

Drone Safety and Reliability Survey and Emerging Technologies Towards the Certification of Autonomous UAVs

Matthew Osborne, Jennifer Lantair, Zain Shafiq,
Xingyu Zhao, Valentin Robu, David Flynn
Smart Systems Group, School of Engineering and Physical Sciences
Heriot-Watt University
Edinburgh, UK
{mho1,jl153,zs2,xingyu.zhao,v.robust,d.flynn}@hw.ac.uk

John Perry
Texo iHub
Texo Group
Aberdeen, UK
john.perry@texo.co.uk

Abstract—The following paper details the results of a survey on safety and reliability of commercial drones, issued to 1500 companies in the UK with a 10% response rate. We verify with previous studies a commercial drone reliability of about $1/10^3$ flight hours. Furthermore we find a reported 49% of companies experience a critical failure within 500 flight hours. The paper details the highest ranked on-board intelligent systems recommended by commercial operators. Subsystems are identified in order of the highest likelihood of failure and the frequency of maintenance and servicing in current practice is reported. Informed by the results of this study and a state of the art literature review, we review emerging technologies and methods, such as, Integrated Vehicle Health Management (IVHM), Prognostics and Health Management (PHM), Formal Methods, Simulations, Assurance Cases, Fault Tolerant Control (FTC) and Air Traffic Control (ATC) technology, as candidate solutions to the reported challenges. The integration of these techniques in a systematic framework with a supporting automatic tool-chain is detailed as a candidate solution and future work of the research program.

Index Terms—autonomous systems, drones, safety and reliability, certification, prognostics and health management, probabilistic model checking, assurance cases, air traffic control, safety-critical systems, reliability.

I. INTRODUCTION

The following paper details the results of a survey issued to commercial drone operators in the UK on the safety and reliability of commercial drones. The use of on-board intelligence to mitigate the on-set of failure modes is of particular interest to permit the safe operation of robots and autonomous systems. Artificial Intelligence (AI) has seen much press attention recently due to the improved performance of Neural Networks for data classification tasks. This is primarily due to the availability of large data sets and advancements in computing power. However for Unmanned Aerial Vehicles (UAVs), Neural Networks offer limited use currently for safety critical systems due to their inherent non-deterministic properties and increased hardware and processing requirements. The current requirement for any on-board UAV system is that it must perform deterministically according to the Certification Specifications detailed by the

Civil Aviation Authority (CAA) CAP 722, [1]. A brief overview of emerging technologies is including at the end of this paper, highlighting techniques to improve safety and reliability, working towards fulfilling certification requirements for autonomous systems via on-board intelligence.

The aim of the survey was to engage with experts in the commercial UAV sector to elicit first hand experience of UAV reliability. Commercial UAVs have developed rapidly from consumer toys to industrial platforms with varying levels of complexity and cost. We are interested in common failure modes currently observed by commercial operators so that research and development of intelligent systems can help to mitigate failures, improve safety and better inform maintenance scheduling in a cost effective way.

A list of UK CAA approved commercial operators was used to contact 1500 companies and issue an electronic survey via a hosting company, SurveyMonkey. The survey was kept to 5 minutes in length and the questions simplified in order to maximise participation. The survey concluded with a 10% response rate. Data from all sectors, operating commercially inclusive of all drone platforms and budgets available for operations was included for the study. The intent of the survey was to identify common failures and the perception within the industry of on-board intelligent systems. The data collected would be used together with evidence from within literature to identify the most common subsystem failures or types of failures observed so that fully autonomous systems could be better designed in the future.

The paper is structured into the following sections, Section II details the questions and responses to the survey and discusses findings, Section III compares related work in UAV reliability to the results found in our survey, Section IV discusses emerging technologies in UAV safety and automation, Section V makes recommendations for future work in safety and reliability for robotic systems and Section VI concludes the findings within the paper.

II. SURVEY RESULTS IN SAFETY AND RELIABILITY

A. Question 1: Are you an approved CAA operator?

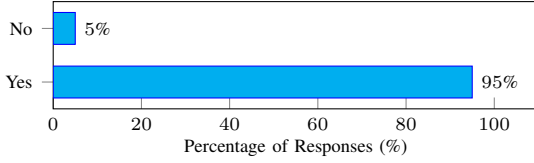


Fig. 1. Question 1 responses, percentage of CAA approved respondents

This question ensured commercial operators were targeted with investment and experience in drone operations. Over 95% of respondents confirmed that they had CAA approved pilot certification.

B. Question 2: Which sector(s) does your company best fit into?

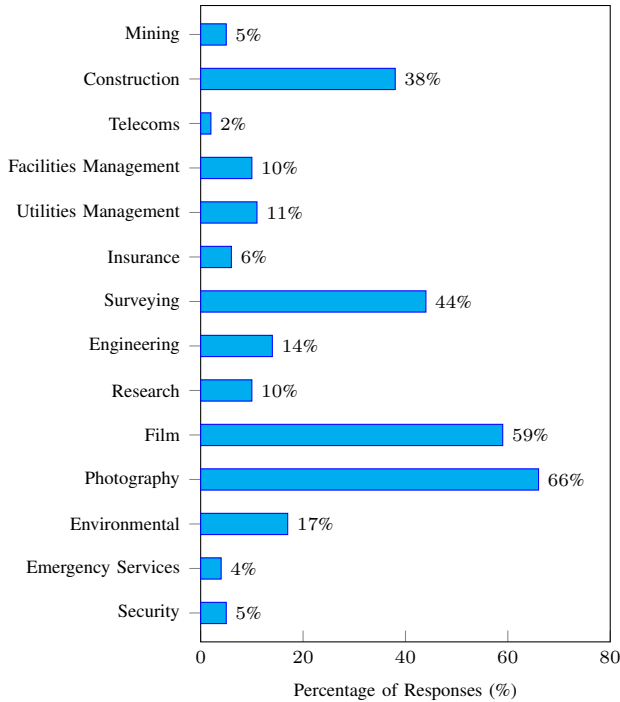


Fig. 2. Question 2 responses, percentage of respondents in each commercial sector.

The majority of respondents reported to operate in the Photography and Film sector, closely followed by the Surveying and Construction sectors. It's important to note that the majority of companies operate in multiple sectors and so identifying any trends per sector has not been included in the study. The type of drone platforms typically used within each sector as well as the performance demands of operations will play a part in the reliability. The safety requirements also play a part in the acceptable level of performance depending upon each use case. Larger companies typically operate with a significant increase in hardware and software sophistication as

well as training and maintenance routines. The intention was to find the common failure modes independent of operating costs or platform complexity and performance levels.

C. Question 3: For routine flight operations, please estimate a mean time before a non-critical failure typically occurs?

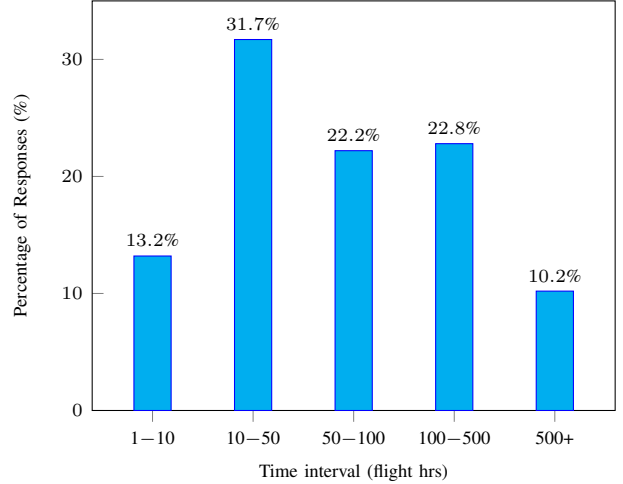


Fig. 3. Question 3 responses, please estimate a mean time before a non-critical failure typically occurs?

The respondents indicated that the most likely time for a non-critical¹ failure was between 10 to 50 hours of operation, although 13% reported non-critical failures occurring within 1 to 10 hrs. This highlights the relative complexity and platform dependence on regular health checks to maintain flight readiness.

The responses depend to some extent on a company's maintenance procedures and the build quality of each drone.

D. Question 4: For routine flight operations, please estimate a mean time before a critical failure typically occurs?

Over 50% of respondents reported that a critical failure would not occur until after 500 flight hours. It should be pointed out that options for 1000 hours or above were not provided, which may have unfairly biased the results. The commercial aviation failure rate is about 1 in 100,000 flight hours whereas for drones, it has been found to be 1 in 1000 flight hours [1]. It could be argued that this falls in line with the survey data if the 50% of respondents reporting greater than 500 flight hours falls into a normal distribution with a mean of 1000. Despite this around 4% of operators reported critical² failures occurring within 50 hours and a further 17% within 100 hours. These types of failures are of particular interest for robust fail-safe systems.

¹Non-critical failures are defined as those that do not compromise mission objectives or safety. This was not explicitly defined in the survey.

²Critical failures are defined as those that compromise mission objectives or safety. This was not explicitly defined in the survey.

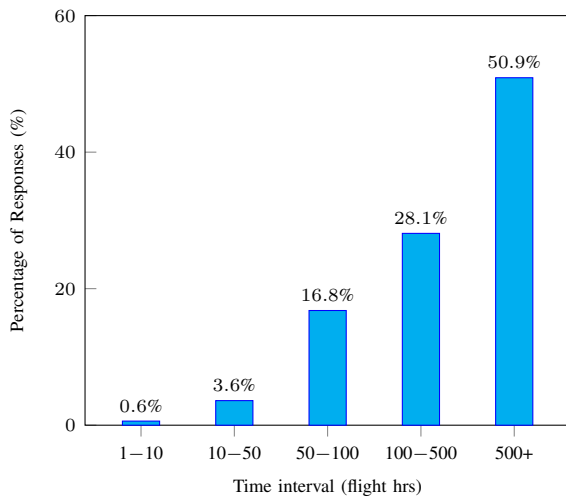


Fig. 4. Question 4 responses, for routine flight operations, please estimate a mean time before a critical failure typically occurs?

E. Question 5: Please estimate how many mishaps might be avoided with increased on-board intelligence to aid the pilot per 100 flight hours. (“On-Board intelligence” might include algorithms that can detect hazards from camera images, fault tolerant stability and control, increased situational awareness or increased reasoning, planning and reporting from flight data.)

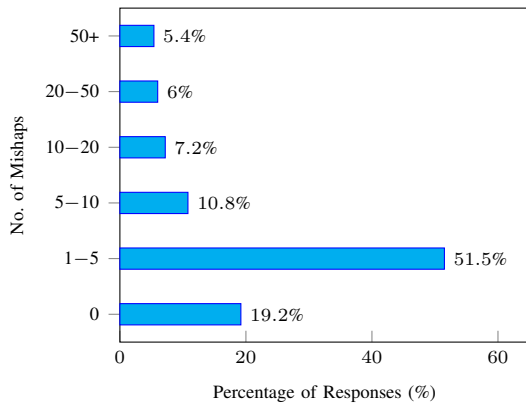


Fig. 5. Question 5 responses, please estimate how many mishaps might be avoided with increased on-board intelligence per 100 flight hours.

51% of respondents estimated that between 1 to 5 mishaps per 100 hours of operation could be avoided with on-board intelligent systems. 20% of participants also said that there was no need for further on-board intelligent systems to avoid mishaps. The responses show that there is, at least from 80% of users, a demand for the development or the supply of intelligent systems to aid the safe operation of drones. 10% of operators suggested that the demand for greater intelligence may mitigate greater than 20 mishaps per 100 flight hours.

F. Question 6: Please rank the following subsystems into the order of those you think most likely to fail. Those most likely at the top.

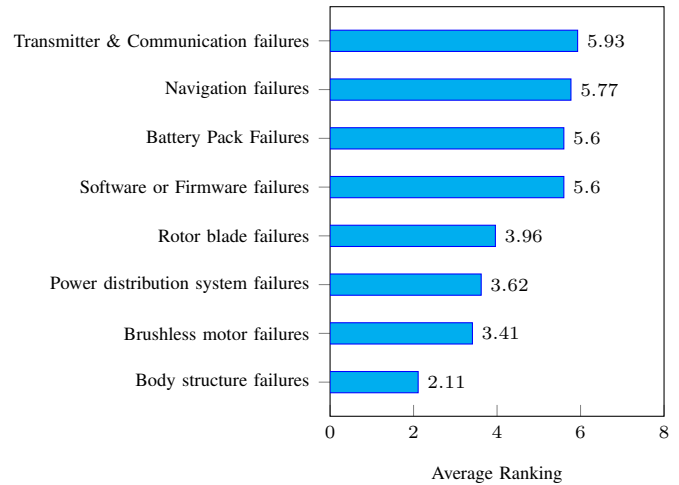


Fig. 6. Question 6 responses, please rank the following subsystems into the order of those you think most likely to fail. Those most likely at the top.

The highest ranked subsystems to protect from failure were transmitter and communication systems. These were closely followed by navigation systems and battery pack failures. Mechanical failures are a lower priority, such as rotor blade damage, brushless motor failures or body structure failures. In terms of the frequency of failure, these components are already robustly engineered for higher reliability on current commercial platforms.

G. Question 7: Please place in order of importance, technologies that you think would be most beneficial for commercial drone operations, the most important at the top.

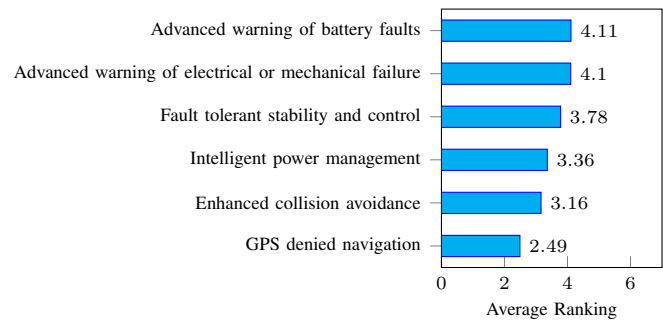


Fig. 7. Question 7 responses, ranking of technologies thought to be most beneficial for commercial drone operations.

The highest ranked intelligent technologies were reported as being, advanced warning systems for battery failures, closely followed by advanced warning of electrical or mechanical failures. Also high on the list are fault tolerant stability and control and intelligent power management. Collision avoidance and GPS denied navigation was reported as lower down on the list

of priorities. This is partly due to technology already being available in this area.

H. Question 8: Please indicate the type of health checks that you carry out during a drone's lifetime.

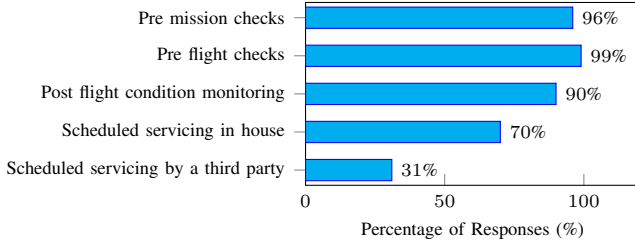


Fig. 8. Question 8 responses, please indicate the type of health checks that you carry out during a drone's lifetime.

Nearly all operators carry out regular checks in the workshop before operations, immediately before take-off (on-site) and carry out post flight checks. Only around 70% of operators carry out scheduled maintenance and of these 31% use a specialist third party service provider. The high importance of regular maintenance checks may promote the use of on-board diagnostic and prognostic technology to better provide condition based maintenance.

I. Question 9: Please indicate approximately the number of hours flown between any scheduled maintenance.

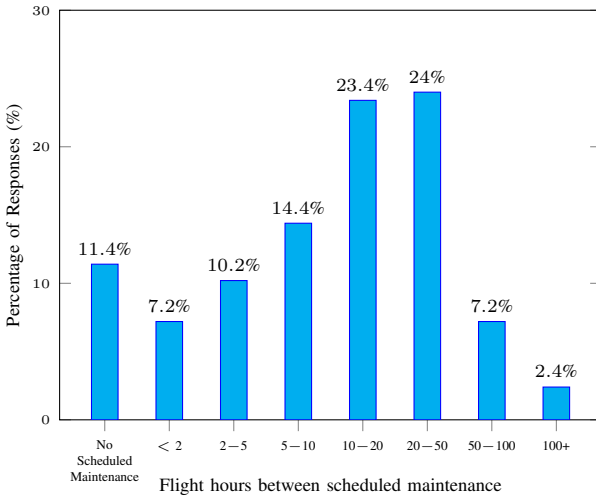


Fig. 9. Question 9 responses, please indicate approximately the number of hours flown between any scheduled maintenance.

Servicing is generally carried out after 20 to 50 hours of flight time for most companies. Around 10% of companies reported that servicing was carried out within the 5 hours of flight time range. A fairly large proportion of companies, 15%, did not have any scheduled maintenance. This could also be better supported with on-board diagnostic and prognostic technology.

J. Question 10: Please comment on any other technology you believe might improve drone flight safety.

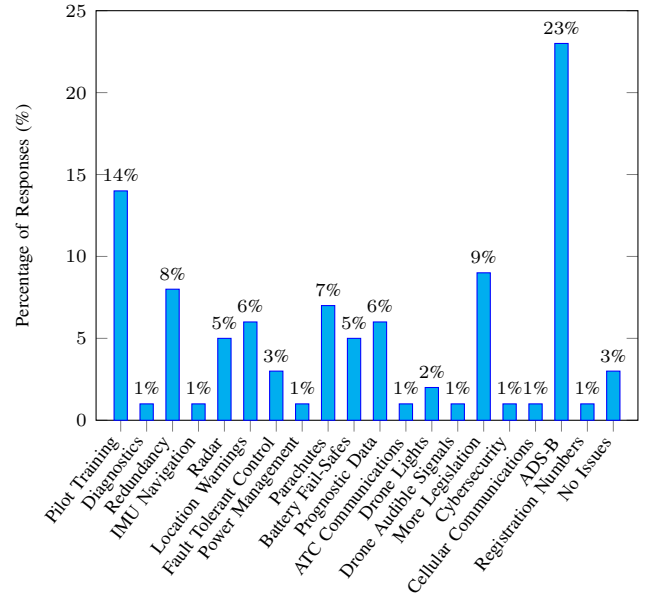


Fig. 10. Question 10 responses, please comment on any other technology you believe might improve drone flight safety.

The individual responses provided a valuable insight into the commercial experience of drone safety and reliability. The bar graph categorises the types of improvements recommended. There is clearly a high demand for ADS-B transponders and for rigorous pilot training. A few companies said that they had experienced no failures during many years of operations. However over 50% of responses related to some form of on-board intelligent augmentation of the current platforms. Some comments do not relate to on-board intelligence but relate to improvements in safety and reliability in general. A need for more legislation was identified for example and clearly a balance between automation, legislation and training will provide a complete safety and reliability solution.

III. RELATED WORK

Previous studies into UAV reliability for military and commercial drone technology have focused on establishing more efficient intervals for maintenance activities [2]. Petritoli et al present a hierarchy of reliability for UAVs for every 1000 failures. They report that reliability of commercial drones has been verified at about $1/10^3$ flight hours, whereas civil aircraft have two orders of magnitude more reliable systems at $1/10^5$ flight hours. They cite the most frequent failures for drones occur from the Power Plant, (411), Ground Control Station, (273), and Navigation Systems, (146). This is broadly in line with our study although we primarily collected data for Lithium Ion Power Plants and multi-rotor systems as opposed to liquid-fuelled, fixed wing systems, the frequency of failures for the power plant are high for both types of system, although as Petritoli et al state the power plant itself is fairly reliable

but the combination of software, power delivery subsystems and communication systems mean that power delivery can fail due to a number of sensitive dependencies. It is also worth noting the difference found between military systems and commercial drones. Where military drones are designed and operated closer to component limits for increased range, autonomy and performance a higher failure rate is observed. This is despite individual components and greater redundancy of subsystems being deployed in the military arena with the associated costs involved [2]. Petritoli et al note also that redundancy of systems is not the only answer as although system safety is improved as a whole, paradoxically this also increases the failure rates requiring more frequent maintenance. An alternative can also be over-sizing and derating to increase single component reliability to maintain safe levels of performance and reduce the need for maintenance to be more cost effective.

IV. EMERGING TECHNOLOGIES IN ASSISTING THE CERTIFICATION OF AUTONOMOUS UAVS

A. Integrated Vehicle Health Management (IVHM)

Integrated Vehicle Health Management (IVHM) is an emerging field arising from the Aerospace sector for large scale complex safety critical and supply chain driven operations, for example civil aviation and space systems, [3]. The premise is that on-board data, prognostics and maintenance planning is more cost effective when the maintenance activity is data driven and planned in advance. This forms the basis of a condition based maintenance program as opposed to traditional scheduled maintenance programs. The concepts used on larger commercial systems are of interest for smaller scale platforms to provide safety and reliability improvements at a reasonable cost. The costs depend upon the selection of sensors, design and validation work and additional data infrastructure to manage the real-time and historical information during operations from critical components and subsystems.

Zhang et al, [4] propose a framework for an IVHM system. The framework refers to large commercial aircraft operations and big data collection whereby important health information such as engine, flight control systems, hydraulic systems, environmental control systems, landing gear systems and fuel systems are collected for analysis. The flight control parameters and sensor data are used for maintenance decisions using PHM algorithms at a data center. Historical data is used to serve future fault diagnosis and prediction and timely decision-making information is exploited for the advanced notice of maintenance procedures.

Roemer and Tang et al [5] in The Handbook of Unmanned Aerial Vehicles detail IVHM and ACM (automated contingency management) systems architecture to support real-time, on-board health state assessment and fault management of UAVs. A hierarchical architecture is described including control re-configuration, and high-level reasoning. The dynamics and performance limitations of the damaged system are also estimated on-line in real time. Adaptive reconfigurable flight controllers are utilised to stabilise and recover the system using

the system dynamic model. Based on the health assessment and newly identified UAV dynamics, the operational flight envelope, ie. maximum speed, power consumption, manoeuvre rates and operating distances, can be assessed to ensure safe flight regimes.

B. Prognostics and Health Management (PHM)

PHM is a growing field of interest which has its roots in many industries, with knowledge gained from areas such as Aerospace engine management, Lithium-Ion battery life prognostics, electrical component failure prognostics, engineering reliability techniques and autonomous space systems, specifically work carried out at the Intelligent Systems Division at NASA [6]. Prognostics and Health Management is the science of predicting future events based on system knowledge and measurements of the system and environment. When the system is found to be operating at off-nominal conditions, physics based modelling, data driven techniques and prediction algorithms must be used to estimate the remaining useful life of components and subsystems. This forms the health management strategy of the engineering system in question. These techniques can be applied to many and varied subsystems within an engineering application. A critical component for any electric vehicle being the battery has meant much interest and research has been carried out into the accurate estimation of the remaining useful life of the battery for both mission time prognostics, state-of-charge (SOC) and maintenance, state-of-health (SOH) prognostics. Numerous studies into battery SOC techniques have been carried out, e.g. the use of Neural Nets [7], Unscented Kalman Filters [8], [9], Unscented Transform [10], Hardy Space H_∞ Observers [11] and Physics Based models [12]. The Coulomb counting and Open Circuit Voltage (OCV) vs SOC lookup table technique combined with equivalent circuit models (ECMs) and variations of the Kalman Filter are the predominant techniques currently applicable to UAVs for online applications [13]. The most sophisticated platforms also employ impedance spectroscopy techniques for both SOC and SOH assessments [14]. The most significant error sources are due to current sensor drift, cell aging, cell manufacturing variations, temperature effects, and hysteresis phenomenon. The battery SOH can be derived by several methods although there are two key techniques; the first is the use of experimental data collected over a large number of battery cycles and the second, adaptive methods where cell degradation must be derived as parameterised equations to determine the effect of a number of cell measurements. Adaptive measurements have higher computational loads whereas experimental data collection is very time consuming and expensive [15]. Specialised diagnostic measurements such as Coulombic efficiency and impedance spectroscopy can also be used for lifetime estimation. Most recently Severson et al [16] developed a machine learning technique using discharge voltage curves from early cycles to predict capacity degradation.

Other areas of interest for UAV prognostics include structural, electrical, software and mechanical fault monitoring. Glover et al [17], discussed the use of a novel approach to

PHM for manned and unmanned aerial systems that combine a Functional Failure Mode and Effects Analysis (FFMEA) with a reasoning system. They discuss the effective integration of the system from the design stage as being key to the benefit of a PHM system. They also describe the use of ‘JACK’ and ‘MADe’ two commercial software tools and the accuracy and advantages of their implementation on an engine health application. The effectiveness of PHM as a design optimisation tool is limited however to the baseline reliability of the subsystem components as found by [18]. They found that an already highly reliable Electrohydrostatic actuator (EHA) used on a manned fighter jet did not benefit from PHM technology in the design process.

Zermani et al [19] present the use of Bayesian networks for the monitoring of embedded applications for UAVs. They exploit the use of reconfigurable computing Field Programmable Gate Arrays (FPGAs). They highlight the importance of on-board resources and time constraints as well as precision as being crucial for autonomous systems like UAVs where it is beneficial to reconfigure dynamically the system in an emergency scenario.

C. Formal Methods

As a result of increasing autonomy, the development, verification and certification of autonomous robots is becoming inherently difficult due to the sheer complexity of the system design [20]–[22]. Testing based techniques have limitation in assuring the safety of autonomous robots, e.g. both [23], [24] show the infeasibility of demonstrating the safety of self-driving cars from road testing alone, and [23], [25] explicitly argue the need for alternative verification methods to supplement testing. Aligned with this idea, [24] proposes a Bayesian approach to combine supplement verification evidence as prior knowledge to the testing. Formal methods, e.g. model checking and theorem proving, offer an opportunity in providing such alternative verification evidence, which indeed has received great attention [26], [27].

In particular, we confine ourselves to Probabilistic Model Checking (PMC) in this paper, since there are inevitably uncertainties in the operation of modern autonomous robots, and probabilistic models are the nature way to capture such uncertainties faced by the systems. PMC [28] has been successfully used to analyze quantitative properties of systems across a variety of application domains, including robotics [27]. The basic steps of PMC are:

- Constructing a probabilistic model – commonly using Discrete Time Markov Chain (DTMC), Continuous Time Markov Chain (CTMC) or Markov Decision Process (MDP) (when considering non-deterministic actions in the modelling) – that formally represents the behaviour of a system over time.
- Specifying the properties of interest with e.g., Linear Temporal Logic (LTL) or Probabilistic Computational Tree Logic (PCTL).
- Then, normally by automatic tools like PRISM [29] and STORM [30], a systematic exploration is performed to

check if a claimed property holds against the probabilistic model.

As mentioned, PMC, as a variant of model checking techniques, emphasises the inherent uncertainties of the formalised system. In [31], [32], the complex and uncertain behaviours of robot swarms are analysed by PMC to assess whether swarms will indeed behave as required. In [33], PMC is used to synthesis and verify the control policies of robots in partially unknown environments. In a hostile environment, the movements of adversaries are modelled probabilistically by MDP in [34] and PMC finds a control strategy that maximises the probability of accomplishing the mission objective. The reliability and performance of Unmanned Underwater Vehicles (UUVs) is guaranteed by reconfiguration (which is optimised by PMC) in [35], [36] when sensor failures occur. In the modelling of UAV missions, both [37], [38] use PMC to synthesis the optimal controller of multiple-UAVs, and discuss the limitations in this context with potential solutions.

There is a notorious problem for most (if not all) model checking techniques that is the verification assumes the formal model (e.g., a DTMC in PMC) accurately reflects the actual behaviour of the real-world system [39]. It becomes an even tougher issue for systems in changing, unexpected environments and with autonomous features. To handle the issue, the appealing idea of doing runtime PMC was proposed in [40], [41] whose essence is to keep the formal model alive and continuously update it when seeing new data at runtime.

Although runtime PMC has been extensively studied for other software-intensive systems, there is little research on runtime PMC for robots. To the best of our knowledge, the first work of runtime PMC on robots is credited to [42] in which it focuses on improving the scalability of runtime PMC by using software engineering techniques. Then in [43], we propose advanced Bayesian estimators which considers robotics features to update the formal model at runtime. For instance, due to the safety-critical feature of robots deployed in assets inspection missions, the Conservative Bayesian Inference (CBI) estimator [44]–[46] was introduced to provide conservative estimates on catastrophic failure related model parameters.

In summary, formal methods build a mathematically rigorous model of a complex system (e.g. UAVs) and then verify the system’s properties in a more thorough fashion than simulated/operational testing. It has been shown that (runtime) PMC, as a variant of model checking techniques, is particularly useful in assuring autonomous robots deployed in extreme environments.

D. Simulation

Similar to formal methods, simulation based testing is frequently used in academia and industry to design, develop, verify and certify autonomous robots. The case for when to use simulation based testing rather than formal methods are nuanced, Matt Schmitt et al. claim that researchers prefer simulations due to the lowered barriers to flight, particularly the reduction in cost of flight and the time saving in terms of health and safety [47], yet these same arguments may be

used in the case for formal methods. Unlike formal methods, simulations may be easily modified, allowing researchers who are operating in complex environments to adjust their system's variables and assets to analyse the effects on the outputs from the simulation. Crucially simulations allow for expedited, repetitive runs of a scenario under multiple different values of selected variables, something which for many researchers would not be practical within their time constraints. The main argument against simulation is that to accurately simulate a scenario the entirety of reality needs to be simulated, something which is currently too complex for us to simulate. The solution many researchers utilise is to model only those areas about which they are concerned, such a model may then be integrated into a larger, simplified overarching system model. Such methodology is practical, yet sub-optimal, without fully modelling the entire system, unforeseen issues may still arise. Conversely probabilistic model checking may handle these large, complex probabilistic systems [48]. Finally many simulators require long periods of time for their initial installation coupled with a demand for powerful hardware. Ana Cavalcanti et al. believe that the current state of simulators is ad-hoc and unverifiable [49], they are in the process of creating a solution to the problem of how to model and consistency check such simulations. There are numerous popular software tools used to simulate autonomous robots, such as: Gazebo [50], ARGoS [51], Webots [52] and CARLA [53].

As well as a more limited selection of software tools designed to specifically simulate UAV: OpenUAV [47], UAV CRAFT [54] and AirSim [55], [56].

Software such as OpenUAV, AirSim and Gazebo have the advantage of being open source and free. Gazebo is already widely used in industry and academia, in part due to its licensing agreements, but also, it's partnership with the Robotic Operating System (ROS) [57] which utilises Gazebo as part of its offerings to users.

E. Fault Tolerant Control

Damage to rotor blades and power loss to rotors on multi-rotor UAVs constitutes a critical failure if the flight controller is unable to maintain safe flight. However to further increase safety a number of research institutions have developed fault tolerant control techniques for multi-rotor UAVs. Early work at MIT and Stanford formed the standard techniques, e.g. Model Referenced Adaptive Control (MRAC), reallocating controllers in the event of failure detection. A review of these techniques can be found in the works by Zhang et al [58]. Successful experimental demonstrations of flight recovery from partial and total loss of rotor blades have been shown at Columbia University [59] as well as flight with the loss of 1, 2 and 3 rotor blades on a quadrotor at ETH Zurich [60]. The technology operates at the flight controller level by detecting off-nominal flight behaviour via Fault Detection and Diagnostic algorithms (FDD). The technology acts either passively, via controllers that accommodate failure, or actively, via reallocation of controllers to manage flight by switching to new flight dynamic modes to prevent uncontrolled descent of

the air-frame. Further research into L_1 controllers at Cranfield University has shown potential improvements in reliability for hexrotor and octotoror configurations.

F. Air Traffic Control (ATC) Technology

As the demand for unmanned aerial vehicles increases the need for increased development of Beyond Visual Line of Sight (BVLoS) technology is required. Operation within this region is permitted if an approved method of collision avoidance and aerial separation is used. Alternatively, the aircraft can be flown in a segregated airspace using Instrument Flight Controls (IFR) and using Air Traffic Control (ATC) clearance [61].

Radar is a prerequisite for UAV traffic management systems. A radar on-board a UAV allows the operator and autopilots with complete situational awareness, detect and avoid system [62]. Radar can be used in multiple weather conditions and also day and night.

Automatic Dependant Surveillance Broadcast (ADS-B) can also be used to gain an understanding of airspace. Aircraft can determine their exact location using a high accuracy GPS. This location can be broadcast to other nearby aircraft and ADS-B ground stations. The ground stations will send this information to air traffic control towers. Aircraft will broadcast their position continuously and if the hardware is on-board the aircraft, it will also be able to receive the broadcast from other aircraft. This continuous and therefore up to date cycle of broadcasts gives pilots and air traffic control an understanding of what is in their airspace. ADS-B is automatic and no extra action is required for the data to be broadcast. The aircraft sending the broadcast may be aware or unaware of whom is receiving the information [63].

One common issue with UAVs is the risk of collision with a commercial aircraft or any other type of aircraft. For this reason UAVs need to know what is in their airspace. Therefore, employing the above technology on-board a UAV will help manage this risk.

G. Assurance Cases

Assurance cases are generally developed to support claims in areas such as safety, reliability, maintainability and security. These assurance cases are often called by some more specific names, e.g. safety cases [64] and security cases [65]. A safety case is a comprehensive, defensible, and valid justification of the safety of a system for a given application in a defined operating environment, thus it is a means to provide the grounds for confidence and to assist decision making in certification [66]. Indeed, safety cases are mandatory in UK regulation for systems used in safety-critical applications, e.g. nuclear energy, medical devices and air traffic control. Thus, developing assurance cases is an inevitable and also important step in UAV certification, the following is a list of the cutting edge research topics related to assurance cases:

- Structured and graphical notations: early research in assurance cases mainly focus on their formulation in terms of claims, arguments and evidence elements based

on fundamental argumentation theories like the Toulmin model [67]. The two most popular notations are CAE [66] and GSN [68] and both provide supporting tools.

- Methodologies in assisting safety case construction: to reduce the effort required in developing safety cases, researchers are looking into safety argument patterns in GSN [69] and reusing blocks in CAE [70] which are derived from extensive empirical analysis of real cases.
- Assessing confidence in safety cases: As arguments and evidence in practice are imperfect, we can never be certain a claim will hold. We may want to quantify confidence in safety cases [71]. Methods based on underlying theories of Bayesian Belief Networks and Dempster-Shafer theory are proposed [72]–[75]. For a detailed review, see [76]. It is worth mentioning that Rushby classifies the safety arguments into deductive and inductive arguments which require differing treatment in propagating confidence in cases [77].
- Model-driven safety cases: for a better integration with other activities in the development process and to combine the benefits of model-driven engineering, model-driven safety cases are proposed, e.g. [78], [79].
- Dynamic safety cases: Due to increasing use of autonomous systems that handle environmental and internal uncertainties by dynamically adjusting their configurations. The notion of dynamic safety cases are proposed to provide a basis of continuously assuring safety requirements [80], [81].

V. CONCLUSIONS AND FUTURE WORK

In this paper the results of a Safety and Reliability Survey issued to UK CAA approved operators have been presented, highlighting the types of failures most frequently observed in commercial operation. The frequency of failures found in operations for both critical and non-critical sub-systems are quantified and the need for on-board intelligent safety systems identified. The results of the survey have been compared and contrasted to previous studies into UAV safety and reliability and the most common concerns and recommendations have been presented from operator responses. Based on the identified challenges, a review on candidate technologies and methods has been presented that align with the challenges of improving the safety and reliability of drones for generating verification & validation (V&V) evidence to facilitate certification.

With the increasing presence of UAVs in a myriad of markets and a technology trend that forecasts increasing interaction between people, infrastructure and robotics, solutions are required that support safe guarding people and infrastructure. With increasing autonomy of UAVs more advanced methods are required to account for dynamic changes in the environment and within the UAV platform. Globally, constraints on BVLOS (beyond visual line of sight) cite reliability as one of the key bottlenecks to increased UAV adoption. To develop a solution for this significant challenge, the technologies reviewed in this paper provide the basis of both improving and

certifying their safety and reliability. A trend is to integrate the above mentioned techniques [49], [82] in a systematic certification framework and the need for an automated tool-chain for the design and implementation of such a framework forms important future work.

ACKNOWLEDGEMENT

This work is supported by the UK EPSRC through the Offshore Robotics for Certification of Assets (ORCA) Hub [EP/R026173/1], Holistic Operation and Maintenance for Energy from Offshore Wind Farms Consortium (HOME-Offshore) [EP/P009743/1], the Centre for Doctoral Training in Embedded Intelligence (CDT-EI) and Texo Drone Survey & Inspection Ltd.

REFERENCES

- [1] C. A. Authority, “CAP 722 Unmanned Aircraft System Operations in UK Airspace—Guidance,” pp. 63–67, 2015.
- [2] E. Petritoli, F. Leccese, L. Ciani, E. Petritoli, F. Leccese, and L. Ciani, “Reliability and Maintenance Analysis of Unmanned Aerial Vehicles,” *Sensors*, vol. 18, no. 9, p. 3171, sep 2018.
- [3] I. Jennions, *Integrated vehicle health management: perspectives on an emerging field*. Warrendale, PA: SAE International., 2011.
- [4] G. Zhang, J. Wang, Z. Lv, Y. Yang, H. Su, Q. Yao, Q. Huang, S. Ye, and J. Huang, “A integrated vehicle health management framework for aircraft - a preliminary report,” *2015 IEEE Conference on Prognostics and Health Management: Enhancing Safety, Efficiency, Availability, and Effectiveness of Systems Through PHAF Technology and Application, PHM 2015*, pp. 1–8, 2015.
- [5] M. J. Roemer and L. Tang, “Integrated vehicle health and fault contingency management for uavs,” in *Handbook of Unmanned Aerial Vehicles*, 2015, pp. 999–1025.
- [6] K. Goebel, J. Celaya, S. Sankararaman, I. Roychoudhury, M. Daigle, and A. Saxena, *Prognostics: The Science of Making Predictions*. New York, NY: USA:CreateSpace, 04 2017.
- [7] D. Gao, M. Huang, and J. Xie, “A novel indirect health indicator extraction based on charging data for lithium-ion batteries remaining useful life prognostics,” *SAE International Journal of Alternative Powertrains*, vol. 6, no. 2, pp. 183–193, 2017.
- [8] W. He, N. Williard, C. Chen, and M. Pecht, “State of charge estimation for electric vehicle batteries using Unscented Kalman Filtering,” *Microelectronics Reliability*, vol. 53, no. 6, pp. 840–847, 2013.
- [9] E. F. Hogge, B. M. Bole, S. L. Vazquez, J. R. Celaya, T. H. Strom, B. L. Hill, K. M. Smalling, and C. C. Quach, “Verification of prognostic algorithms to predict remaining flying time for electric unmanned vehicles,” *International Journal of Prognostics and Health Management*, vol. 9, no. 1, pp. 1–15, 2018.
- [10] M. Daigle and K. Goebel, “Improving computational efficiency of prediction in model-based prognostics using the unscented transform,” *Annual Conference of the Prognostics and Health Management Society*, 2010.
- [11] F. Zhang, G. Liu, L. Fang, and H. Wang, “Estimation of battery state of charge with H_∞ observer: Applied to a robot for inspecting power transmission lines,” *IEEE Transactions on Industrial Electronics*, vol. 59, no. 2, pp. 1086–1095, Feb. 2012.
- [12] W. He, M. Pecht, D. Flynn, and F. Dinmohammadi, “A physics-based electrochemical model for lithium-ion battery state-of-charge estimation solved by an optimised projection-based method and moving-window filtering,” *Energies*, vol. 11, no. 8, p. 2120, 2018.
- [13] R. Zhang, B. Xia, B. Li, L. Cao, Y. Lai, W. Zheng, H. Wang, and W. Wang, “State of the art of lithium-ion battery SOC estimation for electrical vehicles,” *Energies*, vol. 11, no. 7, 2018.
- [14] N. Harting, R. Schenkendorf, N. Wolff, and U. Krewer, “State-of-health identification of lithium-ion batteries based on nonlinear frequency response analysis: First steps with machine learning,” *Applied Sciences*, vol. 8, no. 5, p. 821, 2018.
- [15] M. Bercibar, I. Gandiaga, I. Villarreal, N. Omar, J. Van Mierlo, and P. Van Den Bossche, “Critical review of state of health estimation methods of li-ion batteries for real applications,” 2016.

- [16] K. A. Severson, P. M. Attia, N. Jin, N. Perkins, B. Jiang, Z. Yang, M. H. Chen, M. Aykol, P. K. Herring, D. Fragedakis, M. Z. Bazant, S. J. Harris, W. C. Chueh, and R. D. Braatz, "Data-driven prediction of battery cycle life before capacity degradation," *Nature Energy*, vol. 4, no. 5, pp. 383–391, May 2019.
- [17] W. Glover, J. Cross, A. Lucas, C. Stecki, and J. Stecki, "The use of prognostic health management for autonomous unmanned air systems," *Annual Conf. of the Prognostics and Health Management Society*, 2010.
- [18] D. S. Bodden, W. Hadden, B. E. Grube, and N. S. Clements, "Phm as a design variable in air vehicle conceptual design," *IEEE Aerospace Conference Proceedings*, pp. 1–11, 2005.
- [19] S. Zermani, C. Dezan, R. Euler, and J. P. Diguët, "Bayesian network-based framework for the design of reconfigurable health management monitors," in *2015 NASA/ESA Conference on Adaptive Hardware and Systems, AHS 2015*, 2015.
- [20] M. Fisher, L. Dennis, and M. Webster, "Verifying autonomous systems," *Communication of the ACM*, vol. 56, no. 9, pp. 84–93, Sep. 2013.
- [21] M. Fisher, E. Collins, L. Dennis, M. Luckcuck, M. Webster, M. Jump, V. Page, C. Patchett, F. Dinmohammadi, D. Flynn, V. Robu, and X. Zhao, "Verifiable self-certifying autonomous systems," in *IEEE Int. Symp. on Software Reliability Engineering Workshops*, 2018, pp. 341–348.
- [22] V. Robu, D. Flynn, and D. Lane, "Train robots to self-certify as safe," *Nature*, vol. 553, no. 7688, pp. 281–281, 2018.
- [23] N. Kalra and S. M. Paddock, "Driving to safety: How many miles of driving would it take to demonstrate autonomous vehicle reliability?" *Transp. Research Part A: Policy & Practice*, vol. 94, pp. 182–193, 2016.
- [24] X. Zhao, V. Robu, D. Flynn, K. Salako, and L. Strigini, "Assessing the safety and reliability of autonomous vehicles from road testing," in *the 30th Int. Symp. on Software Reliability Engineering*. Berlin, Germany: IEEE, 2019, in press.
- [25] P. Koopman and M. Wagner, "Autonomous vehicle safety: An interdisciplinary challenge," *IEEE Intelligent Transportation Systems Magazine*, vol. 9, no. 1, pp. 90–96, 2017.
- [26] M. Farrell, M. Luckcuck, and M. Fisher, "Robotics and integrated formal methods: Necessity meets opportunity," in *Proc. of the 14th Int. Conf. on Integrated Formal Methods*, ser. LNCS, vol. 11023. Cham: Springer, 2018, pp. 161–171.
- [27] M. Luckcuck, M. Farrell, L. Dennis, C. Dixon, and M. Fisher, "Formal specification and verification of autonomous robotic systems: a survey," *arXiv preprint arXiv:1807.00048*, 2018.
- [28] M. Kwiatkowska, G. Norman, and D. Parker, "Probabilistic model checking: Advances and applications," in *Formal System Verification: State-of-the-Art and Future Trends*. Cham: Springer International Publishing, 2018, pp. 73–121.
- [29] —, "PRISM 4.0: Verification of probabilistic real-time systems," in *Proc. 23rd Int. Conf. on Computer Aided Verification*, ser. LNCS, vol. 6806. Springer, 2011, pp. 585–591.
- [30] C. Dehnert, S. Junges, J.-P. Katoen, and M. Volk, "A STORM is coming: A modern probabilistic model checker," in *Computer Aided Verification*, ser. LNCS, R. Majumdar and V. Kunčák, Eds., vol. 10427. Cham: Springer International Publishing, 2017, pp. 592–600.
- [31] S. Konur, C. Dixon, and M. Fisher, "Analysing robot swarm behaviour via probabilistic model checking," *Robotics and Autonomous Systems*, vol. 60, no. 2, pp. 199 – 213, 2012.
- [32] P. Gainer, C. Dixon, and U. Hustadt, "Probabilistic model checking of ant-based positionless swarming," in *Towards Autonomous Robotic Systems*. Cham: Springer International Publishing, 2016, pp. 127–138.
- [33] G. Norman, D. Parker, and X. Zou, "Verification and control of partially observable probabilistic systems," *Real-Time Systems*, vol. 53, no. 3, pp. 354–402, May 2017.
- [34] I. Cizelj, X. Ding, M. Lahijanian, A. Pinto, and C. Belta, "Probabilistically safe vehicle control in a hostile environment," *IFAC Proc. Volumes*, vol. 44, no. 1, pp. 11 803–11 808, 2011.
- [35] R. Calinescu, S. Gerasimou, and A. Banks, "Self-adaptive Software with Decentralised Control Loops," in *Fundamental Approaches to Software Engineering*, ser. LNCS, A. Egyed and I. Schaefer, Eds., vol. 9033. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 235–251.
- [36] S. Gerasimou, R. Calinescu, S. Shevtsov, and D. Weyns, "UNDER-SEA: an exemplar for engineering self-adaptive unmanned underwater vehicles," in *IEEE/ACM 12th Int. Symp. on Software Engineering for Adaptive and Self-Managing Systems (SEAMS)*, May 2017, pp. 83–89.
- [37] R. Giacinta, R. Hoffmann, M. Ireland, A. Miller, and G. Norman, "Strategy synthesis for autonomous agents using PRISM," in *NASA Formal Methods*, ser. LNCS, vol. 10811. Cham: Springer International Publishing, 2018, pp. 220–236.
- [38] R. Hoffmann, M. Ireland, A. Miller, G. Norman, and S. Veres, "Autonomous agent behaviour modelled in PRISM – A case study," in *Model Checking Software*, ser. LNCS, D. Bošnački and A. Wijs, Eds., vol. 9641. Cham: Springer International Publishing, 2016, pp. 104–110.
- [39] R. Calinescu, C. Ghezzi, K. Johnson, M. Pezzé, Y. Rafiq, and G. Tamburrelli, "Formal verification with confidence intervals to establish quality of service properties of software systems," *IEEE Tran. on Reliability*, vol. 65, no. 1, pp. 107–125, 2016.
- [40] I. Epifani, C. Ghezzi, R. Mirandola, and G. Tamburrelli, "Model evolution by run-time parameter adaptation," in *Proc. of the 31st Int. Conf. on Software Engineering*. Washington, DC, USA: IEEE, 2009, pp. 111–121.
- [41] R. Calinescu, C. Ghezzi, M. Kwiatkowska, and R. Mirandola, "Self-adaptive software needs quantitative verification at runtime," *Comm. of the ACM*, vol. 55, no. 9, pp. 69–77, Sep. 2012.
- [42] S. Gerasimou, R. Calinescu, and A. Banks, "Efficient runtime quantitative verification using caching, lookahead, and nearlyoptimal reconfiguration," in *Proc. of the 9th Int. Symp. on Software Engineering for Adaptive and Self-Managing Systems*, ser. SEAMS 2014. New York, NY, USA: ACM, 2014, pp. 115–124.
- [43] X. Zhao, V. Robu, D. Flynn, F. Dinmohammadi, M. Fisher, and M. Webster, "Probabilistic model checking of robots deployed in extreme environments," in *Proc. of the 33rd AAAI Conference on Artificial Intelligence*, vol. 33, Honolulu, Hawaii, USA, 2019, pp. 8076–8084.
- [44] P. Bishop, R. Bloomfield, B. Littlewood, A. Povyakalo, and D. Wright, "Toward a formalism for conservative claims about the dependability of software-based systems," *IEEE Transactions on Software Engineering*, vol. 37, no. 5, pp. 708–717, 2011.
- [45] X. Zhao, B. Littlewood, A. Povyakalo, and D. Wright, "Conservative claims about the probability of perfection of software-based systems," in *26th Int. Symp. on Software Reliability Engineering (ISSRE)*. IEEE, 2015, pp. 130–140.
- [46] X. Zhao, B. Littlewood, A. Povyakalo, L. Strigini, and D. Wright, "Modeling the probability of failure on demand (pfd) of a 1-out-of-2 system in which one channel is "quasi-perfect"," *Reliability Engineering & System Safety*, vol. 158, pp. 230–245, 2017.
- [47] M. Schmittle, A. Lukina, L. Vacek, J. Das, C. P. Buskirk, S. Rees, J. Sztipanovits, R. Grosu, and V. Kumar, "Openuav: A uav testbed for the cps and robotics community," in *2018 ACM/IEEE 9th International Conference on Cyber-Physical Systems*, April 2018, pp. 130–139.
- [48] M. Kwiatkowska, G. Norman, and D. Parker, *Probabilistic Model Checking: Advances and Applications*. Cham: Springer International Publishing, 2018, pp. 73–121.
- [49] A. Cavalcanti, A. Sampaio, A. Miyazawa, P. Ribeiro, M. Filho, W. Li, and J. Timmis, "Verified simulation for robotics," *Science of Computer Programming*, vol. 174, pp. 1–37, 2019.
- [50] N. Koenig and A. Howard, "Design and use paradigms for Gazebo, an open-source multi-robot simulator," in *2004 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, vol. 3, September 2004, pp. 2149–2154.
- [51] C. Pinciroli, V. Trianni, R. O'Grady, G. Pini, A. Brutschy, M. Brambilla, N. Mathews, E. Ferrante, G. Di Caro, F. Ducatelle, M. Birattari, L. Gambardella, and M. Dorigo, "Argos: a modular, parallel, multi-engine simulator for multi-robot systems," *Swarm Intelligence*, vol. 6, no. 4, pp. 271–295, 2012.
- [52] O. Michel, "Cyberbotics Ltd. webots™: Professional mobile robot simulation," *International Journal of Advanced Robotic Systems*, vol. 1, no. 1, p. 5, 2004. [Online]. Available: <https://doi.org/10.5772/5618>
- [53] A. Dosovitskiy, G. Ros, F. Codevilla, A. Lopez, and V. Koltun, "CARLA: An open urban driving simulator," in *Proceedings of the 1st Annual Conference on Robot Learning*, 2017, pp. 1–16.
- [54] Presagis, "Uav craft," [Last Accessed: 20th of July 2019].
- [55] Microsoft, "Airsim," 2019, [Last Accessed: 26th of July 2019].
- [56] S. Shah, D. Dey, C. Lovett, and A. Kapoor, "Airsim: High-fidelity visual and physical simulation for autonomous vehicles," in *Field and Service Robotics*, M. Hutter and R. Siegwart, Eds. Cham: Springer International Publishing, 2018, pp. 621–635.
- [57] O. S. R. Foundation, "Robotics operating system," <http://www.ros.org/>, [Last Accessed: 21st of July 2019].
- [58] Y. M. Zhang, A. Chamseddine, C. A. Rabbath, B. W. Gordon, C. Y. Su, S. Rakheja, C. Fulford, J. Apkarian, and P. Gosselin, "Development of advanced fdd and ftc techniques with application to an unmanned

- quadrotor helicopter testbed,” *Journal of the Franklin Institute*, vol. 350, no. 9, pp. 2396–2422, 2013.
- [59] Y. Zhang, A. C. A. F. C. Systems, and undefined 2012, “Fault tolerant flight control techniques with application to a quadrotor uav testbed,” *intechopen.com*, 2012. [Online]. Available: <https://www.intechopen.com/download/pdf/26018>
- [60] M. W. Mueller and R. D’Andrea, “Stability and control of a quadrotor despite the complete loss of one, two, or three propellers,” *Proceedings - IEEE International Conference on Robotics and Automation*, pp. 45–52, 2014.
- [61] L. Davies, R. C. Bolam, Y. Vagapov, and A. Anuchin, “Review of unmanned aircraft system technologies to enable beyond visual line of sight (bvlos) operations,” in *2018 X International Conference on Electrical Power Drive Systems (ICEPDS)*. IEEE, 2018, pp. 1–6.
- [62] L. Davies, R. C. Bolam, Y. Vagapov, and A. Anuchin, “Review of unmanned aircraft system technologies to enable beyond visual line of sight (bvlos) operations,” in *2018 X International Conference on Electrical Power Drive Systems (ICEPDS)*, Oct 2018, pp. 1–6.
- [63] W. Semke, N. Allen, A. Tabassum, M. McCrink, M. Moallemi, K. Snyder, E. Arnold, D. Stott, and M. Wing, “Analysis of radar and ads-b influences on aircraft detect and avoid (daa) systems,” *Aerospace*, vol. 4, no. 3, p. 49, 2017.
- [64] P. Bishop and R. Bloomfield, “A methodology for safety case development,” *Safety and Reliability*, vol. 20, no. 1, pp. 34–42, 2000.
- [65] J. Knight, “The importance of security cases: Proof is good, but not enough,” *IEEE Security Privacy*, vol. 13, no. 4, pp. 73–75, Jul. 2015.
- [66] R. Bloomfield and P. Bishop, “Safety and assurance cases: past, present and possible future - an Adelard perspective,” in *Making Systems Safer*, C. Dale and T. Anderson, Eds. London: Springer London, 2010, pp. 51–67.
- [67] S. Toulmin, *The Uses of Argument*. Cambridge University Press, 1958.
- [68] T. P. Kelly, “Arguing safety: A systematic approach to managing safety cases,” PhD Thesis, University of York, 1999.
- [69] R. Hawkins, K. Clegg, R. Alexander, and T. Kelly, “Using a software safety argument pattern catalogue: Two case studies,” in *Computer Safety, Reliability, and Security*, F. Flammini, S. Bologna, and V. Vitorini, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 185–198.
- [70] R. Bloomfield and K. Netkachova, “Building blocks for assurance cases,” in *2014 IEEE International Symposium on Software Reliability Engineering Workshops*, Nov. 2014, pp. 186–191.
- [71] R. E. Bloomfield, B. Littlewood, and D. Wright, “Confidence: Its role in dependability cases for risk assessment,” in *37th Annual IEEE/IFIP Int. Conf. on Dependable Systems and Networks*, Jun. 2007, pp. 338–346.
- [72] B. Littlewood and D. Wright, “The use of multilegged arguments to increase confidence in safety claims for software-based systems: a study based on a BBN analysis of an idealized example,” *IEEE Transactions on Software Engineering*, vol. 33, no. 5, 2007.
- [73] E. Denney, G. Pai, and I. Habli, “Towards measurement of confidence in safety cases,” in *2011 International Symposium on Empirical Software Engineering and Measurement*, Sep. 2011, pp. 380–383.
- [74] X. Zhao, D. Zhang, M. Lu, and F. Zeng, “A New Approach to Assessment of Confidence in Assurance Cases,” in *Computer Safety, Reliability, and Security*, ser. LNCS, vol. 7613. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 79–91.
- [75] R. Wang, J. Guiochet, and G. Motet, “Confidence assessment framework for safety arguments,” in *Computer Safety, Reliability, and Security*, S. Tonetta, E. Schoitsch, and F. Bitsch, Eds. Cham: Springer International Publishing, 2017, pp. 55–68.
- [76] P. J. Graydon and C. M. Holloway, “An investigation of proposed techniques for quantifying confidence in assurance arguments,” *Safety Science*, vol. 92, pp. 53 – 65, 2017.
- [77] J. Rushby, “The interpretation and evaluation of assurance cases,” Computer Science Laboratory, SRI International, Menlo Park, CA, Tech. Rep. SRI-CSL-15-01, 2015.
- [78] B. Gallina, “A Model-Driven safety certification method for process compliance,” in *2014 IEEE International Symposium on Software Reliability Engineering Workshops*, Nov. 2014, pp. 204–209.
- [79] R. Hawkins, I. Habli, D. Kolovos, R. Paige, and T. Kelly, “Weaving an assurance case from design: A model-based approach,” in *2015 IEEE 16th International Symposium on High Assurance Systems Engineering*, Jan. 2015, pp. 110–117.
- [80] E. Denney, G. Pai, and I. Habli, “Dynamic safety cases for through-life safety assurance,” in *2015 IEEE/ACM 37th IEEE International Conference on Software Engineering*, vol. 2, May 2015, pp. 587–590.
- [81] R. Calinescu, D. Weyns, S. Gerasimou, M. U. Iftikhar, I. Habli, and T. Kelly, “Engineering trustworthy self-adaptive software with dynamic assurance cases,” *IEEE Transactions on Software Engineering*, vol. 44, no. 11, pp. 1039–1069, Nov. 2018.
- [82] X. Zhao, M. Osborne, J. Lantair, V. Robu, D. Flynn, X. Huang, M. Fisher, F. Papacchini, and A. Ferrando, “Towards Integrating Formal Verification of Autonomous Robots with Battery Prognostics and Health Management,” in *The 17th Int. Conf. on Software Engineering and Formal Methods*. Oslo, Norway: Springer, 2019, in press.