given component is reduced.

To use pFMEA, the system must be modelled probabilistically, e.g. using a continuous time Markov chain (CTMC) or Markov decision process (MDP) [27]. Grunske *et al.* represent their metal press system as a CTMC, which allows them to specify the mean time to transition between certain states, incorporating temporal information into the model, e.g. it takes the plunger six seconds to fall from the top to the bottom of the press. Grunske *et al.* state there is a current trend towards state-based models such as Markov models and Stochastic Petri-nets, as these provide a better representation of temporal properties of the system model, such as the order in which a series of component failures will lead to a system-level failure/hazard, than traditional fault-trees.

Norman and Parker [28] present an overview of the field of model checking and quantitative verification. In model checking, the correct behaviour of a system is formally specified (typically using temporal logic). A mathematical model is then constructed that captures all possible executions of the system. This is then analysed to verify correctness properties are satisfied. Norman and Parker state that with the rise of a need for reliable systems operating in unpredictable and unreliable environments, non-functional or quantitative aspects of correctness have become increasingly important. By also modelling the probability and timings of events occurring, model checking may be extended into quantitative verification. This allows questions such as 'is the probability of the robot finishing task a without depleting its battery greater than 0.95?' to be evaluated.

Whilst focussing on plan generation, Feng *et al.* [29] represent their multi-agent surveillance domain as both an MDP and a two-player stochastic game. The domain requires interaction between the two agents — a UAV flies between waypoints autonomously, while a human operator controls the capture of images at waypoints. The UAV may only continue to the next waypoint once the human operator is satisfied with the quality of the images. When modelling the domain as an MDP, Feng *et al.* model the operator and the UAV separately. However, some actions are common to both models which allows the computation of the product of the two MDPs, representing the interaction between the two agents. Feng *et al.* pay particular attention to the modelling of human factors in the operator model, namely operator workload and fatigue, and the effect these have on expected mission completion time and the expected number of visits to high-risk areas. By instead modelling the problem as a stochastic game, the choices made by the operator are much less constrained and do not require the probability distribution of the operators choices to be fully defined, as in the MDP model. The game model represents the chance that a human operator would make fully adversarial choices (e.g. sending the UAV around an infinite loop of waypoints), despite this being highly unlikely in reality. To address this, Feng *et al.* introduce a probability that the human operator instead allows the UAV to make the choice. This delegation probability is easier to define as it is not mission specific and can be calculated from past mission logs.

VI. Proposed representations and quantitative risk analysis methods for the multi-vehicle domain

In Section II we presented our motivating problem, that of an ASV co-operating with an AUV, providing communication and navigational updates to the AUV when necessary. Following our review of the relevant literature and our identification of the key considerations, we now select a combination of techniques to form our proposed risk and reliability solution for our multi-vehicle domain. A multi-vehicle domain in which two complicated platforms, each comprised of many subsystems, interact within the unpredictable and unforgiving environment of the ocean is very difficult to accurately model in a single representation. Instead, we consider the representation and analysis of the risks within the system at varying levels of abstraction.

A. Sub-system-level representation

We propose that many vehicle sub-systems, such as the propulsion system, where the possible failure modes are relatively constrained and the specification formalised and quantified, may be modelled and evaluated using conventional and widely-used techniques such as FMEA or fault-tree analysis. As these systems are typically constructed from off-the-shelf components, data such as mean time between failures may be used to inform component-level failure rates. When combined with model-checking techniques, such as in Grunske *et al's* pFMEA approach [26], the sub-system may also be validated against the specification. pFMEA requires the system to be modelled using a probabilistic representation, such as a CTMC. By utilising a probabilistic representation, the model may be used to investigate the impact of a particular component, e.g. a bearing, on the reliability of the whole sub-system, e.g. the propulsion system. The identification of critical components can then be used to inform further development, maintenance scheduling and the implementation of suitable safety functions.

B. Vehicle-level representation

In order to understand the possible cause of faults and failures, it will be necessary to perform vehicle specific analysis to represent the causality and determine the path of subsystems that may have been involved. A widely-used method is Fault Tree Analysis (FTA) or Event Tree Analysis (ETA), as mentioned earlier. However, it is necessary to have appropriate documentation to understand how the vehicle's subsystems interact to perform each of the vehicle's functions. Therefore, systems block diagrams should be provided as a support documentation to inform FTA or ETA, describing the subsystems that are in series or parallel. Performing FTA for all vehicles to infer causality and estimate probabilities for each potential failure scenario is highly time consuming. A random sampling simulation approach such as Monte Carlo simulation could also be used to estimate the probability density functions of failure within less critical sub-systems. In fact, this could be performed as a preliminary analysis to understand the sub-systems that have the most significant influence on the mission outcome. The balance between accuracy, variability and computational time will drive the ratio of FTAs to simulations performed. The probability density functions could also be approximated more accurately by the combined use of data and expert judgement.

C. Multi-vehicle, mission-level representation

In Section IV, we identified the need for representing probabilities as well as temporal and spatial properties within the mission-level model. From our literature review, Markov chains and MDPs are popular representations for analysing probabilities. As in the work by Brito and Griffiths [16], Markov chains have been used as effective representation for simple AUV deployments, as well as more widely as representations for risk analysis [30]–[32]. However, as mission formats become more dynamic, with vehicle behaviour dependent on interaction between multiple platforms, the problem may be better represented as an MDP, as used by Feng *et al.* [29]. An MDP would allow the choice of action to take at a given state to be modelled, e.g. representing that C-Enduro may send the ALR new commands mid-mission, or that C-Enduro may need to enter a search-behaviour if initial attempts at establishing communication with ALR fail. Feng *et al* model the two agents in their problem as separate MDPs, computing the product MDP for the combined system using actions common to both agents. Such a representation would allow us to consider heterogeneous fleets, where different vehicle types may perform different actions, provided multi-vehicle interactions are defined using common actions. The same MDP representation may be used to model single-vehicle deployments or combined to form product MDPs for multi-vehicle missions. The impact of states and actions on data quality may also be represented using probability distributions. The transition probabilities within the MDP may be defined using techniques such as expert judgement or as a function of the results of sub-system and vehicle-level analysis. In an MDP, the transition function, which describes the probability of transitioning to a state q having performed action a_1 in state p, must be defined for all combinations of states and actions [27]. Given the complexity of our multi-vehicle domain and the infeasible number of possible vehicle and environmental states, it is important to constrain an MDP representation to the most critical factors influencing mission success. By only representing a sub-set of the multi-vehicle system within our model, we are unlikely to be able to calculate accurate estimates of the true probability of mission success. However, we would be able to compare the risk vs reward of one mission plan or strategy against another. For example, in one strategy our ASV and AUV might interact throughout the mission, constraining the magnitude of ALR's position error and improving the quality of the data. However, this may also increase the risk of collisions. Conversely, a second strategy might schedule regular rendezvous points. The ALR's position error will grow whilst not receiving navigational updates from C-Enduro, but the probability of collision is reduced. Such a model would allow us to compare these strategies, evaluating the risk-reward tradeoff. Whilst only modelling a subset of the full multi-vehicle system will reduce the accuracy of the estimates of the true probability of mission success, it is worth noting that expert judgement is still prone to large variation. Combining an MDP model of the key factors influencing mission success with expert judgement where data is sparse may be an effective solution.

A common safety function for AUVs are mission-stage timeouts, e.g. if the vehicle does not reach the target waypoint within a given time, a contingency behaviour (such as surfacing) will be triggered. Equally, if the vehicle does not complete the mission and surface within an expected time, a drop weight may be released to cause the vehicle to float to the surface. These timeouts define definite points in the mission where the behaviour of the vehicle will change. As the behaviour changes, so to will the distribution of risks, e.g. on dropping an abort weight, the vehicle has a reduced chance of failing to surface; however, upon floating to the surface the vehicle is unable to fully manoeuvre and thus cannot continue with the mission. As these timeouts occur at defined points in the mission, it may be sufficient to discretise the representation of time within the model. However, if we also wished to represent the probability of an abort condition being triggered at any point in the plan as a result of a vehicle fault, we may need to consider using a continuous-time Markov chain.

D. Wider considerations

Whilst we have focussed on methods and representations for performing quantitative and qualitative analysis for risk estimation within our specific multi-vehicle scenario, in order for this work to be effective on an industrial scale we will also need to address the wider aspects of the problem as defined in Section III. The most fundamental requirement is to invest in suitable procedures and safety functions to facilitate the collection of risk and reliability data. We have presented many methods for quantifying risk that rely on combining the probabilities of individual faults to calculate the resulting probability of mission success, vehicle loss etc. However, these resultant probabilities are only as good as the model and the individual probabilities which form the input of the risk calculation. As we currently do not have sufficient data to calculate accurate probabilities, expert judgement is necessary. In order to improve our probability estimates, we must seek to facilitate the collection of the required risk and reliability data. Whilst all vehicle data is logged, the poor situational awareness, typical of most marine autonomous vehicles, means that the wider context of the mission is often under-recorded. For example, during a mission, a surface vehicle may record poor energy gains from its solar panels — this could be a result of a fault within the solar panels, or it could be that the weather was cloudy and thus not conducive to effective charging. It is therefore essential that procedures are in place to ensure the mission meta-data, e.g. environmental/weather conditions, what happened to the vehicle prior to and during launch, as well as human factors such as who was involved, what were the shift patterns, are adequately recorded. It is equally important that safety functions are implemented to ensure critical engineering data is collected - e.g. if battery temperature is identified on the critical list, it is essential that the vehicle logs this data with sufficient frequency.

VII. Conclusions

In this paper we have presented a review of existing risk and reliability techniques, both applied to the field of marine autonomy and from other related disciplines. We have highlighted the key risk and reliability considerations when designing a methodology for our multi-vehicle marine domain, focussing on the task of selecting appropriate representations and quantitative analysis methods in this paper. As it is very difficult to accurately represent all aspects of a complicated multi-vehicle system operating in an unpredictable environment in a single model, we instead proposed representing and analysing the risks to different components of the multi-vehicle system at varying levels of abstraction. As conventional techniques such as FMEA have been widely applied to systems where the failure modes are relatively constrained, we propose the use of an FMEA-based approach, such as Grunske *et al's* [26] pFMEA, for vehicle sub-system level risk and analysis. The probabilities of sub-system failure modes may then be combined with knowledge of the system design (e.g. a system block diagram) to determine the effect of individual failures on the likelihood of vehicle-level failure modes by using a method such as Fault Tree Analysis. At the multi-vehicle mission level, we propose modelling each vehicle as an MDP, representing the interaction between the vehicles by computing the product MDP in the manner of Feng *et al.* [29]. The transition probabilities within the MDP may then be defined using the results of the sub-system and vehicle-level analysis combined with expert judgement where there is insufficient data.

We have also highlighted the need to consider the wider aspects of the risk and reliability problem, including the need for safety functions and verification methods, as well as adequate rules and protocols. Protocols relating to the collection of risk and reliability data are especially crucial. Without sufficient data, we have to rely on expert judgement which is labour intensive and prone to large variability. While expert judgement should be used in the absence of data, to improve the accuracy of predictive analysis methods and verify the efficacy of safety functions, it is essential that protocols are implemented to ensure the collection of vehicle risk and reliability data in the future.

Acknowledgements

This work was funded by the Innovate UK project 'Autonomous Surface / Sub-surface Survey System', project number 102304. The authors would like to thank Innovate UK and the project partners: Autonomous Surface Vehicles Ltd, Sonardyne International Ltd and SeeByte Ltd.

References

[1] M. Pebody, "The Contribution of Scripted Command Sequences and Low Level Control Behaviours to Autonomous Underwater Vehicle Control Systems and Their Impact on Reliability and Mission Success," in *Proceedings of OCEANS – Europe*. Aberdeen, UK: Institute of Electrical and Electronic Engineers, June 2007, pp. 1–5.

[2] H. Xu, G. Li, and J. Liu, "Reliability analysis of an Autonomous Underwater Vehicle using Fault Tree," in *Proceedings of the IEEE International Conference on Information and Automation*. Yinchuan, China: Institute of Electrical and Electronic Engineers, August 2007, pp. 1165–1170.

[3] K. Aslansefat, G. Latif-Shabgahi, and M. Kamarlouei, "A strategy for reliability evaluation and fault diagnosis of Autonomous Underwater Gliding Robot based on its Fault Tree," *International Journal of Advances in Science Engineering and Technology*, vol. 2, no. 4, pp. 83–89, Oct. 2014.

[4] M. Brito and G. Griffiths, "On the use of expert judgment elicitation for autonomous underwater vehicle risk prediction and management," in *Proceedings of the European Safety and Reliability Conference*, ser. ESREL'09. Prague, Czech Republic: Taylor and Francis, September 2009, pp. 1221–1227.

[5] T. B. Curtin, J. G. Bellingham, J. Catipovic, and D. Webb, "Autonomous Oceanographic Sampling Networks," *Oceanography*, vol. 6, no. 3, pp. 86–94, 1993.

[6] E. Fiorelli, N. E. Leonard, P. Bhatta, D. A. Paley, R. Bachmayer, and D. M. Fratantoni, "Multi-AUV control and adaptive sampling in Monterey Bay," *IEEE Journal of Oceanic Engineering*, vol. 31, no. 4, pp. 935–948, 2006.

[7] ASV Ltd, "C-Enduro - Autonomous Surface Vehicles (ASV) Ltd - Unmanned Surface Vehicles," Online, available at: http://asvglobal.com/product/c-enduro/, 2016, accessed: 2016-06-16.

[8] M. E. Furlong, D. Paxton, P. Stevenson, M. Pebody, S. D. McPhail, and J. Perrett, "Autosub Long Range: A Long Range Deep Diving AUV for Ocean Monitoring," in *Proceedings of IEEE/OES Autonomous Underwater Vehicles*, ser. AUV'12. Southampton, UK: Institute of Electrical and Electronic Engineers, September 2012.

[9] Gateway to Research, "Autonomous Surface / Sub-surface Survey System," Online, available at: http://gtr.rcuk.ac.uk/projects?ref=102304, 2015, accessed: 2016-06-09.

[10] G. Salavasidis, C. Harris, E. Rogers, and A. B. Phillips, "Co-operative use of Marine Autonomous Systems to enhance navigational accuracy of Autonomous Underwater Vehicles," in *Proceedings of the 17th Towards Autonomous Robotic Systems*, ser. TAROS'16. Sheffield, UK: Springer, June 2016.

[11] P. L. Clemens and R. J. Simmons, *System Safety and Risk Management: NIOSH Instructional Module*, US Department of Health and Human Services, 1998.

[12] Germanischer Lloyd Aktiengesellschaft, "(I-5-3) Unmanned Submersibles (ROV,AUV) and Underwater Working Machines," Online, available at: http://www.gl-group.com/infoServices/rules/pdfs/gl_i-5-3_e.pdf, 2009, accessed: 2016-09-01.

[13] Det Norske Veritas, "Risk management in marine - and subsea operations," Tech. Rep. DNV-RP-H101.

[14] M. Brito, G. Griffiths, and P. Challenor, "Risk Analysis for Autonomous Underwater Vehicle Operations in Extreme Environments," *Risk Analysis*, vol. 30, no. 12, 2010.

[15] X. Bian, C. Mou, Z. Yan, and J. Xu, "Simulation Model and Fault Tree Analysis for AUV," in *Proceedings of the 2009 IEEE International Conference on Mechatronics and Automation*. Changchun, China: Institute of Electrical and Electronic Engineers, August 2009.

[16] M. Brito and G. Griffiths, "A Markov Chain state transition approach to establishing critical phases for AUV reliability," *IEEE Journal of Oceanic Engineering*, vol. 36, no. 1, pp. 139–149, 2009.

[17] K. Angelo, A. Dalhaug, A. Pawinski, E. Haukland, and C. Nieder, "Survival prediction score: A simple but age-dependent method predicting prognosis in patients undergoing palliative radiotherapy," *ISRN Oncology*, vol. 2014, no. Article ID 912865, 2014.

[18] G. P. Freitas, R. Hirata, E. A. Bonfante, N. Tovar, and P. G. Cohelo, "Survival probability of narrow and standard-diamter implants with different implant-abutment connection designs," *International Journal of Prosthodontics*, vol. 29, no. 2, pp. 179–185, 2016.

[19] D. Shah, V. Paly, A. Briggs, M. Sidhu, E. Ma, and V. Bonthapally, "Assessing the impact of restricted follow-up and small sample sizes on survival estimations in prostate cancer using registry data," *Journal of Clinical Oncology*, vol. 34, no. 7, 2016.

[20] E. Soini, M. Holmberg, C. Asseburg, and M.-L. Sumelahti, "Modelling the persistence of disease-modifying drug treatment (dmt) and its independent drivers in finnish multiple sclerosis (ms) patients: Parametric survival modelling." in *International Society of Pharmacoeconomics and Outcomes Research 17th Annual European Congress*, ser. ISPOR'14. Amsterdam, The Netherlands: ESIOR, November 2014.

[21] T. K. Podder, M. Sibenac, H. Thomas, W. J. Kirkwood, and J. G. Bellingham, "Reliability growth of autonomous underwater vehicle - Dorado," in *Proceedings of IEEE OCEANS'04*. Institute of Electrical and Electronic Engineers, November 2004, pp. 856–862.

[22] M. Brito, G. Griffiths, J. Ferguson, D. Hopkin, R. Mills, R. Pederson, and E. MacNeil, "A behavioral probabilistic risk assessment framework for managing autonomous underwater vehicle deployments," *Journal of Atmospheric and Oceanic Technology*, vol. 29, no. 11, pp. 1689–1703, 2012.

[23] H. H. Tadjine, R. Roellig, K. Schulze, and H. Daniel, "New methods and tools for the development and verification of safety functions during development of pedestrian detection systems," in *Computing Technology and Information Management (ICCM), 2012 8th International Conference on*, vol. 1, April 2012, pp. 434–438.

[24] E. Németh and T. Bartha, "Formal verification of safety functions by reinterpretation of functional block based specifications," in *Formal Methods for Industrial Critical Systems: 13th International Workshop*, D. Cofer and A. Fantechi, Eds. L'Aquila, Italy: Springer, September 2008, pp. 199–214.

[25] C. A. Thieme, I. B. Utne, and I. Schjølberg, "A risk management framework for unmanned underwater vehicles focusing on human and organizational factors," in *ASME 2015 34th International Conference on Ocean, Offshore and Arctic Engineering*, vol. 3: Structures, Safety and Reliability. St John's, Canada: American Society of Mechanical Engineers, June 2015.

[26] L. Grunske, R. Colvin, and K. Winter, "Probabilistic model-checking support for fmea," in *Fourth International Conference on the Quantitative Evaluation of Systems*. Edinburgh, UK: Institute of Electrical and Electronic Engineers, September 2007.

[27] R. Howard, *Dynamic Programming and Markov Processes*. Cambridge, MA: Massachusetts Institute of Technology Press, 1960.

[28] G. Norman and D. Parker, "Quantitative verification: Formal guarantees for timeliness, reliability and performance," London Mathematical Society and the Smith Institute, Tech. Rep., 2003.

[29] L. Feng, C. Wiltsche, L. Humphrey, and U. Topcu, "Controller synthesis for autonomous systems interacting with human operators," in *Proceedings of the International Conference on Cyber-Physical Systems*. Seattle, USA: ACM, April 2015.

[30] J. D. Grimes, "On determining the reliability of protective relay systems," Ph.D. dissertation, 1970.

[31] M. Alam and U. M. Al-Saggaf, "Quantitative reliability evaluation of repairable phased-mission systems using markov approach," *IEEE Transactions on Reliability*, vol. 5, no. 35, pp. 498–503, 1986.

[32] K. Furukawa, J. B. Cologne, Y. Shimizu, and N. P. Ross, "Predicting future excess events in risk assessment," *Risk analysis*, vol. 29, no. 6, pp. 885–899, 2009.