Risk-based Regulation of Unmanned Aircraft Systems

A thesis submitted in fulfilment of the requirements for the degree of

Doctor of Philosophy

Achim Washington

Bachelor of Engineering (Aerospace Engineering)

Royal Melbourne Institute of Technology

School of Engineering

College of Science, Engineering and Health

RMIT University

September 2019

“*As far as the laws of mathematics refer to reality, they are not certain; and as far as they are certain, they do not refer to reality*.”

Albert Einstein (1879 to 1955)

Declaration

I certify that except where due acknowledgement has been made, the work is that of the author alone; the work has not been submitted previously, in whole or in part, to qualify for any other academic award; the content of the thesis is the result of work which has been carried out since the official commencement date of the approved research program; any editorial work, paid or unpaid, carried out by a third party is acknowledged; and, ethics procedures and guidelines have been followed.

I acknowledge the support I have received for my research through the provision of an Australian Government Research Training Program Scholarship.

____

ACHIM WASHINGTON

16th September 2019

Acknowledgements

I would like to take this opportunity to acknowledge the support my supervisors, family and friends have provided me with throughout this journey. They have all been an integral part of my research candidature and without each of their support, I would not have been able to achieve the results that I did. To my supervisors, thank you for your patience and continuous guidance. To my family and friends, thank you for always being there and helping me through the ups and downs of this journey. To my parents, thank you for always supporting me. Without your help, I would not be where I am today.

This thesis was supported by the Australian Federal Government Australian Postgraduate Award.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

ALARP	As Low As Reasonably Practicable
BBN	Bayesian Belief Network
CAA	Civil Aviation Authority
CASA	Civil Aviation Safety Authority
CPA	Conventionally Piloted Aircraft
DASA	Defence Aviation Safety Authority
EASA	European Aviation Safety Authority
EoV	Entities of Value
FAA	Federal Aviation Administration
FMEA	Failure Mode Effects Analysis
GRM	Ground Risk Models
ICAO	International Civil Aviation Organization
JARUS	Joint Authorities for Rulemaking on Unmanned Systems
MLE	Maximum Likelihood Estimates
NAA	National Aviation Authorities
PRA	Probabilistic Risk Analysis
PSA	Probabilistic Safety Assessment
QRA	Quantitative Risk Assessment
SARPs	Standards and Recommended Practices
SFARP	So Far as is Reasonably Practicable
SMM	Safety Management Manual
SMS	Safety Management System
SRM	Safety Risk Management
SRMP	Safety Risk Management Process
SSA	System Safety Assessment
SSP	State Safety Programme
SSPR	System Safety Performance Requirements
SSR	System Safety Regulations
UA	Unmanned Aircraft
UAM	Urban Air Mobility
UAS	Unmanned Aircraft Systems

Supervisory Team

The supervisory team comprised of Dr Reece Clothier and Dr Jose Silva. Details of their affiliations are presented below:

Dr Reece Clothier
Joint Primary Senior Supervisor
reece.a.clothier@boeing.com
Global Airspace Integration Manager, Boeing NeXt, Global Airspace Strategy and Execution
Associate Professor (Honorary), School of Engineering, RMIT University

Dr Jose Silva
Joint Primary Senior Supervisor
jose.silva@rmit.edu.au
Associate Professor, School of Engineering, RMIT University

Abstract

The aviation sector is faced with a novel array of new airspace users including Urban Air Mobility (UAM) concepts, personal air mobility vehicles, reusable space launch vehicles, and Unmanned Aircraft Systems (UAS). Focusing on UAS, there is much effort being directed towards the development of safety regulations for this industry. National Aviation Authorities (NAA) have advocated the adoption of a risk-based approach to the development of regulations, whereby regulations are driven by the outcomes of a systematic process to assess and manage identified safety risks.

Central to a risk-based approach is the Safety Risk Management Process (SRMP). A review of relevant aviation safety policy, guidance and regulatory material found that aviation safety literature does not adequately address the uncertainty inherent to any SRMP. For example, when measuring risk, only the likelihood and severity are taken into consideration, with uncertainty generally not being mentioned. Where uncertainty is recognised, it is taken into consideration through the use of conservative worst-case assumptions. This can result in the imposition of overly stringent restrictions or worse, regulations that do not adequately mitigate safety risks. Subsequently, providing a more comprehensive treatment of uncertainty in the aviation SRMP is essential to the uptake of a risk-based approach to rule-making. Further, it follows that if assessments of performance can be uncertain, then these uncertainties also need to be accounted for in other NAA regulatory processes such as the regulatory compliance assessment and compliance finding processes. It was found that the current aviation compliance process does not provide an objective means for accounting for uncertainty. As a consequence, compliance assessments can be subjective and inconsistent, with regulators lacking the tools and processes to be able to make objective compliance findings on the basis of compliance risk. A means to enable NAA to account for uncertainty in regulatory compliance processes is needed.

The overall aim of this thesis is to improve regulatory outcomes under the new paradigm of risk-based regulation, through providing a conceptual framework for the rational, transparent and systematic treatment of uncertainty in the risk assessment and regulatory decision-making processes. The thesis proposes the application of Bayesian methods and normative decision theory to the aviation safety regulatory process. System Safety Regulations (SSR), commonly referred to as “Part 1309” regulations, for UAS are used as a case study. It is posited that the general theoretical approach proposed in this thesis can improve the objectivity, consistency, and transparency of current aviation regulatory processes. The generalised approaches presented in this thesis enable the adoption of risk-based rule-making for new aviation sectors and provides the theoretical basis for risk-based compliance; a paradigm shift in how aviation safety regulators approach risk-based regulation.

Keywords

Unmanned Aircraft Systems

Remotely Piloted Aircraft Systems

Safety

Risk

Uncertainty

Ground Risk Models

Bayesian Analysis

Bayesian Belief Network

Risk Management

System Safety Regulations

1. Introduction

Figure 1: Concept image of an unmanned aircraft operation over Melbourne City, Australia
Image copyright © Achim Washington

"Only those who will risk going too far can possibly find out how far it is possible to go"

T.S. Eliot (1888-1965)

Section §1.1 of this chapter provides a brief overview of the background, highlighting the importance of the research. Following this, the key research questions are clearly outlined in Section §1.2. Next, the aims and objectives (Section §1.3), scope (Section §1.4) and significance of the research (Section §1.5) are detailed in the individual sub sections. Section §1.6 then summarises the main research publications completed during this candidature, detailing: how they link to each other; how they address the overall research questions of the thesis; and how they impact the overall objectives of the thesis. The novel contributions of each of the chapters are also summarised in this sub section.

1.1. Background

The aviation sector is faced with a wide variety of new airspace users including, Urban Air Mobility (UAM) concepts, personal air mobility vehicles, reusable space launch vehicles, and Unmanned Aircraft Systems (UAS). As with any new technology, there is risk associated with the operation of these systems. These emerging airspace users will differ to Conventionally Piloted Aircraft (CPA) not only in relation to the technology and concepts of operation but also in the management of their associated risks. One area in particular where these systems differ is the uncertainty in their associated risks. This uncertainty arises due to a lack of operational data, experience and knowledge [1]. There are less data, experience and knowledge due to several factors including: the relative infancy of the systems, the restrictions imposed on their operations, and the rapid pace of technology development [2]. A systematic approach for managing these uncertainties within the aviation regulatory process is needed to ensure acceptable regulatory outcomes for the sector.

1.1.1. Case Study - Unmanned Aircraft Systems

The UAS industry is an area in the aviation sector that has received considerable amount of attention in recent years. Unlike CPA, UAS do not have a human pilot on board [3]. This unique characteristic allows for a considerable amount of diversity amongst these systems. In terms of size, UAS can range from micro (something that can fit in the palm of one's hand) to large (something comparable to CPA). In terms of configuration, UAS can include fixed wing, multirotor, helicopter and hybrid configurations, to name a few. The list of applications for UAS is ever expanding, with UAS being used in both the civil and military sectors. Common civil applications include law enforcement, emergency rescue, environmental monitoring, crop dusting and aerial photography [4].

Perhaps the greatest non-technical challenge facing the UAS sector is the lack of a suitable regulatory framework governing the safety of their operations [5], [6]. Owing to the inherent differences that exist between CPA and UAS [7], it is widely acknowledged that the use of an "off-the-shelf" approach will not result in an effective airworthiness regulatory framework for UAS [6]. A "one-size-fits-all" approach to the airworthiness of UAS will also prove to be problematic owing to the diversity that exists between these systems [6]. A new and comprehensive framework of safety regulations for UAS is required to fully realise the potential benefits of the sector [6], [8], [9].

The European Aviation Safety Authority (EASA), the Federal Aviation Administration (FAA) and the Joint Authorities for Rulemaking on Unmanned Systems (JARUS) have recommended the adoption of a risk-based approach as a guiding principle in the development of regulations for UAS [10]–[15]. Under this principle, safety risk management (and its sub-processes) should drive the development of regulations, ensuring a clear traceability between the legislated requirement and the risks that are intended to be managed. The intended outcome is a framework of regulations and standards that has a defensible and objective basis in risk with the resulting regulatory requirements proportionate to the safety risks. A risk-based approach acknowledges that regulations are merely the embodiment of the outcomes of a risk management process [16], specifically: "they are legal requirements relating to how various stakeholders (*e.g.*, UAS operators) should go about treating safety risks; requirements relating to the implementation of controls or measures to modify, mitigate, or otherwise reduce the risk".

UAS provide an application case study to explore the practical utility of the extension of risk-based regulatory practices. There are two primary safety hazards associated with UAS operations [16], [17]. These are:

1) A collision or near collision between an Unmanned Aircraft (UA) and another aircraft (whether the other aircraft is in the air or on the ground);
2) The impact of the UA, or its components, with people or structures situated on the ground.

It is important here to note that while there are a number of secondary hazards associated with the top-level primary hazard (e.g. ignition of fires, release of contaminants, collapse of buildings, *etc.*), the discussion provided will be limited to only the top-level primary hazards. Under a risk-based approach, a comprehensive and objective assessment of the risks associated with these two primary hazards forms the principal input to the development of new standards and regulations for the sector. For the purposes of this thesis, the risks associated with the latter of these two hazards are of principal interest.

The risks posed to people and property situated on the ground are largely managed through the development and promulgation of regulations that provide assurance in the airworthiness of the UAS [6]. When coupled with operational regulations (*e.g.*, restrictions in terms of when and where UAS can operate), airworthiness regulations can more effectively manage the risks posed to people and property overflown [6]. Not all UAS types may be required to meet prescriptive codes of airworthiness requirements in order to be safe for operation (*e.g.*, open category of UAS as defined in [18]). However, for those UAS operations that do, they will likely be required to show compliance to a system safety regulation equivalent to the regulations contained in sub-part 1309 to various civil airworthiness codes for CPA.

Compliance with the System Safety Regulations (SSR)[1] is thus a central component to the airworthiness of any aviation system. SSR supplement prescriptive requirements on the design and testing of an aviation system and are, in part, put in place "to ensure that an aircraft is capable of continued safe flight and landing following a failure or multiple failures of systems" [19]. The regulations can be applied to installed sub-systems or an aircraft system as a whole.

There is ongoing debate on the setting of appropriate SSR for UAS [20]. Numerous specifications of SSR for UAS have been proposed by EASA [21], NATO [22] and JARUS [23], to name a few. As stated by the Australian Department of Defence [24]:

> *"... The USAR.1309 AMC, for example, which is fundamental to the safety of a UAS, is unsurprisingly an area of evolution and disagreement. After all, manned aircraft Airworthiness Codes have evolved over many decades, based on extensive in-service experience and a relatively stable technology, whereas UAS currently exhibit neither of these attributes."*

[1] While not common, this acronym has been adopted for use throughout this thesis to refer to system safety regulations.

Regulators have already proposed the adoption of a risk-based approach for the regulation of the sector [10]–[15]. Under the risk-based approach, models that comprehensively capture the nature of the risks posed to people and property on the ground guide the development of airworthiness and operational regulations for UAS. A variety of Ground Risk Models (GRM)[2] that analyse and capture these risks were identified in the literature. Of particular interest to this thesis is how these GRM account for uncertainty and its subsequent input to the rule-making process.

1.2. Research Questions

There are a wide variety of new airspace users in the aviation sector. These users are characterised by a lack of operational data, experience, and knowledge arising due to: 1) the relative infancy of the technology, 2) restrictions imposed on their operations, 3) the rapid pace of technology development, and 4) use of commercial-off-the-shelf components [1]. A uniform set of regulations tailored to their operations are required.

Focusing on UAS, regulatory bodies such as FAA, EASA and JARUS have recently recommended the adoption of a risk-based approach for the development of regulations [10]–[15], central to which is the Safety Risk Management Process (SRMP)[3]. Based on a review of relevant aviation safety policy, guidance and regulatory material (*e.g.* [25]–[30]) it was found that aviation safety literature does not adequately address the uncertainty associated with the SRMP. Measures of risk are limited to only likelihood and severity, with uncertainty generally not taken into consideration. Where uncertainty is recognised, conservative worst-case assumptions are used to address them. This can result in the imposition of overly stringent restrictions on systems where there is uncertainty in the safety risk, something characteristic of new airspace users such as UAS. Subsequently, providing a more comprehensive treatment of uncertainty in the aviation SRMP is essential to the uptake of a risk-based approach to rule-making. This leads to the first research question addressed in this thesis:

1. **What are the uncertainties associated with the safety risk assessment process and how are they addressed within the current aviation safety risk management and regulatory development processes?**

To answer this question, it is necessary to identify the general types of uncertainty and how they can be objectively represented in risk assessment processes. In the context of the case study application, GRMs are reviewed to determine the current state-of-the-art, the components that go into defining these models, and the sources and levels of uncertainty associated with them. It is then important to determine

[2] Alternate terms such as Risk Models (RM) have also been used in the literature. To maintain consistency the term GRM has been adopted for use throughout this thesis.

[3] Alternate terms such as Risk Management Process (RMP) have also been used in the literature. To maintain consistency the term SRMP has been adopted for use throughout this thesis.

how these sources of uncertainty can be incorporated into existing GRM and how best to represent them to the decision makers for input to downstream regulatory processes (*i.e.*, compliance assessment and compliance finding). This research question is further divided into the sub-questions:

1.1. What are sources of uncertainty inherent in safety risk assessment processes and how are they being characterised and represented in existing models?

1.2. How can the identified sources of uncertainty be incorporated into existing aviation safety risk management and regulatory development processes?

1.3. How should the risk and uncertainty measures obtained from the regulatory safety risk assessment processes be represented to decision makers and which of these measures best supports regulatory decision making?

Answering the above research question provides regulators with an objective understanding of the uncertainty in safety risk assessments. Under a risk-based regulatory regime, these assessments underpin National Aviation Authorities (NAA) rule-making and compliance processes. Looking at the compliance processes, if assessments of performance are uncertain, then these uncertainties are also inherent in the assessments required to show compliance to regulations. The current aviation compliance process does not provide an objective means for accounting for uncertainty. As a consequence, compliance assessments can be subjective and inconsistent, with regulators lacking the tools and processes to be able to make objective compliance findings on the basis of compliance risk.

The existing notion of risk-based regulation has only been applied to one part of the overall regulatory process, that of developing regulations (rule-making) [25]–[28], [31], [32]. Specifically, how to develop and apply a suitable code of requirements that have traceability to, and are proportionate with, the degree of operational risk posed by a given aircraft system or sub-system. The risk-based principles can also be applied to other regulatory processes including compliance assessment and compliance finding as illustrated in Figure 2.

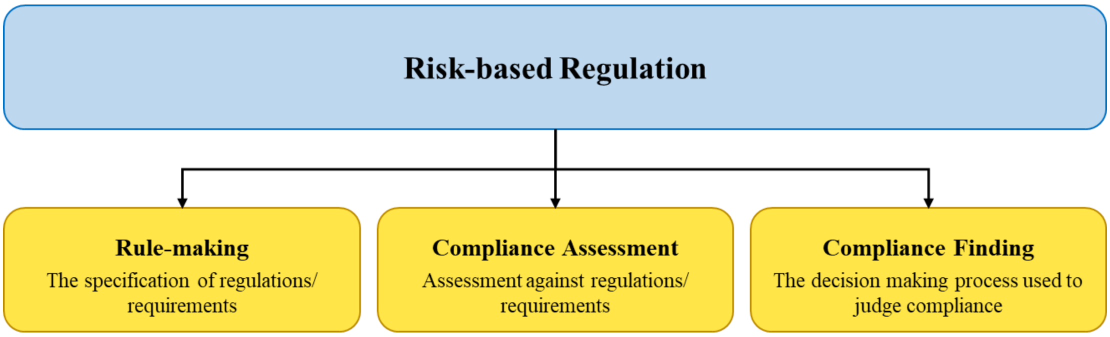

Risk-based Regulation
Rule-making
The specification of regulations/ requirements
Compliance Assessment
Assessment against regulations/ requirements
Compliance Finding
The decision making process used to judge compliance

Figure 2: Components of Risk-based Regulation

The challenge explored in this thesis is how to apply the general principles of risk-based regulation to include the regulatory processes of compliance assessment and compliance finding. Such an extension is necessary to account for the uncertainty inherent in the state of compliance of an aviation system against a specific requirement. Thus, the second question of this thesis is:

2. **How can uncertainty associated with the SRMP be accounted for in existing aviation rule-making and compliance processes?**

Answering this question requires an understanding of the fundamental concepts of risk, uncertainty and decision making, and their application within aviation risk and regulatory processes. This leads to the following sub-questions:

2.1. What are the uncertainties and how are they currently managed in the aviation safety compliance assessment and compliance finding processes?

2.2. How can the uncertainties in these processes be represented and accounted for to support more objective and consistent regulatory outcomes?

2.3. What are some of the potential benefits of the extended risk-based philosophy in the aviation sector?

1.3. Aims and Objectives

The aim of this thesis is to improve regulatory outcomes under the new paradigm of risk-based regulation, through providing a conceptual framework for the rational, transparent and systematic treatment of uncertainty in the risk assessment and regulatory decision-making process. The objectives of this thesis are as follows:

1. To identify and characterise the various sources of uncertainty inherent in risk assessment and decision-making processes and determine how this is currently managed, with application to the aviation regulatory framework;
2. Drawing on contemporary risk and uncertainty theory, to develop a new compliance assessment and compliance finding decision-making process that incorporates the varying sources of uncertainty inherent in them;
3. To apply the above to the regulation of UAS, in particular, the system safety "Part 1309" regulations.

It is posited that the framework proposed in this thesis improves the objectivity, consistency, and transparency of regulatory processes; a paradigm shift in how aviation safety regulators approach risk-based regulation. This research broadens the current understanding of risk-based regulation in the aviation sector. Under the proposed framework, risk-based regulation considers the risks associated with: 1) the specification of regulations or requirements (rule-making), 2) the processes of assessment against regulations or requirements (compliance assessment), and 3) the decision-making process used to judge compliance (compliance finding).

1.4. Scope

The general theoretical concepts and frameworks developed in this thesis are applicable to any regulatory process, however, the scope of application in this thesis is limited to airworthiness regulations (and in particular, SSR) for UAS. Risk models and regulations relating to the operation of UAS in unsegregated airspace are not considered. Whilst the case study of UAS is used in this thesis, it must be emphasised that this approach can be applied more broadly to any aviation regulation or compliance assessment process.

1.5. Significance of Research

In the presence of uncertainty, regulatory authorities tend to adopt a "precautionary approach" [10]–[15] applying overly conservative restrictions that can significantly inhibit UAS operations. Current aviation risk assessment and risk management practices do not provide regulatory authorities with a systematic process for managing uncertainty. As a result, regulatory processes, which are based on outcomes of the SRMP (*i.e.*, rule-making, compliance assessment and compliance finding) can be subjective. On successful completion of this thesis, a novel approach for showing compliance to the SSR will be provided through the development of a new decision-making framework that is capable of taking varying sources of risk and uncertainty into consideration. This will allow for a more rational, transparent and systematic treatment of uncertainty in the risk assessment and regulatory decision-making process and in turn, outcome regulations that are more proportionate to the risks they aim to address.

The outcomes of this research can be potentially employed by NAA worldwide. The extension of the risk-based approach to better account for uncertainty in regulatory processes can be applied to any aviation sector. Thus, this research has the potential to not only help shape regulations for the UAS sector but other aviation sectors in the future. This includes UAM concepts, personal air mobility vehicles and reusable space launch vehicles, to name a few. These industries are similar to the UAS industry as they typically have low data and high uncertainty associated with them.

1.6. Account of Research Progress

The body of this thesis (Chapter 3 through to Chapter 7) comprises of individual journal and conference papers that were authored during the PhD candidature. A list of publications that directly relate to the overall aims and objectives of this thesis has been provided in Table 1 of Section §1.6.1. The linkage between these publications (Section §1.6.2) provides an overall outline of this thesis and allows the reader to get a clear understanding of how, when viewed in conjunction with each other, these papers address the research questions, aims and objectives of this thesis. All these papers are included "as published" without editing. Additional papers were also co-authored during this period; however they have not been included in the main body of the thesis as they do not directly relate to the overall objectives of this thesis.

1.6.1. List of Publications

The body of this thesis comprises of five publications (three journal publications and two full paper peer reviewed conference publications). Each of these papers have already been published. The individual papers form the chapters of this thesis as indicated in Table 1. The publication details are also provided in Table 1. The order in which these papers are presented is based on how they relate to the research questions and not the order in which they were published. This relationship is described in Section§1.6.2. A complete list of all the journal papers, conference papers, conference presentations and technical presentations that are submitted in support of this thesis are included in Appendix A.

Table 1: List of publications

Chapter 3	
Title of Paper	*A Review of Unmanned Aircraft Systems Ground Risk Models*
Authors	Achim Washington, Reece Clothier, Jose Silva
Journal	Progress in Aerospace Sciences
Status	Published
Impact Factor	6.814
Link	https://www.sciencedirect.com/science/article/pii/S0376042117301392
Chapter 4	
Title of Paper	*A Bayesian Approach to System Safety Assessment and Compliance Assessment for Unmanned Aircraft Systems*
Authors	Achim Washington, Reece Clothier, Brendan Williams
Journal	Journal of Air Transport Management
Status	Published
Impact Factor	2.412
Link	https://www.sciencedirect.com/science/article/pii/S0969699716304768
Chapter 5	
Title of Paper	*Managing Uncertainty in the System Safety Assessment of Unmanned Aircraft Systems*
Authors	Achim Washington, Reece Clothier, Brendan Williams, Jose Silva
Conference	17th Australian International Aerospace Congress (AIAC 17), Melbourne, Australia, 27th and 28th February, 2017
Status	Published in proceedings (full paper peer reviewed)
Link	https://search.informit.com.au/documentSummary;res=IELENG;dn=739801934595508
Chapter 6	
Title of Paper	*Adoption of a Bayesian Belief Network for the System Safety Assessment of Remotely Piloted Aircraft Systems*
Authors	Achim Washington, Reece Clothier, Natasha Neogi, Jose Silva, Kelly Hayhurst, Brendan Williams
Journal	Safety Science
Status	Published
Impact Factor	3.619
Link	https://www.sciencedirect.com/science/article/pii/S0925753518312670
Chapter 7	
Title of Paper	*Managing Uncertainty in Unmanned Aircraft System Safety Performance Requirements Compliance Process*
Authors	Achim Washington, Reece Clothier, Jose Silva
Conference	International Conference on Unmanned Aircraft Systems (ICUAS 2018, Amsterdam), 10th and 11th May, 2018
Status	Published in proceedings (full paper peer reviewed)
Link	https://waset.org/publications/10008962/managing-uncertainty-in-unmanned-aircraft-system-safety-performance-requirements-compliance-process

1.6.2. Linkage Between Publications and Thesis Outline

The aviation sector is rapidly evolving with the introduction of a number of new and novel airspace users such as UAS. As with any new technology, there is risk and uncertainty associated with the operation of these systems. In order to ensure that these systems are able to operate alongside their manned counterparts, it is imperative to take this risk and uncertainty into consideration. That brings us to the concept of risk-based regulation.

Achieving risk-based regulation warrants consideration of the uncertainties inherent to the risk assessment and decision-making processes that underpin the regulatory processes of: 1) rule-making, 2) compliance assessment, and 3) compliance finding. The existing notion of risk-based regulation of an aviation sector, however, only addresses the first of these processes. This research broadens the current understanding of risk-based regulation in the aviation sector to include the risks (*i.e.* uncertainty and consequence severities) associated with the compliance assessment and compliance finding regulatory processes. By doing so, the research allows for a risk-based approach to the regulation of a system to be applied to new and evolving technologies such as UAS.

The overall structure of the thesis is provided in Figure 3. The concept of risk-based regulation is outlined in the first two levels of this figure, providing an overview of the regulatory processes of interest for this thesis. The third level of Figure 3 highlights the different theoretical concepts (that form part of the literature review) that are used to get a better understanding of these regulatory process of interest. The review of these theoretical concepts also helps identify the research gaps in the chosen areas of application for this thesis (*i.e.* GRM and SSR), that are highlighted in the fourth level of this figure. This provides a clear indication of the main areas of focus for this research.

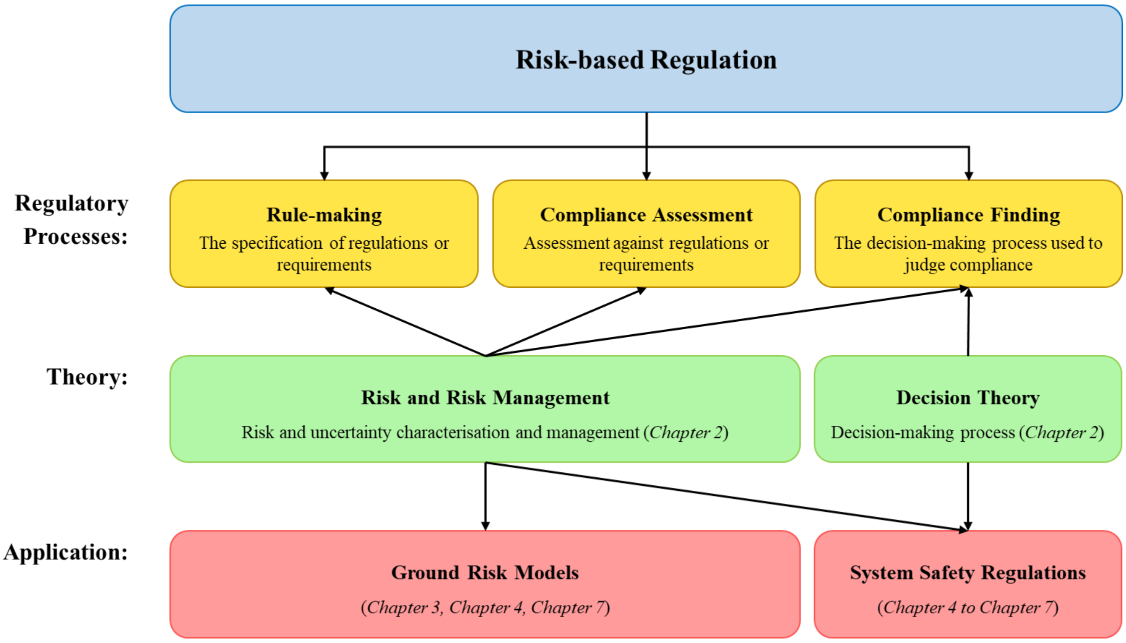

Risk-based Regulation
Regulatory Processes:
Rule-making
The specification of regulations or requirements
Compliance Assessment
Assessment against regulations or requirements
Compliance Finding
The decision-making process used to judge compliance
Theory:
Risk and Risk Management
Risk and uncertainty characterisation and management (Chapter 2)
Decision Theory
Decision-making process (Chapter 2)
Application:
Ground Risk Models
(Chapter 3, Chapter 4, Chapter 7)
System Safety Regulations
(Chapter 4 to Chapter 7)

Figure 3: Linkage between chapters and their collective contributions

Together, these four levels provide a clear linkage between the different chapters of the thesis and show how the research gaps identified through the literature review (Chapter 2) are addressed through the chosen areas of application (Chapter 3 to Chapter 7). The following sub sections provide an in-depth summary of the individual chapters, highlighting the aims and objectives of the chapters; the overall structure of the chapters; and how the aims and objectives of the thesis are met taking the novel contributions of the chapters into consideration. They clearly show how different elements of the research questions are addressed and help highlight the novel contributions of the research. The difference between each of the chapters and the growth and progression between these chapters is also clearly highlighted in these sub sections.

1.6.2.1. Chapter 2: Literature Review

The fundamental theory necessary to understand the overall concept of risk-based regulation is provided in Chapter 2 and summarised in the third level of Figure 3. The gaps in the literature, which led to the development of the research problems and the narrowing of the scope of this thesis were arrived at through the literature review presented in this chapter. The chapter first introduces a number of fundamental concepts including: events and scenarios; hazards; consequences; accidents, incidents and mishaps; and safety (Section §2.1). The concept of uncertainty while also fundamental to understanding the concept of risk, was reviewed in a separate section as it is central to the overall research undertaken (Section §2.2). Understanding each of these fundamental concepts was essential to understanding the overall concept of risk, which in itself was reviewed in great detail (Section §2.3). The final concept that needed to be reviewed before the SRMP could be introduced was decision theory (Section §2.4). This provided the fundamentals necessary to get a better understanding of how decisions can be made, something integral to the SRMP. Once each of these concepts were clearly understood, the SRMP was introduced and explored in detail (Section §2.5). This not only involved conducting an in-depth review of each of the sub-processes that underpin the SRMP (*i.e.* establish the context, risk identification, risk analysis, risk evaluation, risk treatment, communication and consultation and monitor and review) but also understanding the various sources of uncertainty associated with each of these sub-processes and looking at how these sources of uncertainty are taken into consideration. Discussion on the application of the SRMP in the aviation industry is also provided in this section.

The following section then looks to get a better understanding of the concept of risk-based regulation and its application within the aviation sector (Section §2.6). This is particularly important as it not only better helps define the overall problem, but also highlights the shortcomings of the current risk-based approach adopted by the industry. In essence, it is seen that the risk-based principles are only applied to the rule-making process and no uncertainty is taken into consideration in any of the components that go into defining risk-based regulation (rule-making, compliance assessment and compliance finding). On carefully analysing and evaluating these shortcomings it is evident that, the current framework and tools used by the industry cannot be applied to new and evolving technologies such as UAS where there is limited data and high uncertainty. Thus, research needed to be undertaken to not only expand the current understanding of risk-based regulation to include a risk-based approach to compliance assessment and compliance finding but also look at how uncertainty associated with each of these sub-processes can be considered.

Taking the case study example of UAS into consideration, owing to the limited data and high uncertainty associated with these systems, the next section (Section §2.7) then looks to limit the scope of the discussion, as outlined in the fourth level of Figure 3. The various sources of uncertainty associated with UAS are briefly identified, highlighting the need for a framework that is able to take this uncertainty into consideration. In adopting a risk-based approach to the regulation of the industry, it is important to not only understand the risks posed by the system but also how these risks can be evaluated and how decisions can be made based on this risk. Limiting the discussion to UAS, models that comprehensively capture the risks posed by these systems to people and property on the ground are essential to the development of airworthiness and operational requirements. These models are referred to as GRM and form the first area of focus for this thesis (Section §2.7.2). Given the risks are clearly identified, models that are able to manage these risks are then required. This is largely done through the development and promulgation of regulations that provide assurance in the airworthiness of the UAS. Not all UAS types may be required to meet prescriptive codes of airworthiness requirements in order to be safe for operation, however, those that do, will likely be required to show compliance to SSR, also referred to as Part 1309 regulations. This is the second area of focus of this research (Section §2.7.3). It is important here to note that, detailed reviews on both GRM and SSR are provided in the individual chapters where these topics are discussed. In order to avoid repetition, these reviews are not included in this section. The literature review undertaken in this chapter is meant to supplement, rather than replace the literature reviews provided in the individual publications and is needed to provide a better understanding of how each of the publications relate. Throughout the proceeding chapters, these theoretical areas are applied to the regulatory processes of rule-making, compliance assessment and compliance finding. For details, the reader is directed to the individual chapters. The following chapter summaries will look to show how each of the identified research questions are addressed and how together they help achieve the overall aim of this thesis. They aim to address the key challenges involved in the incorporation of uncertainty into the risk analysis and regulatory decision-making processes. As a collection, they broaden the current understanding and scope of risk-based regulation in the aviation sector to include each of the regulatory processes outlined in the second level of Figure 3.

1.6.2.2. Chapter 3: A Review of Unmanned Aircraft Systems Ground Risk Models

As with any new technology, there is a considerable amount of risk and uncertainty associated with the operation of any new system. Before these risks can be evaluated and decisions regarding them made (risk evaluation and risk treatment), it is first important to clearly identify the risks and see how they relate to each other (risk identification). This is part of the risk assessment process, which in itself is divided into the three sub-processes of risk identification, risk analysis and risk evaluation. In the context of UAS, there are two primary hazards of interest: a collision or near collision between a UA and another aircraft (whether the other aircraft is in the air or on the ground) ; and the impact of the UA, or its components, with people or structures situated on the ground [16], [17]. The focus of this chapter and the thesis in general is on the characterisation of the latter of these two hazards. The risks associated with this hazard are identified in the chapter. These risks are largely managed through the development and promulgation of regulations that provide assurance in the airworthiness of the UAS [6]. As described in [6], airworthiness regulations can be combined with operational regulations (*e.g.*, restricting where and when UAS can be operated) to more effectively manage the risks posed to people and property overflown. Under the risk-based approach, models that effectively capture the nature of the risks posed to people and property on the ground (*i.e.* GRM) are essential to the development of airworthiness and operational regulations for UAS.

The objectives of this chapter are thus to: 1) provide a comprehensive review of existing GRM and the component models that go into defining them; 2) describe how these component models and the uncertainty surrounding them impact different elements of the safety regulations for UAS; and 3) identify where future research into the development of models is needed to support the development of effective regulations for UAS. Relating this to the overall objectives of the thesis, it is evident that the paper aims to answer elements of the first research objective, that is, to identify and characterise the various sources of uncertainty inherent in the risk assessment process and determine how this is currently managed, with application to the aviation regulatory framework (Research Objective 1).

The paper starts by first introducing the concept of a GRM and identifying all of the component models (*i.e.* failure model, impact model, recovery model, stress model, exposure model, incident stress model and harm model) that go into defining a GRM. Arriving at this set of component models was in itself the result of an extensive literature review undertaken. In order to understand how the identified GRM and component models identify and manage uncertainty, a framework for systematically describing the treatment of uncertainty in modelling is needed. In this paper, Paté-Cornell's [33] framework for describing the "six levels of treatment of uncertainties in risk analysis" is used to assess how each of the reviewed models manages uncertainty. Identifying the uncertainty and providing a means for managing this uncertainty allows for the setting of appropriate regulations under the risk-based approach to rule-making. Each of the component models were then analysed independently providing: a detailed description of the component model; a review of the literature associated with the component model, highlighting the assumptions made in relation to the component model; a description of how the component model was substantiated in the literature; a summary of how uncertainty is represented in the component model (based on Paté-Cornell's framework [33]); and a clear linkage between the component model and the regulations, highlighting not just the component of the regulations that are affected but also how the associated assumptions and uncertainty impacts these regulations. The paper concludes with some overall findings relating to: 1) the diversity of the models, 2) cascading assumptions; and 3) inadequate treatment of uncertainty and the implications of these findings on the overall GRM and component models.

In providing such an in-depth review of GRM, the paper was able to highlight the sources of uncertainty associated with the safety risk assessment process (Research Question 1.1) and show how they are addressed within the current aviation safety risk management and regulatory development processes (Research Question 1.2). These sources of uncertainty are defined with respect to each component model and then related to the regulatory framework, showing how they are likely to impact the safety risk management and regulatory development processes. By adopting Paté-Cornell's [33] framework to identify the levels of uncertainty accounted for in each of the component models, the paper showcases where additional research efforts need to be directed. The goal is to adopt a Level 5 treatment of uncertainty, where uncertainties about fundamental hypotheses are displayed by a family of risk curves. By clearly highlighting this objective and recognising the limitations associated with the lower levels of treatment of uncertainty in terms of the risk management and regulatory development process, this chapter also addresses elements of Research Question 1.3.

In addition to being one of the first review papers of its kind and proving an in-depth review of the GRM and component models that go into defining them, this paper makes a number of novel contributions to theory. It provides a conceptual framework for describing the component models of GRM, and in turn, providing a general theoretical basis for the systematic development and analysis of models proposed in the literature. In addition to this it also identifies various sources of uncertainty with respect to each of the component models and shows how failing to account for such uncertainties can impact various elements of the regulation. The research lays the foundations necessary to help meet the remaining objectives of the thesis.

1.6.2.3. Chapter 4: A Bayesian Approach to System Safety Assessment and Compliance Assessment for Unmanned Aircraft Systems

As mentioned in Section §1.6.2.1, in order to limit the scope of the discussion and make significant contributions to theory, this chapter and the thesis in general focuses on one part of the regulations, namely the SSR. The SSR or Part 1309 regulations supplement prescriptive design requirements and are put in place to ensure that an aircraft or system is capable of continued safe flight and landing following a failure or multiple failures of systems [19]. At a high level, they specify a number of requirements, the most important for this research being, the System Safety Performance Requirements (SSPR). For further details on the SSR and SSPR, the reader is directed to the individual chapter.

This chapter explores a new approach to the certification of UAS to the Part 1309 regulations, where the system safety compliance process is modelled as a decision-making process under uncertainty. The chapter builds on the literature review conducted in Chapter 2 and Chapter 3 of this thesis to understand the various sources of uncertainty and see how they are currently managed in the compliance assessment and compliance finding processes. The overall aim of this chapter is to improve the objectivity, transparency, and rationality of compliance findings in those cases where there is uncertainty in the assessments of the system. Relating this to the overall objectives of the thesis it is evident that the focus of this chapter is on the second and third research objectives. That is, to draw on contemporary risk and uncertainty theory, to develop a new compliance assessment and compliance finding decision-making process that incorporates the varying sources of uncertainty inherent in them (Research Objective 2) and to apply the above to the regulation of UAS, in particular, the system safety "Part 1309" regulations (Research Objective 3). Elements of the first research objective are also addressed in this chapter.

The chapter first introduces the SSR, identifying the particular requirement of interest for the research, namely, the SSPR. Each of the sub-processes that go into defining the SSPR compliance process, namely, the System Safety Assessment (SSA) process, Compliance Assessment (CA) process and Compliance Finding (CF) process are then described in detail. On critically analysing the Traditional SSPR compliance process, the various sources of uncertainty inherent to the process were identified. Taking the CA and CF decision-making processes into consideration, it was seen that there currently does not exist any means of accounting for the uncertainty in any of the outputs from the SSA process. As such, there is no objective means for expressing the resulting uncertainty in the output state of compliance. In order to address these limitations an Extended SSPR compliance process is then presented in this chapter. The uncertainty in the failure rate (Average Probability of Failure per Flight Hour (APFH)) of the system (one of the outputs of the SSA process) is taken into consideration by adopting a Bayesian analysis approach. This provides a probability distribution representing the uncertainty in the APFH of the system as opposed to a single point estimate. The CA process is then updated to take the uncertainty in this output into consideration. It makes use of a Bayesian hypothesis test to provide the probability of the system meeting the requirements rather than providing a "TRUE or FALSE" output assessment. Finally, a normative approach to decision-making is applied to the CF process. This provides a more rational, transparent and systematic mathematical framework for making compliance findings based on compliance risk. The mathematics and rationale behind the adopted approaches, and a case study example exemplifying the features of the model are also provided in this chapter. For details, the reader is directed to the individual chapter.

By showing how the identified sources of uncertainty can be incorporated into existing aviation safety risk management and regulatory development processes through the adoption of Bayes theorem, Bayesian hypothesis testing and normative decision theory, the research is able to help answer Research

Question 1.2. By clearly identifying how the outputs from the risk assessment process should be represented to the decision maker (*i.e.* as a family of risk curves) and showing how this can be taken into consideration, the research also helps answer Research Question 1.3. The focus of this chapter is however on Research Question 2. The uncertainty inherent in the Traditional SSPR compliance process can lead to inconsistent, subjective, and potentially erroneous regulatory outcomes. This situation arises due the absence of a systematic and objective means for representing uncertainty to decision makers, and a framework that enables decision makers to make rational, logical, transparent, and consistent decisions when faced with uncertainty. By clearly identifying the various sources of uncertainty and how they are currently managed in the aviation safety compliance assessment and compliance finding processes, the research has addressed elements of Research Question 2.1. By providing a means to represent and account for the uncertainties in not just the SSA process, but also the CA and CF processes, this research also helps support more objective and consistent regulatory outcomes, thus helping address Research Question 2.2.

This Extended SSPR compliance process marks a significant step forward compared to the Traditional SSPR compliance process. It provides a means of taking the high uncertainty associated with new and evolving technologies such as UAS into consideration in not only the SSA process, but also the CA and CF decision making processes that follow. With reference to Paté-Cornell's "six levels of treatment of uncertainties" [33]; the revised framework provides for the highest treatment of the uncertainty associated with estimates of one of the outputs of the SSA process, *i.e.*, the APFH. This facilitates a more rational, transparent and systematic compliance approach to decision-making. It directly addresses the second research objective by drawing on contemporary risk and uncertainty theory, to develop a new compliance assessment and compliance finding decision-making process that incorporates the varying sources of uncertainty inherent in them. By focusing on the SSR, the third and final research objective is also considered.

In terms of novel contributions, this research has helped in the development of the overall concept for risk-based assessment and compliance processes, showing how the theoretical concepts described evolve towards a more comprehensive treatment of uncertainty. The potential benefits and challenges associated with this process are also highlighted. In addition to this, the research proposes a new risk-based approach to the regulatory compliance process, through reframing it as a problem of decision-making under uncertainty. This approach developed and demonstrated a mathematically robust approach for accounting for uncertainty in performance/compliance assessments. It also allowed for the systematic treatment of uncertainty in the aviation regulatory compliance assessment and compliance finding processes by the application of a normative decision theory, combined with assessments of the consequence of the different compliance finding outcomes. This provides NAA with a systematic basis for making compliance decisions (findings) on the basis of compliance risk.

While this chapter in conjunction with the previous chapter answers most of the research questions outlined previously, there are a number of assumptions and limitations associated with the Extended SSPR compliance process that have yet to be addressed. Firstly, in relation to the APFH, in accordance with SSA guidance materials, the Extended SSA process makes use of a Poisson failure rate model, which assumes a constant failure rate. Currently, most commercial UAS do not exhibit the constant failure rates typical of mature aviation systems. For small UAS, their changing configuration may mean that they never achieve a stable failure rate. This brings into question the validity of the assumption of a constant failure rate model. Secondly, looking at the Extended SSA process, it can be observed that only the uncertainty in one of the outputs, namely the APFH of the system, is taken into consideration. Additional research needs to be undertaken to show how the uncertainty associated with each of the remaining outputs of the SSA process can also be taken into consideration. The following chapters look to address both of these limitations.

1.6.2.4. Chapter 5: Managing Uncertainty in the System Safety Assessment of Unmanned Aircraft Systems

The Extended SSPR compliance process developed in the previous chapter marks a significant step change over the Traditional SSPR compliance process. Limiting the discussion to the SSA process, the Extended SSPR compliance process provides a means to take the uncertainty in the APFH of the system into consideration through the adoption of a Bayesian analysis approach. While this was an important extension to make, on carefully analysing the output, it was observed that one factor that wasn't taken into consideration is the variable failure rate of the system. In keeping with SSA guidance materials, the Extended SSA process assumes a constant failure rate and makes use of a Poisson failure rate model to represent the likelihood distribution (one of the inputs to the Bayesian analysis process). While this may be suitable for well-established technologies such as manned aircraft that are in the "Useful Life" phase of their life cycle (exhibiting a stable failure rate), the same cannot be said for new and evolving technologies such as UAS. The rapid pace of development of the technology and the use of Commercial-off-the-shelf (COTS) components, creates a constantly changing system baseline for these systems. This in turn means it is difficult to build heritage in a particular configuration of a system. Components are not designed or manufactured to accepted standards. Further, many small UAS are not subject to routine maintenance. The rapid evolution of technology may mean that many UAS types may never achieve a constant failure rate. The main objective of this paper is thus to provide a means to account for this variable failure rate in the Extended framework. Relating this to the overall objectives of the thesis, it is evident that this research aims to address elements of Research Objective 2.

This paper starts by introducing the SSR and outlining the main output of the SSA process that is of interest to this research, namely, the set containing the failure rate estimates for the system. A linkage is then provided to the previous research, describing how the Extended SSA process is able to take the uncertainty in this output into consideration by adopting a Bayesian analysis approach. Following this, the limitation of the constant failure rate is then outlined and a means to take it into consideration proposed. The research proposes the adoption of a Weibull distribution to model the likelihood distribution as it is representative of the “bathtub curve” typically used to model the failure rate of a system. The mathematics behind this is then explored. Finally, a case study is undertaken to highlight the advantages of the approach.

In conjunction with the framework proposed in the previous chapter, this extension has a number of advantages compared to the Traditional SSA process that only provides a point estimate on the failure rate of the system. Firstly, it allows for the variable failure rate associated with new and novel technologies such as UAS to be taken into consideration. This is an important extension to make as it is representative of real-world systems. In addition to this, by adopting a Weibull distribution, the decision maker is provided with further information in relation to the uncertainty of the model. For example, the particular phase of the life-cycle the system is in can be determined with greater certainty using the additional outputs obtained from the model. Finally, by using this model the decision maker is able to make a number of additional inferences (predictions) on the future failure performance of the fleet, something that was not possible using the Traditional approach.

As is evident from the preceding discussion, this chapter aimed at addressing one of the limitations of the Extended SSPR compliance process, *i.e.* the limitation associated with the use of a constant failure rate. The focus of this chapter was thus on Research Question 2.1 and Research Question 2.2. By critically analysing the Extended SSPR compliance process, the research was able to identify an additional source of uncertainty associated with the failure rate of the system that was previously not taken into consideration (*i.e.* the uncertainty associated with the constant failure rate assumption). The research then goes on to show how this uncertainty can be represented and accounted for to support more objective and consistent regulatory outcomes.

In terms of novel contributions, this research builds on the previous chapter, looking to address the limitation associated with the use of a constant failure rate. The research was able to demonstrate how types of model uncertainty can be accounted for in the assessment and compliance processes, something fundamental to the adoption of a risk-based approach to the regulation of the industry.

1.6.2.5. Chapter 6: Adoption of a Bayesian Belief Network for the System Safety Assessment of Remotely Piloted Aircraft Systems

Using the case study example of the SSR, the Extended SSPR compliance process developed in Chapter 4 provided a means of taking the uncertainty in each of the sub-processes that go into defining the SSPR compliance process (*i.e.* the SSA process, CA process and CF process) into consideration. In doing so, it provided a more rational, transparent and systematic means of making compliance findings based on compliance risk, taking uncertainty into consideration. This allowed the framework to be applied to new and novel systems such as UAS that are characterised by limited data and high uncertainty. The research also clearly highlighted the importance of extending the current understanding of risk-based regulation to include a risk-based approach to compliance assessment and compliance finding. While this in itself is a significant novel contribution, as was made evident in Chapter 4, there were a number of shortcomings in the Extended SSPR compliance process that were yet to be addressed. The main objective of this chapter is to provide a means of taking the uncertainty associated with each of the remaining outputs of the SSA process into consideration and show how this can be used to provide additional information to the decision maker, thus allowing for a higher level of treatment of uncertainty, not just in the SSA process, but also the CA and CF decision making processes that follow. It thus addresses Research Objective 2 and helps achieve the overall aim of the thesis.

The paper first introduces the SSR, outlining the overall structure of the Traditional SSPR compliance process. The Extended SSPR compliance process developed in Chapter 4 is then reintroduced to show how uncertainty in this process (in particular the SSA process) is taken into consideration. In order to account for the uncertainty in the remaining outputs of the SSA process, a Proposed SSPR compliance process is then outlined. This framework is then applied to a generic UAS (referred to as RPAS in the chapter) to help identify: a set of failure conditions (which in itself comprises of a set of system-level functions and failure modes); a set of failure condition severity categories; and a set of failure probability objectives (the three remaining outputs from the SSA process). The chapter then goes on to show how the updated output set associated with the APFH can be assessed given this new framework. A Bayesian Belief Network (BBN) is proposed as a suitable tool to model the outputs from the SSA process. The fundamental theory associated with a BBN is outlined and then applied to the framework. Finally, a means to account for the additional data and information (associated with the updated outputs from the SSA process) in the CA process is briefly discussed. The chapter concludes with a hypothetical case study example that exemplifies the features of the model and highlights some of its advantages.

Under the proposed framework it is now possible to associate multiple possible failure condition severities with a given set of failure conditions, and in turn, explore the compliance of the system as a whole in relation to all of its potential consequential outcomes. The generic framework enables the assessment of multiple outcomes for a given system (*e.g.* UAS), system function (*e.g. Propulsion*), or failure condition (*e.g. Propulsion* leading to UDS). Assessments using the proposed framework can be performed using existing techniques, namely Functional Hazard Assessment (FHA), Failure Modes and Effects Analysis (FMEA), Fault Tree Analysis (FTA), *etc*. and the applicable SSR, to specify the output sets for a given UAS and concept of operation. By adopting the BBN within the SSA process, this framework allows for assessments of the APFH to be determined in situations of high uncertainty. Referring to Paté-Cornell’s [33] framework for describing the “six levels of treatment of uncertainties in risk analysis", it is evident that the outputs from the SSA process have evolved from a Level 2 or Level 3 treatment of uncertainty in the Traditional SSA process to a Level 5 treatment of uncertainty in the Proposed SSA process. This in conjunction with the extended CA and CF process allow for the highest level of treatment of uncertainty in the overall SSPR compliance process, thus supporting a risk-based approach to the regulation of the industry.

Being closely related to the Extended SSPR compliance process outlined in Chapter 4, it is evident that the main focus of this chapter was on addressing Research Question 2.1 and Research Question 2.2. The Proposed SSPR compliance process not only highlights the additional sources of uncertainty that were not taken into consideration in the Extended SSPR compliance process, but also shows how these sources of uncertainty can be represented and accounted for in the Proposed SSPR compliance process, through the adoption of a BBN. This allows for the highest level of treatment of uncertainty and shows how this additional data and information can be represented and accounted for in the CA process, thus addressing elements of Research Question 1.3 as well.

In terms of novel contributions, the chapter: develops a general template for high level classification of functions and failures which can be applied to any aircraft system; advocates the adoption of a BBN as a valid approach for capturing uncertainty in the assessed compliance scenario (this removes the requirement for assessing single credible (often worst-case) scenarios, thus extending compliance scenarios to multiple assessments); and is the first to apply a BBN within an aviation SSR "Part 1309" system safety context.

1.6.2.6. Chapter 7: Managing Uncertainty in Unmanned Aircraft System Safety Performance Requirements Compliance Process

This chapter links together all of the work undertaken from Chapter 4 through to Chapter 6. The overall aim is to highlight the challenges associated with the application of the Traditional SSPR compliance process to new and evolving systems such as UAS and summarise the advantages associated with the Extended and Proposed SSPR compliance process. In doing so, the research helps fortify the research undertaken in Chapter 4 to Chapter 6 and thus helps address elements of Research Objective 2.

The chapter starts by providing a brief overview of the SSR, focusing the discussion on the SSPR compliance process. The Traditional SSPR compliance process is outlined, highlighting the limitations of this process. Following this, the challenges associated with the application of this process to the system safety certification of UAS are then explored. Discussion on the differences between UAS and CPA is also provided to better understand the limitations of applying the Traditional SSPR compliance process to new and evolving technologies such as UAS. By relating the identified challenges to the limitations of the Traditional SSPR compliance process, the paper clearly identifies the various gaps in the literature that exist and shows how the Extended and Proposed SSPR compliance processes look to address these gaps. The Extended SSPR compliance process is then outlined, with the various outputs identified and the general advantages of this process described. The direction of future research efforts is also provided.

In general, the paper provides a top-level view of the overall research problem and clearly outlines the overall concept of risk-based assessment and compliance decision-making processes, showing how the theoretical concepts described in previous chapters evolve towards a more comprehensive treatment of uncertainty. The paper concludes that a more comprehensive treatment of uncertainty (as proposed by the research undertaken in this thesis) has the potential to result in more rational, transparent and systematic outcomes from the regulatory process, particularly for new or novel aviation systems such as UAM concepts, personal air mobility vehicles, reusable space launch vehicles, and UAS. By clearly outlining the limitations of the current approach and the benefits of the extended framework, the research directly answers Research Question 2.3.

While this chapter does not make any novel contributions of its own, it was essential in laying out the overall research problems, as well as in presenting a holistic overview of all the steps associated thereof. In addition to this, it highlights the need for the research undertaken in each of the previous chapters by clearly outlining the overall limitations associated with the Traditional SSPR compliance process and its application to the system safety certification of UAS.

2. Literature Review

Figure 4: Northrop Grumman RQ-4 Global Hawk Model at Avalon Air Show
Image copyright © Achim Washington

"This report by its very length, defends itself against the risk of being read"

Winston Churchill (1874-1965)

This literature review explores the fundamental theoretical concepts underpinning risk-based regulation, and its application in aviation safety frameworks (Figure 3). The review is divided into eight sections. The first section, Section §2.1, introduces the basic theoretical concepts fundamental to risk. The concept of uncertainty is then explored in Section §2.2. Next, Section §2.3 defines the concept of risk and highlights the different approaches used to measure risk. Section §2.4 then briefly introduces the concept of decision theory. Each of these concepts are related to the Safety Risk Management Process (SRMP) in Section §2.5. This section also provides an overview of the general SRMP, identifying the various sources of uncertainty inherent in the process. The concept of risk-based regulation is then introduced in Section §2.6. This is then related to the case study application of the System Safety Regulation (SSR) of Unmanned Aircraft Systems (UAS) in Section §2.7. Finally, Section §2.8 provides an overall summary of the literature review, showing how it helped arrive at the primary research questions. A critical analysis of the literature along with main findings made in relation to the literature are provided in this section.

2.1. Fundamental Concepts

This section provides a summary of the fundamental concepts necessary to understand the overall concept of risk. As will be observed through the course of this section, no single set of definitions of any of the fundamental concepts is widely accepted in the literature. The primary objective of this thesis is not to propose new definitions, rather to get an understanding of the fundamental concepts and their use within an aviation safety context.

2.1.1. Event and Scenario

Ayyub [34] defines an event as an "occurrence or outcome or change of a particular set of circumstances". An event, in its most general sense, can be considered as a change in the state of a system or its environment. Here, a system is defined as "a group of interacting, interrelated, or interdependent elements, such as people, property, materials, environment, and processes" [34]. In the context of aviation safety, the FAA [35] defines an event as "an internal or external occurrence that has its origin distinct from the airplane". These occurrences can include atmospheric conditions, runway conditions, cabin and baggage fires, *etc.* but does not include deliberate acts of sabotage [35].

Ayyub [36] initially defines a scenario as "a hypothetical sequence of events that are constructed to focus attention on causal processes and decision points or nodes". Ayyub later goes on to define a scenario as "joint events and system state(s) that lead to an outcome of interest" or "joint occurrence of events following a particular order or sequence in occurrence" [34]. Clothier [37] further defines a scenario by the measures of two key fundamental properties of the modern world, namely loss and likelihood. Other similar definitions can be found in [34], [38], [39]. Taking all these into consideration, a scenario can simply be defined as a sequence of events that has the potential to lead to an undesirable outcome. A scenario is a complete description of a sequence of events inclusive of potential consequential outcomes and its initiating cause(s).

2.1.2. Hazard

A hazard is part of the specification of a scenario; it is the condition for loss or harm. Numerous definitions for hazard have been proposed in the literature [25], [26], [44]–[46], [27], [28], [34], [35], [40]–[43]. While a hazard is quite closely related to the concept of risk and is often used in the definition of risk, it is important to understand how it differentiates from risk. A hazard simply exists as a source, while a risk includes the likelihood of conversion of that source into actual delivery of loss, injury or some form of damage [38].

On review of some of the definitions of a hazard (Table 2), it was observed that there are three main components to a definition of a hazard. These are expressions of 1) condition, 2) potential and 3) harm. While some definitions provide more details of the "condition" (e.g. [34], [40]) others may focus on defining the “harm” (e.g. [25], [47]–[49]). For the purpose of this thesis, the definition provided by ICAO [25] will be used. According to ICAO [25], a hazard is “a condition or an object with the potential to cause injuries to personnel, damage to equipment or structures, loss of material, or reduction of ability to perform a prescribed function”.

A hazard is not necessarily damaging or a negative component of a system. A hazard damage potential is only a safety concern when it interfaces with the operation of the system aimed at service delivery [25]. Clothier [37] identifies four different types of hazard: exogenous, endogenous, system-exclusive or environmental-exclusive depending on how each of its components (*i.e.* stress, strength and loss) are defined in relation to the boundary of the system of interest.

Table 2: Common definitions of a hazard focusing on the condition and harm

Definitions focused on the “condition”	
• A source of potential harm or a condition, which may result from an external cause (e.g., earthquake, food, or human agency) or an internal vulnerability, with the potential to initiate a failure mode. It is a situation with a potential to cause loss, that is, a risk source.	[34]
• A hazard is a present condition, event, object, or circumstance that could lead to or contribute to an unplanned or undesired event such as an accident.	[40]
Definitions focused on the “harm”	
• A condition or an object with the potential to cause injuries to personnel, damage to equipment or structures, loss of material, or reduction of ability to perform a prescribed function.	[25]
• A real or potential condition that could lead to an unplanned event or series of events (*i.e.* mishap) resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.	[47]
• Any real or potential condition that may result in injury, illness, death to personnel, damage to the environment, business interruption or loss of assets.	[49]
• Any real or potential condition that can cause degradation, injury, illness, death or damage to or loss of equipment or property.	[48]

2.1.3. Consequence

The realisation of a hazard can have more than one consequence associated with it, which can be expressed qualitatively or quantitatively and have positive or negative connotations [50]. A consequence can simply be defined as the “outcome of an event” [50]. The definitions provided in [34], [42] provide varying levels of detail in relation to the outcome, nature of harm and how this outcome relates to the initiating event. Other definitions of a consequence can also be found in [28], [46], [51],

[52] where terms such as “adverse effects”, “unknown” or “undesired”, “undesirable outcome” and “loss” of something of “value” are used to describe a consequence.

One of the most difficult and debated steps in determining the risk associated with a system can be quantification of the consequences and severities. The type and scale used to define harm is determined by the objectives and values of stakeholders involved in the SRMP. Often the type of harm and measurement can be subjective. While placing a cost on property is easy enough, consequences such as, the loss of human life and damage to the environment are not as easily quantified [34]. According to Clothier [37], arriving at a clear and uniform understanding of the type and degree of loss is a subjective process that depends on the values held by an individual or the community at large. An objective specification of consequence is important as it is found that risk-decisions are often more influenced by consequence rather than by overall risk, which over time could have a negative impact on how we live our lives [53]. As put by Bernstein [54], while “the risk-averse make choices based on the consequences without regard to the probability involved … the foolhardy make choices based on the probability on an outcome without regard to its consequences’’. To get a more accurate representation of risk one must consider both, the extent of harm and the probability of the event.

According to ICAO [25], a consequence is “the potential outcome (or outcomes) of a hazard”. The damaging potential of a hazard only materialises through one or more consequences [25]. This can relate to people, property, financial damage, environmental damage, corporate reputation, *etc.* Assuming a consequence occurs, the severity of occurrence can range from negligible to catastrophic [25]. These classifications can vary based on the type of loss, the industry and the regulatory body.

2.1.4. Accident, Incident and Mishap

Accidents, incidents and mishaps are three specific types of events that are often used interchangeably in the literature but are intended to better describe the type and level of detrimental outcome, loss or consequence associated with an event. A list of some definitions identified in the literature is provided in Table 3. As can be observed from Table 3, there is no consensus in defining these terms. For the purposes of this thesis, definitions such as those presented by ICAO [55] and FAA [56] are used.

The term accident describes an event of a specific level of loss (usually the highest) degree of loss or consequential outcome possible. The severity of this event is a measure of the degree of its seriousness in terms of the extent of injury or death resulting from the accident [57]. Examples of common definitions include [26], [42], [46], [56]–[58]. Definitions used within the aviation safety literature can be found in [3], [25], [26], [28]. The general definition used in this thesis is provided by the ICAO [55]:

“*An occurrence associated with the operation of an aircraft which, in the case of a manned aircraft, takes place between the time any person boards the aircraft with the intention of flight until* *such time as all such persons have disembarked, or in the case of an unmanned aircraft, takes place between the time the aircraft is ready to move with the purpose of flight until such time as it comes to rest at the end of the flight and the primary propulsion system is shut down, in which ... A person is fatally or seriously injured, ... the aircraft sustains damage or structural failure ... the aircraft is missing or is completely inaccessible*."

Like an accident, an incident is another event defining a lesser degree of consequence. Examples of common definitions used to describe an incident are provided in Table 3. Definitions based on aviation safety literature can be found in [28], [55], [56]. The general definition used in this thesis is provided by the FAA [56] and is defined as:

"*… a near miss accident with minor consequences that could have resulted in greater loss. ... an unplanned event that could have resulted in an accident, or did result in minor damage, and which indicates the existence of, though may not define, a hazard or hazardous condition*."

Common definitions of a mishap are provided by [47], [56]. While the degree of loss varies between these definitions, they generally describe it as a condition that results in varying levels of loss.

Table 3: Common definitions of an accident, incident and mishap

Accident	
• An undesired and unplanned (but not necessarily unexpected) event that results in (at least) a specified level of loss.	[46]
• An unintended event, or sequence of events, that causes harm.	[42]
• An external event that could directly lead to death or injury.	[57]
• An unplanned fortuitous event that results in harm.	[56]
Incident	
• An event that, under slightly different circumstances, could have been an accident.	[59]
• The occurrence of a hazard that might have progressed to an accident, but did not.	[42]
• An event that involves no loss (or only minor loss) but with the potential for loss under different circumstance.	[46]
• An occurrence, other than an accident, associated with the operation of an aircraft which affects or could affect the safety of operation.	[55]
Mishap	
• An event or series of events resulting in unintentional death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.	[47]
• A source of irritation, annoyance, grievance, nuisance, vexation, mortification … a minor accident.	[56]

2.1.5. Safety

Williams [45] states that human nature, personality and perception are very much involved with one's accepted definition of the word 'safe'. Williams [45] further goes on to state that while safe is often taken as the reciprocal of a magnitude of a risk, safety is not merely dependent on risk but is a compromise between risk, cost, and benefit. Taking this into consideration, it poses the question of whether safety is truly the antonym of risk and whether absolute safety truly relates to zero risk [60]. Jardine *et al* [61], Williams [45], Moller [62] and Moller *et al.* [60] provide some insight into these concepts and help define what constitutes a safe condition.

The definitions of safety are generally divided into two distinct groups, namely, absolute safety and relative safety. These two interpretations are perhaps best described by Moeller [62] through the use of a simple example relating to the question, "is my car safe?". One way to answer this question, which highlights the concept of absolute safety, is "No, since there is always a risk of being in an accident" [62]. An alternate answer, that which highlights a relative concept of safety is "Yes, the car is safe, since the risk of an accident in this car is low, and the latest safety features it comes equipped with also minimize the risk of a severe damage in case of an accident" [62]. Both interpretations are justified, and it is only how one perceives the risk associated with the event and how much they deem acceptable that distinguishes the two. The absolute definition of safety implies that the risk is completely eliminated. The relative interpretation is based on the assumption that the risk can be reduced or controlled to an acceptable level in accordance with an agreed set of management principles (*e.g.* As Low As Reasonably Practicable (ALARP) and So Far As Reasonably Practicable (SFARP) frameworks). Table 4 provides a summary of some common definitions used to describe absolute safety and relative safety. Definitions based on aviation safety literature can be found in [3], [25], [26], [28].

While in an ideal world, absolute safety would be the condition one would want to strive towards, such conditions are generally impossible to achieve. According to ICAO [25], "while the elimination of accidents and/or serious incidents and the achievement of absolute control is certainly desirable, they are unachievable goals in open and dynamic operational contexts". Uncertainty is inherent and inescapable in all real world systems, therefore there will always be some risk associated with any action or event.

Aviation safety frameworks adopt a relative concept of safety, for example ICAO [3], FAA [26], CAA [63], CASA [28] DASA [64]. Here safety is the outcome of a risk management process, whereby an identified risk has been reduced to an accepted or tolerable level, where the process of managing the risk is consistent with a defined set of risk management principles. Examples of such management principles include the ALARP and SFARP frameworks [65]. For details on these frameworks used in aviation safety literature refer to [66]–[69].

Table 4: Common definitions of absolute and relative safety

Absolute Safety	
• The conservation of human life and its effectiveness, and the prevention of damage to items, consistent with mission requirements	[62]
• Freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment	[44]
• A property of a system, whereby it does not produce or encourage accidents.	[58]
Relative Safety	
• A state in which the possibility of harm to persons or of property damage is reduced to, and maintained at or below, an acceptable level through a continuing process of hazard identification and safety risk management	[3]
• A system can be considered safe if risk has been demonstrated to have been reduced to a level that is ALARP (As Low as Reasonably Possible) and broadly acceptable or tolerable, and relevant prescriptive safety requirements have been met, for a system in a given application in a given operating environment.	[42]
• The state in which the risk of harm to persons or property damage is acceptable.	[26]
• The state in which the probability of harm to persons or property is reduced to, and maintained at, a level which is as low as reasonably practicable through a continuing process of hazard identification and risk management.	[28]

2.1.6. Summary

There is considerable diversity in the definition of fundamental risk concepts, a finding also made in [37], [51], [60], [70]. According to Covello and Merkhofer [52], the cause of this conflicting array of concepts is the result of the fragmented way in which the field has developed. Arriving at a clear and concise understanding of these concepts is imperative to understanding the overall concept of risk and to taking the uncertainty associated with each of these concepts into consideration. The review presents a diverse array of definitions of fundamental theoretical concepts presented in safety literature. For the purposes of this thesis, those definitions prevalent in aviation safety literature are used (refer to the sub-sections for detail). A consolidation of concepts is a separate area of research.

2.2. The Concept of Uncertainty

There are numerous perspectives on the meaning of uncertainty. Dezfuli et al. [71] states that uncertainty is a “state of knowledge”, where knowledge is defined as something that is “known from gathered information” [71]. Ayyub [36] defines uncertainty as “knowledge incompleteness due to inherent deficiencies with acquired knowledge”, while Aven [50] states that uncertainty reflects a “lack of knowledge about the performance of a system (the ‘world’), and observable quantities in particular”. Summarising these points of view, uncertainty can be considered as “the state of deficiency in information” [34]. It is “a component of ignorance” which is nothing but “deficiency in knowledge” and suggests a “complete or partial deficiency in understanding or knowledge of an event, its consequence, or likelihood” [34].

2.2.1. Types of Uncertainty

A number of different classifications of uncertainty exist in the literature, including those provided by Wynne [72], Knight [73], van Asselt and Rotmans [74]**,** Walker et al. [75] and Ayyub [76]. van Asselt and Rotmans [74] distinguishes between uncertainties due to lack of knowledge and those arising due to the inherent variability of nature [77]. Walker et al. [75] distinguish between location, levels, and nature of uncertainty. For details on each, the reader is directed to [75]. The latter of these three classifies uncertainty on the basis of source into: epistemic and ontological uncertainties. This classification is similar to the approach presented by van Asselt and Rotmans [74]. Ayyub [76] presents yet another approach to classifying uncertainty, where uncertainty is classified on the basis of source into three types: Ambiguity, Approximation and Likelihood. For details on each, the reader is directed to [76].

The most widely used approach identified in the literature (*e.g.* [34], [71], [74]–[76]) to classify uncertainty, divides uncertainty into two types: aleatory and epistemic [34], [71]. Uncertainty arising through variation in measurable phenomena is classified as aleatory uncertainty and uncertainty due to a lack of our understanding of the physical phenomena being studied is classified as epistemic uncertainty [34], [77].

2.2.1.1. Aleatory Uncertainty

Aleatory uncertainty relates to “stochastic (non-deterministic) events” [71]. It is “the inherent, random, or non-reducible uncertainty” and may be described through the use of objective or classical frequency-based probability measures [33], [34]. It represents the “randomness” or “variability in samples” inherent in the system that cannot be reduced by further observations but is acknowledged and integrated into mathematical models [33].

2.2.1.2. Epistemic Uncertainty

Epistemic uncertainty pertains to “the degree of knowledge of models and their parameters” [71]. It is “the knowledge-based, subjective uncertainty that can be reduced with the collection of data or attainment of additional knowledge” and can be described by subjective probability measures [34]. Epistemic uncertainties represent fundamental uncertainties and are often “ignored and tend to be under-reported” [33]. They are particularly significant in those situations where the evidence base is small [33]. They are more difficult to treat than aleatory uncertainties as they stem from incomplete knowledge about fundamental phenomena [33] but can be reduced with further information (*e.g.*, via observation) of the system.

Both aleatory and epistemic types of uncertainty are inherent to the SRMP, which is further discussed in Section §2.5.

2.2.2. Sources of Uncertainty

Epistemic and aleatory uncertainties are an inherent and inescapable part of the modelling and assessment of any real-world system and can arise from a number of different sources.

Aven [78] associates aleatory and epistemic uncertainty in relation to the inputs, model, outputs (including parameters of interest) and the decision criteria.

Riesch [77] and Spiegelhalter and Riesch [79] identify uncertainties relating to: the outputs (*e.g.* due to the essential unpredictability of events); parameters (*e.g.* due to limitations of information or simply lack of empirical information); model (*e.g.* due to the choice of alternate model structures based on limited knowledge about the extent to which each competing model reflects reality); acknowledged inadequacies (*e.g.* due to limitations in the model representing the real world, which may arise due to omission of some known aspects, extrapolations from data or limitations in computations); and unknown inadequacies (*e.g.* due to ignorance and unknown limitations in understanding).

Ayyub [36] identifies a number of sources of uncertainty relating to the model and the engineering system from which it is abstracted. The analyst creates a model from this abstraction. Following this, decisions regarding what aspects should or should not be included in the model must be made by the analyst. This is a subjective process [36] and includes uncertainty in both the aspects that are abstracted and not abstracted. These include ambiguity, approximations, and likelihood. Uncertainty relating to unknown aspects of the system that can exist due to blind ignorance also need to be taken into consideration [36]. Donald Rumsfeld [80] refers to this uncertainty as ‘‘unknown unknowns’’ or “things we do not even know what we don’t know”. In engineering and science, decisions are commonly based on expert judgements. “Experts render subjective opinions based on existing knowledge and information available to them” [81]. There is uncertainty inherent in the use of expert judgement, including conflicting or confusing opinions, that need to be taken into consideration [36].

Macgill and Siu [82] identify uncertainty inherent in the use of probability as a measure of risk. Unless probability has a value of zero or one, there is uncertainty about whether an event or outcome will actually occur. This uncertainty can also result from imprecision due to either rounding errors or the use of misleading specificity and distortion [82].

The various sources described above can be summarised as shown in Table 5. There is uncertainty that exists in the engineering system being modelled and the model itself, which is an abstraction of the engineering system [36], [49], [77]–[79], [82]. Focusing on the model, it is clear that there is uncertainty in the inputs (data and parameters) and outputs to the model [49], [77]–[79]. Owing to the lack of data, expert judgement and assumptions are often used at various stages of the model. These are other major sources of uncertainty prevalent in some models that need to be accounted for [36], [49], [77], [79]. Finally, there are unknown inadequacies in the model that can influence most models [36], [77], [79]. It is important to recognise their existence. Aven [78], Spiegelhalter and Riesch [79], Riesch [77], Ayyub [36], Macgill and Siu [82] and Zio and Pedroni [49] focus on different sources, providing detailed descriptions on the sources acknowledged. The above sources of uncertainty are relevant to the SRMP, which makes use of a wide range of data sources, models, and abstractions of real-world systems (discussed further in Section §2.5).

Table 5: Summary of sources of uncertainty

		Reference				
		Aven [78]	Spiegelhalter and Riesch [79] and Riesch [77]	Ayyub [36]	Macgill and Siu [82]	Zio and Pedroni [49]
Source of uncertainty	Input and data	✓	✓			✓
	Model and engineering system	✓	✓	✓	✓	✓
	Output	✓	✓			
	Decision criteria	✓				
	Acknowledged inadequacies		✓			
	Unknown inadequacies		✓	✓		
	Expert judgements			✓		✓

2.2.3. Measuring Uncertainty

While uncertainty can be measured in a variety of ways [78], [83], [84], it is generally measured through the use of probability theory [83]. Probability and probability calculus are often considered to be "the sole means for expressing uncertainty" [50], [62]. Probability theory measures uncertainties by the probabilities associated with events [84], where an event is defined as an "occurrence or outcome or change of a particular set of circumstances" [34] and "corresponds to any of the possible states a physical system can assume, or any of the possible predictions of a model describing the system" [84]. According to Ayyub [34], the term probability has a precise mathematical definition but when used to represent uncertainties it is subject to two different interpretations: that of the Frequentist (objective or classical interpretation), and the Bayesian (subjective interpretation) [34], [85].

2.2.3.1. Frequentist Interpretation

The Frequentist school embodies classical statistical thinking and considers probability as a "true property of nature" [86] or "a property of the external world" [62] that can be measured objectively. It considers the probability of an event to be the frequency with which it would occur in a long series of similar trials [34]. "More precisely, it is the value to which the long-run frequency would converge as the number of experiments increases toward infinity" [52]. This approach is based on the "Law of Large Numbers" [52], according to which, if independent trials with the same probability of outcomes are repeated, the average value of the trials converges to the expected value. In other words, in the long run, given the above assumptions, actual value converges to the expected value [62]. One of the main advantages of the Frequentist approach is that "it involves only objective treatment of statistical samples" [33]. It is based on well-known principles of statistical inference that makes use of empirical data and empirically validated models [52], [83]. The limitations of this approach is that it only takes aleatory uncertainties into account and cannot be applied when the data is insufficient [33], [52]. This can be problematic for complex systems where epistemic uncertainty is high and in situations where data is scarce, *e.g.* for the risk analysis of UAS that have low data and high uncertainty associated with them.

2.2.3.2. Bayesian Interpretation

According to the Bayesian school probability is "the rational degree of belief that one holds in the occurrence of an event" [34]. This is based on the concept of subjective probabilities; where probability is interpreted as "a number, expressing a state of knowledge or degree of belief that depends on the information, experience, and theories of the individual who assigns it" [52]. It is viewed as "a function not only of the event, but of the state of information. Different people may assign different probabilities and the probability assigned by any one person may change over time as new information is acquired" [52]. Probability quantifies the state of knowledge and represents the plausibility of an event or hypothesis [71]. Although subjective probabilities are judgmental in nature they are by no means arbitrary. They need to satisfy the same basic axioms as those in classical probability theory [52].

The Bayesian approach uses both objective and subjective information to estimate probabilities, which are "conceived of as representing all aspects of a decision-maker's lack of knowledge" [62]. The fact that it is capable of taking both objective and subjective measures of uncertainty into consideration [86] is one of the main advantages of this approach. In contrast to the Frequentist approach, the Bayesian approach can be used when data is scarce [83] and can take both epistemic and aleatory uncertainties into consideration [33]. Furthermore, its use also allows the analyst to make use of all the available information to allow for better parameter estimation and improved decision making [33], [71].

Due to the advantages above, the Bayesian approach has been used in a number of industries to evaluate and represent uncertainty. This includes: the space launch industry [87]–[92], nuclear power industry [93]–[97], fishery industry [98], ecological management industry [99]–[101] and bio management industry [102], [103], to name a few. Bayesian analysis techniques have also been applied in the field of aviation safety in the past. Specifically, through the use of a Bayesian Belief Network (BBN) to model accident causation, human-system interaction, and safety risks [104]–[106].

There are a number of concepts and tools that are fundamental to this Bayesian interpretation, such as, Bayes Theorem, Bayesian Credible Intervals, Bayesian hypothesis Testing and BBN. These concepts and tools are used throughout the thesis, in each of the individual chapters. A brief description of them is provided in Appendix D. For further details, the reader is directed to the individual references.

2.2.4. Summary

Based on the review conducted in this section, it is evident that there are two main types of uncertainty: epistemic uncertainty and aleatory uncertainty. This uncertainty can arise from a number of different sources as outlined in Table 5. In measuring uncertainty, the simplest and most common approach is through the use of probability theory [83]. Central to this is probability, which when applied to the representation of uncertainties, is subject to differing interpretations: that of the Frequentist (objective or classical interpretation), and the Bayesian (subjective interpretation) [34], [85]. In the context of risk, uncertainty would relate to both components of risk, *i.e.*, likelihood and magnitude of loss or severity. Bayesian methods are identified as the contemporary approach for representing uncertainty.

2.3. The Concept of Risk

A diverse array of definitions of risk are identified in the literature, some of which are summarised in Table 14 of Appendix C. In contrast to a hazard that simply exists as a source, a risk includes the likelihood of conversion of that source into actual delivery of loss, injury or some form of damage [38]. This section will provide a summary of some of the major definitions of risk (including those accepted in aviation safety literature) and their measurement (Table 15 of Appendix C).

2.3.1. Definitions of Risk

There is a negative connotation associated with risk and thus risk can be considered as “something that people fear or regard as negative” [107]. Based on an extensive review, Moller [62] describes three basic approaches to defining risk, specifically: the scientific, psychological and cultural approaches. While recognising the relevance of both the psychological approach and the cultural approach, the focus of this study remains on the scientific approach to risk as used in aviation safety literature. The scientific or "objective" perspective considers risk to be a phenomenon that can be consistently studied and measured through the use of statistical and probabilistic tools. For further details on the other two approaches the reader is directed to [62].

On reviewing existing definitions of “objective risk” (*e.g.* [34], [38], [42], [47], [52], [62], [83], [107]), it is clear that there are two elements implicit in the concept of “objective risk”. Firstly, for risk to exist there must be “a potential source of damage or loss *i.e.* a hazard (threat) to a “target”, such as people or the environment” [49]. Secondly, there must be “uncertainty that the hazard translates from potential to actual damage, bypassing safeguards and protections” [83]. Risk exists when “there is the chance, but not the certainty” that something undesirable may happen [52]. These elements can further be broken down to include event or scenario, probability, consequence and uncertainty.

In keeping with the two elements described above, Covello & Merkhofer [52] specify three conditions that need to be satisfied for a risk to exist. These include: a source of risk to introduce the risk agent into the system, an exposure process through which “people or the things they value may be exposed to the released risk agent” and a causal process by means of which exposures produce adverse consequences [52]. Each of these conditions can be viewed as “links in a risk chain” [108]. The quantification of risk requires the quantification of knowledge and uncertainty about each link in this chain [52]. There is no risk if any of these elements are absent [52].

Definitions such as [53], [86], [109] (Equation 1 to Equation 3 in Table 15 of Appendix C) define risk in terms of two components, probability and consequence. Kaplan and Garrick [38] provide the “triplet definition of risk”, which is widely accepted as a technical definition of risk (Equation 4 in Table 15 of Appendix C). Kaplan and Garrick [38] went on to make several advancements to this definition as can be seen in Equation 5 and Equation 6 in Table 15 of Appendix C, with the latter definition taking uncertainty into consideration. Other contemporary definitions of risk provided by Ayyub (Equation 7 in Table 15 of Appendix C) [34] and Aven (Equation 8 through to Equation 13 in Table 15 of Appendix C) [110] also include measures of uncertainty in the measures of risk. These definitions are however significantly more complicated. While going into such detail is only likely to strengthen the treatment of uncertainty within risk management processes, their complexity can make them difficult to apply in practical risk management settings.

In its vernacular and broadest sense, risk has been the subject of much discussion, and literature on the topic is abundant [25]. The definitions provided in Table 14 and Table 15 of Appendix C are only some of the many definitions of risk identified in the literature. The vernacular use of the term is too frequent, quite generic and generally vague, which is a potential source of confusion [25]. ICAO [25] suggests the use of a narrower term, “safety risk” to address some of this confusion, distinguishing the term and limiting its scope.

2.3.2. Measurement of Risk

The literature review identified two common elements to most definitions of risk as being: probability and consequence (outcomes) (*e.g.* [53], [86], [109]). Severity is generally used to characterise the consequences [110]. A third element, an event (initiating event or scenario) (*e.g.* [38], [83]) is also often included in most definitions of risk. Uncertainty is not as common, but is identified in a number of contemporary definitions of risk (*e.g.* [34], [38], [110]) and is often expressed through probabilities [110]. There are thus four elements that need to be taken into consideration: event or scenario, probability, consequence and uncertainty. A number of approaches to measure each of these elements currently exist. In addition, there are a variety of methods used to combine these elements. To measure risk, we must assess its defining components, and measure the chance, its negativity and potential rewards or benefits [34].

The definitions of risk often make use of the term frequency instead of probability. According to Kaplan and Garrick [38], probability and frequency are two distinct terms. While probability is a numerical measure of a state of knowledge, a degree of belief or a state of confidence, frequency refers to the outcome of an experiment involving repeated trials. Probability (and frequency) can be measured in several ways. Nilsen and Aven [86] identify three distinct approaches to measure probability: the traditional approach (based on principles and methods of classical statistics), the classical approach with uncertainty analysis (also referred to as the probability of frequency framework) and the predictive Bayesian approach. These interpretations fall under the Frequentist interpretation and the Bayesian interpretation described in Section §2.2.3. The latter interpretation is more suitable for systems with limited operational data and unique operating conditions [86].

Each failure of a system can have one or more consequences associated with it [34]. In many applications, it is appropriate to identify different types of damage or consequence [38]. In these cases, damage can be regarded as a multidimensional or vector quantity. These consequences can be in the form of financial loss, property damage, environmental damage and injury or fatality of human life. The MIL-STD-882E [47] defines loss in terms of damage to people, equipment or property, or the environment. These types of loss define the different domains of consequence [17]. They are quantified in terms of failure-consequence severities and make use of relative or absolute measures for various consequence types to facilitate risk analysis [34].

In the engineering context, risk is often linked to the expected loss. However, this equates situations with high consequence and low probabilities to situations with low consequence but high probabilities, as long as the sums of the products of the possible outcomes and the associated probabilities are equal [110]. As described by Faber [109], the risk associated with an activity with only one event with potential consequences is the probability that this event will occur multiplied with the consequence, given the event occurs. Based on this approach to measuring risk, “if the likelihood of an accident increases, so does the risk; likewise, if the severity of an outcome increases, so does the magnitude of the risk" [62]. According to Kaplan, it would be more accurate to measure risk as "probability and consequence" [38], this is in keeping with the ways risk is most commonly measured in standards and in scientific literature [110]. Examples of this approach can be found in [34], [38], [51], [110], [111]. ICAO [25] adopts a similar procedure with risk measured using likelihood and severity.

2.3.3. A Contemporary Definition of Risk

The classical view in decision theory distinguishes between situations with known probabilities such as coin tossing and situations where probabilities are unknown or only partially known; such as determining the probability of a major accident in a complex plant [62], [73]. While the risk associated with the former situation can be described with probabilities, the risk associated with the latter situation cannot. It involves epistemic uncertainty which "may not be reducible to a unique probability value in a rational way" [62]. It is thus imperative to move from a probability-based definition, to one that takes uncertainty into consideration. Examples of such definitions are provided in [34], [38], [110]. For a detailed list of definitions that take uncertainty into consideration refer to Table 14 of Appendix C. For details on the Frequentist and Bayesian approach the reader is directed to Section §2.2.3.

2.3.4. Summary

There is a progressive shift in the definition of risk from one based on probability towards one that take varying levels of uncertainty into consideration (*e.g.* [34], [38], [110]). Table 14 of Appendix C summarises some of these definitions. Taking all of the above into consideration, the definition of risk adopted in this thesis will be in keeping with those presented by Kaplan [38], Ayyub [34] and Aven [110] and will take uncertainty into consideration.

2.4. Decision Theory

In a SRMP decisions are generally made on the basis of risk assessment (discussed in Section §2.5). Decision theory describes the theory of rational decision making [112], [113]. The overall objective of decision theory is to "formulate hypotheses about rational decision making that are as accurate and precise as possible" [112]. Under decision theory, a rational decision-maker needs to make a choice between the available alternatives on the basis of their consequences [113]. There are two main branches of decision theory: descriptive decision theory and normative decision theory [112]–[115]. Descriptive theory seeks to describe and predict how decisions are actually made by individuals based on consistent rules [112], [115]. This is an empirical discipline, stemming from experimental psychology [112]. Normative theory on the other hand seeks to make prescriptions about what decisions a rational decision-maker should make [112], [115]. It identifies the best decision to make, assuming the decision-maker is fully informed and able to compute with perfect accuracy, and is fully rational [114]. "How people actually behave is likely to change over time and across cultures, but a sufficiently general normative theory can be expected to withstand time and cultural differences" [112]. For more details on each of these approaches the reader is directed to [112]–[115].

2.4.1. Decision Making Under Uncertainty

A risk-based approach to decision-making is required to provide a defensible basis for making decisions. Under a risk-based approach, objective decisions are made based on a systematic and objective assessment of the risk associated with different decision options. This risk-based approach helps identify the greatest risks and prioritises efforts to minimise or eliminate them [116].

A deterministic approach to decision-making involves: identifying a group of failure event sequences leading to credible worst-case accident scenarios; predicting their consequences; and designing appropriate safety barriers which prevent such scenarios and protect from, and mitigate, their associated consequences [117]. In general, the use of conservative worst-case assumptions, that are characteristic of a deterministic approach, does not take the uncertainty associated with systems and their operation into consideration.

A probabilistic approach to decision-making provides an effective way to analyse system safety that takes all feasible scenarios and their related consequences into consideration. These alternate scenarios will have probabilities associated with them, that need to be quantified in order to rationally and quantitatively handle uncertainty [116]. Under this approach, definitions of risk such as that provided by Kaplan and Garrick [38] are needed. This looks at risk as a set of three elements: scenario, likelihood and consequence, with uncertainty associated with the latter two components. Defining risk in this way supports risk management by: distinguishing between high-probability, low-consequence outcomes and low-probability, high consequence outcomes; allowing for proactive risk management controls; and helping identify areas where investment is needed to reduce uncertainty [118].

The bottom line concern with decision-making under uncertainty is to provide the decision-makers with a clearly informed picture of the problem upon which they can confidently reason and deliberate [83], [117]. Jaynes [119] describes the desiderata of rationality and consistency for plausible reasoning in the presence of uncertainty. The general preface is that decision makers can only make inferences (or propositions) about the state of the world based on the uncertain knowledge and information on hand. Bayesian inference provides a means for measuring uncertainty in relation to these hypotheses by producing information based on models, data, and other information [71]. Bayesian inference can also be used to progressively update the state of knowledge (degree of belief in the hypothesis) as new data or experience in the operation of the system are gained. For these reasons Bayesian techniques are used in the probabilistic assessment of the risks in industries like the space launch industry [87], [88], and the nuclear power industry [93]. Thus, to better account for uncertainties in decision making processes, a definition of risk and associated measures that account for uncertainty are needed.

2.5. Safety Risk Management Process

Safety Risk Management (SRM) “encompasses the assessment and mitigation of safety risks” [25]. It involves “weighing the potential costs of risks against the possible benefits of allowing those risks to stand uncontrolled” [40] and is a control task “focused on maintaining a particular hazardous, productive process within the boundaries of safe operation” [120]. There are a number of definitions of SRM provided in the literature, some of which are summarised in Table 16 of Appendix C. ISO 31000:2018 [121] defines the SRMP as, “the systematic application of policies, procedures and practices to the activities of communicating and consulting, establishing the context, and assessing, treating, monitoring, reviewing, recording and reporting risk”. Some common definitions of the SRMP from aviation safety literature can be found in [26]–[28], [31], [56], [122].

2.5.1. Structure of the Safety Risk Management Process

The main goal of risk management is not to reduce all risks to zero but rather to reduce risk to an acceptable level so that routine risk management and cost-benefit analysis become sufficient to ensure overall safety and integrity [34], [107]. There are three main strategies to evaluate and manage risks. These are risk-based strategies, precautionary strategies and discursive strategies. For details on each, the reader is directed to [107]. In general, there are seven sub-processes that go into defining the SRMP outlined in Figure 5.

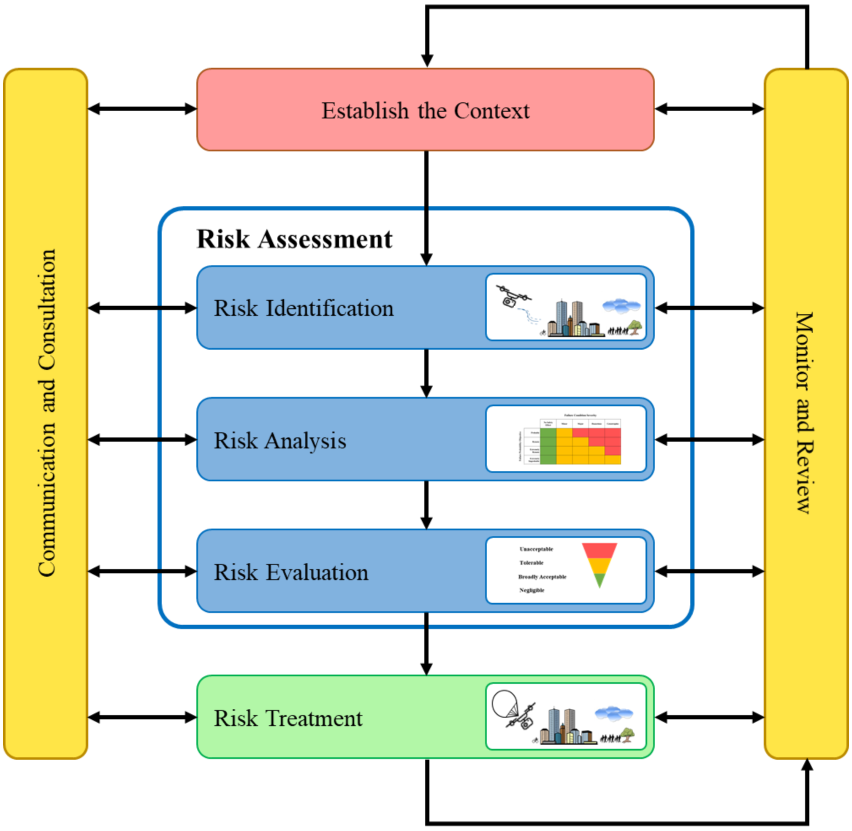


Figure 5: The safety risk management process, based on [111]

The international standard has recently been updated to include an additional process of recording and reporting as described in [121], however, in keeping with the definitions outlined in aviation safety literature, this research will only focus on the above seven mentioned sub-processes. Each of these sub-processes will be discussed in brief in the following sub-sections. Section §2.5.4 will look at the uncertainty associated with each of these processes. For further details on each of the sub-processes, the reader is directed to [17], [25]–[28], [40], [66], [111], [121].

2.5.1.1. Establish the Context

This is the process of "defining the external and internal parameters to be taken into account when managing risk, and setting the scope and risk criteria for the risk management policy" [111]. Recently, ISO 31000:2018 [121] stated that, while setting the risk criteria, "the nature and type of uncertainties that can affect outcomes and objectives (both tangible and intangible)" should be considered. The risk identification process involves consideration of a number of factors including the "cultural, social, political, legal, regulatory, financial, technological, economic, natural, and competitive environment" in which the system will operate [111]. The relationships with, and perception and values of the stakeholders is another key element of this process. In general, the process of establishing the context defines the input, desired outputs, and the boundaries and constraints on decisions made throughout the SRMP [17]. This is followed by the risk assessment process.

2.5.1.2. Risk Assessment

Risk assessment is defined as "a systematic process for describing and quantifying the risks associated with hazardous substances, processes, action, or events" [52]. It is "a technical and scientific process by which the risks of a given situation for a system are modeled and quantified" [34]. It comprises of three sub processes: risk identification, risk analysis and risk evaluation [121]. According to ISO 31000:2018 [121], "risk assessment should be conducted systematically, iteratively and collaboratively, drawing on the knowledge and views of stakeholders. It should use the best available information, supplemented by further enquiry as necessary". The objective of the risk assessment process is to comprehensively characterise the risks associated with the operation of the system (risk identification) and consequently determine which of the characterised risks can be tolerated and which require mitigation or treatment (risk analysis and risk evaluation) [17].

The purpose of risk identification is to "find, recognize and describe risks that might help or prevent an organization achieving its objectives" [121]. According to ISO 31000:2018 [121], there are uncertainties that may affect one or more of these objectives that organisations should identify using a variety of techniques. In general, the risk identification process identifies how the system can fail, how these failures and conditions manifest as hazards, and the potential undesired outcomes that can result from the occurrence of the hazard [17]. Output from this process is a set of characterised scenarios. The set of all scenarios identified with a given activity is described as the risk profile [17]. According to ISO 31000:2018 [121], “Relevant, appropriate and up-to date information is important in identifying risk”.

The purpose of risk analysis is to “comprehend the nature of risk and its characteristics including, where appropriate, the level of risk” [121]. It describes the process of characterising the nature and level of the risks (likelihood and consequence) for each of the identified scenarios [17]. Likelihood and consequence are used to assess the risk based on a range of qualitative and quantitative scales [17]. Input to the risk analysis process are the scenario descriptions output from the risk identification process. In general, output from the risk analysis process are measures of the likelihood and consequence of risk. ISO 31000:2018 [121] also mentions the need to consider uncertainty in the risk analysis process.

The purpose of risk evaluation is to “support decisions” [121]. Risk evaluation is essentially a decision-making process that requires decisions about the acceptability of risk to be made [37]. It is the process of comparing the results of risk analysis with the established risk criteria to determine whether additional action is required [121]. A number of decision making processes can be used within the risk evaluation process; including the ALARP and SFARP frameworks [66]–[68]. Based on this, safety risks can generally be assessed as being acceptable, tolerable or intolerable. For more details on this, the reader is directed to Ref. [25].

2.5.1.3. Risk Treatment

Once the risks are assessed, they need to be treated. This process is called risk treatment and is also a decision-making process. The purpose of this process is to select and implement options for addressing risk [121]. It involves identifying, implementing, and evaluating suitable measures to reduce (mitigate, modify, treat or control) the risk [17]. The inputs to this decision-making process are measures of risks and assessments of the effectiveness, costs and benefits associated with available risk treatment options. The outputs are the specification of risks to be treated (the subjective decision function of ranking risks) and the specification of treatment options to be implemented for each specified risk (the subjective decision function involving the trading-offs of risks, costs and benefits) [37].

2.5.1.4. Monitor and Review

The purpose of monitor and review is to “assure and improve the quality and effectiveness of process design, implementation and outcomes” [121]. Owing to the dynamic nature of risk, it is important to monitor and review the SRMP in response to changes in the risk. The process of monitoring and reviewing ensures the management of risks is constantly maintained and improved. It is undertaken at all stages of the SRMP.

2.5.1.5. Communication and Consultation

Finally, the communication and consultation process ensures that the broader stakeholder concerns and the issues stemming from the lack of knowledge of the risks and the benefits associated with the operation are addressed [17]. The purpose of the communication and consultation process is to “assist relevant stakeholders in understanding risk, the basis on which decisions are made and the reasons why particular actions are required” [121]. Communication and consultation is key to “avoiding potential conflict in the safety decision-making process, for ensuring that stakeholder concerns are being addressed, and for reducing uncertainty in the decisions and outcomes” [17]. Like the monitoring and reviewing process, this process is also undertaken at all stages of the SRMP.

2.5.2. Data Collection

Data forms the basis on which risk assessment are made. Data can include information about “the possible failures, failure probabilities, failure rates, failure modes, possible causes, and failure consequences” [34]. Such information may not be available for new systems or technologies like UAS. This lack of data and information is a major source of epistemic uncertainty. In such cases, data from similar systems may be used. Alternatively, expert judgement can serve as a source of information if the above approaches are not applicable [34]. Combinations of the above can also be used to provide a more detailed analysis of the problem at hand. Referring to Table 5, it is clear that uncertainty can result from the inputs, data, outputs and use of expert judgement which all need to be taken into consideration while collecting data. It is important to identify and represent any uncertainty regarding the quality of the data, as this will assist in the decision-making process. When collecting data and statistics concerning the events it is of paramount importance to ensure that this data is as accurate, complete and consistent as possible.

If extensive data are available, straightforward statistical analysis can be used to analyse the frequency and consequences of risks. When data are lacking, models need to be constructed [52]. It is often argued that insufficient data and scientific understanding limit the usefulness and effectiveness of risk assessment. However “while insufficient data and scientific understanding may rule out the use of some data-intensive risk assessment methods, it does not necessarily follow that other systematic methods designed to quantify uncertainty will not be helpful to decision makers” [52]. According to Zio & Pedroni [49], the lack of information, data, or knowledge, the existence of too much information, data or knowledge and the selection of an appropriate model to be used in the risk analysis process are all major sources of uncertainty that again need to be taken into consideration. This uncertainty can be classified as both epistemic and aleatory uncertainty and consequently require the adoption of a Bayesian approach to measure the uncertainty. The Bayesian approach uses both objective and subjective information to estimate probabilities, which are “conceived of as representing all aspects of a decision-maker’s lack of knowledge” [62].

2.5.3. Quantitative Risk Assessment

Risk assessments can be qualitative (descriptive or categorical treatments of information) or quantitative (mathematical analyses of numerical data) [123]. In situations where data, time or other resources are limited it may only be possible to conduct a qualitative risk assessment. However, in general quantitative risk assessments are preferred to qualitative risk assessments [123]. This is because quantitative methods "express risk in the language of numbers" which are more precise than words and provide "more useful inputs for a decision on what to do about risks" [52]. Quantifying risk helps risk managers make "coherent risk management decisions under uncertainties and within resource constraints" [33]. Example of quantitative risk models and tools that support this process for industries with low data can be found in [124], [125].

Within the context of quantitative risk assessment, two distinct approaches are defined in the literature: namely the deterministic approach and the stochastic approach. A deterministic approach is referred to as a point estimate approach while a stochastic approach is referred to as a probability approach. "The primary difference between these two approaches is in their description of the inputs to a risk assessment" [123]. The point-estimate approach uses single values (such as average) as inputs to a risk assessment and produces a single value for the risk estimate. The stochastic or probabilistic approach looks at all the available data. Instead of a single point estimate to describe the risk parameters, it uses probability distributions which look at a range of values and specifies the frequency of these values. These distributions are based on empirical data, knowledge, and even expert opinions if no other information is available. The output of this approach is a risk distribution "that characterizes the range of risk that might be experienced by an individual or population" [123]. There can be uncertainty associated with the accuracy and correctness of the assumed model describing a probability distribution or the parameters and data used to substantiate the model that needs to be taken into consideration.

A powerful tool used by many industries to analyse the identified risks and uncertainties, is the Probabilistic Risk Analysis (PRA) tool. According to Paté-Cornell, "Engineering risk analysis generally relies on probabilistic tools designed to quantify and display uncertainties when the information base is incomplete" [33]. For example, when the risk of operations of nuclear power plants was assessed in the early nineteen seventies there had not been any nuclear accidents. Consequently these studies were based on PRAs which proved to be a definite improvement on previous deterministic approaches [33]. Even though the probabilistic approach is more complex, this method is preferred for quantitative risk assessments. This is because it takes account of "the variability and uncertainty in the information used to derive the risk estimate" [126].

2.5.4. Uncertainty in the SRMP

Uncertainty can pervade in all stages of the SRMP. The perception and values of the stakeholders are taken into consideration while establishing the context. Uncertainty influences the level of risk perceived by the stakeholders and the risk treatment options adopted [17]. Having an effective communication and consultation process is important to addressing the uncertainty of the stakeholders [17]. There is however uncertainty associated with the communication and consultation process as well. This can be introduced through the communication of the model and its outputs to other stakeholders.

A particular issue in the SRMP, especially for new and evolving systems such as UAS, is managing the uncertainty in the risk assessment process [17]. Zio & Pedroni [49] identify many factors which could lead to uncertainty in risk analysis that need to be taken into consideration based on [127], [128]. These factors will be taken into consideration in the proceeding discussion and include:

- the lack of information, data, or knowledge;
- the existence of too much information, data or knowledge;
- the selection of an appropriate model to be used in the risk analysis process;
- the conflicting nature of the data (due to errors in the data or due to the fact that some of the data is not relevant);
- the bias in the model chosen by the analyst;
- the measurement errors made by the analyst performing the measurement;
- the subjectivity of the way the analyst interprets the available information and data;
- the language used by the analyst (due to the interpretation of the language used by the analyst).

According to ISO 31000:2018 [121], successful implementation of the SRMP through engagement of stakeholders, enables organisations to explicitly address uncertainty in decision-making, while also ensuring any new or subsequent uncertainty can be taken into account as it arises.

2.5.4.1. Uncertainty in the Risk Identification Process

A number of different tools, data and techniques can be used to identify and characterise a risk-profile that is output from the risk identification process. Risk identification tools can be classified as historical (*i.e.* review of accident and incident data), brainstorming (*e.g.* elicitation of knowledge from domain experts), and systematic (*e.g.* formal tools and processes) techniques [31]. Referring to Section §2.2.2 and Zio and Pedroni [49], it can be seen that the scarce availability of data, imprecision of the data and information available on the system, measurement errors, use of subjective expert judgement and even the models and tools used in this process are all potential sources of uncertainty that need to be taken into consideration in the risk identification process. In general, models are approximate and simplified representations of reality and is a potential source of uncertainty to the overall analysis. In addition, the processes used for the identification of the hazards themselves and the contributing failures and conditions that result in these hazards are additional sources of uncertainty that need to be addressed. Uncertainty can also arise due to the possibly incomplete identification of the hazards [49]. The final component of risk identification is assessing the potential consequence. Consequences can be in the form of damage to people, equipment or property, or the environment (domains of consequence) [47]. The qualitative and quantitative spectrum of consequences (severity) needs to be defined for each domain of consequence identified. The use of limited data, expert opinion and decision criteria to assess these potential consequences is another source of uncertainty that needs to be taken into consideration in this sub-process.

2.5.4.2. Uncertainty in the Risk Analysis Process

Uncertainty in the quantitative analysis of the accident sequence typically affects "the values of the conditional probabilities of events comprising the accident scenarios", "the modelling of the accident scenarios by means of traditional event tree and fault tree methodologies", and "the consequences of the accident scenarios" [49].

An event can have "multiple causes and consequences and can affect multiple objectives" [121]. The potential outcomes of a given risk scenario are mapped to the consequence levels (qualitative or quantitative) [17]. The limited data and use of expert judgement in this process is a potential source of uncertainty. Mathematical models that are usually translated to computer codes are often used to determine a quantitative estimate of the consequence. This can be a potential source of uncertainty including aleatory parametric uncertainty, epistemic parametric uncertainty and epistemic model uncertainty. For further details on each, the reader is directed to [49]. In addition, as there can be more than one consequential outcome associated with the occurrence of a single risk scenario, the mapping is typically based on the worst-possible outcome identified. This implies strong elements of "subjectivity and arbitrariness in the definition of the accidental events, which may lead to the consideration of scenarios characterized by really catastrophic consequences, although highly unlikely" [49]. This may prove to be a conservative approach that fails to take the uncertainty associated with the process into consideration.

Assessments of the likelihood of occurrence can be based on a range of information sources including incident and accident data, component reliability data and expert knowledge. Referring to Section §2.2.2 and Zio and Pedroni [49], it can be seen that the limited data, use of expert judgement and even the models and tools used in these processes are all potential sources of uncertainty that need to be considered. Epistemic uncertainties may arise due to 1) the lack of knowledge and/or data on the physical phenomena involved and/or 2) the limited or (possibly) null operating experience of the corresponding component or system over the wide range of conditions encountered during the operation of the system [49]. This typically affects the values of the probabilities and frequencies of the events included in the accident scenarios of interest and is a particular problem for systems employing new technologies [49]. This is another source of uncertainty that needs to be recognised.

2.5.4.3. Uncertainty in the Risk Evaluation Processes

Risk evaluation involves decision-making in relation to the risks associated with the accident scenarios identified and quantified in the previous step. As there is uncertainty in the outputs of the risk analysis process, this inputs into the risk evaluation process as well. Consequently, a risk-based decision-making process that takes this uncertainty into consideration is required. By accounting for the potential uncertainty in the inputs to the risk evaluation process, it is possible to base decisions in relation to the acceptability (or need for mitigation) of risk (uncertainty and consequence). Consequence could be expressed in terms of the potential losses associated with different potential decision outcomes.

The risk evaluation process compares the results of the risk analysis with the established risk criteria to determine whether additional action is required [121]. A number of decision-making processes can be used within the risk evaluation process; including the ALARP and SFARP frameworks. For details on each the reader is directed to [66]–[68]. Focusing on the ALARP framework, determining that risks have been reduced to a level ALARP involves: an assessment of the risk to be avoided; of the sacrifice or costs (e.g., in money, time, and trouble) involved in taking measures to treat that risk; and a comparison of the two components to see if there exists a gross disproportion [68]. There are "psychological, social, and practical difficulties in the specification and sole use of quantifiable criteria" within the ALARP framework [17]. Clothier *et. al.* [69] identify various difficulties in applying the ALARP framework to the UAS sector. As described in [69] most of these challenges arise due to uncertainty in assessments and decision criteria, which are not currently accounted for in the ALARP process. Consequently, qualitative frameworks that focus on demonstrating that all reasonably practicable measures have been undertaken to reduce a risk as opposed to making quantifiable comparisons of the assessed risks are adopted. The limited operational data, decision criteria, assumptions and use of expert judgement are sources of uncertainty that need to be taken into consideration. As described in Section §2.2.2 and Zio and Pedroni [49], uncertainty in the framework used to model this process (*e.g.* ALARP framework) is also a source of aleatory uncertainty that needs to be considered.

One final source of uncertainty that has not been discussed yet is that associated with the adoption of risk matrices. While the adoption of a risk matrix is standard practice in industry, there is potential uncertainty associated with the application of this risk matrix which is being propagated throughout the SRMP. Cox [129] highlights some of the limitations associated with the adoption of such risk-matrices. While addressing them is beyond the scope of this thesis, it is important to understand the uncertainty associated with them and how it impacts this sub-process.

2.5.4.4. Uncertainty in the Risk Treatment Processes

Risk treatment involves decision-making in relation to the evaluated risks. As there is uncertainty in the outputs of the risk evaluation process, this inputs into the risk treatment process as well. Consequently, a risk-based decision-making process that takes this uncertainty into consideration is required. Those risk scenarios that are not tolerable need to be reduced (mitigated, modified, treated or controlled) [17]. As multiple risk scenarios may exist, the treatment options also need to be prioritised. The uncertainty in the output data, use of expert judgement and inadequacies in the model are all sources of uncertainty that need to be further considered while undertaking the risk treatment process.

2.5.4.5. Uncertainty in the Safety Decision-making Process

It is suggested that the manner in which uncertainty is treated in a risk analysis depends on the level of uncertainty present [33]. Paté-Cornell's framework provides a generic high-level way of describing the degree to which risk assessments characterise and present uncertainties to support decision making [33]. Paté-Cornell's [33] framework for describing the "six levels of treatment of uncertainties in risk analysis" is summarised in Table 6. While the quantification of uncertainties is desirable and should be part of a risk assessment, a full uncertainty analysis can often prove to be a "difficult and costly enterprise" and should only be undertaken if it is relevant to risk management [33].

Table 6: Treatment of uncertainties (adapted from [33]*)*

Level	Description	Example
0	Does not require any quantification of risk. Only involves the detection of potential hazards and identification of the different ways in which the system can fail, without attempting to quantitatively assess the risk.	Hazard detection and failure modes identification (*e.g.* Failure Mode and Effect Analysis (FMEA)).
1	Based on the accumulation of worst-case assumptions. Yields, in theory, maximum loss level. Does not involve any notion of probability.	Identification of worst-case conditions.
2	Evaluation of the worst possible conditions that can be reasonably expected when there is uncertainty about what the worst case could be or when the worst case is so unlikely that it is meaningless. Such assessments usually do not involve the assessment of probabilities.	Evaluation of 'plausible upper bounds' or 'quasi-worst cases'.
3	Relies on 'best estimates' and/or on a central value (e.g. mean, median or mode) of the outcome (e.g. loss) distribution, generally through 'best estimates', of different variables. The disadvantage of central values is that the risk is still characterized by a single point estimate.	Best estimates of central values or the Maximum Likelihood Estimates (MLE) of the parameter.
4	Makes use of PRA to obtain a probability distribution based on best estimates of the models and parameter values. Classical Frequentist methods are used to take account of aleatory uncertainties. It includes both epistemic and aleatory uncertainties, however the use of a single risk curve limits the information available.	PRA (also referred to as Quantitative Risk Assessment (QRA) or Probabilistic Safety Assessment (PSA)) and a single risk curve.
5	Uncertainties about fundamental hypotheses are displayed by a family of risk curves. Could be done by using Bayesian inference on the existing data. Alternately, a group of experts could be individually asked to use their preferred model to provide risk assessments and to provide their estimations of parameter values for a given model.	PRA and multiple risk curves.

2.5.5. Risk Management in the Aviation Industry

The International Civil Aviation Organization (ICAO) advocates the adoption of SRM procedures to identify the hazards and mitigate the risks posed by systems [25]. This involves the two key concepts of a State Safety Programme (SSP) and a Safety Management System (SMS). A clear understanding of the relationship between an SSP and an SMS is essential for concerted safety management action within States [25]. Each State is required to establish a SSP in order to achieve an acceptable level of safety as established by the State. Example descriptions can be found in [25]–[28]. This involves "an integrated set of regulations and activities aimed at improving safety" [3].

The ICAO Safety Management Manual (SMM) [25] provides guidelines to the States on the procedures for the development and implementation of a SSP in accordance with the international Standards and Recommended Practices (SARPs) contained in Annexes 1, 6, 8, 11, 13 and 14. The main objective of a SMS is to foster a sound safety culture across all levels in the organisation by relying, amongst other things, on a systematic and effective (informed) risk management process. A SMS is "a system to assure the safe operation of aircraft through effective management of safety risk" [122]. One of the outcomes of a SMS is a documented safety case necessary to obtain approvals for operation. As part of the SMS, operators need to identify hazards and specify how safety risks will be managed. As specified in the ICAO [25], a SMS should comprise of four basic components: safety policy and objectives, safety risk management, safety assurance and safety promotion. The focus of this thesis is on the SRMP. In general, aviation industry follows the standard SRMP as described in Section §2.5. For more details, the reader is directed to [25].

Existing aviation safety regulatory and associated guidance materials are reviewed to ascertain how risk and in particular uncertainty is characterised and addressed within the aviation safety framework. ICAO [25] define safety risk as, "the assessment, expressed in terms of predicted probability and severity, of the consequences of a hazard, taking as reference the worst foreseeable situation". The definitions adopted by CAA [31], FAA [26], CASA [27], [28] and EASA [32] can be found in the individual references. Based on these definitions it can be seen that, in general, there is no mention of uncertainty. Risk is measured in terms of probability (likelihood) and consequence (severity). A standard risk-matrix is used in the risk assessment process [17]. This can prove to be a limiting factor, especially when dealing with new and evolving technologies such as UAS that have uncertainty associated with them. To better account for the uncertainty in the aviation sector, the definitions of risk outlined in aviation safety literature needs to be aligned with more contemporary risk concepts as described in Section §2.3.

In addition to the probability and consequence associated with a particular event, contemporary definitions incorporate uncertainty into their definitions of risk (*e.g.* [34], [38], [110], [121]). In taking this uncertainty into consideration, contemporary approaches adopt a Bayesian approach to measuring uncertainty while measuring risk [86]. The SRMP adopted by aviation safety regulatory bodies [25]–[28], [31], [32] generally make the assumption of a worst-case consequential outcome and tend not to take uncertainty into consideration in the risk analysis process [25], [31]. This approach is often referred to as a structuralist defense-in-depth-approach [49]. Within this approach, safety margins against the identified scenarios are enforced "through conservative regulations of system design and operation, under the creed that the identified worst-case, credible accidents would envelop all credible accidents for what regards the challenges and stresses posed on the system and its protections" [49]. Consequently, the adoption of a Frequentist approach to measuring probability and in turn risk is more common practice for quantitative assessments. This is not in keeping with contemporary definitions of risk [34], [38], [110]. Referring to Paté-Cornell's [33] "six levels of treatment of uncertainties in risk analysis", it can be seen that in general, the level of uncertainty taken into consideration in the aviation industry is Level 2. It involves evaluation of the worst possible conditions that can be reasonably expected when there is uncertainty about what the worst case could be or when the worst case is so unlikely that it is meaningless [33].

As objective assessments of the uncertainty are generally not input into the aviation safety risk management decision-making processes (*i.e.* risk evaluation and risk treatment), there is potential for subjectivity in the decision-making processes. If the aviation industry is going to move towards a risk-based approach to developing regulations (rule-making) [25]–[28], [31], [32] and there is uncertainty associated with this risk, then it is important to adopt a risk-based approach that takes uncertainty into consideration in the decision-making processes that follow. Adopting a risk-based approach to decision-making would provide a defensible basis for making decisions and help identify the greatest risks and prioritise efforts to minimise or eliminate them [116].

Aviation safety risk assessments make use of a broad array of data (*e.g.* accident and incident data, events, non-conformance or deviations, *etc.*). These data can originate from a variety of sources (*e.g.* historical data, expert judgement, *etc.*) and are used in both the development of models and as input to the models. Both epistemic and aleatory uncertainties are inherent to the risk assessment process. Further, there is potential uncertainty associated with the setting of safety criteria, and in assessment of the effectiveness of risk treatments against these criteria. Uncertainty can also be introduced through the communication of the model and its outputs to other stakeholders. For example, aleatory uncertainty arising due to homophony, linguistic or lexical ambiguity, channel distortion, trust, *etc*. Owing to the importance of the data quality, ICAO [25] does recommend organisations assess the data using certain criteria: validity, completeness, consistency, accessibility, timeliness, security and accuracy. This would ensure the data used is of the highest quality, thus reducing the uncertainty associated with it.

2.6. Risk-based Regulation in the Aviation Industry

National Aviation Authorities (NAA) policy and rule-making activities follow a risk-based approach, whereby a safety argument is provided to support and justify the development of airworthiness regulations [16]. A risk-based approach in the aviation industry acknowledges that regulations are merely the embodiment of the outcomes of a risk management process [16], specifically: “they are legal requirements relating to how various stakeholders should go about treating safety risks; requirements relating to the implementation of controls or measures to modify, mitigate, or otherwise reduce the risk”. Risk management should drive the development of regulations, ensuring a clear traceability between the legislated requirement and the risks it is in place to manage. The intended outcome is a framework of regulations and standards that has a defensible and objective basis in risk.

Aviation regulatory bodies such as ICAO, FAA, EASA, CASA and CAA [25]–[28], [31], [32] take the risks associated with the operation of aviation systems into consideration when developing regulations (*i.e.* rule-making). However, it was found that existing aviation SRMP do not adequately account for uncertainty. Based on the review conducted in Section §2.5.4, it was made clear that uncertainty is inherent in all steps of the SRMP. Thus, in moving towards a contemporary definition of risk, it is important to take this uncertainty into consideration in the risk-based approach to rule-making adopted by aviation regulatory bodies. This uncertainty in the performance assessments in the SRMP also results in uncertainty in the regulatory decision-making processes of compliance assessment and compliance finding.

Compliance assessment is the process of assessing the traits or properties of a system (or process) that are needed to verify requirements. In general, the current compliance assessment processes used in the aviation sector are subjective and make use of deterministic binary “pass or fail” processes to make compliance assessments. These processes are often unable to take the uncertainty in the performance assessments that are input into the compliance assessment process into consideration. This leads to risk and uncertainty in the outputs of the compliance assessment process.

Compliance finding is a deterministic decision-making process where the system is deemed compliant if it meets the necessary conditions of the regulation or standard, and all the necessary documentation on the assessment outcomes, people, tools, and data used are provided to have adequate assurance in that assessment. However, this assurance (confidence) tends to be subjective. The binary outputs from the compliance assessment process are input into the compliance finding process. As there is uncertainty in these outputs, there is also potential risk and uncertainty associated with the decision-making process of compliance findings. Current compliance approaches do not objectively account for uncertainty in the state of compliance. A decision maker uses a subjective and somewhat “black box” process for making compliance findings. Currently, aviation decision makers cannot account for compliance risk for all possible compliance decision outcomes, which can include [2]:

1. Certifying the system as compliant when it is in fact compliant; a desirable outcome;
2. Certifying the system as compliant when it is in fact non-compliant. This is the least desirable outcome, which can lead to the operation of a system that does not meet the minimum safety standards;
3. Not certifying a system as compliant when it is in fact compliant. This is a less than desirable outcome where an unnecessary cost is borne by the system manufacturer;
4. Not certifying a system as compliant when it is in fact non-compliant; a desirable outcome;
5. Requiring further data and analysis to be undertaken when the system is in fact compliant. This is a less than desirable outcome where an unnecessary cost is borne by the system manufacturer;
6. Requiring further data and analysis when the system is in fact non-compliant; this is a less than desirable outcome where an unnecessary cost is borne by the system manufacturer in undertaking additional assessment on a non-compliant system.

A means to take this uncertainty into consideration in both the compliance assessment and compliance finding regulatory processes is thus required. Extending the risk-based approach to the regulatory processes of compliance assessment and compliance finding will allow for this uncertainty to be taken into consideration and support compliance findings to be made based on compliance risk.

In the aviation industry, ICAO [25] outlines certain criteria that enforcement decisions must follow. They must: a) be fair and follow due process; b) be transparent to those involved; c) take into account the circumstances of the case and the attitude/actions of the service provider when considering action; d) take consistent actions/decisions for like/similar circumstances; and e) be subject to appropriate internal and external review [25]. Whilst these principles apply to regulatory enforcement, they can be identified as desirable traits of any other regulatory process. Taking this into consideration, the objectivity, transparency, and consistency of the normative approach to decision-making make them particularly suited to the aviation industry. Subsequently, this approach will be used in any decision-making process adopted in this thesis. It is important here to note that, as uncertainty forms such an integral part of the concept of risk, the decision-making process adopted will take uncertainty into consideration.

2.7. Risk-based Regulation in the UAS Industry

The case study of UAS is used as a practical example to develop and illustrate the theoretical contributions of this thesis. This is a pertinent example, as NAA have advocated the adoption of risk-based principles for the regulation of the sector [10], [11], [13]–[15]. Such a risk-based approach “marks a significant change in the way aviation safety regulations are developed, becoming proportionate to the risks they aim to address” [130].

2.7.1. Uncertainty in the UAS industry

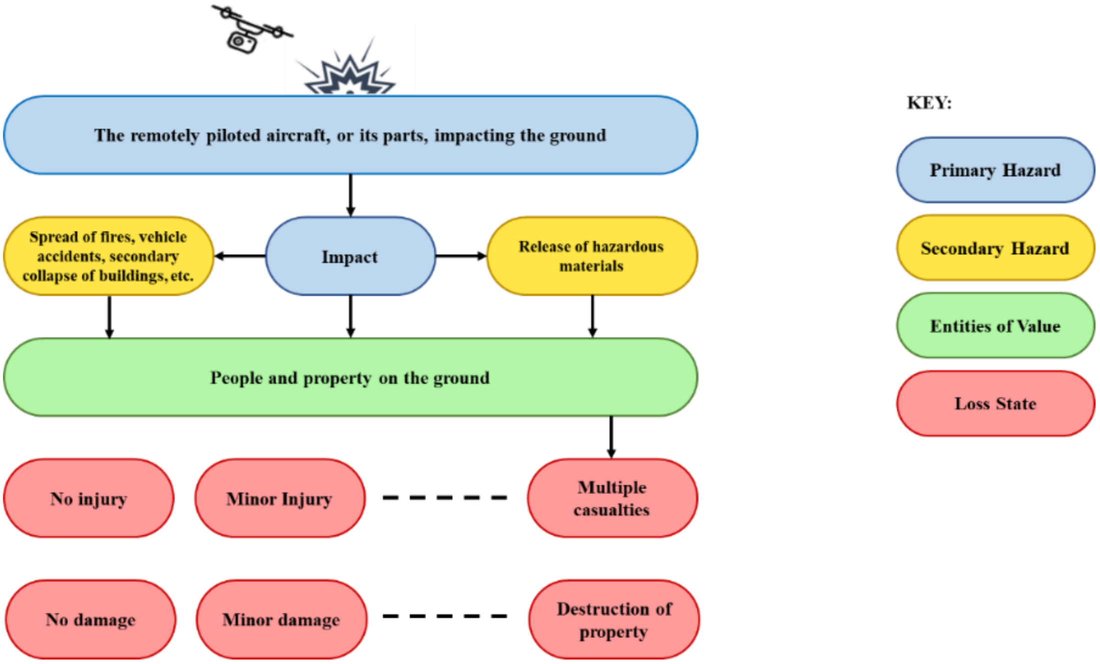
The UAS industry is an area in the aviation sector that has been receiving a considerable amount of attention in recent years. UAS are inherently different to Conventionally Piloted Aircraft (CPA) [7] and are quite diverse in terms of size, performance and risk. They have a number of applications [4]. Like any new technology, it takes some time to build a comprehensive state of knowledge in the technology and its associated operational risks. For UAS this situation is compounded by the low data needed to inform estimates of UAS reliability, which arises due to: 1) changing system design baselines; 2) the use of components that are not designed to standards and subject to quality assurance; 3) the non-homogeneity of the UAS fleet (*i.e.*, the diversity of designs and their concepts of operation, which limits the conclusions which can be drawn from aggregating data across types). There are a number of other factors that limit the amount of operational data available on UAS (refer to [1]) that can impact their certification. As a consequence, there is a considerable amount of uncertainty associated with these systems.

As a result of the differences that exist between UAS and CPA, there is a general lack of knowledge and operational data, and a lack of trust in the knowledge and data that is available on these systems; both of which are needed to support airworthiness assessments and compliance regulatory processes (compliance assessment and compliance finding) for UAS. There can be considerable uncertainty associated with the certification of civil or commercial UAS, which in turn can lead to high certification risk (*i.e.*, the risk associated with certifying a UAS as compliant, and therefore safe for operation, when indeed it is not). It is thus clear that there is a need for a comprehensive approach to characterise and incorporate uncertainty in not only the development of regulations for UAS but the compliance assessment and compliance finding regulatory processes that follow.

Under the risk-based approach, models that comprehensively capture the nature of the risks posed to people and property on the ground are essential to the development of airworthiness and operational regulations for UAS. These models are referred to as Ground Risk Models (GRM) and form the first area of focus for this thesis. The risks posed to people and property situated on the ground are largely managed through the development and promulgation of regulations that provide assurance in the airworthiness of the UAS [6]. When coupled with operational regulations (*e.g.*, restrictions in terms of when and where UAS can operate), airworthiness regulations can more effectively manage the risks posed to people and property overflown [6]. Not all UAS types may be required to meet prescriptive codes of airworthiness requirements in order to be safe for operation (*e.g.,* Open category of UAS as defined in [18]). Those that do however, will likely be required to show compliance to SSR, also referred to as Part 1309 regulations. This forms the second area of focus for this thesis.

2.7.2. Ground Risk Models

GRM describe the magnitude of risk to entities of value (EoV) (*e.g.* people and property) in the regions overflown by an Unmanned Aircraft (UA) due to the realisation of one or more of the scenarios illustrated in Figure 6. With the exception of [131], none of the reviewed GRM address secondary hazards, and hence the scope of the review is limited to the primary risk scenario of a direct impact between an UA (or its components) and one or more EoV on the ground (refer to Chapter 3 for detailed review of GRM).



The remotely piloted aircraft, or its parts, impacting the ground
Spread of fires, vehicle accidents, secondary collapse of buildings, etc.
Impact
Release of hazardous materials
People and property on the ground
No injury
Minor Injury
Multiple casualties
No damage
Minor damage
Destruction of property
KEY:
Primary Hazard
Secondary Hazard
Entities of Value
Loss State

Figure 6: Ground risk scenarios for UAS [132]

Based on the review, seven component-models could be identified in these GRM as illustrated in Figure 7. These include the failure model, impact location model, recovery model, stress model, exposure model, incident model and harm model.

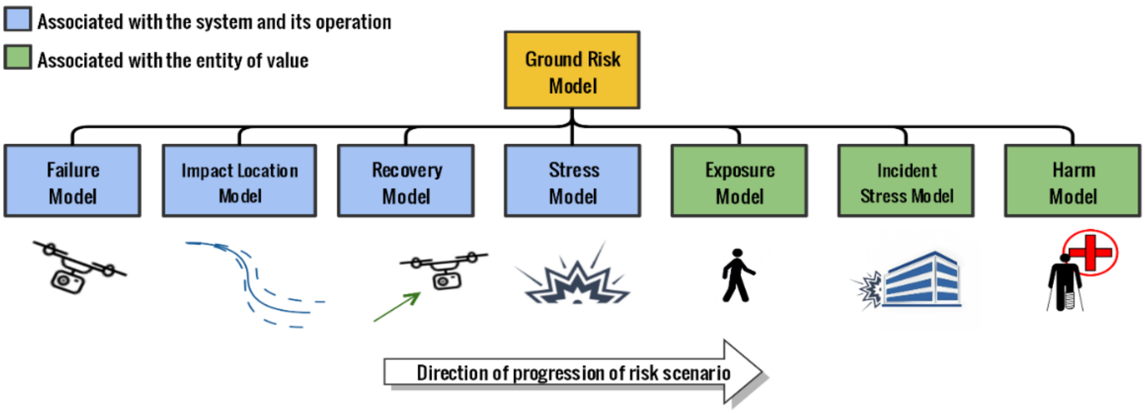


Figure 7: General components of a ground risk model for UAS [132]

Chapter 3 provides an extensive review of the current state-of-the-art in ground risk modelling for UAS operations. By identifying each of the sub-models that go into developing GRM and relating them to various aspects of the aviation regulatory framework, this work also provides a means for identifying where future research efforts need to be focused and how this will potentially influence the ongoing development of regulations for the sector. For the sake of brevity, this review has not been repeated here. For further details refer to Chapter 3.

2.7.3. System Safety "Part 1309" Regulations

System safety "Part 1309" regulations are intended to supplement prescriptive standards on the design, manufacture, and installation of aircraft components. At a high-level, the SSR specify the requirement for [133]:

1. A documented analysis showing that equipment and systems perform as intended under foreseeable operating and environmental conditions;
2. The adoption of principles from fail-safe and fault-tolerant design [134]; and
3. The demonstration (through a documented qualitative or quantitative analysis) that the expected frequency of failure of equipment and systems, when considered separately and in relation to other systems, is inversely-related to the severity of its effect on the safe operation of the system. This is commonly referred to as the System Safety Performance Requirements (SSPR).

A complete description of the Part 1309 regulations can be found in [21], [22], [135]–[138] and associated guidance material [35], [134].

As the SSR form an integral part of this research, each of the papers published in Chapter 0 to Chapter 7 provide a more detailed review of these regulations, with particular emphasis placed on the SSPR. Again, for the sake of brevity this detail has not been repeated here. For more details, the reader is directed to the individual chapters.

2.8. Analysis of Literature and Summary of Findings

The literature review presented in this chapter was intended to supplement rather than replace the extensive literature reviews undertaken in each of the proceeding chapters. The focus of this section is to provide a high-level linkage between the elements of the literature review, showing how, as a whole, it helps identify the research gaps, motivating the particular direction of research. A high-level breakdown of this chapter is provided in Figure 8, showing the linkage between the individual sections. The arrows help highlight how different sections influence each other. For example, in order to understand the overall concept of risk, it was important to have a clear understanding of various fundamental concepts and the concept of uncertainty. This relationship can clearly be seen in Figure 8. Each of these theoretical concepts are then linked to the various regulatory processes of interest, with the case study application also identified. Again, these relationships are highlighted in Figure 8.

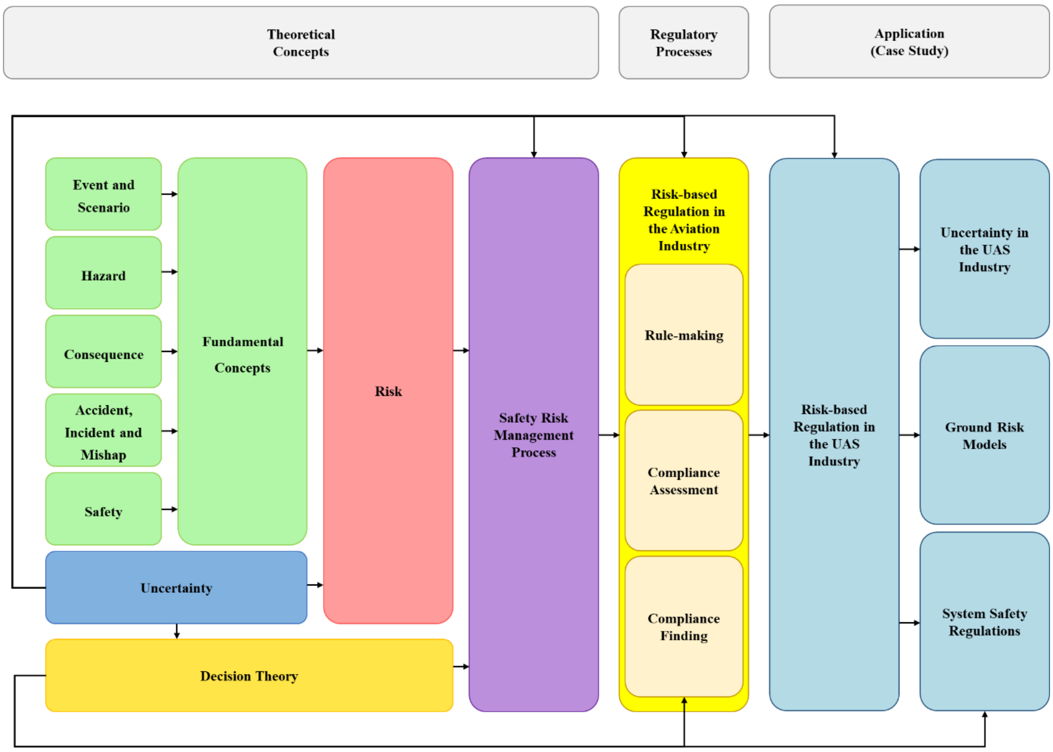


Figure 8: High-level breakdown of literature review highlighting case-study applications

2.8.1. Fundamental Concepts

The literature review undertaken in this section identified a set of fundamental concepts that are integral to the definition of risk. These fundamental concepts include: event and scenario; hazard, consequence; accident, incident and mishap; and safety. Based on the review of these concepts a number of important conclusions were drawn which directly helped in addressing the main research questions of this thesis.

Firstly, on review of the literature, both general and aviation specific, it was seen that there exists a considerable amount of diversity amongst the definitions used to describe these concepts. This diversity has the potential to lead to uncertainty in the interpretation of each of these concepts. This clearly highlighted the need to adopt a uniform set of definitions that could be used throughout the thesis. Where possible definitions adopted by aviation safety authorities are used throughout this thesis. These fundamental concepts along with the concept of uncertainty (introduced in the following section) help in the development of a clearer understanding of the overall concept of risk.

Secondly, in relation to the consequence, it was observed that arriving at a clear and uniform understanding of the type and degree of loss is a subjective process that depends on the values held by an individual or the community at large. This subjectivity leads to uncertainty in the type and level of loss which could inevitably lead to the imposition of overly conservative restrictions to mitigate or manage the risk. It was thus concluded that a means to take this uncertainty into consideration is needed.

Finally, in relation to the concept of safety, it was observed that there are two main interpretations of safety: absolute safety and relative safety. While in an ideal world, absolute safety is the condition one would want to strive towards (as it implies that the risk has been completely eliminated), it is not always possible to achieve this owing to the uncertainty associated with most real-world systems. The relative definition of safety takes this uncertainty into consideration and is based on the assumption that the risk can be reduced or controlled to an acceptable level in accordance with an agreed set of management principles. It was thus concluded that this relative interpretation of safety would be adopted in this thesis, as is common practice in aviation safety literature. Understanding this relative definition of safety was extremely important as it forms the basis of most management principles (e.g. ALARP and SFARP frameworks) that are fundamental to the SRMP.

2.8.2. The Concept of Uncertainty

This section focused on the concept of uncertainty. While this in itself is fundamental to the definition of risk, it was reviewed independently as it is an integral part of this research and as such required further detail. The review involved: identifying the various types of uncertainty; sources of uncertainty; and means of measuring uncertainty. Based on the review a number of conclusions were drawn.

Firstly, it was observed that there are two main types of uncertainty: aleatory uncertainty and epistemic uncertainty. Aleatory uncertainty is inherent to most systems (such as UAS) and the models used to evaluate the risks posed by them. Similarly, the limited data associated with new and evolving systems such as UAS is a potential source of epistemic uncertainty that needs to be considered (other sources of uncertainty were also identified). On critically analysing both of these types of uncertainty and relating it to the overall aims and objectives of the thesis and the case study application of UAS, it was concluded that any treatment of uncertainty would require both of these types of uncertainty to be considered.

Next, based on the extensive literature review undertaken, multiple sources of uncertainty were identified. These sources include the: input and data; model and engineering system; output; decision criteria; acknowledged inadequacies; unknown inadequacies; expert judgements. Each of these sources are inherent to the SRMP which in itself is central to the risk-based approach to the regulation of the industry. Taking the case study application of UAS into consideration, it was thus concluded that any risk-based approach to the regulation of the industry must take the uncertainty associated with this process into consideration (or at a minimum recognise its existence).

Finally, a means of measuring the identified types and sources of uncertainty was needed. Based on the extensive literature review undertaken it was observed that the main approach to measure uncertainty is through probability theory. Taking this into consideration, it was observed that there are two main interpretations of probability, the Frequentist interpretation and the Bayesian interpretation. When looking at the case study application of UAS, it is evident that these systems are characterised by limited data and high uncertainty (both epistemic and aleatory). It was thus concluded that applying a

Frequentist interpretation of probability to measure the uncertainty associated with these systems would not be suitable. The Bayesian interpretation provides a suitable alternative as it not only takes both aleatory and epistemic uncertainty into consideration, but it can also be used for applications where there is limited data, such as in the UAS industry. Other industries such as the space launch industry, nuclear power industry, fishery industry, ecological management industry, bio management industry and even the aviation industry, that are similar to the UAS industry in that they have limited data and high uncertainty associated with them have also adopted this Bayesian approach. This provided added confidence that such an approach would be suitable for the case study application of the UAS industry.

In addition to helping describe the overall concept of risk, the fundamental theory and knowledge gained in this section was used to help identify the research gaps that exist in the literature. As uncertainty is such an integral part of the definition of risk, a means to take this uncertainty into consideration is needed. This was an important conclusion drawn from the literature as it helped highlight the limitations of the current SRMP and the risk-based approach to the regulation of the aviation industry currently adopted.

2.8.3. The Concept of Risk

The concept of risk is central to the adoption of a risk-based approach to the regulation of the industry. Each of the fundamental concepts described in Section §2.1 along with the concept of uncertainty detailed in Section §2.2 were used in the analysis of the concept of risk. The section not only identifies a variety of definitions of risk but also shows how risk can be measured taking the various elements that go into defining this concept into consideration. Based on this review it was observed that there is a considerable amount of diversity that exists between these definitions. This diversity existed not only in terms of the elements that go into defining risk but also in terms of how these elements can be combined together to describe the risk. Earlier definitions of risk were based on probability and consequence, with risk being measured in terms of the product of these two elements. However this approach equated low probability and high consequence events with high probability and low consequence events, which proved to be limiting. To address this shortcoming later definitions described risk as a set of three element: scenario; probability; and consequence. Building on this, more contemporary definitions of risk were also found to take uncertainty into consideration. There was a clear shift of the definitions from ones based on probability to ones that account for uncertainty. In adopting the risk-based approach to the regulation of the industry and evaluating the SRMP, it was thus imperative to evaluate how uncertainty is currently taken into consideration. Most definitions of risk used in aviation safety literature do not mention uncertainty. This is not a major limitation when dealing with CPA, as these systems have acquired a considerable amount of data over the years. In addition to this, as the EoV are onboard the aircraft, the potential consequence associated with a failure is always going to be high. Hence assessing for the worst-case consequential outcome is desirable, and the uncertainty associated with this may not need to be considered. When dealing with UAS, as the EoV are on the ground or on-board other aircraft, the consequence associated with a failure can vary significantly. Hence to negate the need for overly conservative restrictions on these systems, and the associated costs, it is imperative to take the uncertainty associated with these risk estimates into consideration. It was thus concluded that uncertainty (both aleatory and epistemic) needed to be accounted for in any definition of risk adopted as part of this thesis.

2.8.4. Decision Theory

Decision making is an integral part of the SRMP, where decisions are made based on the risk assessments. A risk-based approach to decision-making is required to provide a defensible basis for making decisions. Decision theory describes the theory of rational decision making and hence it is important to have a clear understanding of this theory. This was the main focus of this section. Based on the review undertaken it was observed that there are two main branches of decision theory: Descriptive decision theory and Normative decision theory. While the Descriptive decision theory seeks to describe how decisions are actually made by individuals based on consistent rules, normative decision theory looks to make prescriptions about what decisions a rational decision-maker should make. Taking this into consideration it was concluded that a normative approach to decision theory would be more suitable in adopting a risk-based approach to the regulation of the UAS industry.

As uncertainty is an integral part of the definition of risk, it was concluded that it is important to take uncertainty into consideration in any decision-making process that underpins the risk-based approach to the regulation of the industry. A deterministic approach to decision-making makes use of a conservative worst-case assumption and hence does not take the uncertainty associated with a system and its operation into consideration. A probabilistic approach however provides an effective way to analyse system safety that takes all feasible scenarios and their related consequences into consideration, thus accounting for the uncertainty. This provides the decision maker with a clearly informed picture of the problem upon which they can confidently reason and deliberate. It was thus concluded that in using normative decision theory it was imperative to adopt a probabilistic approach to decision-making. Relating this back to the review on uncertainty undertaken in Section §2.2, it is clear that a Bayesian approach would consequently need to be adopted to take the uncertainty associated with this process into consideration. Other industries such as the space launch industry and nuclear industry adopt similar procedures, which provides added confidence in the chosen approach.

2.8.5. Safety Risk Management Process

The overall aim of the thesis is to “Improve regulatory outcomes under the new paradigm of risk-based regulation, through providing a conceptual framework for the rational, transparent and systematic treatment of uncertainty in the risk assessment and regulatory decision-making process”. Central to this is the SRMP. The reviews undertaken in Section §2.1 to Section §2.4, laid the foundations that were necessary to help in the critical analysis of the SRMP. Each of these concepts were used to get a better understanding of the SRMP and helped identify the research gaps that existed in the literature. The section starts by introducing the SRMP and each of the sub-processes that go into defining this process. As data forms such an integral part of any SRMP, the process of data collection was also explored here. Taking this into consideration, the concept of quantitative risk assessment was also introduced.

Based on the review of the concept of risk undertaken in Section §2.3, it was observed that most contemporary definitions of risk take uncertainty into consideration. However, on reviewing the SRMP it was seen that in general there is no mention of uncertainty. It was thus concluded that a means to take the uncertainty associated with the SRMP was needed. This led to the first research question, "What are the uncertainties associated with the safety risk assessment process and how are they addressed within the current aviation safety risk management and regulatory development processes?". In order to help answer this question, a more in-depth review of the SRMP to help identify the different sources of uncertainty (both epistemic uncertainty and aleatory uncertainty) associated with the SRMP was needed. The review of uncertainty undertaken in Section §2.2 provided the necessary information in relation to the concept of uncertainty to help in this endeavour. Applying this to the SRMP, a number of different sources of uncertainty were identified in relation to each of the sub-processes.

As there is uncertainty in the risk identification and risk analysis process, and this is generally not taken into consideration (or where considered, accounted for by assuming a worst-case consequential outcome), it is evident that this uncertainty will be input into the risk evaluation process. Consequently a risk-based approach to decision-making that is capable of taking uncertainty into consideration is needed. However, as was observed from the literature, in general, there is no uncertainty accounted for in this decision-making process. Similarly, uncertainty in the risk treatment process, which is also a decision-making process, is also not taken into consideration. It was thus concluded that a means of taking the uncertainty in the decision-making process into consideration is needed. This led to the second research question, "How can uncertainty associated with the SRMP be accounted for in existing aviation rule-making and compliance processes?". The review of decision theory undertaken in Section §2.4, helped identify different approaches that could be used to this accord. If the aviation industry is going to move towards a risk-based approach to the development of regulations and there is uncertainty associated with this risk (as is the case with UAS), then it is evident that it is important to adopt a risk-based approach that takes uncertainty into consideration in not only the rule-making but also the decision-making processes that follow.

2.8.6. Risk Management in the Aviation Industry

The SRMP and the sub-processes that go into defining this process are used to get a better understanding of what is meant by risk-based regulation and how it is applied in the aviation sector. This is summarised in Section §2.6. Based on an extensive review undertaken, it was observed that NAA policy and rule-making follow a risk-based approach, whereby a safety argument is provided to support and justify the development of airworthiness regulations. The intended outcome is a framework of regulations and standards that has a defensible and objective basis in risk. While risk is taken into consideration in this process, it was concluded that the SRMP that underpins this approach generally makes the assumption of a worst-case consequential outcome and tends not to take uncertainty into consideration.

The uncertainty in the performance assessments in the SRMP also results in uncertainty in the regulatory decision-making processes of compliance assessment and compliance finding. The compliance assessment approaches adopted in the aviation sector were found to be subjective, making use of a deterministic binary “pass or fail” process. This is often unable to take the uncertainty in the performance assessments that are input into the compliance assessment process into consideration. The compliance finding process adopted by the aviation sector is also a deterministic decision-making process that is generally unable to take the uncertainty associated with this process into consideration. A decision maker uses a subjective and somewhat “black box” process for making compliance findings, with the decision maker unable to account for the compliance risk for all possible decision outcomes.

As identified previously, uncertainty is inherent to the definition of risk and hence in adopting a risk-based approach to the development of regulations it is of paramount importance to take this uncertainty into consideration. It was thus concluded that in order to better account for the uncertainty in the aviation sector, the definitions of risk outlined in aviation safety literature needed to be aligned with more contemporary risk definitions (examples of such contemporary definitions of risk were identified previously in the literature review). A means of taking the uncertainty into consideration in not only the rule-making process but also the compliance assessment and compliance finding decision-making processes that follow is needed.

On relating this back to the uncertainty theory described in Section §2.2, it was evident that a Bayesian approach would need to be adopted here to take both the epistemic and aleatory uncertainties associated with these processes into consideration. In addition to this, to aid in the decision-making and account for the associated uncertainties, the normative decision theory identified in Section §2.4 would need to be explored further. By extending the risk-based approach to the compliance assessment and compliance finding processes and ensuring that uncertainty in each of the three processes is considered, this framework will be able to support compliance findings based on compliance risk. This is particularly important for new and evolving technologies such as UAS that have limited data and high uncertainty associated with them.

2.8.7. Risk-based Regulation of the Aviation Industry

From the preceding discussion, it was made evident that not only is it important to extend the current understanding of risk-based regulation from a risk-based approach to rule-making to a risk-based approach to compliance assessment and compliance finding as well, but in keeping with contemporary definitions of risk, it is important to take the uncertainty associated with each of these three processes into consideration. This led to the overall aim of the thesis, which was to “improve regulatory outcomes under the new paradigm of risk-based regulation, through providing a conceptual framework for the rational, transparent and systematic treatment of uncertainty in the risk assessment and regulatory decision-making process”. In order to achieve this aim, it was important to narrow the scope of the discussion by focusing on a particular case study example.

On reviewing NAA policy and rule-making activities, it was observed that a risk-based approach is adopted, whereby a safety argument is provided to support and justify the development of airworthiness regulations. The intended outcome is a framework of regulations and standards that has a defensible and objective basis in risk. On critically analysing this risk-based approach to rule-making, it was observed that while a risk-based approach is indeed adopted, there is no mention of uncertainty. In addition to this, it was observed that such risk-based principles were not applied to the compliance assessment and compliance finding processes that follow. The current compliance assessment process tends to be subjective and make use of deterministic binary “pass or fail” processes to make compliance assessments. The compliance finding process is also a deterministic decision-making process, where the decision maker uses a somewhat “black box” approach to make compliance findings. There is uncertainty associated with both of these processes that is not taken into consideration. It was thus concluded that in order to account for this uncertainty, it was important to extend the current understanding of risk-based regulation to include a risk-based approach to compliance assessment and compliance finding as well. This will allow for compliance findings to be made based on compliance risk and provide a means of taking the uncertainty into consideration.

2.8.8. Risk-based Regulation of the UAS industry

Based on the literature review presented thus far, it is evident that: 1) risk-based regulation warrants the consideration of more than just a risk-based approach to rule-making, it must also include a risk-based approach to compliance assessment and compliance finding; 2) the SRMP is central to the adoption of a risk-based approach to the regulation of the industry; 3) the concepts of risk, uncertainty and decision theory are central to the SRMP; 4) uncertainty is central to most contemporary definitions of risk; and 5) the current SRMP adopted by aviation regulatory bodies does not take uncertainty into consideration in the risk assessment and compliance decision-making processes. Each of these findings helped motivate the particular research direction of this thesis.

2.8.8.1. Uncertainty in the UAS industry

In order to limit the scope of the discussion and make significant contributions to theory, as mentioned previously, it was considered important to focus the research efforts on a particular case study application. As uncertainty is central to the overall research objectives, the case study application would need to look at the regulatory approach applied to a new and evolving system that is characterised by limited data and high uncertainty. While there are a number of examples of such systems in the industry, the case study application of UAS was selected. UAS are not only inherently different to CPA but are also quite diverse in their size, performance and level of risk posed by their operations. In addition to this, there are a number of other factors that were identified that limit the amount of operational data available on these systems. Consequently there is a considerable amount of uncertainty associated with these systems. Furthermore, there is uncertainty associated with the certification of these systems, which in turn can lead to high certification risk. This made them the ideal case study application for this thesis.

In applying a risk-based approach to the regulation of these systems, models that comprehensively capture the risks posed by these systems to people and property on the ground are needed. These models, referred to as GRM, are essential to the development of airworthiness and operational regulations for UAS and form the first area of focus for this research. Not all UAS types may be required to meet prescriptive codes of airworthiness requirements in order to be safe for operation (*e.g.,* Open category of UAS as defined in [18]). Those that do however, will likely be required to show compliance to SSR, also referred to as Part 1309 regulations. This forms the second area of focus for this thesis. While a detailed review of both of these components are provided in the individual chapters, a summary of some of the findings that supported the particular research direction, that were identified in the individual chapters are outlined below.

2.8.8.2. Ground Risk Models

The focus of this section and the associated chapter (Chapter 3) is on the first research question; "What are the uncertainties associated with the safety risk assessment process and how are they addressed within the current aviation safety risk management and regulatory development processes?". From the preceding discussion it was seen that uncertainty is inherent to most contemporary definitions of risk. Hence in developing a model to comprehensively capture the risks posed by UAS to people and property on the ground it is important to take the uncertainty associated with these systems and their operation into consideration. The review on GRM was used to first identify the different component models that go into defining the overall GRM. Based on the review seven component models were identified, namely, failure model, impact model, recovery model, stress model, exposure model, incident stress model and harm model. Each of these models were then reviewed independently to provide a detailed description of the component-model; a review of the literature associated with the component model, highlighting the assumptions made in relation to the component model; a description of how the component model was substantiated in the literature; a summary of how uncertainty is represented in the component-model (based on Paté-Cornell's framework [33]); and a clear linkage between the component model and the regulations, highlighting not just the component of the regulations that are affected but also how the associated assumptions and uncertainty impacts these regulations. Based on this review several conclusions were drawn in relation to each of the component models. For details on this, the reader is directed to the individual chapter. In addition to this a number of high-level findings were made based on the review. These findings were in relation to the diversity between the models, the use of conservative assumptions and the treatment of uncertainty. For details the reader is again directed to Chapter 3.

2.8.8.3. System Safety Regulations

The focus of this section and the associated chapters (Chapter 4 to Chapter 7) is on the second research question, "How can uncertainty associated with the SRMP be accounted for in existing aviation rule-making and compliance processes?". Narrowing the scope further, the particular part of the SSR that is of interest to this thesis is the SSPR.

The main findings in relation to the literature on SSR are made in Chapter 4. Here the SSR process are introduced for the first time highlighting the particular component of interest for the research, namely, the SSPR compliance process. On critically analysing the Traditional SSPR compliance process, the various sources of uncertainty associated with the SSA, CA and CF processes were identified, and the limitations of the assumptions made in relation to them highlighted. From the discussion presented in Section §2.2, it was clear that a Bayesian approach would be adopted to take this uncertainty into consideration. Following this, Chapter 4 then goes on to describe how Bayes theorem would be used to take the uncertainty in the APFH of the system into consideration and how the outputs from the SSA process would vary accordingly. As there was uncertainty in the outputs of the SSA process, this would input into the CA and CF processes and hence a means to take this uncertainty into consideration in each of these sub-processes would also be required. A further analysis of the Traditional SSPR compliance process however found that uncertainty was not considered in either of these sub-processes. From the preceding discussion it was made evident that uncertainty is inherent to most contemporary definitions of risk. It was thus concluded that in adopting a risk-based approach to the regulation of the industry, it was important to take the uncertainty associated with each of the sub-processes into consideration. The Extended SSPR compliance process developed looked to address these limitations and take some of the uncertainty associated with these processes into consideration. Various concepts fundamental to the adoption of Bayes theorem are discussed, including the selection of the prior and likelihood distributions and the implications of using conjugate and uninformed priors. Other concepts such as Bayesian hypothesis testing and normative decision theory are also discussed in this chapter, with the mathematics on how to apply them also described.

The Extended SSPR compliance process had certain limitations which were addressed in subsequent chapters. It makes use of a Poisson distribution which assumes a constant failure rate and it only takes the uncertainty associated with one of the outputs of the SSA process into consideration, *i.e.* the uncertainty associated with the APFH . To address these limitations, further analysis on uncertainty and its treatment was required. The literature review presented in Chapter 5 looks to provide further insight with regards to the selection of the likelihood distribution and shows how alternate distributions such as the Weibull distribution can be used to take the unique characteristic associated with UAS into consideration. Chapter 6 introduces the concept of BBN and clearly describes how this can be used to take the uncertainty in the remaining outputs of the SSA process into consideration, allowing for the highest level of treatment of uncertainty with respect to the SSPR compliance process. It thus presents the Proposed SSPR compliance process. For details on each of these contributions, the reader is directed to the individual chapters.

In addition to helping answer elements of the first research question, this section and the associated chapters clearly identify the sources of uncertainty in the aviation safety compliance assessment and compliance finding processes and show how they are currently managed. It also clearly shows how the uncertainties in each of these sub-processes can be represented and accounted for, to support more objective and consistent regulatory outcomes. This research highlights some of the potential benefits of the extended risk-based philosophy in the aviation sector. Thus it is clear that this section and the associated chapters clearly address each of the elements of the second research question.

2.8.9. Summary

From the literature review it was made clear that:

1. The aviation SRMP does not provide a systematic way for managing uncertainty in the safety risk assessment and decision-making processes, *i.e.* there is a risk to the compliance decisions;
2. Existing aviation rule-making and compliance processes have no means for accounting for the uncertainty inherent in a SRMP.

If the SRMP is to be used for risk-based rule-making for industries like UAS, then more comprehensive treatment of uncertainty is needed. Further, if assessments of performance are uncertain, a method for making compliance assessments and compliance findings, accounting for these uncertainties is needed. This effectively extends the concept of risk-based regulation from just rule-making to the compliance decision-making regulatory processes of compliance assessment and compliance finding, thus allowing compliance findings to be made based on compliance risk. This leads to the two research questions:

1. **What are the uncertainties associated with the safety risk assessment process and how are they addressed within the current aviation safety risk management and regulatory development processes?**
2. **How can uncertainty associated with the SRMP be accounted for in existing aviation rule-making and compliance processes?**

By answering these questions, this thesis endeavours to improve regulatory outcomes under the new paradigm of risk-based operations, though providing a conceptual framework for the rational, transparent and systematic treatment of uncertainty in the risk assessment and regulatory decision-making process.

3. A Review of Unmanned Aircraft Systems Ground Risk Models

Figure 9: Concept image of an unmanned aircraft operation over Piccadilly Circus, London, UK
Image Copyright © Achim Washington

"Trouble in the air is very rare. It is hitting the ground that causes it"

Amelia Earhart (1897-1939)

This chapter titled: "A Review of Unmanned Aircraft Systems Ground Risk Models" focuses on Research Question 1.1 and Research Question 1.2. It develops a conceptual framework for describing the component-models of GRM with the aim of providing a general theoretical basis for the systematic development and analysis of the models proposed in the literature. The paper conducts an in-depth review of the state of the art in UAS GRM and uses this to evaluate the risks posed by the operation of UAS to people and property on the ground. This helps identify the various sources of uncertainty inherent in the safety risk assessment process (Research Question 1.1). It then relates the GRM and component sub-models to the regulations to show how the uncertainty in these sub-models and the conservative assumptions used to manage them, impact different components of the regulations (Research Question 1.2). By clearly identifying the different levels of treatments of uncertainty and highlighting the limitations associated with the lower levels of treatment of uncertainty, the chapter also addresses elements of Research Question 1.3.

3.1. Statement of Authorship

The authors listed in Table 7 have certified* that:

1. They meet the criteria for authorship (refer to Appendix B: Definition of Authorship) in that they have participated in the conception, execution, or interpretation, of at least that part of the publication in their field of expertise;
2. They take public responsibility for their part of the publication, except for the responsible author who accepts overall responsibility for the publication;
3. There are no other authors of the publication according to these criteria;
4. Potential conflicts of interest have been disclosed to (a) granting bodies, (b) the editor or publisher of journals or other publications, and (c) the head of the responsible academic unit; and
5. They agree to the use of the publication in the student's thesis and its publication on the Australian Digital Thesis database consistent with any limitation set by publisher requirements.

Table 7: Statement of authorship – paper one

Title of Paper:	A Review of Unmanned Aircraft Systems Ground Risk Models			
Contributor	**Area of Contribution and percentage contribution to paper: ***			
	(i)	(ii)	(iii)	(iv)
	Conception and Design	Analysis and Interpretation	Drafting Sections	Critically Revising
Mr Achim Washington	80%	90%	90%	10%
Dr Reece Clothier	20%	10%	10%	60%
Dr Jose Silva				30%

Principal Supervisors confirmation

I have email or other correspondence from all co-authors confirming their certifying authorship

Dr Reece Clothier	25th August 2018
Name	**Date**
Dr Jose Silva	25th August 2018
Name	**Date**

**for further details refer to Appendix B: Definition of Authorship*

Progress in Aerospace Sciences 95 (2017) 24–44

Contents lists available at ScienceDirect

Progress in Aerospace Sciences

journal homepage: www.elsevier.com/locate/paerosci

A review of unmanned aircraft system ground risk models

Achim Washington [a,*], Reece A. Clothier [b,1], Jose Silva [a]

[a] Royal Melbourne Institute of Technology (RMIT), Melbourne, Australia
[b] Boeing Research & Technology – Australia, Melbourne, Australia

ARTICLE INFO

Keywords:
Unmanned aircraft systems
Ground risk models
Risk
Uncertainty

ABSTRACT

There is much effort being directed towards the development of safety regulations for unmanned aircraft systems (UAS). National airworthiness authorities have advocated the adoption of a risk-based approach, whereby regulations are driven by the outcomes of a systematic process to assess and manage identified safety risks. Subsequently, models characterising the primary hazards associated with UAS operations have now become critical to the development of regulations and in turn, to the future of the industry. Key to the development of airworthiness regulations for UAS is a comprehensive understanding of the risks UAS operations pose to people and property on the ground. A comprehensive review of the literature identified 33 different models (and component sub models) used to estimate ground risk posed by UAS. These models comprise failure, impact location, recovery, stress, exposure, incident stress and harm sub-models. The underlying assumptions and treatment of uncertainties in each of these sub-models differ significantly between models, which can have a significant impact on the development of regulations. This paper reviews the state-of-the-art in research into UAS ground risk modelling, discusses how the various sub-models relate to the different components of the regulation, and explores how model-uncertainties potentially impact the development of regulations for UAS.

1. Introduction

UAS are a rapidly growing sector of the aviation industry. However, as with any new technology, UAS still face a number of challenges, resulting in the imposition of a significant amount of operational restrictions on them [1–4]. Of these challenges, perhaps the most significant non-technical challenge facing the UAS sector is the absence of a suitable regulatory framework aimed at governing the safety of their operations [3,4]. In the interim, the de facto stance taken by regulatory bodies the world over is to apply existing standards and regulations developed for conventionally piloted aircraft (CPA) to UAS. However, owing to the inherent differences that exist between UAS and CPA [5], it is widely acknowledged that the “off-the-shelf” approach will not result in an effective airworthiness regulatory framework for UAS [4]. Owing to the diversity that exists amongst UAS, it is also acknowledged that the application of a “one size fits all” approach to the airworthiness of UAS will prove problematic [4]. Regulations tailored to the operation of UAS are required [4,6,7].

The European Aviation Safety Authority (EASA) and Federal Aviation Administration (FAA) have recently recognised the importance of adopting a “risk-based” approach to the development of a regulatory framework for Unmanned Aircraft (UA)[2] [8]. A risk-based approach acknowledges that regulations are merely the embodiment of the outcomes of a risk management process [9], specifically: “they are legal requirements relating to how various stakeholders (*e.g.*, UAS operators) should go about treating safety risks; requirements relating to the implementation of controls or measures to modify, mitigate, or otherwise reduce the risk”. As such, risk management (and its sub-processes) should drive the development of regulations, ensuring a clear traceability between the legislated requirement and the risks it is in place to manage. The intended outcome is a framework of regulations and standards that has a defensible and objective basis in risk.

The risk management process is defined in Ref. [10] and its general application to UAS is described in Ref. [11]. The risk assessment process entails the sub-processes of risk identification, risk analysis and risk evaluation [10]. In the context of UAS, the outcomes are assessments of the risk associated with the two primary hazards of:

- A collision or near collision between a UA and another aircraft (whether the other aircraft is in the air or on the ground);

* Corresponding author.
E-mail addresses: s3270338@student.rmit.edu.au (A. Washington), reece.a.clothier@boeing.com (R.A. Clothier), jose.silva@rmit.edu.au (J. Silva).

[1] Dr Reece A Clothier is an Adjunct Associate Professor at RMIT University.

[2] UA is the flying component of an unmanned aircraft system (UAS).

https://doi.org/10.1016/j.paerosci.2017.10.001
Received 8 August 2017; Accepted 4 October 2017
Available online 10 November 2017

List of Abbreviations

AIS	Abbreviated Injury Scale
BBN	Bayesian Belief Networks
BC	Blunt Criteria
CASA	Civil Aviation Safety Authority
CFIT	Controlled Flight Into Terrain
CONOPs	Concept of Operations
CPA	Conventionally Piloted Aircraft
DOJC	Dropped Or Jettisoned Components
EASA	European Aviation Safety Authority
EoV	Entities of Value
ETA	Event Tree Analysis
FAA	Federal Aviation Administration
FMEA	Failure Mode and Effect Analysis
FMECA	Failure Mode, Effects, and Criticality Analysis
FTA	Fault Tree Analysis
GRM	Ground Risk Model
KE	Kinetic Energy
LOC	Loss of Control
MLE	Maximum Likelihood Estimates
PRA	Probabilistic Risk Analysis
PSA	Probabilistic Safety Assessment
QRA	Quantitative Risk Assessment
RBD	Reliability Block Diagram
RCC	Range Commanders Council
RP	Remote Pilot
RPA	Remotely Piloted Aircraft
RPAS	Remotely Piloted Aircraft Systems
SSPR	System Safety Performance Requirement
UA	Unmanned Aircraft
UAS	Unmanned Aircraft Systems
UDS	Unpremeditated Descent Scenario

- The impact of the UA, or its components, with people or structures situated on the ground [9,11].

The scope of this paper is limited to risk models characterising the latter of these two hazards. The risk posed to people and property on the ground is largely managed through the development and promulgation of regulations that provide assurance in the airworthiness of the UAS [4]. As described in Ref. [4], airworthiness regulations can be combined with operational regulations (*e.g.*, restricting where and when UAS can be operated) to more effectively manage the risks posed to people and property overflown. Under the risk-based approach, models that comprehensively capture the nature of the risks posed to people and property on the ground are essential to the development of airworthiness and operational regulations for UAS.

The risk scenarios associated with the hazard of a ground impact are illustrated as connected pathways in Fig. 1. A variety of models for assessing the risks associated with each of the scenarios illustrated in Fig. 1 are identified in the literature. Thus, the objectives of this paper are to:

1. Provide a comprehensive review of existing models;
2. Describe how the components of these models relate to different elements of safety regulation for UAS; and
3. Identify where future research into the development of models is needed to support the development of effective regulations for UAS.

A general overview of the sub-models comprising the ground risk model (GRM) is presented in Section §2. The various ways in which the components of these models can be used to influence the development of regulations is also presented. Section §3 then provides some general points of discussion on each of the component models, followed by a brief summary of some of the major findings observed, presented in Section §4. Concluding remarks are then presented in Section §5.

2. UAS ground risk models

GRMs describe the magnitude of risk to entities of value (EoV) (*e.g.* people and property) in the regions over-flown by an UA due to the realisation of one or more of the scenarios illustrated in Fig. 1. With the

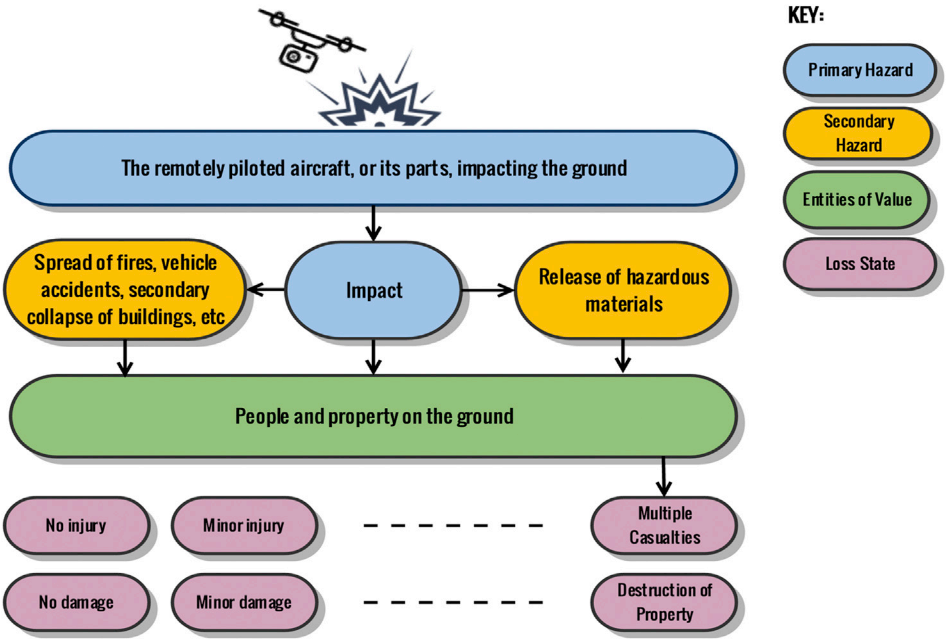

KEY:
Primary Hazard
Secondary Hazard
Entities of Value
Loss State
The remotely piloted aircraft, or its parts, impacting the ground
Spread of fires, vehicle accidents, secondary collapse of buildings, etc
Impact
Release of hazardous materials
People and property on the ground
No injury
Minor injury
Multiple Casualties
No damage
Minor damage
Destruction of Property

Fig. 1. UAS ground risk scenarios.

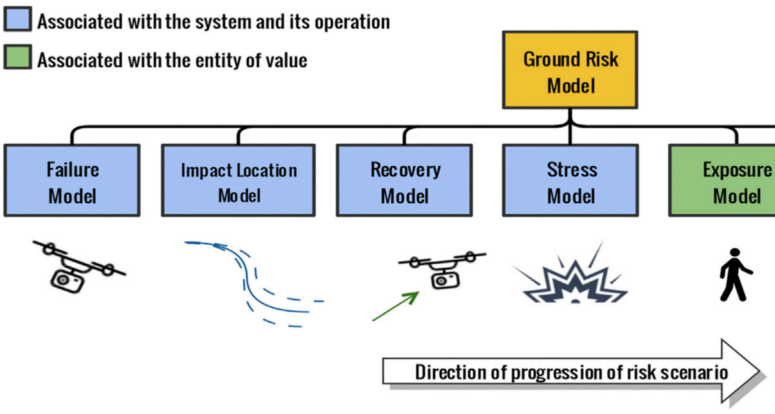


Fig. 2. General components of a ground risk model for UAS.

Table 1
Treatment of uncertainties (adapted from Ref. [13]).

Level	Description	Example
0	Does not require any quantification of risk. Only involves the detection of potential hazards and identification of the different ways in which the system can fail, without attempting to quantitatively assess the risk.	Hazard detection and failure modes identification (*e.g.* Failure Mode and Effect Analysis (FMEA)).
1	Based on the accumulation of worst-case assumptions. Yields, in theory, maximum loss level. Does not involve any notion of probability.	Identification of worst case conditions.
2	Evaluation of the worst possible conditions that can be reasonably expected when there is uncertainty about what the worst case could be or when the worst case is so unlikely that it is meaningless. Such assessments usually do not involve the assessment of probabilities.	Evaluation of 'plausible upper bounds' or 'quasi-worst cases'.
3	Relies on 'best estimates' and/or on a central value (*e.g.* mean, median or mode) of the outcome (*e.g.* loss) distribution, generally through 'best estimates, of different variables. The disadvantage of central values is that the risk is still characterised by a single point estimate.	Best estimates of central values or the maximum likelihood estimates (MLE) of the parameter.
4	Makes use of probabilistic risk analysis (PRA) to obtain a probability distribution based on best estimates of the models and parameter values. Classical Frequentist methods are used to take account of aleatory uncertainties. It includes both epistemic and aleatory uncertainties, however the use of a single risk curve limits the information available.	PRA (also referred to as quantitative risk assessment (QRA) or probabilistic safety assessment (PSA)) and a single risk curve.
5	Uncertainties about fundamental hypotheses are displayed by a family of risk curves. Could be done by using Bayesian inference on the existing data. Alternately, a group of experts could be individually asked to use their preferred model to provide risk assessments and to provide their estimations of parameter values for a given model.	PRA and multiple risk curves.

exception of [12], none of the reviewed GRMs address secondary hazards, and hence the scope of this review is limited to the primary risk scenario of a direct impact between an UA (or its components) and one or more EoV on the ground.

The literature review identified 18 GRMs for UAS. Based on the review, seven component-models could be identified in these GRMs as illustrated in Fig. 2. It is important to note that not all of the reviewed GRMs explicitly implement all seven of the component models. In many cases, the component models are implicitly considered in the model assumptions. The review of the literature also identified research into the characterisation of one or more of these component models (15 additional models identified). These models could be used as part of a GRM and hence are also included in the review.

The setting of appropriate regulations requires an understanding of how the various models identify and manage uncertainty. For example, whether the model is based on worst case assumptions, and hence represents a conservative position for the setting of regulations. A framework for systematically describing the treatment of uncertainty in modelling is thus needed. In this paper Paté-Cornell's [13] framework for describing the "six levels of treatment of uncertainties in risk analysis" is used to assess how each of the reviewed models manages uncertainty. This framework is summarised in Table 1.

2.1. Failure model

The first sub-model of a GRM is the failure model. The failure model describes the uncertainty in the occurrence of failure modes given a particular system configuration, environmental conditions, and mission profile. Each failure (defined as any event causal to the occurrence of a particular failure mode potentially leading to a ground impact) can result in one or more failure modes. Literature [14] define four high level failure modes relevant to the hazard of UA ground impact, specifically:

1. **Unpremeditated descent scenario (UDS)** – a failure (or combination of failures), which results in the inability of the UA to maintain a safe altitude above the surface or distance from objects and structures;
2. **Loss of control (LOC)** - a failure (or combination of failures), which results in loss of control of the UA and may lead to impact at high velocity;
3. **Controlled flight into terrain (CFIT)** - when an airworthy UA is flown, under the control of a qualified remote pilot (RP) or certified autopilot system, unintentionally into terrain (water, structures, or obstacles);
4. **Dropped or jettisoned components (DOJC)** - failures that result in a component of the UA (including its payload or stores) being dropped or jettisoned from the UA.

Input to the development of a failure model is a list of potential failures (*e.g.*, loss of propulsion, loss of power, human error, bird strike, *etc.*), their contributing conditions (*e.g.*, environmental and mission factors), and their associated failure modes (*e.g.*, impact or the continued safe operation of the UA). The output from this model are measures describing the uncertainty in the occurrence of one or more of the four high level failure modes.

Under certain assumptions, the failure model can be considered as a model of the reliability of a component, sub-system(s), or the UAS as a whole. Different assumptions and underlying models will lead to different output measures (*e.g.* measures of the "system failure rate" [15], "probability of failure" [16], or "probability of loss of aircraft" [17]). The failure models identified in the literature are summarised in Table 2 of Appendix A.

2.1.1. *Review of failure models*

Of the 17 failure models identified in the literature, only two explored different types of failures and failure modes. The model presented by Burke et al. [16] takes two failure modes into consideration. The first being UDS (*e.g.* resulting from failure of propulsion system) and the second a LOC (*e.g.* resulting from main spar buckling under load, failure of all flight control systems, loss of a flight critical control surface, *etc.*). Similarly Barr et al. [18] looks at multi-dependent failures resulting in LOC and CFIT failure modes. The majority of models however assume a single system-level failure and associated failure mode.

The type of failure mode is a significant factor in determining the nature of the risk to the EoV; directly influencing the impact location, recovery, and stress component-models. For example, there is more likely to be control over the impact location for those failures classified as having a UDS failure mode over those classified as having a CFIT or LOC failure mode. A single failure can also give rise to more than one failure mode. For example, a LOC can lead to the over-stressing of the airframe, and in turn, the realisation of a DOJC failure mode. Such "second order" considerations (dependencies between failure mode models) have not been addressed in any of the reviewed models.

Another assumption made by all of the reviewed models is that the likelihood of occurrence of the failure (or in most cases, the expected rate of occurrence) is assumed constant. Subsequently, potential variations in the likelihood of failure with factors such as phase, duration, environmental conditions, or mission flight profile are not considered. In addition to this, for a population of UAS, a constant failure rate ignores the fact that once a failure occurs the operator is likely to adopt measures to counter this failure in the future. Furthermore, it fails to recognise that some UAS might have recovery measures put in place to address these failures (*e.g.* use of redundant systems).

2.1.2. *Substantiation of models*

The failure models were substantiated using one of two methods:

1. Historical failure or accident and incident data;
2. Expert opinion.

Determining the probability of failure of the aircraft using historical data involves simply accounting for the number of mishaps an aircraft platform (UA or CPA) has over a given period of time and then dividing these mishaps by the number of flight hours the platform has over the same period of time [15]. Different sources of data can be used for this, including historical data for manned aircraft [19–21] and manufacturer specifications [22,23].

There is limited reliability data available on UAS owing to the relative infancy of the technology and the diversity that exists amongst these systems. Thus the use of a system/functional approach to determine the failure rate of the system might prove to be more suitable for UAS. Burke et al. [16] and Hayhurst et al. [24] provide examples of functional and structural decompositions of UAS that can be used to develop such a model. A similar approach is applied in the space launch industry [25,26], that also shares the problem of low data and high uncertainty. While a greater level of structural/functional decomposition would increase the potential sources of data that can be used in the model, reliability data at this level may not be available or may come at a significant monetary cost [16]. Thus a proper balance between these two aspects must be reached while developing these models.

In general, the use of historical data may not be appropriate for rapidly evolving systems such as UAS. In these instances, the elicitation of expert opinion which makes use of system/functional level data may be used. The models presented by Refs. [20–22,27–29], implicitly make use of expert opinion in determining the failure rate of the system. Some of the models base the results on past knowledge gathered through historical data. Details on how the expert data were elicited are scarce and as such adds uncertainty to the model. Knott et al. [15] make use of a Reliability Block Diagram (RBD) to determine the probability of loss of the aircraft. Other approaches, including Fault Tree Analysis (FTA), Event Tree Analysis (ETA) and Failure Mode, Effects and Criticality Analysis (FMECA) can also be used to evaluate the reliability of the system. More recently, Bayesian Belief Networks (BBN) have also been adopted (*e.g.* Refs. [18,30]) to this effect.

The elicitation of expert opinion and the adoption of a functional or structural decomposition of a UAS provide a mathematical basis for determining the failure rate of a system taking system specific data into consideration. Existing models have however not accounted for the failures due to human error, which has been determined as a contributing factor in 60.2% of UAS mishaps [31]. As such, the results from these models are likely to underestimate the mishap rates when compared to historical mishap rates [15].

2.1.3. *Representation of uncertainty*

There is significant uncertainty (epistemic and aleatory) in the identification and modelling of failures for UAS. This uncertainty arises due to a lack of reliability data, the changing system configurations, use of non-certified components, and limited operational experience [5].

The process of identifying and modelling the occurrence of failures is a key source of uncertainty in the generation of a GRM. Specifically, whether the set of identified failures is complete and whether the model (or assumptions) characterising the uncertainty in the occurrence of a failure provide an accurate representation of the failure phenomena being studied. The absence of a formal accident and incident reporting framework, particularly for small UAS, may prove to be a major source of data uncertainty for these models. A majority of the studies make use of data points based on self-reports, thus negating the impact of data uncertainty on the model (*e.g.* Refs. [18,30]). Further, many of the existing models make use of accident, incident and failure data from CPA to inform the development of their models. The use of such data implicitly assumes adequate similarities exist between the conditions contributing to failures (and resulting failure modes) between manned and unmanned aircraft. The validity of such assumptions are not explored in the literature.

Failure to account for both the epistemic and aleatory uncertainties could directly impact the level of risk posed by these systems. From Table 2, it can be seen that, the highest treatment of uncertainty is described by Ancel et al. [30] and Barr et al. [18] and is classified as 'Level 4'. While these models do make use of a Bayesian approach to take the uncertainty into consideration, the outputs are still represented as point values. Similarly, the models presented by Lum and Waggoner [22], Lum et al. [23] and Bradley and Hillestad [32] are classified as 'Level 3'. While classified as 'Level 3', all of these models were based on a number of conservative assumptions, the compounding effect of which is not explored. This will have an impact on the setting of appropriate regulations moving forward.

2.1.4. *Relationship to regulations*

Failure models drive all aspects of the technical airworthiness and certification of UAS and its associated equipment. This includes minimum design performance criteria and requirements on the ongoing airworthiness (*i.e.*, maintenance) of the system. Those failure modes associated with human performance will be key to determining medical, training, and duty requirements for the remote crew. The failure model will also be important in the setting of system safety objectives (Part 1309 requirements) and for showing compliance to them. System safety regulations are intended to supplement prescriptive standards on the design, manufacture, and installation of aircraft components. At a high-level, they specify the requirement for [33]:

1. A documented analysis showing that equipment and systems perform as intended under foreseeable operating and environmental conditions;
2. The adoption of principles from fail-safe and fault-tolerant design [34]; and
3. The demonstration (through a documented qualitative or quantitative analysis) that the expected frequency of failure of equipment and systems, when considered separately and in relation to other systems, is inversely-related to the severity of its effect on the safe operation of the system. This is commonly referred to as the system safety performance requirement (SSPR).

A complete description of the Part 1309 regulations can be found in Refs. [24,35–39], and associated guidance material [34,40]. Guidelines on the system safety assessment process and accepted assessment tools and techniques can be found in Refs. [37,38,41,42]. The failure model combined with assumptions in relation to the other component-models, are key to establishing appropriate failure probability objectives for UAS. A mapping between the existing failure modes (*i.e.*, UDS, LOC, CFIT, and DOJC) and the failure severity levels defined in Part 1309 regulations (*e.g.*, Catastrophic, Hazardous, Major, Minor, No Safety Effect) must be established. Once established, the most probable failure mode assigned to an identified failure would be used to determine its failure condition severity level. This can then be used to establish the appropriate failure probability objective for the particular component/sub-systems associated with the particular failure.

The effect of conservative assumptions underlying the development of UAS failure models is two-fold. Firstly, they will lead to the establishment of more stringent failure probability objectives for UAS. Secondly, the same models are used to then show compliance with these objectives. As such, conservative modelling assumptions can lead to overly conservative design performance criteria for components.

2.2. *Impact model*

The impact model characterises the spatial-temporal uncertainty in the location of UA impact and the size of the area impacted (referred to as the lethal area) given the occurrence of a failure. Some models assume that the UA will impact at a single point (no uncertainty), others assume that there are a number of potential locations the UA can impact, given a particular trajectory. The latter approach defines a boundary within which all the potential impact locations of the UA lie. This boundary is based on a number of factors (*e.g.* maximum glide distance) and the area within it is called the impact area. The location of impact and size of the lethal area depends on the trajectory of the UA (or its components for DOJC failure modes), which is determined by the:

1. Initial conditions at the time of failure (*e.g.*, position, velocity, attitude);
2. Failure mode (*i.e.*, UDS, LOC, CFIT or DOJC);
3. Type of UA (*e.g.*, fixed wing, blimp, multi-rotor, helicopter, *etc.*);
4. Input made by a RP, auto-pilot, or recovery system (including pre-programmed behaviours);
5. Activation of mitigation devices (*e.g.*, parachutes, air bags, destructive flight termination systems, *etc.*); and
6. Environmental factors (*e.g.*, wind, terrain).

The choice of initial conditions serves to bound the potential distribution of impact locations. For example, if a fixed-wing UA experiences a loss of power, it is likely that it will still be able to glide a certain distance before impacting the ground. The key factors determining the impact point being, the glide performance of the UA, the initial altitude at the time of the failure, and the prevailing wind conditions.

The particular failure mode will determine the degree of controllability on-board control systems or the RP has over the UA, and in turn, the location of impact. A range of trajectory models would be required to accurately represent the uncertainty in the impact location for different failure modes. For example, a ballistic trajectory model may be appropriate for DOJC failure modes whereas more complex dynamic models would be required to represent other failure modes like a LOC or UDS.

The type of UA will be a key factor in determining its trajectory under a given failure mode. For example, a loss of power for a multi-rotor UA is likely to lead to a LOC failure mode, and in turn an impact distribution characterised by the free fall characteristics of the UA skewed in the direction of its initial velocity vector. Whereas a loss of power on a fixed wing UA will result in a UDS failure mode, which will have a much larger impact distribution characterised by the glide and turn performance of the aircraft (*e.g.* Ref. [43]).

Inputs to the system made by the RP or autopilot systems post-failure will also influence the impact distribution. For example, many missions have pre-defined flight termination sequence or automated functionality that attempt to recover the UAS to a specified location. The designation of recovery or ditching areas will tend to skew the likely impact distribution for those failure modes where there remains a degree of controllability over the UA (*i.e.*, lead to multi-modal spatial impact distributions). Other auto-scripted features such as return to launch or hold over an area will have a similar effect on the impact probability distribution.

The activation of parachutes and other forms of flight termination systems will influence the spatial and temporal characteristics of the impact distribution in a similar manner (*e.g.* Ref. [44]). It will also be necessary to model human pilot performance (situational awareness, decision making and action) post the occurrence of the failure for those situations where the contingency behaviours are not automated.

Operational factors (*e.g.* wind, terrain, weather, and visibility) will contribute to the uncertainty in the trajectory of the UA, and in turn, its impact location. The underlying terrain and structures will also be key factors in determining the impact location for CFIT failure modes.

The UA is not a point mass and numerous approaches have been proposed for describing the size of the region on the ground exposed to the potentially harmful characteristics of the UA. This is commonly referred to as the casualty or lethal area. The size and factors going into the determination of the lethal area depend on the EoV, the type of stress being considered (refer to Section §2.4), the mechanism for harm being considered (refer to Section §2.7), the characteristics of the UA (*e.g.*, dimensions) and its trajectory immediately prior to impact (*e.g.*, steep vertical dive, or shallow glide). For blunt force or crushing harm mechanisms, the lethal area is often determined based on the dimensions of the UA and the radius of an upright person. If the mechanism for harm was a blast wave, then a radius relating to the propagation of the shock wave centred on the point of impact, would need to be defined.

2.2.1. *Review of impact models*

The literature review revealed 24 impact models (Table 3 of Appendix A) used to evaluate the impact location and lethal area of the UA, given the occurrence of a failure. With the exception of [17,45], each of these models used a geometric approach to evaluate the impact model. This in turn required input parameters in the form of position, velocity, attitude, *etc.*

The impact location distribution is highly dependent on the failure mode, however, the majority of identified models failed to specify the type of failure mode(s) considered. Of those models that did, most assumed catastrophic failure conditions, and subsequently assumed either a LOC or UDS failure mode.

Impact distribution models based on fixed wing configurations were assumed for a majority of the models. The models described in Refs. [12,20,30,46–52] however also looked at multi-rotor configurations in evaluating the impact model. As previously described, the type of the UA has a significant influence on the nature of the impact distribution.

Specific models for each different UA type are thus needed.

A number of the existing models (*e.g.* Refs. [29,48,52,53]) do not take the size of the lethal area into consideration, assuming the impact occurs at a finite point in space and time. This assumption limits the risk evaluation to that of individual risks (*i.e.*, further assumptions must be made in order to evaluate measures of group or collective risk). Models like those presented in Refs. [16,23,54] provide calculations of the lethal area, which differs from the impact area by including overlapping dimensions of the EoV. Finally, with the exception of [44] there were no existing models accounting for impact location given the activation of a contingency mechanism (*e.g.*, parachute, auto-rotation, *etc*.).

2.2.2. *Substantiation of models*

A summary of impact models reviewed is provided in Table 3 of Appendix A. Melnyk et al. [17] describe two methods used to substantiate these models, specifically:

1. Hypothetical prediction models (geometry based); and
2. Empirical prediction models (weight, size, or category based).

The hypothetical prediction models (*e.g.* Refs. [12,16,20,27]) use aerodynamic models and simulation as the basis for determining the impact distribution. The hypothetical prediction models can be further divided into planform, gliding, and vertical descent models. The planform approach takes advantage of the shape and layout of the aircraft wing. The gliding approach (*e.g.* Refs. [12,27,54]) assumes that the UA will continue its descent profile and glide at a certain angle (based on the lift to drag ratio of the UA) before impacting with the ground. The vertical descent models (*e.g.* Refs. [12,16,27]) which are based on a steep geometric assumption, use a circle based on the UA wingspan to determine the boundaries of the potential impact distribution. Most models use both the gliding and vertical descent models to evaluate the impact location. Wu et al. [43] use a dynamic model assessed for various failure conditions to determine the maximum boundary (and in turn area) of the impact distribution for fixed wing UA. However, like most models, it assumes a uniform impact distribution within these boundaries. Such assumptions fail to account for the existence of higher impact probabilities in the regions immediately surrounding the mission flight path, or around nominated recovery or hold points. An exception to this are the models presented by Lum et al. [23] and Cour-Harbo [48]. These models make use of a probability distribution function to characterise the crash potential within the given area, thus taking the uncertainty associated with this factor into consideration.

Empirical prediction models make use of historical data from aircraft crashes (manned and unmanned) as a basis for determining the impact location. Melnyk et al. [17] further classifies these models into weight-based (*e.g.* Ref. [19]) and size or aircraft category based (*e.g.* Ref. [32]) prediction techniques. While historical data from the UAS industry would be ideal for these models, owing to the relative infancy of the technology, data from CPA are often used as inputs. Impact location models based on CPA accident and incident data make the implicit assumption of similarity in the behaviour of a CPA and an UA under a particular failure. The validity of this assumption is not adequately explored in the existing literature and is particularly significant for those cases where CPA data is used to develop impact location models for small UA or unique UA types for which there is no direct CPA comparison. The basic mathematical models for some of these models are provided in Table 9 of Appendix B.

Various models are used to describe the lethal area. The majority use a simple deterministic model based on the dimensions of the UA, the radius of a person, and the product of the height of the person impacted and the cotangent of the glide angle [23]. Second order factors including skid, roll, explosion, and fragmentation can be taken into consideration in the characterisation of the lethal area (*e.g.* Refs. [12,47]). Models (*e.g.* Refs. [12,16,27]) characterise the lethal area for steep vertical trajectories using a circle of diameter equal to the wingspan of the UA. Melnyk et al. [17] compared the lethal areas calculated from some of the hypothetical and empirical prediction models to actual or approximated lethal areas documented in accident and incident reports. While the data used in the study were limited, it was observed that the geometric methods continually under predicted the lethal area when compared to actual data, with the gliding approach producing the most accurate results, followed closely by the weight and size/category based approach.

2.2.3. *Representation of uncertainty*

As can be seen from Table 3, with the exception of [23,46,48] all of the other models did not characterise the uncertainty at a high level. Each of the factors described above contribute to the level of uncertainty associated with the impact models and consequently impact the development of regulations for these systems.

2.2.4. *Relationship to regulations*

The impact model will be significant in the development of operational regulations for UAS. Specifically, regulations specifying the:

- Minimum clearance distance to be maintained from people, buildings, or populous areas for a given height above ground and UA type;
- Minimum height over which an overflight of a populous area can occur;
- Extents of operating areas including mission and flight boundaries.

The impact model can also be used as a basis for determining whether UAS are required to be equipped with containment assurance devices (*e.g.* geo-fences and tethers) or systems for flight termination (*e.g.* autoland and parachutes). The minimum performance requirements for these systems will be largely determined by their contribution to the overall safety case. For example, routine operations over populous areas may require forced landing and flight termination systems to meet high design assurance levels. The impact model may also be used in operational planning to determine the size and location of emergency and failure recovery areas and as an input to determining minimum performance standards for UAS navigation systems.

2.3. *Recovery model*

The recovery model characterises the uncertainty in the ability of the UAS to recover to a nominal or degraded operational state given the occurrence of the failure. Some factors critical to the characterisation of the recovery model include:

1. Type of failure and its failure mode;
2. Equipage of the UAS with failure detection, warning and recovery/mitigation devices;
3. Situational awareness of the RP;
4. Reliability and performance of automated failure recovery systems.

The probability of recovery depends on the type of failure, its failure mode, and the operational situation. For example, if the UA experiences a failure resulting in a LOC failure mode, then the presence of a recovery mechanism (*e.g.* parachute) would reduce the descent velocity, thus reducing the potential harmful characteristics resultant from the failure.

The equipage of the UAS with failure detection, warning, and recovery/mitigation devices directly influence the probability of recovery. More specifically, the absence of a mechanism for failure detection and alerting would result in the inability to deploy a recovery mechanism by either automated systems or the RP. The probability of recovery will also have temporal dependencies, *e.g.* the RP may not detect the failure in sufficient time to recover the UA.

The situational awareness of the RP and their ability to recover the UA under a failure mode also has a direct impact on the probability of recovery. For example, the RP may not be able to take manual control in those instances where the UA is operating outside of direct visual line of sight or beyond radio range of the UAS.

Finally, the reliability of the recovery systems needs to be taken into account as a factor in the recovery risk model.

2.3.1. Review of recovery models

A summary of the recovery models (part of other GRMs or component models) reviewed is presented in Table 4 of Appendix A. With the exception of [21,29,30,44,53,55,56] none of the other identified models considered recovery measures in the evaluation of the risks posed by UAS to people and property on the ground. The models provided by McGeer et al. [21] and Ford and McEntee [29] make assumptions in relation to the ability of the UAS to follow a glide path with maximum range, while the model provided by Shelley [44] and Bleier [53] explore the effectiveness (*i.e.*, the risk reduction) of parachutes. Weibel and Hansman [55] suggest several mitigation measures which can be put in place to reduce the risk. Some of these measures include 1) reducing the exposure to risk of the public on the ground, 2) ensuring UAV system reliability, 3) facilitating safe recovery from failures, 4) reducing the effects of UAV ground impact. This is incorporated into the model by introducing a factor "P_{mit}" which indicated "the proportion of accidents for which mitigation prevents the occurrence of ground fatality" [55].

2.3.2. Substantiation of models

While few of the models reviewed incorporated a recovery sub-model, none of them provided a quantitative assessment on it. The best way to substantiate these models would be to look at historical data on other systems or conduct case study experiments, to determine the amount of risk reduction that would be achieved through the incorporation of recovery measures. Elicitation of expert opinion may also be used to substantiate these models.

2.3.3. Representation of uncertainty

As was seen from the literature reviewed, only six of the models reviewed took this component of the GRM into consideration. While these models clearly highlight what mitigation measures they accounted for, with the exception of [53], these models fail to provide any details in relation to the mitigation measures adopted. As such, it can be assumed that a 'Level 0' uncertainty was taken into consideration by each of the models. Failure of these models to account for this component of the GRM, limits the impact of not incorporating the uncertainty in this parameter into the models.

2.3.4. Relationship to regulations

A clear understanding of the recovery models can directly impact technical design features and operational processes. For example, if a UA were to experience a technical failure during operation, then auto-recovery capabilities in software could reduce the probability of a UDS (*e.g.* engine restart). As the recovery measures have the ability to reduce the negative consequences associated with a failure, this model could also influence standards in the training of RP and development of operational procedures for the management of contingency scenarios.

The presence of recovery measures (*e.g.* automatic recovery parachute) could influence the decision on whether to relax or remove the requirement to obtain consent to operate outside some of the standard operating conditions. When looking at the Civil Aviation Safety Authority (CASA) regulations, this could thus help define the properties of "excluded" or "open" categories of UA. Similarly, when looking at the regulations outlined by EASA, the presence or absence of recovery measures could help define the properties of "open", "specific" or "certified" categories of UA. The Civil Aviation Authority for New Zealand in a new Civil Aviation Rule Part 102 proposed in 2015 notes that in "deciding whether to relax or remove the requirements to obtain consent", one of the consideration would include "system redundancy (such as an acceptable automatic recovery parachute)" [57].

In addition to this, the recovery model could also help influence the adoption of principles of fail safe and fault tolerant designs (something characteristic of Part 1309 regulations).

2.4. Stress model

The stress model describes the uncertainty in harmful conditions (stresses) being realised at a given point and time. The particular harmful condition modelled depends on the type of EoV and the type of harm being characterised as part of the risk assessment. For example, if the consequence to be managed was the physical injury to people, then stresses could include the kinetic energy (KE), momentum, or energy density of the UA. The different stresses can be related to the harmful outcome through one or more harm mechanisms. Example physical harm mechanisms for people include: blunt force, penetration, crushing, blast, burns, lacerations, *etc.* [58]. Factors influencing the characterisation of the stress model include:

1. Type and level of harm of interest (*e.g.*, serious physical injury to a person);
2. Spatial and temporal aspects associated with the UA (*e.g.*, time of impact);
3. Type and design of the UA (*e.g.*, exposed rotating parts, size, frangibility, *etc.*);
4. Conditions at the point of impact (*e.g.*, speed, orientation, *etc.*);
5. Type of EoV (*e.g* people, animals, vehicles, *etc.*)
6. Secondary effects associated with the UA on impact (*e.g.*, blast waves);

UA can have multiple stress characteristics, which can relate to one or more mechanisms of harm, and these can differ with the type of UA. For example, an UA with exposed rotating blades has the ability to cause injury through penetration. If the same UA has sufficient size and momentum, then it may also cause blunt force trauma.

The probability and magnitude of stress can also vary with time and the spatial location of impact. For example, the mass of the UA can reduce with time as fuel or stores are consumed, reducing the potential magnitude of energy on impact. Further, it is more likely to have a higher energy on impact at locations close to the ballistic point than in locations at the extremes of its potential impact distribution.

The properties of the UA and its trajectory can be modified to change the stress characteristic at the point of impact. For example, an UA can have air bags or frangible characteristics that reduce the amount of energy potentially transferred on impact. Similarly, the UA can be placed in an energy minimal configuration (*e.g.*, deep stall, or gradual spiral) prior to impact. While the characterisation of the stress distribution is determined independent of the EoV, the relevant type of stress used in the GRM will depend on the type of EoV.

Debris scattering, sliding, or secondary effects like explosions and the release of hazardous materials will have different associated stress properties that need to be modelled. These stress characteristics can change the size of the impact area. For example, the probability of lethal level of KE is likely to reduce with the increasing distance that the UA slides over the ground. Similarly, the magnitude of pressure associated with a blast wave tends to dissipate with increasing distance from the explosive source.

In summary, the stress model is a key component to the characterisation of consequential outcomes given an impact. Underpinning this model are the various mechanisms for harm. No single mechanism for harm will be suitable for all types of UA. For some UA, one harm mechanism will dominate, while for others, multiple harm mechanisms may need to be considered in order to comprehensively characterise the conditions most likely to give rise to harm to an impacted individual (or other type of EoV). Mechanisms for harm are further discussed in Section §2.7.

2.4.1. Review of stress models

A summary of the stress models identified in the literature are presented in Table 5 of Appendix A. Only 10 of the 33 models (GRMs and component sub models) reviewed explicitly incorporate a stress model. All of the identified models used the KE associated with the UA as the stress characteristic, with the model presented by Ball et al. [12] discussing the effects of explosions and thermal radiation as well. The models used a range of mass and speed values to determine the KE at impact, which is a source of variation between the outputs of the stress models. For example, while determining the KE for small UA flying at low altitudes, Dalamagkidis et al. [49] suggested the use of terminal velocity (or alternatively maximum operating velocity increased by 40%) even though it would be an over-conservative estimate. Ancel et al. [30] makes a similar assumption while evaluating the impact KE. Other models (*e.g.* Ref. [18]) simply assume the maximum velocity while determining the impact energy.

It is noted that the primary mechanism for harm considered in existing models is trauma caused through blunt force impact. For UA of small mass, blunt force trauma may not be the primary mechanism for harm. For example, small multi-rotor UA are more likely to cause physical trauma through penetration (*i.e.*, cutting due to exposed propellers). The Micro-UAS ARC [59] recognise the importance of considering laceration injuries in the stress model. According to Arterburn et al. [60] while small UAS may cause injuries in the form of deep cuts (from vehicles as small as 1–2 lbs), they are unlikely to represent a lethal threat to people in terms of laceration injuries. Until recently there have been limited models that adequately characterise the stress characteristics specific to multi-rotors. This gap led to a number of recent studies characterising the stress (and harm) specific to multi-rotors (*e.g.* model presented in Refs. [18,60]).

Few models account for the stress factors associated with UA with significant on-board stored energy sources (*e.g.*, stored chemical potential, *etc.*) or high kinetic energies, which have the potential to cause secondary hazards such as an explosion. These secondary effects have additional stress characteristics (*e.g.*, thermal radiation, shock waves, fragmentation, *etc.*), which would need to be considered in a comprehensive assessment of the risks. A preliminary discussion of such factors is provided by Ball et al. [12].

2.4.2. *Substantiation of models*

The models that did explicitly mention the importance of the stress model, provided limited detail as to how they were substantiated. The standard KE equations were used to determine the energy the UA had on impact, with modifications made for vertical and gliding descent profiles. The properties of the aircraft (*e.g.* mass, velocity) were UA specific, with certain generalised assumptions made with regards to their terminal velocities. This method of model substantiation could be classified as a hypothetical approach. In addition to this, expert opinion and historical data can also serve as potential sources of input data for these models.

2.4.3. *Representation of uncertainty*

There are a number of factors that influence the stress model. Each of these factors is a source of uncertainty that will directly influence the model. For example, if a small UA crashes into an individual on the ground, then the amount of energy possessed by the system on impact will vary significantly with the type of UA, the relative velocity at the point of impact, the frangibility of the system, the orientation of the UA on impact, the presence of recovery measures, *etc.*. The uncertainty relating to each of these factors will directly impact the amount of energy possessed by the system on impact. In addition to this, the type and characteristics of the EoV on impact and the uncertainty surrounding this, also plays an important role in determining the level of severity the system can impart. Finally, there is limited data from which to develop these models. As each of these models are based on worst case assumptions, they are categorised as having only provided a “Level 1” treatment of uncertainty.

2.4.4. *Relationship to regulations*

The output from the stress model can directly influence the technical regulations relating to the crashworthiness of the UA. These are the design characteristics of the UA that minimise the potential magnitude of stress transferred to an EoV and the probability of secondary hazards occurring. Examples include requirements for the equipage of protective shrouds, or standards specifying the degree of frangibility of leading edges/structure, the protection of fuel stores, and the need for recovery measures such as parachutes to minimise the amount of energy on impact. The stress model can also influence operational guidelines on the design of failure trajectories and requirements for flight termination profiles that minimise the amount of energy on impact (*e.g.* deep stall, gradual spiral).

2.5. *Exposure model*

The exposure model characterises the uncertainty in the presence of EoV at a given location and time. In the context of aviation risk management, we are largely concerned about the risks to people and property, and secondarily the aircraft system. These EoV are classified as [14]:

1. First parties - people and property directly associated with the operation of the Remotely Piloted Aircraft Systems (RPAS) (*e.g.*, the RP, Remotely Piloted Aircraft (RPA) observers, the RPA itself, *etc.*);
2. Secondary parties - people and property not associated with the operation of the RPAS but directly derive benefit from its operation (*e.g.*, a farmer whose crop is being sprayed by a RPA, infrastructure being inspected by the RPA, *etc.*);
3. Third parties - people and property not associated with, nor deriving direct benefit from, the operation of the RPAS.

Aviation regulations prioritise the management of risks to third parties. As such, we limit our discussion to these EoV. In conjunction with the incident stress model (Section §2.6), this factor can have a significant influence on the expected number of casualties.

2.5.1. *Review of exposure models*

Based on the models reviewed (21 exposure models identified in Table 6 of Appendix A), the exposure models can be classified into two main types:

1. Uniform exposure models
2. Comprehensive exposure models

The most commonly used population exposure model is a uniform exposure model. The use of this model ignores potential clustering of a population within a defined geospatial area, and in effect, averages the potential contribution of the exposure factor to the overall risk assessment. Thus, potential peaks in resulting risk arising due to population clustering are not adequately captured by a GRM utilising a uniform exposure model.

A comprehensive exposure model endeavours to account for spatial variations in population distribution (*e.g.*, clustering) and changes in this distribution with time. Geospatial clustering, within buildings or areas of interest, can occur. For example, at sporting stadiums, in schools, or places of work. The distribution is not static, with daily, weekly, and seasonal changes. For example, it is more likely for a student to be indoors during school hours than it is during the hours immediately following the end of the school day. This behaviour will however change during the winter months when the students are on break from school. Such temporal effects have a major role in determining variations in exposure and in turn, variations in the level of risk presented by a UA operation over populous areas.

Models such as those developed by Burke et al. [16] and Melnyk et al. [17] attempt to incorporate temporal aspects, recognising how people spend their day (*i.e.* the kind of job they have, whether or not they go to school, *etc.*). Melnyk et al. [17] provides an example of a comprehensive exposure model, highlighting temporal dependencies in population exposure. According to [61], people spent 68.7% of their time in residence, 7.6% outdoors, 5.5% in vehicles, 5.4% at offices/factories, and another 12.8% in other indoor locations. Melnyk uses this information, along with the information on what a typical area is comprised of (residence (21%), vehicles (7%), open (63%) and other/commercial (9%)) to specify their exposure model. These factors were not taken into consideration in a majority of the models reviewed.

2.5.2. Substantiation of models

Data used to quantify exposure models include:

1. Census data;
2. Geographical data from satellite imagery (*e.g.* Google maps); and
3. Expert opinion.

The source of the census data varied depending on when the individual studies were conducted and what areas were being evaluated. For example, Clothier et al. [27] made use of the Australian Bureau of Statistics data, Burke et al. [16] made use of the U.S. Census Bureau and Stevenson et al. [62] made use of data gathered from the Canadian Census Bureau. The challenge with the use of this data is the low geo-spatial resolution and the lack of temporal information. The models presented by Lum and Waggoner [22] and Waggoner [54] use satellite images to further refine models based on census data. In addition to census data and map information, Di Donato et al. [63] also made use of mobile phone data to provide a more dynamic model of the population distribution. Ancel et al. [30] aims to make use of near real-time population distribution and density via census data augmented by cellular network activity. Other models (*e.g.* Ref. [44]), utilised expert opinion to quantify exposure models.

2.5.3. Representation of uncertainty

Looking at the uncertainty levels in Table 6 of Appendix A, it is seen that the maximum level of uncertainty taken into consideration is ‘Level 1’. The input data for the exposure models come from census data. The uncertainty associated with this model is determined by the spatial-temporal resolution and accuracy of the underlying data.

2.5.4. Relationship to regulations

The exposure model is primarily determined by properties of the environment and the EoV as opposed to the technical design of the UAS. It is a key input for determining the effectiveness of operational restrictions such as limitations on the time of flight, and types of areas overflown (*e.g.*, the definition of a “congested” or “populated” areas), on the overall risk posed by a UAS operation.

2.6. Incident stress model

The incident stress model describes the uncertainty in the magnitude of stress the EoV is exposed to. It characterises the variation in the amount of stress that is transferred to a specific EoV due to a wide range of factors that attenuate (or amplify) the magnitude of stress on impact. Two aspects are incorporated in any incident stress model:

1. The probability that a particular attenuating or amplifying factor is present; and
2. The probability of it having a particular attenuating or amplifying effect given its presence.

For the EoV of people, examples of factors incorporated in an incident stress model include the protection provided by structures or vehicles, or the use of personal protective equipment such as helmets or glasses. Both of which serve to absorb or otherwise reduce the magnitude of energy imparted on a human. An example of an amplifying effect is the concentration of pressure (blast waves) due to surrounding terrain or structures.

The probability of people being sheltered within buildings and the degree of protection provided by a building will depend on the type of area overflown, and the time when the overflight occurs. For example, a residential area will have different structures to that of a light industrial or central business district. Large variations in the number of people in these structures can be expected depending on the time of day as well. For example, people will be expected to be at work under the protection of a building during the day and at home during the night. Differences in the amount of protection provided by these shelters can thus be taken into consideration by accounting for the time of day in which the operation is being undertaken.

2.6.1. Review of incident stress models

A summary of the incident stress models reviewed can be found in Table 7 of Appendix A. Many of the identified GRMs do not account for variation in the incident stress. As such, the models implicitly assume that the EoV is exposed to the entire magnitude of the stress at the point of impact. For example, it is assumed that 100% of the KE of the UA is transferred to an impacted EoV. Whilst a conservative assumption, it can lead to the overestimation of the resulting level of harm.

Of the models reviewed, only 13 incorporated an incident stress model. These models make use of a simple KE model based on worst case scenarios to determine the amount of energy different shelters can absorb, thus providing an overly conservative estimate, and reducing its impact on the GRM. Based on the case study example, the model presented by Waggoner [54] assumes a fatality rate taking the characteristics of the UAS into consideration (*e.g.* fatality rate of one for the Reaper). Similarly, the model presented by Clothier et al. [27] assumes the conditional probability that a strike results in a casualty is one. Both these models thus fail to take the potential sheltering into consideration. They however recognise the limitation of such an assumption. Clothier et al. [27] clearly states that a more accurate model would have to take into consideration the transfer of KE to the individual and sheltering provided by structures. According to Melnyk [17], as these risk models also assume a uniform population distribution, the failure to incorporate the incident stress model into the overall risk model, has a negligible impact on the expected number of casualties. Those risk models that do assume a comprehensive exposure model could however benefit greatly from the incorporation of an incident stress model into the overall risk model. The approaches presented by Melnyk et al. [17] and Ball et al. [12] illustrate different methods of representing the incident stress model using the sheltering factor.

Taking advantage of the studies conducted by the Columbia Accident and Investigation Board and the Department of Defence, Melnyk et al. [17] describes one approach for modelling the incident stress by accounting for population distribution within different kinds of shelters (residential buildings and commercial buildings). The model also accounts for differences in the degree of protection offered by the different types of structures. In addition to this, the model also recognises the importance of taking chemical energy effects due to fuel into consideration.

The model presented by Ball et al. [12] looks at the influence of the incident stress model on the overall risk posed by the system by subtracting the amount of KE that is absorbed by the shelter as it deforms, breaks, and moves due to an incident KE. The deformation models are based on existing studies for inert debris impacts [64].

2.6.2. Substantiation of models

The output from the incident stress models were either a point estimate on the sheltering factor or a representation of the amount of energy various shelters can absorb, and consequently the amount of protection they provide. Incident stress models were quantified using census data, expert opinion, or a combination thereof. The majority of models used expert opinion to quantify the sheltering factor by providing a value ranging from 0 (100% shelter) to 1 (no shelter) to represent the amount of shelter provided for the case study scenario. The protective characteristics of different structures, when considered in a model, were based on historical studies of inert debris impacts [64,65]. These studies assume an inert and infrangible impactor, which may prove to be limiting, taking the unique characteristics of the UA into consideration.

2.6.3. Representation of uncertainty

The incident stress model encapsulates the uncertainty in the attenuating (or potentially amplifying) aspects of the environment on the impact stress and ultimately, the magnitude of stress the EoV is exposed to. Data in relation to the distribution of population to shelters are limited to broad area population models, such as that provided through census data. Similarly, the type and structural composition of shelters are largely limited to local government databases. This results in a considerable amount of epistemic uncertainty. More recent work [30] has utilised satellite imagery to provide higher resolution models of structure locations in a smaller defined area. A second source of uncertainty lies in the modelling of the energy absorbed by certain types of structures. The reviewed models all utilise existing impactor studies, which were based on impact data from inert and infrangible debris. Thus, the models implicitly inherit the assumption that the impacting UA is also inert and does not undergo deformation. UA will undergo deformation on impact, consequently, the structures are likely to offer greater protection than characterised by these models.

2.6.4. Relationship to regulations

The incident stress model will be a key factor in determining operational restrictions for different types of UA. Specifically, the incident stress model will contribute to what defines a populous area relevant for different types of UA. For example, it may be acceptable to operate small UA over populated areas where people are adequately sheltered but not over exposed groups. Alternatively, for small UA, permissions to operate at night over populous areas may be enabled due to the higher proportion of people protected in structures. The incident stress model can also be used as a basis for determining the minimum level of protective personal equipment for operational personnel (first and second parties) or building design criteria for airport structures.

2.7. Harm model

The harm model characterises the uncertainty in the level of consequence/damage caused to an EoV given their exposure to an incident level of stress. Put simply, the harm model characterises the response of the individual to one or more incident stresses. For example, the harm model can describe the probability that an incident stress of certain magnitude (*i.e.* energy, momentum, *etc.*) will result in an injury of varying degrees of severity (*e.g.* minor, major, fatal). A harm model relates the incident stress to the type and severity of the outcome. Characteristics that influence the development of the harm model include the:

1. Type of EoV being considered;
2. Mechanism of harm being evaluated;
3. Degree of independence between mechanisms of harm; and
4. Characteristics of a specific EoV that influence its response.

What constitutes harm will depend on the type of EoV at risk. For example, people, property, animals, the environment, or the UAS itself. The type of EoV determines the types of harm and harm mechanisms that need to be evaluated. An incident stress can cause harm to an EoV through one or more harm mechanisms. In the context of physical harm to people, these mechanisms can include blunt force, penetration, crushing, blast, burns, and laceration. The properties of the UA and the types and magnitudes of the incident stress on impact will determine which harm mechanisms need to be modelled. For example, the dominant mechanism for harm for very small and small multi-rotor UA are penetration and laceration, whereas for large UA, it is crushing and blunt force trauma. While each of these harm mechanisms have the potential of causing serious injury on their own, when considered together, they may have even more severe consequences. The harm model needs to account for each potential mechanism of harm in isolation and in combination. The specific characteristics of individual EoV will influence their response to an incident stress. For example, an individual's height, weight, and build, and their position on impact (*e.g.* sitting, standing, or lying down), will influence their physical response to an incident stress.

2.7.1. Review of harm models

A total of 17 harm models were identified. A summary of identified harm models is provided in Table 8 of Appendix A. It was found that many of the existing GRMs did not incorporate a harm model. In so doing, it is implicitly assumed that the probability of a human casualty given an impact (*i.e.,* level of incident stress) is one. Whilst conservative, this assumption is not valid for all types of UA and can lead to an overestimation of the risk for smaller UA. According to the Range Commanders Council (RCC) an exception may be made to the use of unit probability in the case of very light systems [66] such as small UA. In this case a limit must be defined that divides UAS into two categories, those that do, and those that do not have the potential to cause fatal injury [50]. Weibel et al. [55] introduced a penetration factor for calculating the probability of fatality to take into consideration the fact that a person might survive a UAS impact.

Of the harm models identified most do not specify the particular harm mechanism considered. Of those that do, the most commonly modeled harm mechanism is that of a blunt force trauma. According to Shelley et al. [44], the most likely impact injuries are injuries to the head, particularly skull fracture. More recent research (*e.g.*, [67]) has started to explore the importance of studying the human response to cutting and penetration (the likely dominant mechanism for harm for small multi-rotor UA). This study was based on another study conducted by Ref. [68] that looked at the damage caused by actual remotely controlled helicopter blades to human cadaver eyes. While the experiments were not well documented and the blades used were for very light weight indoor models, with weak motors and light blades, it serves as one of the only current sources of data for characterising a model of the penetration harm mechanism [67].

In the context of UAS safety analysis, the identified models have not explored the combined effects of multiple harm mechanisms. This will be particularly important in the characterisation of harm for those UA where no particular harm mechanism dominates (*e.g.*, small to medium sized multi-rotor RPA). This marks an area requiring further research. In addition to this, with the exception of the model developed in Ref. [67], the identified harm models assume the EoV impacted is an adult male, which, by virtue of their physiology, are on average more resilient to harm than other sub-categories of the general population (*e.g.*, children, the elderly, or females, *etc.*).

A few of the harm models reviewed (*e.g.* Refs. [44,50]) model the conditional probability of harm based on experimental data collected in historical studies. One such study is that conducted by Feinstein et al. [69] where the effects of blast, debris and other factors to people were investigated. Distributions characterising the probability of fatality as a function of incident KE for various impact locations have been developed [69]. The model describes the harm response of an average male, averaged over varying impact orientations. A standard logistic curve for the probability of fatality described in Ref. [44] is presented in Eqn. (1):

$$P(fatality|impact) = \frac{1}{1 + e^{-k\left(E_{imp} - E_o\right)}} \tag{1}$$

Where E_o is the impact energy associated with a 50% probability of a fatality (measured in Joules), E_{imp} is the impact energy and k is a constant. A number of advancements over this standard equation have been presented by Dalamagkidis et al. [70] and Shelley et al. [44] to name a few.

Magister [56] makes use of a blunt criteria (BC) that relates the kinetic energy on impact with the body's ability to tolerate the energy on impact, which is expressed using the Abbreviated Injury Scale (AIS). When compared to impact kinetic energy alone, this has a stronger potential of predicting the level of injury upon impact [71].

Models also vary in how they specify the resulting harm. People hit by a falling unmanned aircraft, but not fatally injured, may have received injuries of varying severity, depending on the force of the impact [44]. Casualty and fatality are two terms often used to describe the resulting harm and have different limits for the KE associated with them. For example, the RCC set a limit of 15 J (11 ft lb) for casualty (*i.e.* reversible injury) and 34 J (25 ft lb) for fatality (*i.e.* non-reversible injury or death). The AIS appears to be emerging as a common scale for describing a level of traumatic injury (another scale used to relate the impact energy to the severity of skull fracture is the Head Injury Criterion). The AIS represents the threat to life associated with the injury, rather than the comprehensive assessment of the severity of the injury [67]. The scale ranges from zero to six, where zero represents no injury and six represents a fatal injury. Injuries with an AIS of greater than three are considered life-threatening.

Finally, on review of the models, it was made evident that only direct physical harm has been considered. Longer term physical (morbidity) and psychological effects have not been modelled. Such harmful outcomes may be more significant than the direct physical harm caused by the UA, particularly for smaller UA. Other forms of harm, such as economic loss or environmental damage have also not been considered in existing models.

2.7.2. *Substantiation of models*

The three different approaches used to substantiate harm models include:

1. expert elicitation;
2. historical accident and incident data and;
3. impactor studies.

The models presented in Refs. [22,27,30,54,55] use expert judgement to assign fixed probabilities of fatality given specified characteristics of the UA. Specifically, the probability of a fatality given an impact for a larger UA such as a Reaper is assumed as one, while a lighter UA such as the ScanEagle is assumed to have a probability of fatality of 0.5 [22,54]. Similarly, Clothier et al. [27] and Weibel et al. [55] assume a probability of casualty and probability of fatality (respectively) of one, for any UA that strikes an individual.

Historical data for accidents and incidents have been used to inform the development of harm models (*e.g.* Refs. [16,17,46,67,72]). While historical data can be used to evaluate the level of harm a particular UA can cause in terms of KE imparted, there are a number of factors that need to be taken into consideration. These include the characteristics of the UA, type of EoV being considered, mechanism of harm being evaluated, degree of independence between mechanisms of harm and characteristics of a specific EoV that influence its response. Using historical data (particularly from manned systems) to determine the level of harm might bring to question the suitability of the approach, owing to the rapidly evolving pace of the technology, continually changing system baselines and the uncertainty associated with the operation of these systems.

Existing harm models based on experimental impactor studies have also been adapted and applied (*e.g.* models presented in Refs. [12,28,44,49,50,60]). Most commonly used is the blunt force trauma model developed in Ref. [69], which describes the probability of fatality as a function of impactor KE. Other physiological models based on experimental data are presented in Refs. [73–75] and are used to estimate the force causing skull fracture. The model presented in Ref. [67] looks at both impact to the thorax and head and recognised the importance of extending the harm model to include cutting injuries from rotating blades.

2.7.3. *Representation of uncertainty*

According to Melnyk et al. [17] the actual deaths or severe injury of a human caused by a falling object or debris is a highly complex problem that cannot be accurately modelled in a physics-based approach. Melnyk et al., however, make use of other studies of injuries caused by explosives and debris to provide the best possible model given the limited data. These studies often make use of impactors in the form of projectiles that are assumed to be inert, *i.e.* no deformation occurs on impact. UA would however behave differently and are more likely to deform and break during impact. In addition to this, most of these models make the assumption that on impact all of the energy from the projectile is imparted to the object. It is however argued that if the mass of the projectile is comparable or larger than that of the body part struck, not all of the KE will be absorbed by the impacted person. After impact the object will continue to move, in unison with the body, retaining some of the KE. Failure to take this into consideration may add to the uncertainty in the model. While this may provide a conservative estimate on the risk, it needs to be taken into consideration while developing the model. In addition to this, assuming an adult male in evaluating the amount of energy an average person can withstand may result in an underestimation of the risk as it ignores potentially more susceptible sub-groups within an exposed population. The uncertainty associated with the demographic of the person impacted is another factor that needs to be taken into consideration while developing the harm model. Next, most of the models assume the reference is standing upright when impacted by the UA. The orientation of the individual in conjunction with the orientation of the UA can greatly influence the level of harm imparted by these systems and thus marks another area where research effort needs to be focused. Finally, most of the models only take blunt force trauma into consideration. Failure to take the effect of cutting or lacerations into consideration may result in an underestimate of the risk. Each of these factors may result in a non-conservative estimate of the risk and as such the uncertainty associated with it should be taken into consideration while developing the models and consequently setting the regulations associated with them.

2.7.4. *Relationship to regulations*

An understanding of different thresholds for harm will be a key factor in determining operational and airworthiness categorisations of UA and has been the focus of most research to date. Understanding the impact of different harm mechanisms (*e.g.* penetration, lacerations*)* on the human body, will allow regulators to determine whether or not certain type of UA (*e.g.* small UA) should be allowed to operate. It would also provide a justifiable means of evaluating the need for certain harm mitigation measures (*e.g.* need for protective shrouds), and their inclusion in the airworthiness requirements of the system. Looking at blunt force trauma, based on the threshold energy the human body can absorb, regulators will be able to define weight restrictions and operational restrictions for certain UA.

3. Discussion

Based on the preceding discussion it is evident that there are a number of areas where opportunity for future research exists.

Firstly, failure models need to be modified to take the variable failure rate associated with UAS into consideration. Adoption of a Bayesian approach to take the limited data and high uncertainty associated with UAS into consideration is needed. Future work is looking at adopting a BBN to model this component of the GRM. BBN are graphical structures that make use of probabilistic reasoning to ascertain information about the unknown [85] and are beneficial when expert opinion is ambiguous, incomplete or uncertain [86]. They explicitly model causal factors; allow for reasoning from effect to cause and vice versa; reduce the burden of parameter acquisition; allow for previous beliefs to be overturned in light of new evidence including both subjective beliefs and objective data and arrive at decisions based on visible, auditable reasoning [87].

Secondly, a more transparent representation of the factors influencing impact sub-models is required. In addition to this, a means to incorporate the uncertainty associated with the overall impact model and the individual factors that go into defining it is also needed. Future work needs to look at improving the fidelity of the impact location model; going beyond the uniform impact distribution models currently used. This sub-model is particularly important to the development of operational regulations for UAS. Impact sub-models need to be extended to include different failure modes and the biasing effects emergency procedures and recovery systems have on the potential distribution of impacts.

Currently there is very limited research into the development of recovery sub-models. The presence of recovery mechanisms can significantly reduce the risk posed by certain UAS and subsequently, are widely used as a risk control within UAS safety cases.

Looking at the stress model, it is evident that future work needs to look at the influence of some of the additional harm mechanisms (*e.g.,* lacerations), the relationship between the types/size of UAS and the probable mechanisms of harm, and the combined effect multiple mechanisms for harm have on an EoV. No research to date has been conducted on the non-physical effects of an UA impact. Non-physical effects can be the dominant harm mechanism for very small and small UA. Secondary hazards, such as vehicle accidents, bush fires, blasts, or release of hazardous materials, should also be characterised.

Future research into GRMs should seek to adopt more comprehensive population distributions for the areas of operation. The use of novel approaches such as those that take advantage of mobile phone data to determine the population distribution may also prove to be beneficial. Additional census data on employment and dwelling types can be used to improve the fidelity over uniform exposure models. The models presented in Refs. [61] and [76], while not directly applied to the risk modelling of UAS operations, provide examples of more comprehensive approaches to the broad area of population distribution modelling.

Future research efforts should focus on developing a better representation of the distribution of third party people in shelters and of the protective properties of different types of shelters. This will be an important factor in determining regulatory requirements, particularly in relation to the operation of small UAS over populous areas.

Finally, harm models need to be expanded to include consideration of human response to multiple mechanisms of trauma. The combined effect of multiple harm mechanisms could have severe consequences, and cannot be considered as independent. An industry standard harm scale (*e.g.*, AIS) should be used to ensure consistent measurement of consequence and to facilitate intra- industry and inter-industry risk comparisons. Furthermore, extending the assumed demographic to include a more realistic population demographic will ensure peak risks to more susceptible sub-populations are captured. Whilst not a topic of objective risk assessment, how the public respond to various harmful outcomes should also be considered.

4. Summary

There are a number of high level findings that can be made on the basis of the preceding review. Of these, perhaps the most significant findings relate to 1) the diversity of models; 2) cascading assumptions, and 3) the inadequate treatment and representation of uncertainty.

4.1. Diversity of models

There is significant diversity in the developed models. This diversity arises due to differences in 1) the nature of the risks associated with a particular UA type and its Concept of Operations (CONOPs), 2) the treatment of uncertainty (*e.g.*, underlying assumptions), or 3) the specific question that needs to be answered by the model (*e.g.*, support for a particular aspect of the regulation). As international aviation safety regulators move towards a set of harmonised, outcome based, and risk-informed regulations for UAS, the need for a consistent approach for assessing and managing the risks associated with their operation will increase. Whilst the conditions describing acceptable risk will vary between regulatory authorities, the method used to assess the risk should be consistent. For reasons discussed in the previous sub-sections, a single universal risk model is not practical; risk models will need to be developed and tailored to the particular UAS type and general CONOPs. However, it is possible to define the high level components of a risk model and identify the influencing aspects that need to be addressed, in the development of specific GRMs for UAS. Such requirements on the development of GRMs would aid in the systematic and consistent assessment of the risk UAS operations pose to people and property overflown. The framework of sub-models illustrated in Section §2 and the discussion presented in the preceding sections of this paper could provide the basis for the development of such a set of requirements.

4.2. Cascading assumptions

This relates to the inadequate treatment of uncertainty but warrants discussion in its own right. Numerous assumptions are made in existing models. The review found that many of these assumptions are implicit and undocumented, and where explicit, their impact on the resulting assessments of risk are not explored. Assumptions are an inescapable necessity in any modelling task, particularly in situations of low data, low operational experience, and complex systems. Assumptions relating to the development of the model itself (*e.g.*, model components and data used to qualify the model) give rise to epistemic uncertainty in the assessment of risk. Whilst the risk analyst's default position is to reach for the conservative "worst case" position when faced with an uncertainty, these assumptions may not represent the "conservative" position for all UA types and operations. More specifically, the justification for a particular assumption may not be valid for a particular UAS type or CONOPs. The cascading effect of these assumptions within a single model have not been explored. A series of conservative assumptions can lead to overly conservative risk estimates, and in turn, impose unnecessary regulatory cost on the industry. The reviewed models do not adequately document their assumptions nor provide a rigorous analysis of their potential impact. Such analysis would be required of a GRM used as the basis for the development of regulations for UAS.

4.3. Treatment of uncertainty

Under a risk-informed regulatory approach the output of the GRMs are intended to support decision making in relation to various aspects of the regulation of UAS. Objective, systematic and justifiable decision making on the basis of the outputs from these models requires a

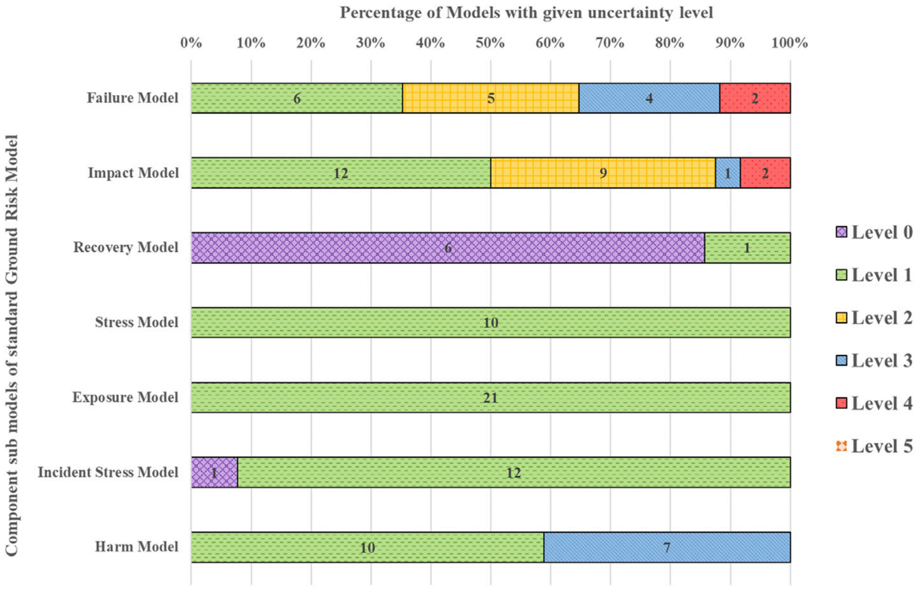


Fig. 3. Comparison of the levels of treatment of uncertainty in component models.

comprehensive and objective presentation of the associated uncertainties in the estimates. These uncertainties are broadly characterised as epistemic and aleatory in their nature. The treatment and presentation of uncertainty varies between risk models. A visual illustration of the different levels of uncertainty observed across the identified sub-models and GRMs is presented in Fig. 3. The levels of treatment of uncertainty are based on the definitions provided by Pate-Cornell [26] as summarised in Table 1. Evident in Fig. 3 is the variation in the treatment of uncertainty between sub-models. Comprehensive methods characterising and presenting uncertainty in failure and impact sub-models have begun to be developed. Whereas analysts have provided only a cursory treatment of uncertainty in the stress and exposure sub-models.

From the review it was also seen that the treatment of uncertainty varied across the sub-models within a single GRM. The highest level of uncertainty taken into consideration was Level 4, and this was seen in Refs. [18,30] (failure models) and [46,48] (impact models). None of the existing models provided a comprehensive treatment of uncertainty (Level 5).

The general argument for a more comprehensive treatment of uncertainty in risk assessments is well established (*e.g.*, see Refs. [13,77]) and for brevity is not repeated here. When considered in the context of supporting the development of regulations for UAS, a comprehensive treatment of uncertainty across all component sub-models of the GRM is needed to ensure objective decision making. This in turn supports more transparent, systematic, and consistent regulatory decision making; necessary for the development of justifiable regulations that have a clear and traceable relationship to the safety risks they are intended to manage.

5. Conclusion

This paper provides an extensive review of the current state of the art in ground risk modelling for UAS operations. By identifying each of the sub-models that go into developing a GRM, and relating them to various aspects of the current aviation regulatory framework, this paper also provides a means for identifying where future research efforts need to be focused and how this will potentially influence the ongoing development of regulations for the sector.

The review highlighted three major findings in existing models: 1) the diversity that exists amongst the models; 2) the prevalence of cascading assumptions and 3) the inadequate treatment and representation of uncertainty. Each of these findings will have a significant impact on the development of regulations for UAS. The diversity amongst these models can lead to a lack of consensus and variability in the risk assessment outputs that are input into regulatory decision making process. The inadequate treatment and representation of uncertainty and adoption of conservative assumptions has the potential to lead to overly conservative regulations and the imposition of unnecessary restrictions and cost on the sector. Like the nuclear and space industries, the UAS industry has limited data and high uncertainty associated with it. In order to bring the risk assessment process for the UAS industry in line with other more contemporary models proposed by the nuclear and space industry, it is of paramount importance to take the uncertainty associated with these systems into consideration. In addition to this, the review also clearly highlights certain sub models where future research efforts could be focused (*e.g.* recovery model, stress model). Developing these sub models will directly influence the overall risk model and the regulations they impact.

Regulators are increasingly moving towards the development of risk-based regulations. With it, there is a growing need for risk models that provide decision makers with a more comprehensive representation of uncertainty associated with assessments of the risk. Such models are needed to support more transparent, systematic, and consistent regulatory decision making; necessary for the development of justifiable regulations that have a clear and traceable relationship to the safety risks they are intended to manage.

Acknowledgements

This research was supported, in part, by the Australian Government Research Training Program Scholarship, provided by the Australian Government.

Appendix A

Table 2
Summary of failure models.

Reference	Failures/Modes Addressed	Failure Model	Method of Model Substantiation	Assumptions and Notes	Uncertainty Level
Aalmoes et al. [46]	Single non-specific system failure mode	Constant Failure Rate	Based on historical data from current conventional manned aircraft. Data from National Transport Safety Board (NTSB) used for cruise phase.	Flight divided into three phases, take-off phase, cruise phase and a landing phase. Risk for each phase is evaluated and then summed up for the whole flight.	Level 2
Ancel et al. [30]	Single system failure mode (unpowered descent/terminated flight)	Constant Failure Rate	Dynamic aircraft health data used. However development phase was based on historical data (manned), numerical distributions and military operational data (manned and unmanned)	–	Level 4
Awad [45]	Single non-specific system failure mode	Constant failure rate	Based on historical Class A mishap rate data from National Transport Safety Board (NTSB).	Acknowledges that failure rates vary depending on several factors (*e.g.* for manned aircraft, failure rate is higher near airports). Case study example of MQ-9 Reaper and ScanEagle used.	Level 1
Barr et al. [18]	Multi-dependent failures LOC and CFIT	Constant failure rate (Poisson distribution)	Based on arbitrary and preliminary data to illustrate concept (historical and expert opinion)	Includes four major aircraft system failures (propulsion, power, flight controls and navigation), two inappropriate ground personnel actions (operator/pilot and maintenance related actions), two low-level hazards (inappropriate/impaired flight control input and aircraft state conducive to LOC) and three main hazards (inappropriate guidance, loss of control and loss of aircraft structural integrity). Makes use of Bayesian Belief Networks	Level 4
Burke et al. [16]	LOC (Catastrophic) and UDS	Constant Failure Rate	Calculated based on geometry and population density (Expert opinion)	Makes use of system/functional level breakdown of the UAS to relate lower-level failures to a system level failure mode	Level 2
Clothier et al. [27]	Single non-specific system failure mode (Hazardous failures)	Constant Failure Rate	Assumed value of 10^{-5} per flight hour (expert opinion)	Hazard of discontinuance of flight due to Unrecoverable flight critical event	Level 2
Ford et al. [29]	Catastrophic failures and Hazardous failures	Constant Failure Rate	Assumed to be 10^{-5} per flight hour for catastrophic and 10^{-4} per flight hour for hazardous (expert opinion)	Failure was considered to be catastrophic if it resulted in an uncontrolled flight termination. In comparison hazardous failures posed a reduced risk of casualty. These values were chosen to be an order of magnitude worse than the nominal definitions of improbable and remote frequencies.	Level 1
King et al. [20]	Catastrophic LOC	Constant Failure Rate	Based on manned aircraft limits (from regulations) and properties of systems (historical data)	–	Level 1
Lum et al. [23]	Catastrophic LOC	Constant Failure Rate	Based on experimental results and hardware in the loop simulation.	Failures were introduced at random times, uniformly sampled from the reference flight.	Level 3
Lum et al. [22]	LOC	Constant Failure Rate	Based on historical data of case study UA (different values for each scenario).	As UAS tend to have high mishap rates during take-off and landing, the failure rate used will only represent mid-flight failures (to avoid overestimation of the risk) if take-off and landing are performed in a restricted area free of pedestrians.	Level 3
McGeer et al. [21]	Single non-specific system failure mode	Constant Failure Rate	Use of general aviation limits and case study examples (*e.g.* data from Boeing 747). (historical data)	Model is based on general aviation. Data for Aerosonde used to evaluate model.	Level 2
Shelley [44]	Single non-specific system failure mode	Constant Failure Rate	Assumed from data used by FAA UAS task force (100 h, MTBF).	MTBF (Mean Time Between Failures). The reciprocal of MTBF gives the expected number of failures per hour.	Level 2
Stevenson et al. [62]	Single non-specific system failure mode	Constant Failure Rate	Assumed MTBF 10^5 for sub-urban and 10^6 for urban areas based on expert judgement.	–	Level 1
U.S. Army Corps of Engineers [28]	Catastrophic	Constant Failure Rate	Historical data used from space shuttle, shuttle orbiter and X-15 descent used	Risk analysis for generic UAS used. No fault tree or FMEA.	Level 3
Waggoner [54]	Single non-specific system failure mode	Constant Failure Rate	Based on historical data of case study UA (different values for each scenario).	–	Level 1
Weibel et al. [55]	Single non-specific system failure mode	Constant Failure Rate	Reliability estimated based on, impact area, population density, probability of penetration, mitigation factor and target level of safety.	Failures are measured as any general type that leads to an accident, including mechanical and software failures, human error, and combinations of events that result in a ground impact.	Level 3
Wolf [78]	Single non-specific system failure mode	Constant Failure Rate	Logistic regression and artificial neural network failure prediction models were used. Based on historical data from Air Force Research Laboratory Munitions Directorate that comprises of over two dozen types of UAS and has five years' worth of data.	Logistic regression and artificial neural network failure prediction models were used for failure prediction, damage prediction and comparison of human vs. mechanical errors.	Level 1

Table 3
Summary of impact models.

Reference	Failure Modes	UA Type	Point or Area	Lethal area	Method of Model Substantiation	Assumptions and Notes	Uncertainty Level
Aalmoes et al. [46]	Single non-specific system failure mode	Tilt-rotor and multi-rotor	Area	Yes	Hypothetical: Geometry (Gliding)	Bivariate normal distribution used based on [27].	Level 4
Ancel et al. [30]	CFIT, LOC	Multirotor (octocopter)	Area	Yes	Hypothetical: Geometry (Gliding)	Descent rate assumed to be equivalent to terminal velocity. 2- sigma impact point uncertainty obtained by Monte Carlo analysis	Level 2
Awad [45]	Single non-specific system failure mode	Fixed-wing	Point	Yes	Empirical: size based (NTSB data for manned aircraft)	Based on Lum and Waggoner [22]	Level 1
Bleier et al. [53]	UDS	Fixed-wing	Area	No	Hypothetical: Geometry (Gliding)	Evaluates scenario of an unrecoverable loss of propulsion (*e.g.* motor failure). Assumes that the aircraft is still steerable and the gliding performance is not degraded.	Level 1
Bradley et al. and Ball et al. [12,47],	Single non-specific system failure mode	Fixed-wing and rotary-wing	Area	Yes	Hypothetical: Geometry (Gliding and Vertical)	Also takes skid distance into consideration. LCA is based on assumption of fixed wing geometry.	Level 2
Burke et al. [16]	UDS and LOC	Fixed-wing	Point	Yes	Hypothetical: Geometry	Assumes aircraft does not breakup during flight. Assumes model between Gliding and Vertical.	Level 1
Clothier et al. [27]	Flight Critical Failures	Fixed-wing	Area	Yes	Hypothetical: Geometry (Gliding and Vertical)	Assumed Bi-variate normal distribution used for case study.	Level 2
Cour-Harbo [48]	UDS (Complete loss of lift)	Fixed-wing and multirotor	Area	No	Hypothetical: Geometry (Ballistic)	Based on a second order drag model with probabilistic assumptions on the least well-known parameters of the flight, and includes the effect of wind. Probability density function used for travelled distance.	Level 4
Dalamagkidis et al. [49]	Single non-specific system failure mode	Fixed-wing and multi-rotor	Point	Yes	Hypothetical: Geometry (Gliding and Vertical)	–	Level 1
Dalamagkidis et al. [50]	Single non-specific system failure mode	Fixed-wing and rotary-wing	Point	Yes	Hypothetical: Geometry (Gliding and Vertical)	–	Level 1
Ford et al. [29]	Flight critical catastrophic and hazardous failures	Fixed-wing	Area	No	Hypothetical: Geometry (Gliding and Vertical)	Maximum range dictated by the unpowered glide ratio. Variation in side forces, such as wind, is neglected, such that the aircraft is equally likely to impact to the right or left of its position. (based on [27])	Level 2
Foster et al. [52]	LOC	Multirotor	Point	No	Hypothetical: Geometry (Gliding and Vertical)	Based on simulations and wind tunnel tests	Level 1
Guglieri et al. [79]	Single non-specific system failure mode	Fixed-wing and multi-rotor	Area	Yes	Hypothetical: Geometry (Gliding and Vertical)	Based on studies conducted by the FAA for commercial space launch and re-entry missions. Glide angle for MH850 set equal to 45°. For QX-Rotor, vertical impact crash is considered, therefore glide angle is set equal to 90°.	Level 1
Haartsen et al. [51]	Single non-specific system failure mode	Fixed wing and multi-rotor	Area	Yes	Hypothetical: Geometry (Gliding and Vertical)	Based on simulations and [43]	Level 1
King et al. [20]	LOC	Multi-rotor (VTOL) UAV	Area	Yes	Hypothetical: Geometry (Gliding and Vertical)	Based on Columbia accident investigation board study. Based on ballistic properties.	Level 2
Lum et al. [22]	Catastrophic (System Failures)	Fixed-wing	Point	Yes	Hypothetical: Geometry (Gliding and Vertical)	For crashes due to system failure it is assumed that upon failure the UAS glides towards the ground at maximum L/D (worst case scenario) with glide angle γ.	Level 2
Lum et al. [23]	Catastrophic	Fixed-wing	Area	Yes	Hypothetical: Geometry (Gliding)	Point of impact is used to develop a PDF which can be used to determine the horizontal distance travelled before impact likelihood. Based on simulations.	Level 3
McGeer et al. [21]	Single non-specific system failure mode	Fixed-wing	Area	Yes	Hypothetical: Geometry (Gliding)	Based on Aerosonde case study example	Level 1
Melnyk et al. [17]	Single non-specific system failure mode	Fixed-wing	Point	Yes	Empirical: Weight based (linear)	Based on model developed by Ref. [19] for manned aircraft. Different values used for built up and open areas.	Level 2
Shelley [44]	Single non-specific system failure mode	Fixed-wing	Point	Yes	Hypothetical: Geometry (Vertical)	–	Level 2
Stevenson et al. [62]	Catastrophic	Fixed-wing	Point	Yes	Hypothetical: Geometry (Gliding)	–	Level 1
Waggoner [54]	Single non-specific system failure mode	Fixed-wing	Point	Yes	Hypothetical: Geometry (Gliding and Vertical)	–	Level 2
Weibel et al. [55]	Single non-specific system failure mode	Fixed-wing (varying sizes)	Point	Yes	Hypothetical: Geometry (planform area)	–	Level 1

Table 3 (*continued*)

Reference	Failure Modes	UA Type	Point or Area	Lethal area	Method of Model Substantiation	Assumptions and Notes	Uncertainty Level
Wu and Clothier [43]	Unrecoverable Flight Critical Failures	Fixed-wing	Area	Yes	Hypothetical: Geometry (Gliding)	6 Degree of Freedom impact footprint boundary model used	Level 1

Table 4
Summary of recovery models.

Reference	Recovery Mechanism	Assumptions	Uncertainty Level
Ancel et al. [30]	Return to base command	Assumed minimum acceptable navigation capability and lost link status	Level 0
Bleier et al. [53]	Parachutes	Location of parachute deployment is based on decision making process that aims to minimise the risk of endangering humans, minimise the chance of property damage and maximize the expectation of aircraft survival.	Level 1
Ford et al. [29]	Ability to put the system into glide to maximize glide range	Wind and other transient acceleration effects are ignored	Level 0
Magister [56]	Engine emergency termination system with propeller braking supplemented with optional propeller blades folding for more effective injury minimization. Use of airbags or parachutes also recommended.	Assumed that parachute is capable of reducing impact velocity to below $v_{\min}$	Level 0
McGeer et al. [21]	Deadman's switch	Loss of flight computer, would cause loss of tracking performance. This would trigger Deadman's switch and kill the engine, the aircraft would then crash with equal probability, anywhere within the gliding range.	Level 0
Shelley [44]	Parachutes	Target descent speed of 4.6 m/s is assumed for this analysis	Level 0
Weibel [55]	Mitigation measures which include 1) reduce the exposure to risk of the public on the ground, 2) ensure UAV system reliability, 3) facilitate safe recovery from failures, 4) reduce the effects of UAV ground impact.	Type of mitigation is dependent upon vehicle class, type of operation, and the level of safety required.	Level 0

Table 5
Summary of stress models.

Reference	Stress Characteristic	Mechanism	Type	Notes	Uncertainty Level
Arterburn et al. [60]	KE	Blunt force, penetration, lacerations	Multi-rotor	Terminal velocity used in developing estimate stress (KE)	Level 1
Ball et al. [12]	KE, Explosion, Thermal Radiation	Blunt force	Fixed-wing and rotary-wing	A more likely source of injury and lethality to 3rd persons was the effects of primary and secondary fires due to unspent aviation fuel. Using algorithms provided by the Department of Energy, the amount of heat released from a resultant fire in a crash could be determined. This was then correlated with the time it takes human tissue to burn, as well as fatality studies that relate burn amount to lethality.	Level 1
Barr et al. [18]	KE	–	Fixed-wing and multi-rotor	Terminal velocity used in developing estimate of stress (KE)	Level 1
Burke et al. [16]	KE	Blunt force	Fixed-wing	All small UAS are going to reach effectively the same terminal velocity during an uncontrolled crash. With this assumption, the KE variation between the different aircraft is reduced to a function of its mass or weight.	Level 1
CASA [67]	KE	Blunt force	Fixed-wing and multi-rotor	KE function of mass and velocity	Level 1
Dalamagkidis et al. [49]	KE	–	Fixed-wing and multi-rotor	The KE imparted at impact is a function of impact speed that may vary depending on the UAS and the trajectory of descent. Maximum operating velocity increased by 40% is proposed. Terminal velocity also used for case study.	Level 1
Guglieri et al. [79]	KE	–	Fixed-wing and multi-rotor	KE function of mass and velocity. Different velocities used for different case study examples. For MH850 the maximum operative speed increased by 40% is used. For QX-Rotor, the freefall velocity from 70 m is used.	Level 1
Magister [56]	KE	Blunt force	Fixed-wing	KE is a proportional factor to the aircraft hazard potential. Two scenarios evaluated. The unpremeditated descent scenario with impact at velocity 30% over minimal (*i.e.* stall airspeed with UA is under control but unable to maintain altitude) and Loss of control scenario with UA impacting at velocity 40% higher than maximum airspeed attainable in level flight.	Level 1
Melnyk et al. [17]	KE	Blunt force	Fixed-wing	KE based on the mass of the air vehicle and a value of 1.4 times the maximum speed of the vehicle as proposed by Ref. [49].	Level 1
Skobir et al. [72]	KE	Blunt force	Fixed-wing	KE based on the maximum take-off mass of the vehicle and UA impact ground speed which in still weather equals the air speed and depends upon the UA crash scenario.	Level 1

Table 6
Summary of Exposure models.

Reference	Exposure Model	EoV at Risk	Method or Data used in Substantiation of Model	Assumptions and Notes	Uncertainty Level
Aalmoes et al. [46]	Comprehensive	Third party people	Evaluated based on simulations	–	Level 1
Ancel et al. [30]	Comprehensive	Third party people	Case study example (occupants of buildings used with longitude and latitude information to determine population around each building, parking lots and walkways)	Model allows for percentage of population to be out in the open. Future work: develop near real-time population distribution and density via census data augmented by cellular network activity	Level 1
Andrew et al. [80]	Uniform	Third party people	Census data from the 2012 U.S. Census Bureau used.	Population density for any given area is a function of the localised population divided by the area.	Level 1
Awad [45]	Uniform	Third Party people	Census data from U.S. Census Bureau	Pedestrian density is equal to population density	Level 1
Barr et al. [18]	Uniform	Third Party people	Population values obtained from demographia [81] and based on expert opinion.	Five individual cases considered, namely, sporting event, urban environment, suburban environment, rural setting and remote setting. Variety of assumptions made for each.	Level 1
Burke et al. [16]	Uniform	Third party people	Correlation of population density data from U.S. census data with sectional maps for the U.S. using geographic information systems program.	Population density divided into four categories (unpopulated, sparsely populated, densely populated and open air assembly).	Level 1
Clothier et al. [27]	Uniform	Third party people and property	Population density data from 2001 Census data collected by Australian Bureau of statistics.	Resolution of population distribution is dependent on the size of the census geographical collection districts	Level 1
Dalamagkidis et al. [49]	Uniform	Third party people	–	Assumed population density based on case study examples. Case 1 Easy: 50 people/km^2 Case 2 Hard: 5000 people/km^2 Case 3 Average: 200 people/km^2	Level 1
Dalamagkidis et al. [50]	Uniform	Third party people	Population density of 200 people/km^2 (for suburban regions) based on value provided by EASA is used.	The population density is typically estimated using the average population density over the area the UAS will operate.	Level 1
Di Donato et al. [63]	Comprehensive	Third Party people	Mobile phone data, census data and OpenStreetMap information	–	Level 1
Ford et al. [29]	Comprehensive	Third party people	Combines data from 2000 U.S. Census Bureau with LandSat data from the United States Geological Survey	A strong correlation between the population density and structure density was assumed. Thus, population is more likely to be concentrated in developed areas.	Level 1
Guglieri et al. [79]	Uniform and Comprehensive	Third party people	Two case study scenarios evaluated. First assumes uniform exposure (25 habitants/square kilometre). Second uses census data to determine population density around Torino Aeritalia Airport.	For second case study scenario, area and consequently population density is divided into nine squares and different densities are assigned to each based on the type of area and data available.	Level 1
King et al. [20]	Comprehensive	Third party people	Population density of each city/county as determined from 2000 U.S. Census Bureau	Flight path data including time spent over different population densities was used. Mission type also taken into consideration.	Level 1
Lum et al. [22]	Uniform	Third party people and property	Data from U.S. Census Bureau refined by the information gathered from Google maps satellite images.	Ignore time of day and work. Make use of housing unit density as well. Ignore population and housing densities for three biggest cities.	Level 1
Lum et al. [23]	Uniform	Third party people	Census data and satellite imagery used to estimate local bystander distribution.	Structural densities also extracted from census data.	Level 1
McGeer et al. [21]	Uniform	Ships, houses, third party individuals	Assumed values based on case study example	Assume distribution of ships is random. Average dimensions of target assumed.	Level 1
Melnyk et al. [17]	Comprehensive	Third party people	Data from 2000 U.S. Census bureau was used.	Data from Ref. [61] used to determine how people spent their days. Includes time of day and type of work.	Level 1
Shelley [44]	Constant	Third party people	Population densities from 0.05 to 4 people/m^2 were evaluated	Various population densities considered, including densities representative of crowds at a public event.	Level 1
Stevenson et al. [62]	Comprehensive	Third party people	Used Census data from 2011 Census for Canada.	Data calculated for several hypothetical regions over which the UAS would operate.	Level 1
Waggoner [54]	Uniform	Third party people and property	Data from U.S. Census Bureau refined by the information gathered from Google maps satellite images.	Ignore time of day and work. Make use of housing unit density as well. Ignore population and housing densities for three biggest cities.	Level 1
Weibel et al. [55]	Uniform	Third party people	Population density data were used from the 2000 U.S. Census Bureau	The probabilistic expectation assumes that the population is evenly distributed over the area.	Level 1

Table 7
Summary of incident stress models.

Reference	Stress Property	How was it calculated	Assumptions	Sheltering Model	Method of Model Substantiation	Uncertainty Level
Aalmoes et al. [46]	–	–	Assumed as percentage of fatality. Includes shelter effects.	Parameter model	Estimated value of 17% chance of fatality (based on [82])	Level 1
Ancel et al. [30]	KE	–	–	KE model	Based on studies conducted by the range safety group. Different classes of buildings/roofs can absorb different amount of energy	Level 1
Ball et al. [12]	KE	–	It is assumed that the aircraft remains intact until impact with the ground (*e.g.* no mid-air breakup)	KE Model	Difference in structure performance between roof-top and sidewall accounted for. Blast effects also taken into account.	Level 1
Burke et al. [16]	KE	KE variation between different aircraft is reduced to a function of its mass or weight.	It is assumed that the amount of hard shelter is proportional to the population density.	Parameter model. Based on type of shelter.	Shelter factor is divided into two different variables. Hard shelter and soft shelter.	Level 1
CASA [67]	KE	Mass and Velocity	Assumes perfectly inelastic collision	KE Model	Uses limit set by Ref. [83]	Level 1
Dalamagkidis et al. [49]	–	–	Average value of 0.5 assumed for sheltering, with higher values meaning better sheltering and a lower probability of fatality for the same KE.	Parameter model	Assumed for different case study examples: Case 1 Easy: 0.6 Case 2 Hard: 0.4 Case 3 Average: 0.5	Level 1
Dalamagkidis et al. [50]	KE	Terminal velocity used to calculate KE (different case studies evaluated)	This model implies a type of “absolute sheltering”, where any person considered sheltered, is not affected by the impact.	KE Model	Sheltering factor takes a value from 0 to 1.	Level 1
Guglieri et al. [79]	–	–	Values assumed based on case study scenario and terrain under evaluation.	Parameter model	Two case study scenarios evaluated. For the first scenario, no sheltering is considered. For the second scenario, area around Torino Aeritalia Airport is divided into 9 parts, shelter factor estimated for each of them based on expert opinion, and then average value evaluated (average shelter factor equal to 4.81).	Level 1
Lum et al. [22]	KE	–	Percentage of times the UAS penetrates the building is assumed, along with the number of fatalities.	–	Fatality rates assumed for case study examples. Border patrol: 0.42 deaths/strike estimated. Environmental monitoring: 0.02 deaths/strike estimated. Urban patrol: 0.02 fatalities/ building strike.	Level 0
Melnyk et al. [17]	KE and Chemical Energy	–	Chemical energy only included in the penetration decision in 13% of all crashes based on [84]	KE and Chemical Energy Model	Data from Refs. [64,84], used as inputs in the model	Level 1
Stevenson et al. [62]	–	–	Assumed values based on UAS evaluated and terrain	Location model (dependent on terrain)	Value based on terrain: For wilderness: 0.75 For urban areas: 0.25 For sub-urban areas: 0.5 For no shelter: 0	Level 1
U.S. Army Corps of Engineers [28]	KE	Each fragment was characterised by a ballistic coefficient.	Assumes UAS and building is frangible (impact of fragments also studied) All fragments in the break up lists were assumed to be inert, that is not capable of sustaining an explosion on impact.	Parameter model, linked to population density, shelter type and occupation.	Census data from western United States and Canada was used. Probability studies used to determine impact of fragments on roof.	Level 1
Weibel et al. [55]	KE	–	–	Parameter model.	Calculated based on class of vehicle.	Level 1

Table 8
Summary of harm models.

Reference	Stress Characteristic	Mechanism of Harm	Assumed Demographic	Harm Measure/Output	Method of Model Substantiation and assumptions/notes	Uncertainty Level
Aalmoes et al. [46]	–	–	Unspecified	–	Historical accident and incident data. Constant value of 17% lethality was selected based on other studies.	Level 1
Ancel et al. [30]	KE	–	Unspecified	–	Expert elicitation. Assumed that if a UAS strikes an individual, it will result in a casualty.	Level 1
Arterburn et al. [60]	KE	Blunt trauma	ATD Hybrid III 50th percentile male crash test dummy used	AIS level 3, Impact KE that will not result in skull fracture range from 114 to 141 ft-lbs for Phantom 3	Impactor studies. Upper limit based on study conducted by Dr Yofanandan's translated to the case study example of a Phantom 3.	Level 1
Ball et al. [12]	KE	Blunt trauma	95th percentile American male ages 20-30 (190.1 cm tall, waist 51.6 cm, weight 98.5 kg)	Energy level cut-off: 56 ft lb of KE (Skull fracture 15 ft. lb)	Impactor studies. This value is determined through empirical analysis of animal and cadaver testing.	Level 3
Burke et al. [16]	KE	Blunt trauma	Unspecified	Energy level cut-off: 68 ft lb. of KE	Historical accident and incident data. Energy limit based on different studies conducted.	Level 3
CASA [67]	KE	Blunt trauma, lacerations	5th percentile of females (50 kg body mass, thin body wall)	AIS level 3 Blunt Criteria of 1.61 (limit to head injury severity)	Historical accident and incident data. Based on other studies. The probability of death for this type of injury is less than 10%.	Level 3
Clothier et al. [27]	–	–	Unspecified	–	Expert elicitation. Assumed that if a UAS strikes an individual, it will result in a casualty	Level 1
Dalamagkidis et al. [49]	KE	–	Unspecified	–	Impactor studies. Probability of fatality calculated based on the shelter factor, impact energy required for a fatality probability of 50% with shelter factor equal to 0.5 and the impact energy required to cause a fatality as the sheltering factor goes to zero.	Level 1
Dalamagkidis et al. [50]	KE	–	Unspecified	Energy level cut-off: 34J of KE	Impactor studies. Logistic Curves used. Value used as parameter of model to calculate probability of fatality given exposure. Based on limit provided by the RCC	Level 3
Lum et al. [22]	–	–	Unspecified	–	Expert judgement. Value ranging from 0 to 1 representing the fatality rate for pedestrian strike. Fatality rate (deaths per strike) based on case study; Reaper: 1; Scan Eagle: 0.5	Level 1
Magister [56]	KE	Blunt Trauma	5th percentile female, 50th percentile male and 95th percentile male	AIS level calculated as a factor of blunt criteria (BC) AIS = 1328BCE + 0603	The BC correlates the kinetic energy deforming the body on impact with the body's ability to tolerate the energy on impact. Expert elicitation to test various case study scenarios. BC based on UA mass, impact velocity, characteristic diameter, human body mass and chest wall thickness.	Level 1
Melnyk et al. [17]	KE (and Chemical energy)	–	Unspecified	Energy level cut-off: 58 ft-lbf	Historical accident and incident data. Based on other studies. In open areas, all individuals considered as casualties if the energy imparted by the UA exceeds the 58 ft-lbf limit. Inside shelter 30% casualties if penetration occurs.	Level 3
Shelley [44]	KE	–	Unspecified	AIS levels for different levels of severity of injury specified.	Impactor studies. Makes use of Logistic Curves.	Level 3
Skobir et al. [72]	KE	–	Unspecified	Energy level cut-off: 78 J	Historical accident and incident data. Energy levels assumed based on other studies.	Level 3
U.S. Army Corps of Engineers [28]	–	–	Unspecified	AIS Level 3 (or greater)	Impactor studies. Two standards for acceptable risk to ground populations are applicable: RCC criteria and Range Safety Requirements for the Eastern and Western Range. This study makes use of maximum casualty expectation (30×10^{-6})	Level 1
Waggoner [54]	–	–	Unspecified	–	Expert elicitation. Fatality rate (deaths per strike) based on case study; Reaper: 1; Scan Eagle: 0.5	Level 1
Weibel et al. [55]	–	–	Unspecified	–	Expert elicitation. Assumed that, if debris penetrate shelter, then fatality has occurred.	Level 1

Appendix B

Table 9
Comparison of Models used to determine the Impact Area of UAS based on [17].

S. No	Equation	Citation
Geometry Based		
1	$LA_{Gliding} = (W_{Aircraft} + 2 \times R_{Person}) \times (L_{Aircraft} + L_{GlideGround} + 2 \times R_{Person})\ LA_{Vert} \quad = \pi \times \left(\frac{1}{2} \times W_{Aircraft} + R_{Person}\right)^2$	[27]
2	$AL = \pi \times b^2$	[16]
3	***Vertical Descent*** $IA_{vert\ FW} = \pi \times \left(\frac{1}{2} \times b_{aircraft} + R_{person}\right)^2$ ***Gliding Descent*** $W_{Haz} \ = b_{aircraft} + (2 \times R_{Person})L_{Glide} = \frac{H_{95th}}{\tan(\gamma)} \ = H_{95^{th}} \times \left(\frac{L}{D}\right)_{Max} L_{Skid\ Length} = (V_{Glide}t_{safe}) - (\mu_{glide} \times g \times t_{safe}^2\ )t_{safe} = \frac{V_{Glide} - V_{Min\ Kill}}{2 \times \mu_{slide} \times g}$ $V_{Min\ Kill} = \sqrt{2 \times \frac{W_{lbs}}{g} \times KE_{Lethal}} IA = W_{Haz} \times (L_{glide} + L_{Skid\ Length})$ Similar equations presented for Rotary Wing Aircrafts	[12]
4	$A_C = f(\beta_{UAV})\beta = \frac{GW}{drag} drag = 0.9 \times length \times width$	[20] [a]
Weight Based		
5	Debris Area in Built up Area = 1.0764 ft^2/lb MTOW Debris Area in Open Area = 1.3455 ft^2/lb MTOW	[19]
Size/Category Based		
6	Small Aircraft Steep Impact: 1.3 Hectares Large Aircraft Steep Impact: 3.89–5.18 Hectares Small Aircraft Shallow Impact: 2.59–3.89 Hectares Large Aircraft Shallow Impact: 5.48–6.48 Hectares	[32]

[a] Uses weight component as well.

References

[1] CAA, CAP-722, Unmanned Aircraft System Operations in UK Airspace - Guidance, London UK Civil Aviation Authority (CAA), Department of Transport (DfT), London, UK, 2015.

[2] DOD, Unmanned Systems Roadmap 2007-2032, Office of Secretary of Defense, Washington D.C., USA, 2007.

[3] JAA/EUROCONTROL, UAV Task-force Final Report: a Concept for European Regulations for Civil Unmanned Aerial Vehicles (UAVs), 2004.

[4] R.A. Clothier, J.L. Palmer, R.A. Walker, N.L. Fulton, Definition of an airworthiness certification framework for civil unmanned aircraft systems, Saf. Sci. 49 (6) (2011) 871–885.

[5] R.A. Clothier, B.P. Williams, J. Coyne, M. Wade, A. Washington, Challenges to the development of an airworthiness regulatory framework for unmanned aircraft systems, in: 16th Australian International Aerospace Congress (AIAC 16), 2015, pp. 87–98.

[6] R.A. Clothier, N.L. Fulton, R.A. Walker, Pilotless aircraft: the horseless carriage of the twenty-first century? J. Risk Res. 11 (8) (2008) 999–1023.

[7] R.A. Clothier, R.A. Walker, Determination and evaluation of UAV safety objectives, in: 21st International Unmanned Air Vehicle Systems Conference, 2006, pp. 18.1–18.16.

[8] EASA, Concept of Operations for Drones a Risk Based Approach to Regulation of Unmanned Aircraft, 2015. Cologne, Germany.

[9] R.A. Clothier, B.P. Williams, A. Washington, Development of a template safety case for unmanned aircraft operations over populous areas, in: SAE 2015 AeroTech Congr. Exhib. 22-24 Sept, Seattle, Washington, USA, 2015.

[10] ISO, ISO 31000:2009, Risk Management-principles and Guidelines, 2009 [Online]. Available, http://www.iso.org/iso/catalogue_detail?csnumber=43170 (Accessed 05 November 2015).

[11] R.A. Clothier, R.A. Walker, Safety risk management of unmanned aircraft systems, in: K.P. Valavanis, G.J. Vachtsevanos (Eds.), Handbook of Unmanned Aerial Vehicles, Springer, Netherlands, 2015, pp. 2229–2275.

[12] J.A. Ball, M. Knott, D. Burke, Crash Lethality Model, Naval Air Warfare Centre Aircraft Division, Maryland, USA, 2012.

[13] M.E. Paté-Cornell, Uncertainties in risk analysis: six levels of treatment, Reliab. Eng. Syst. Saf. 54 (2–3) (1996) 95–111.

[14] R.A. Clothier, B.P. Williams, K.J. Hayhurst, Managing the Risks UAS Pose to People and Property on the Ground, 2016.

[15] M. Knott, R. Cochran, D. Burke, Third Party Risk Assessment Tool (3PRAT), Naval Air Warfare Centre Aircraft Division, Maryland, USA, 2012.

[16] D.A. Burke, C.E. Hall, S.P. Cook, System-level airworthiness tool, J. Aircr. 48 (3) (2011) 777–785.

[17] R. Melnyk, D. Schrage, V. Volovoi, H. Jimenez, A Third-party Casualty Prediction Model for UAS Operations, Georgia Institute of Technology, 2013.

[18] L.C. Barr, R. Newman, E. Ancel, C.M. Belcastro, J.V. Foster, J. Evans, D.H. Klyde, Preliminary risk assessment for small unmanned aircraft systems, in: 17th AIAA Aviation Technology, Integration, and Operations Conference, 2017.

[19] B.J.M. Ale, M. Piers, The assessment and management of third party risk around a major airport, J. Hazard. Mater. 71 (1–3) (2000) 1–16.

[20] D.W. King, A. Bertapelle, C. Moses, UAV failure rate criteria for equivalent level of safety, in: International Helicopter Safety Symposium, 2005.

[21] T. McGeer, L.R. Newcome, J. Vagners, Quantitative Risk Management as a Regulatory Approach to Civil UAVs, The Insitu Group, Adroit Systems Inc., University of Washington, 1999.

[22] C.W. Lum, B. Waggoner, A risk based paradigm and model for unmanned aerial systems in the national airspace, in: Proc. AIAA Infotech@Aerospace 2011 Conference, St. Louis, MO, 2011, pp. 1–31.

[23] C.W. Lum, K. Gauksheim, C. Deseure, J. Vagners, T. McGeer, Assessing and estimating risk of operating unmanned aerial systems in populated areas, in: 11th AIAA Aviation Technology, Integration, and Operations (ATIO) Conference, 2011, pp. 1–13.

[24] K.J. Hayhurst, J.M. Maddalon, P.S. Miner, G.N. Szatkowski, M.L. Ulrey, M.P. DeWalt, C.R. Spitzer, Preliminary Considerations for Classifying Hazards of Unmanned Aircraft Systems, 2007. NASA/TM-2007-214539.

[25] S. Guarro, Risk assessment of new space launch and supply vehicles, in: 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012, PSAM11 ESREL 2012, 2012.

[26] S.D. Guikema, M.E. Pate-Cornell, Bayesian analysis of launch vehicle success rates, J. Spacecr. Rockets 41 (1) (2004) 93–102.

[27] R.A. Clothier, R.A. Walker, N. Fulton, D.A. Campbell, A casualty risk analysis for unmanned aerial system (UAS) operations over inhabited areas, in: AIAC12: Twelfth Australian International Aerospace Congress, Second Australasian Unmanned Air Vehicle Conference, Melbourne, Australia, 2007, pp. 1–15.

[28] Air Force Flight Test Center, Final Quantitative Risk Analysis for Generic Unmanned Lifting Entry Vehicle Landing at Edwards Air Force Base, 2001.

[29] A.T. Ford, K.J. McEntee, Assessment of the risk to ground population due to an unmanned aircraft in-flight failure, in: 10th AIAA Aviation Technology, Integration and Operations (ATIO) Conference, Fort Worth, Texas, 2010, pp. 1–12.

[30] E. Ancel, F.M. Capristan, J.V. Foster, R.C. Condotta, Real-time risk assessment framework for unmanned aircraft system (UAS) traffic management (UTM), in: 17th AIAA Aviation Technology, Integration, and Operations Conference,Denver, Colarado, 2017, pp. 1–17.

[31] W.T. Thompson, US military unmanned aerial vehicle mishaps: assessment of the role of human factors using Human Factors Analysis and Classification System (HFACS), in: US Air Force 311th Hum. Syst. Wing, 2005.

[32] S.D. Brady, R.J. Hillestad, Modelling the External Risks of Airports for Policy Analysis, RAND, 1995.

[33] R.A. Clothier, P.P. Wu, A review of system safety failure probability objectives for unmanned aircraft systems, in: 11th International Probabilistic Safety Assessment and Management (PSAM11) Conference and the Annual European Safety and Reliability(ESREL 2012) Conference, Helsinki, 2012.

[34] FAA, Advisory Circular 25.1309–1A, System Design and Analysis, US Department of Transportation, Federal Aviation Administration, 1988.

[35] JARUS Working Group 6, Safety assessment of remotely piloted aircraft systems, AMC RPAS 1309 (2) (2015).

[36] EASA, Policy for Unmanned Aerial Vehicle (UAV) Certification, 2005. Advance - Notice of Proposed Amendment (NPA) No 16/2005.

[37] NATO Standardization Agency (NSA), STANAG 4671 (Edition 1) - Unmanned Aerial Vehicles Systems Airworthiness Requirements (USAR), Brussels, Belgium, 2009.
[38] NATO Standardization Agency, AEP-83, Light Unmanned Aircraft Systems Airworthiness Requirements, 2014.
[39] RTCA DO-344, Operational and Functional Requirements and Safety Objectives (OFRSO) for Unmanned Aircraft Systems (UAS) Standards, vol. 2, 2013.
[40] FAA, Advisory Circular 23.1309–1E, System Safety Analysis and Assessment for Part 23 Airplanes, 2011.
[41] SAE ARP 4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, SAE International, 1996.
[42] SAE ARP 4754A, Guidelines for Development of Civil Aircraft and Systems, SAE International, 2010.
[43] P.P. Wu, R.A. Clothier, The development of ground impact models for the analysis of the risks associated with unmanned aircraft operations over inhabited areas, in: 11th Probabilistic Safety Assessment and Management Conference (PSAM11) and the Annual European Safety and Reliability Conference (ESREL 2012), Scandic Marina Congress Center, Helsinki, 2012.
[44] A.V. Shelley, A model of human harm from a falling unmanned Aircraft : implications for UAS regulation, Int. J. Aviat. Aeronaut. Aerosp. 3 (3) (2016).
[45] A. Awad, An Analysis of the Risk from UAS Missions in the National Airspace, University of Washington, 2013.
[46] R. Aalmoes, Y.S. Cheung, E. Sunil, J.M. Hoekstra, F. Bussink, A conceptual third party risk model for personal and unmanned aerial vehicles, in: 2015 International Conference on Unmanned Aircraft Systems (ICUAS), Denver, CO, USA, 2015, pp. 1301–1309.
[47] N. Bradley, D. Burke, Potential Crash Location (PCL) Model, Department of the Navy, Naval Air Warfare Center Aircraft Division, Patuxent River, Maryland, 2012.
[48] A. La Cour-Harbo, Ground impact probability distribution for small unmanned aircraft in ballistic descent, 2017.
[49] K. Dalamagkidis, K.P. Valavanis, L.A. Piegl, Evaluating the risk of unmanned aircraft ground impacts, in: 16th Mediterranean Conference of Control and Automation, Ajaccio, France, 2008, pp. 709–716.
[50] K. Dalamagkidis, K. Valavanis, L.A. Piegl, On Integrating Unmanned Aircraft Systems into the National Airspace System, second ed., Springer, 2012.
[51] Y. Haartsen, R. Aalmoes, Y.S. Cheung, Simulation of unmanned aerial vehicles in the determination of accident locations, in: 2016 International Conference on Unmanned Aircraft Systems, (ICUAS), 2016, pp. 993–1002.
[52] J.V. Foster, D. Hartman, High-fidelity multi-rotor unmanned aircraft system (UAS) simulation development for trajectory prediction under off-nominal flight dynamics, in: 17th AIAA Aviation Technology, Integration, and Operations Conference, Denver, Colorado, 2017, pp. 1–19.
[53] M. Bleier, F. Settele, M. Krauss, A. Knoll, K. Schilling, Risk assessment of flight paths for automatic emergency parachute deployment in UAVs, IFAC-PapersOnLine 48 (9) (2015) 180–185.
[54] B. Waggoner, Developing a Risk Assessment Tool for Unmanned Aircraft System Operations, University of Washington, 2010.
[55] R.E. Weibel, R.J. Hansman, Safety Considerations for Operation of Unmanned Aerial Vehicles in the National Airspace System, MIT International Center for Air Transportation, 2005.
[56] T. Magister, The small unmanned aircraft blunt criterion based injury potential estimation, Saf. Sci. 48 (10) (2010) 1313–1320.
[57] Civil Aviation Authority of New Zealand, Advisory Circular AC102–1: Unmanned Aircraft - Operator Certification, 2015.
[58] J.W. Melvin, D. Mohan, R.L. Stalnaker, Human injury mechanisms and impact tolerance, in: Transportation Research Board, National Research Council, National Academy of Sciences, USA, vol. 586, 1976, pp. 11–22.
[59] FAA, Micro Unmanned Aircraft Systems Aviation Rulemaking Committee (ARC), ARC Recommendations Final Report, 2016.
[60] D.R. Arterburn, C.T. Duling, N.R. Goli, Ground collision severity standards for UAS operating in the national airspace system (NAS), in: 17th AIAA Aviation Technology, Integration, and Operations Conference, Denver, Colorado, 2017.
[61] N.E. Klepeis, W.C. Nelson, W.R. Ott, J.P. Robinson, A.M. Tsang, P. Switzer, J. V Behar, S.C. Hern, W.H. Engelmann, The National Human Activity Pattern Survey (NHAPS): a resource for assessing exposure to environmental pollutants, J. Expo. Anal. Environ. Epidemiol. 11 (3) (2001) 231–252.
[62] J.D. Stevenson, S.O. Young, L. Rolland, Estimated levels of safety for small unmanned aerial vehicles and risk mitigation strategies, J. Unmanned Veh. Syst. 3 (4) (2015) 205–221.
[63] P.F.A. Di Donato, E.M. Atkins, Evaluating risk to people and property for aircraft emergency landing planning, J. Aerosp. Inf. Syst. 14 (5) (2017) 259–278.
[64] M.J. Hardwick, J. Hall, J.W. Tatom, R.G. Baker, Approved Methods and Algorithms for DoD Risk-based Explosives Siting, Department of Defense Explosives Safety Board, 2009. Technical Paper (TP) 14.
[65] M. Crull, J.W. Tatom, R.T. Conway, SPIDER 2 Tests - Response of Typical Wall Panels to Debris and Fragment Impact, U.S. Army Engineering and Support Center, Huntsville, AL, 2010.
[66] Range Commanders Council, Range Safety Criteria for Unmanned Air Vehicles - Rationale and Methodology Supplement, 2001. Range commanders council white sands missile range nm.
[67] Civil Aviation Safety Authority, Human Injury Model for Small Unmanned Aircraft Impacts, 2013.
[68] V.D. Alphonse, Injury Biomechanics of the Human Eye during Blunt and Blast Loading, Virginia Tech, 2012.
[69] D.I. Feinstein, W.F. Heugel, M.L. Kardatzke, A. Weinstock, Personnel Casualty Study, Defense Technical Information Center, 1968.
[70] K. Dalamagkidis, K.P. Valavanis, L.A. Piegl, Current status and future perspectives for unmanned aircraft system operations in the US, J. Intell. Robot. Syst. 52 (2) (2008) 313–329.
[71] C. Bir, D.C. Viano, Design and injury assessment criteria for blunt ballistic impacts, J. Trauma-Injury Infect. Crit. Care 57 (6) (2004) 1218–1224.
[72] Z. Skobir, T. Magister, Assessment of a light unmanned aircraft ground impact energy, Promet-Traffic Transp. 23 (2) (2011) 97–104.
[73] N. Yoganandan, F.A. Pintar, A. Sances, P.R. Walsh, C.L. Ewing, D.J. Thomas, R.G. Snyder, Biomechanics of skull fracture, J. Neurotrauma 12 (4) (1995) 659–668.
[74] D. Raymond, C. Van Ee, G. Crawford, C. Bir, Tolerance of the skull to blunt ballistic temporo-parietal impact, J. Biomech. 42 (15) (2009) 2479–2485.
[75] T.A. Mattei, B.J. Bond, C.R. Goulart, C.A. Sloffer, M.J. Morris, J.J. Lin, Performance analysis of the protective effects of bicycle helmets during impact and crush tests in pediatric skull models, J. Neurosurg. Pediatr. 10 (6) (2012) 490–497.
[76] Columbia Accident Investigation Board, Determination of Debris Risk to the Public, Due to the Columbia Breakup during Reentry, vol. 2, 2003. Appendix D 16.
[77] A. Washington, R.A. Clothier, B.P. Williams, A Bayesian approach to system safety assessment and compliance assessment for unmanned aircraft systems, J. Air Transp. Manag. 62 (2017) 18–33.
[78] S.E. Wolf, Modelling Small Unmanned Aerial System Mishaps Using Logistic Regression and Artificial Neural Networks, Air Force Institute of Technology, 2012.
[79] G. Guglieri, F. Quagliotti, G. Ristorto, Operational issues and assessment of risk for light UAVs, J. Unmanned Veh. Syst. 2 (4) (2014) 119–129.
[80] D. Andrew, M. Knott, D. Burke, Population Density Modeling Tool, Department of the Navy, Naval Air Warfare Center Aircraft Division, Patuxent River, Maryland, 2012.
[81] Demographia, Suburban, Core & Urban Densities by Area: Western Europe, Japan, United States, Canada, Australia & New Zealand [Online]. Available: http://www.demographia.com/db-intlsub.htm (Accessed 29 March 2016).
[82] Y. Cheung, D.L. Haij, J. Smeltink, J. Stevens, A Model to Calculate Third Party Risk Due to Civil Helicopter Traffic, NLR, 2007.
[83] R.A. Clothier, J.L. Palmer, R.A. Walker, N.L. Fulton, Definition of airworthiness categories for civil unmanned aircraft systems (UAS), in: Proceedings of the 27th International Congress of the Aeronautical Sciences, Nice, France, 2010, pp. 1–12.
[84] G. Li, S.P. Baker, Crash risk in general aviation, J. Am. Med. Assoc. 297 (14) (2007) 1596–1598.
[85] C.G. Kevorkian, UAS Risk Analysis using Bayesian Belief Networks: An Application to the Virginia Tech ESPAARO, 2016.
[86] F.V. Jensen, T.D. Nielsen, Bayesian Networks and Decision Graphs, 2nd ed., Springer Science & Business Media, 2009.
[87] N. Fenton, M. Neil, Risk Assessment and Decision Analysis with Bayesian Networks, CRC Press, Taylor and Francis Group, 2013.

This page is intentionally left blank.

4. A Bayesian Approach to System Safety Assessment and Compliance Assessment for Unmanned Aircraft Systems

Figure 10: Concept image of an unmanned aircraft operation over Dandenong Ranges, Australia
Image Copyright © Achim Washington

> *"True genius resides in the capacity for evaluation of uncertain, hazardous and conflicting information."*
>
> **Winston Churchill (1874-1965)**

This paper titled, *"A Bayesian Approach to System Safety Assessment and Compliance Assessment for Unmanned Aircraft Systems"* aims to present a new approach to showing compliance to system safety requirements for aviation systems. While the primary focus is on Research Question 2, it also delves into elements of Research Question 1. It explores how the uncertainty which was identified in the previous chapter can be taken into consideration in the SRMP (Research Question 1.2, Research Question 1.3 and Research Question 2.1). Looking at the case study of the SSR and reframing it as a problem of decision-making under uncertainty, it demonstrates how the concept of risk-based regulation can be extended to include a risk-based approach to the regulatory processes of compliance assessment and compliance finding (Research Question 2.2). This allows for compliance decisions to be made on the basis of compliance risk. The model developed in this paper makes certain simplifying assumptions which are addressed in subsequent chapters.

4.1. Statement of Authorship

The authors listed in Table 8 have certified* that:

1. They meet the criteria for authorship (refer to Appendix B: Definition of Authorship) in that they have participated in the conception, execution, or interpretation, of at least that part of the publication in their field of expertise;
2. They take public responsibility for their part of the publication, except for the responsible author who accepts overall responsibility for the publication;
3. There are no other authors of the publication according to these criteria;
4. Potential conflicts of interest have been disclosed to (a) granting bodies, (b) the editor or publisher of journals or other publications, and (c) the head of the responsible academic unit; and
5. They agree to the use of the publication in the student's thesis and its publication on the Australian Digital Thesis database consistent with any limitation set by publisher requirements.

Table 8: Statement of authorship – paper two

Title of Paper:	A Bayesian Approach to System Safety Assessment and Compliance Assessment for Unmanned Aircraft Systems			
Contributor	**Area of Contribution and percentage contribution to paper: ***			
	(i)	(ii)	(iii)	(iv)
	Conception and Design	Analysis and Interpretation	Drafting Sections	Critically Revising
Mr Achim Washington	80%	90%	90%	20%
Dr Reece Clothier	20%	10%	10%	60%
Mr Brendan Williams				20%

Principal Supervisors confirmation

I have email or other correspondence from all co-authors confirming their certifying authorship

Dr Reece Clothier	25th August 2018
Name	**Date**
Dr Jose Silva	25th August 2018
Name	**Date**

** for further details refer to Appendix B: Definition of Authorship*

Journal of Air Transport Management 62 (2017) 18–33

Contents lists available at ScienceDirect

Journal of Air Transport Management

journal homepage: www.elsevier.com/locate/jairtraman

A Bayesian approach to system safety assessment and compliance assessment for Unmanned Aircraft Systems

Achim Washington [a, *], Reece A. Clothier [a, b], Brendan P. Williams [b]

[a] School of Engineering, RMIT University, Melbourne, Australia
[b] Boeing Research & Technology – Australia, Brisbane, Australia

ARTICLE INFO

Article history:
Received 25 November 2016
Received in revised form
8 February 2017
Accepted 9 February 2017
Available online 2 March 2017

Keywords:
Unmanned aircraft systems
System safety
Bayesian
Uncertainty
Regulation
Part 1309

ABSTRACT

This paper presents a new approach to showing compliance to system safety requirements for aviation systems. The aim is to improve the objectivity, transparency, and rationality of compliance findings in those cases where there is uncertainty in the assessments of the system. A Bayesian approach is adopted that facilitates a more comprehensive treatment of the uncertainties inherent to all system safety assessments. The assessment and compliance framework is reformulated as a problem of decision making under uncertainty, and a normative decision approach is used to illustrate the approach. A case study system safety assessment of a civil unmanned aircraft system is used to exemplify the proposed approach. The proposed approach could be readily applied to any regulatory compliance process and would represent a significant change to, and advancement over, current aviation safety regulatory practice. This paper is the first to describe the application of Bayesian techniques to the field of aviation system safety analysis. The adoption of the proposed compliance approach would bring aviation system safety practitioners in line with more contemporary (and well established) approaches adopted in the nuclear power and space launch industries.

1. Introduction

Unmanned Aircraft Systems (UAS) are one of the fastest growing sectors in the aviation industry. However, like all technologies there are risks associated with their use. To date, aviation safety regulators have largely managed these risks through imposing substantial restrictions on their operation (CAA, 2015; Clothier et al., 2011; JAA/EUROCONTROL, 2004; US DoD, 2007), including limiting their operation to non-populated areas. Key to the relaxation of these restrictions is the provision of greater assurance in the airworthiness of the UAS. Numerous challenges to the development of a regulatory framework for UAS are described by Clothier et al. (2015) and it is widely accepted that the existing airworthiness regulatory framework used for conventionally piloted aircraft (CPA) is not suitable for all UAS types and missions (Clothier and Walker, 2006).

A central component of airworthiness regulations are system safety regulations; commonly referred to as “Part 1309” regulations as they are contained in subpart 1309 of the respective civil codes of aviation safety regulations (*e.g.* CS/FAR 23.1309 (FAA, 2011) and CS/FAR 25.1309 (FAA, 1988)). System safety regulations supplement prescriptive design requirements and are put in place to ensure that an aircraft or system is capable of continued safe flight and landing following a failure or multiple failures of systems (JARUS Working Group 6-Safety and Risk Assessment, 2015). Disparate specifications of Part 1309 regulations for UAS have been proposed (EASA, 2005; JARUS Working Group 6-Safety and Risk Assessment, 2015; NATO Standardization Agency (NSA), 2009). As stated by the Australian Department of Defence, Part 1309 regulations will be “fundamental to the safety of UAS” but are also “an area of evolution and disagreement” (ADF, 2016). Some of the various issues and points of contention surrounding the specification of Part 1309 regulations for UAS are discussed by Clothier and Wu (2012) and EUROCAE (2013).

System safety regulations will be particularly critical to the airworthiness of UAS during their early years of certified operations. This is due to a lack of data and knowledge to inform the specification of prescriptive design requirements; knowledge that is only typically gained through extensive in-service experience. This uncertainty, in turn, places greater emphasis on the need for assurance in the system safety of the UAS.

* Corresponding author.
E-mail addresses: s3270338@student.rmit.edu.au (A. Washington), reece.a.clothier@boeing.com (R.A. Clothier), brendan.p.williams@boeing.com (B.P. Williams).

http://dx.doi.org/10.1016/j.jairtraman.2017.02.003
0969-6997/© 2017 Elsevier Ltd. All rights reserved.

Providing assurance in the system safety of UAS has a number of challenges. Namely, the low data needed to inform estimates of UAS reliability, which arises due to:

1. changing system design baselines;
2. the use of components that are not designed to standards and subject to quality assurance;
3. the non-homogeneity of the UAS fleet (*i.e.*, the diversity of designs and their concepts of operation, which limits the conclusions which can be drawn from aggregating data across types).

As a consequence, there is significant uncertainty in the system safety assessment of UAS. The current method for assessing the system safety of civilian aviation systems (SAE ARP 4761, 1996; SAE ARP 5150, 2013) does not comprehensively address uncertainty in the input data, models, and assessment process. Instead it is suggested that uncertainty be ‘handled’ through the setting of conservative assumptions and the use of sensitivity analysis to determine “upper bounds” on quantitative estimates (SAE ARP 5150, 2013). Nor is uncertainty in the assessments objectively represented and accounted for in regulatory decision making; potentially leading to subjective regulatory compliance findings. A more comprehensive treatment of uncertainty is required for more rational, objective, and consistent compliance decision making (Apostolakis, 1990; Paté-Cornell, 1996).

This paper explores a new approach to the certification of UAS to Part 1309 regulations. In this paper the system safety compliance process is modelled as a decision-making process under uncertainty. This approach to aviation regulations was inspired by the work of Perez et al. (Perez, 2013; Perez et al., 2013, 2012a, 2012b), who explore new methods for the assessment of autonomous systems. The approach presented herein is in line with contemporary safety assessment and decision making approaches first proposed by the nuclear power industry (United States Nuclear Regulatory Commision, 1975).

It is important to note that the use of Bayesian analysis to evaluate and represent uncertainty is not a new concept and has readily been employed in a number of industries. The space launch industry (Guarro, 2012; Guikema and Pate-Cornell, 2004; Kelly and Smith, 2008; Lindsey et al., 2013; Maranzano and Krzysztofowicz, 2008; Morris and Beling, 2001), nuclear power industry (Apostolakis, 1981; Huang et al., 2006; Ozbay and Noyan, 2006; United States Nuclear Regulatory Commision, 1975; Wieland and Lustosa, 2009), fishery industry (Punt and Hilborn, 1997), ecological management industry (Ellison, 1996; Marcot et al., 2001; McCann et al., 2006) and bio management industry (Mallick et al., 2009; Wade, 2000), to name a few, have already recognised the importance of using Bayesian analysis to take the uncertainty associated with the systems into consideration. Bayesian analysis techniques have also been applied in the field of aviation safety in the past. Specifically, through the use of Bayesian Belief Networks to model accident causation, human-system interaction, and safety risks (Ancel et al., 2014; Ancel and Shih, 2015; Luxhøj and Matthew, 2015). In this paper, we explore how a Bayesian approach can be applied to the system safety analysis and compliance finding process.

A brief introduction to system safety regulations is presented in Section §2. Uncertainty, its types, sources, representation, and incorporation into decision-making are presented in Section §3. The revised model of the Part 1309 regulatory compliance process is presented in Section §4, and a case-study assessment presented in Section §5.

2. System safety regulations

Part 1309 regulations are intended to supplement prescriptive standards on the design, manufacture, and installation of aircraft components. At a high-level, system safety regulations specify the requirement for (Clothier and Wu, 2012):

1. A documented analysis showing that equipment and systems perform as intended under foreseeable operating and environmental conditions;
2. The adoption of principles from fail-safe and fault-tolerant design (FAA, 1988); and
3. The demonstration (through a documented qualitative or quantitative analysis) that the expected frequency of failure of equipment and systems, when considered separately and in relation to other systems, is inversely-related to the severity of its effect on the safe operation of the system. This is commonly referred to as the system safety performance requirement (SSPR).

A complete description of the Part 1309 regulations can be found in (EASA, 2005; Hayhurst et al., 2007; JARUS Working Group 6-Safety and Risk Assessment, 2015; NATO Standardization Agency, 2014; NATO Standardization Agency (NSA), 2009; RTCA DO-344, 2013) and associated guidance material (FAA, 2011, 1988). Guidelines on the system safety assessment process and accepted assessment tools and techniques can be found in (NATO Standardization Agency, 2014; NATO Standardization Agency (NSA), 2009; SAE ARP 4754A, 2010; SAE ARP 4761, 1996). The focus of this paper is on the specification of, and process for demonstrating compliance to, the SSPR.

2.1. System safety performance requirements

The SSPR defines the minimum acceptable level of reliability of aviation equipment and components (Clothier and Wu, 2012). Compliance to the SSPR is essential to the airworthiness certification of the system. The current SSPR compliance process is illustrated in Fig. 1. It comprises three main sub processes, namely, the system safety assessment, compliance assessment, and compliance finding processes.

2.1.1. System safety assessment process

The system safety assessment process determines the various ways in which the component, sub-system, or system, can fail; the magnitude of the potential negative impacts of these failures on the overall safety of flight; and an estimate of the Average Probability per Flight Hour (APFH) of these failures. Where, the APFH is defined as “the probability of occurrence, normalised by the flight time of a failure condition during a single flight” (FAA, 2011).

The system safety assessment process starts with an analysis of each component to determine its various modes of failure (referred to as failure conditions) and their potential impact on the safety of the aircraft system. The analysis is first undertaken for the components in isolation, and then as an integrated part of the aircraft system. To represent this mathematically we must first define the finite integer set Q, which is used to index the various outputs from the system safety assessment process, as given in Equation (1).

$$Q = \left\{ n | n \in \mathbb{Z}^{+},\ n \leq N \right\} \tag{1}$$

where N corresponds to the total number of unique failure conditions identified. We can then define the outcome of the first step in the system safety assessment process as the set F containing N failure condition descriptions, as given in Equation (2).

$$F = \{ f_n : n \in Q \} \tag{2}$$

The next step in the system safety assessment process is to

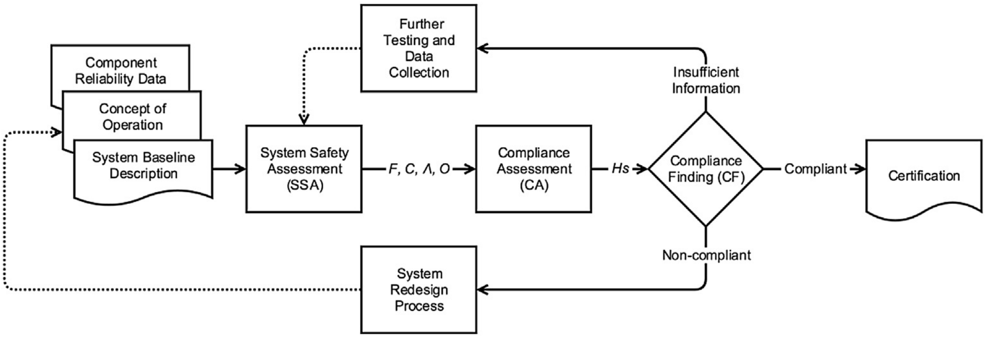

Component Reliability Data
Concept of Operation
System Baseline Description
System Safety Assessment (SSA)
F, C, Λ, O
Compliance Assessment (CA)
Hs
Compliance Finding (CF)
Compliant
Certification
Further Testing and Data Collection
Insufficient Information
Non-compliant
System Redesign Process

Fig. 1. Overview of the SSPR compliance process.

assign a failure severity condition to each of the identified failure conditions in *F*. Each failure condition f_n is assigned a failure severity category, c_n, based on the potential severity of the impact of the failure condition on the safety of the aircraft. System safety regulations and guidance materials describe a range of possible failure condition severity scales and these are summarised in Appendix A. The output of this assignment process is the set *C*, which comprises the failure condition severity assigned to each respective failure condition in *F*, as given in Equation (3).

$$C = \{c_n : n \in Q\} \tag{3}$$

Analysis is then undertaken to estimate the APFH for each failure condition. The APFH is assessed on qualitative or quantitative “failure probability scales” defined in Part 1309 regulations. Example failure probability scales are summarised in Fig. 2.

Assessment of the APFH is undertaken for each failure condition in *F*. The APFH can be determined through a combination of data from testing, modelling and simulation, expert judgement, and structured analysis techniques as detailed in SAE ARP 4761 (1996). The output of the assessment is the specification of the set Λ as given in Equation (4). Λ comprises *N* assessed APFHs; one associated with each of the failure conditions defined in *F*.

$$\Lambda = \{\lambda_n : n \in Q\} \tag{4}$$

The failure condition severity, c_n, for a particular failure mode, f_n, is then used to determine the applicable failure probability objective. Failure probability objectives specify the maximum APFH permissible for a failure condition of a given failure severity category. The failure probability objectives are defined within the Part 1309 regulations and are the criteria that the assessments of the APFH must be evaluated against. An example qualitative description of failure probability objectives is provided in CS-25 25.1309 (b) (EASA, 2015b) as follows:

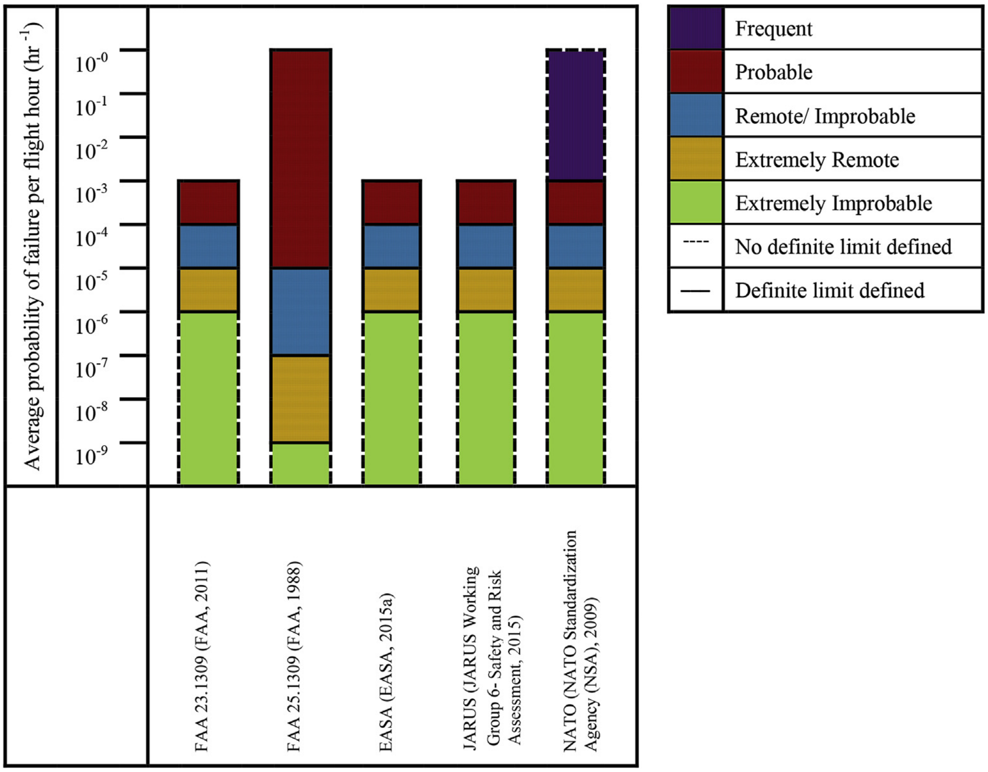


Fig. 2. Comparison of quantitative failure probability scales.

"*(b) The aeroplane systems and associated components, considered separately and in relation to other systems, must be designed so that-*
(1) *Any catastrophic failure condition*
(i) *Is extremely improbable; and*
(ii) *does not result from a single failure; and*
(2) *Any hazardous failure condition is extremely remote; and*
(3) *Any major failure condition is remote.*"

Quantitative specifications of the objectives are also provided in the Part 1309 regulations, as illustrated in Fig. 3.

The output is the definition of the set *O*, which contains the failure probability objective associated with each failure condition defined in *F*, as given in Equation (5).

$$O = \{o_n : n \in Q\} \tag{5}$$

The outcomes of the system safety process are the four related sets: *F, C, Λ* and *O*. The index variable *n* can be used to reference the assessment for each identified failure mode; describing the tuple:

$$\langle f_n, c_n, \lambda_n, o_n \rangle \quad where \;\; n \in Q; \tag{6}$$

Further details on the system safety process and the tools used in performing an assessment are provided in SAE ARP 4754A (2010) and SAE ARP 4761 (1996).

2.1.2. Compliance assessment process

Following the system safety assessment process is the compliance assessment process (Fig. 1). Each tuple, as given in Equation (6), represents an independent compliance assessment point.

Compliance assessment is a simple deterministic binary "pass or fail" process, where the state of compliance for the n^{th} identified failure mode, H_n, is *TRUE* when the assessed APFH (λ_n) is shown to be less than its applicable failure probability objective (o_n), as given in Equation (7).

$$H_n = \begin{cases} True & \text{if} |\lambda_\text{n}| \leq o_n \\ False & otherwise. \end{cases} \tag{7}$$

This compliance assessment process must be undertaken for all *N* failure conditions, with the overall state of compliance of the system, H_s, being determined as *True* if it can be shown that all of the assessed APFH satisfy their applicable failure probability objective, as shown in Equation (8).

$$H_s = \begin{cases} True & \text{if } H_n = True \quad \forall n \in Q \\ False & \quad otherwise. \end{cases} \tag{8}$$

2.1.3. Compliance finding process

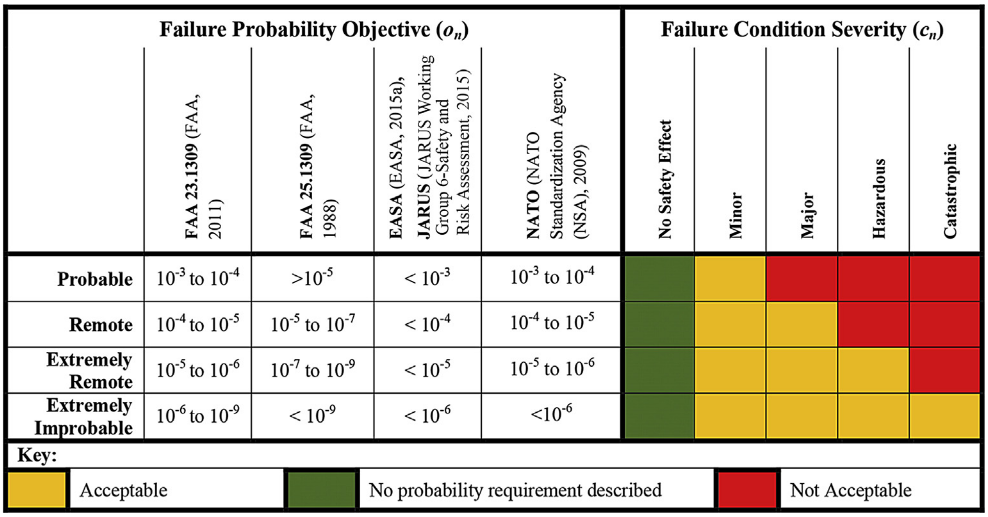
As shown in Fig. 1, the final step is the compliance finding process. Compliance finding is a simple deterministic decision making process, where a system is deemed compliant to the Part 1309 SSPR if:

1. H_s is assessed as *True*; and
2. All necessary documentation on the assessment outcomes, people, tools, and data used as part of the system safety assessment and compliance processes is provided.

If the system is determined to be non-compliant (*i.e.*, $H_s = False$) then an iterative engineering process is undertaken to reduce the APFH and/or the failure condition severity, as shown by the dotted line in Fig. 1. It is possible for regulators to declare a system as non-compliant on the basis of insufficient evidence of compliance. In such cases, further information or a reassessment is required (shown as a feedback path in Fig. 1). However, reaching this decision outcome is entirely subjective as the current assessment and compliance process does not explicitly handle uncertainty. Uncertainty in the outcomes from the system safety assessment process and subsequently, uncertainty in the compliance assessments are not input to the compliance finding process.

3. Incorporating uncertainty in the SSPR compliance process

There are a number of perspectives on the meaning of uncertainty. In its general sense, uncertainty is a "state of knowledge" (Dezfuli et al., 2009). Ayyub (2001) defines uncertainty as "knowledge incompleteness due to inherent deficiencies with acquired knowledge", while Aven (2003) describes it as a "lack of knowledge about the performance of a system (the 'world'), and observable quantities". Central to these definitions is the concept of knowledge, where knowledge is defined as something that is "known from gathered information" (Dezfuli et al., 2009).



	Failure Probability Objective (o_n)				Failure Condition Severity (c_n)				
	FAA 23.1309 (FAA, 2011)	**FAA 25.1309** (FAA, 1988)	**EASA** (EASA, 2015a), **JARUS** (JARUS Working Group 6-Safety and Risk Assessment, 2015)	**NATO** (NATO Standardization Agency (NSA), 2009)	**No Safety Effect**	**Minor**	**Major**	**Hazardous**	**Catastrophic**
Probable	10^{-3} to 10^{-4}	$>10^{-5}$	$< 10^{-3}$	10^{-3} to 10^{-4}	🟩	🟨	🟥	🟥	🟥
Remote	10^{-4} to 10^{-5}	10^{-5} to 10^{-7}	$< 10^{-4}$	10^{-4} to 10^{-5}	🟩	🟨	🟨	🟥	🟥
Extremely Remote	10^{-5} to 10^{-6}	10^{-7} to 10^{-9}	$< 10^{-5}$	10^{-5} to 10^{-6}	🟩	🟨	🟨	🟨	🟥
Extremely Improbable	10^{-6} to 10^{-9}	$< 10^{-9}$	$< 10^{-6}$	$<10^{-6}$	🟩	🟨	🟨	🟨	🟨

Key:

🟨	Acceptable	🟩	No probability requirement described	🟥	Not Acceptable

Fig. 3. Comparative illustration of the Part 1309 safety objectives/failure probability objectives.

3.1. *Types of uncertainty*

Uncertainty is traditionally divided into two types: aleatory and epistemic (Ayyub, 2014; Dezfuli et al., 2009). The basis of this classification lies in the origin of the uncertainty; uncertainty arising through variation in measurable phenomena (aleatory uncertainty) and uncertainty due to a lack of our understanding of the physical phenomena being studied (epistemic uncertainty) (Ayyub, 2014; Riesch, 2013).

The term aleatory stems from the Latin word “alea” (game of chance, die) and pertains to “stochastic (non-deterministic) events, the outcome of which is described by probability” (Dezfuli et al., 2009). According to Ayyub (2014), aleatory uncertainty relates to “the inherent, random, or non-reducible uncertainty” and may be described through the use of objective or classical frequency-based probability measures (Ayyub, 2014; Paté-Cornell, 1996). It represents the “randomness” or “variability in samples” inherent in the system that cannot be reduced by further observations but is acknowledged and integrated into mathematical models (Paté-Cornell, 1996).

Epistemic has Greek origins, stemming from the word “episteme” meaning “knowledge” and pertains to “the degree of knowledge of models and their parameters” (Dezfuli et al., 2009). According to Ayyub (2014) epistemic uncertainty is “the knowledge-based, subjective uncertainty that can be reduced with the collection of data or attainment of additional knowledge” and can be described by subjective probability measures. Epistemic uncertainties represent fundamental uncertainties and are often “ignored and tend to be under-reported” (Paté-Cornell, 1996). They are particularly significant in those situations where the evidence base is small (Paté-Cornell, 1996). They are more difficult to treat than aleatory uncertainties as they stem from incomplete knowledge about fundamental phenomena (Paté-Cornell, 1996) but can be reduced with further information (*e.g.*, via observation) of the system.

3.2. *Sources of uncertainty*

Epistemic and aleatory uncertainties are an inherent and inescapable part of the modelling and assessment of any real world system. Aven (2010) describes uncertainty in relation to the inputs, model, outputs (including parameters of interest) and the decision criteria. For example, uncertainty can be associated with the inaccuracy, incompleteness, and imprecision of the data, models, and information used in an assessment process. Uncertainty can also be introduced through subjectivity and errors made in the assessment process itself. Extending Aven's model, uncertainty can also be introduced through the communication of the model and its outputs to other stakeholders. For example, uncertainty arising due to homophony, linguistic or lexical ambiguity, channel distortion, trust, *etc*. A detailed literature review identified additional sources of uncertainty relating to the modelling process (Riesch, 2013; Spiegelhalter and Riesch, 2011), engineering systems (Ayyub, 2001), and the use of expert opinion (Ayyub, 2001).

3.3. *Measuring uncertainty*

There are numerous approaches for measuring uncertainty (Aven, 2010; Aven and Zio, 2011; Zio and Pedroni, 2013), with the simplest and most common of which being probability theory (Aven and Zio, 2011). Under this approach, uncertainties are characterised by the probabilities associated with events (Zio and Pedroni, 2013), where an event is defined as an “occurrence or outcome or change of a particular set of circumstances” (Ayyub, 2014) and “corresponds to any of the possible states a physical system can assume, or any of the possible predictions of a model describing the system” (Zio and Pedroni, 2013). As discussed by Ayyub (2014), the term probability has a precise mathematical definition but its meaning, when applied to the representation of uncertainties, is subject to differing interpretations: that of the Frequentist (objective or classical interpretation), and that of the Bayesian (subjective interpretation) (Ayyub, 2014; Bolstad, 2007).

3.3.1. *Frequentist interpretation*

The Frequentist school, which includes classical statistical thinking, views probability as a “true property of nature” (Nilsen and Aven, 2003) or “a property of the external world” (Moller, 2012) that can be measured objectively. According to this view the probability of an event is the frequency with which it would occur in a long series of similar trials (Ayyub, 2014). “More precisely, it is the value to which the long-run frequency would converge as the number of experiments increases toward infinity” (Covello and Merkhofer, 1993). This approach is based on the “Law of Large Numbers” (Covello and Merkhofer, 1993), which states if independent trials with the same probability of outcomes are repeated, the average value of the trials converges to the expected value. In other words, in the long run, given the above assumptions, actual value converges to the expected value (Moller, 2012). One of the main advantages of the Frequentist interpretation of probability is that “it involves only objective treatment of statistical samples” (Paté-Cornell, 1996). It is based on well-known principles of statistical inference that makes use of empirical data and empirically validated models that can provide added confidence in the approach (Aven and Zio, 2011; Covello and Merkhofer, 1993). The limitations to the Frequentist approach is that it only takes aleatory uncertainties into account and cannot be applied when the data is insufficient (Covello and Merkhofer, 1993; Paté-Cornell, 1996). Thus the use of a Frequentist interpretation of probability can be problematic for complex systems where epistemic uncertainty is high and any situation where data are scarce.

3.3.2. *Bayesian interpretation*

A Bayesian interpretation defines probability as “the rational degree of belief that one holds in the occurrence of an event” (Ayyub, 2014). It is based on the concept of subjective probabilities; where probability is interpreted as “a number, expressing a state of knowledge or degree of belief that depends on the information, experience, and theories of the individual who assigns it” (Covello and Merkhofer, 1993). According to this view, “probability is a function not only of the event, but of the state of information. Different people may assign different probabilities and the probability assigned by any one person may change over time as new information is acquired” (Covello and Merkhofer, 1993). Probability under a Bayesian perspective quantifies the state of knowledge and represents the plausibility of an event or hypothesis (Dezfuli et al., 2009). Although subjective probabilities are judgmental in nature they are by no means arbitrary. They need to satisfy the same basic axioms as those in classical probability theory (Covello and Merkhofer, 1993).

One of the main advantages of the Bayesian interpretation of probability is that it is capable of taking both objective and subjective measures of uncertainty into consideration (Nilsen and Aven, 2003). In contrast to the Frequentist approach, the Bayesian approach can be used when data is scarce (Aven and Zio, 2011) and can take both epistemic and aleatory uncertainties into consideration (Paté-Cornell, 1996). Furthermore, its use also allows the analyst to make use of all the available information to allow for better parameter estimation and improved decision making (Dezfuli et al., 2009; Paté-Cornell, 1996). Bayesian methods provide an accepted, structured, and consistent way (logically and mathematically) to perform quantitative inferences in situations where one has experience and data, however limited this may be. According to Jaynes (2003), Bayesian methods provide the comprehensive representation of the state of knowledge needed by decision makers to make rational and consistent decisions in the presence of uncertainty.

3.4. Decision making under uncertainty

Jaynes (2003) describes the desiderata of rationality and consistency for plausible reasoning in the presence of uncertainty (see p.17, (Jaynes, 2003)). The general preface is that decision makers can only make inferences (or propositions) about the state of the world based on the uncertain knowledge and information on hand. Bayesian inference provides a means for measuring uncertainty in relation to these hypotheses by producing information based on models, data, and other information (Dezfuli et al., 2009). Bayesian inference can also be used to progressively update the state of knowledge (degree of belief in the hypothesis) as new data or experience in the operation of the system is gained. These techniques are already accepted as the standard in a number of industries and used in the probabilistic assessment of the risks associated with space launch activities (Guarro, 2012; Guikema and Pate-Cornell, 2004), and in the nuclear power industry (United States Nuclear Regulatory Commission, 1975). Both of these applications are analogues to the system safety assessment of UAS; complex systems with relatively low data.

3.5. Uncertainty in the SSPR compliance process

Uncertainty is inherent to all stages of the SSPR compliance process illustrated in Fig. 1. This uncertainty is compounding and can ultimately lead to errors in compliance findings.

3.5.1. Uncertainty in the system safety assessment process

There is significant uncertainty associated with the input data and modelling undertaken as part of the system safety assessment process, irrespective of whether it is undertaken for a manned or unmanned aircraft. However, the uncertainty in a system safety assessment for a UAS is likely to be higher due to:

- Limited operational data and experience – Operational data and experience is a principal input to the assessment process, being used in the identification of failure modes, the characterisation of their effects, and the assessment of the probability of their occurrence. There is a significant amount of data and experience on CPA, their operation, component systems, and various means of failure. Conversely, for UAS, there is less data and experience due to the relative infancy of the systems, the restrictions imposed on their operations, and the rapid pace of technology development. In addition, the diversity of the UAS fleet and the nature of their operations makes it difficult to draw conclusions from other operational systems.
- Use of commercial off the shelf (COTS) components – Most CPA types make use of certified quality-assured components. Such components have been designed, manufactured, and tested to defined standard(s), which can be used as a basis for estimating component reliability. The standards are common to the industry; hence a wealth of data and information on the failure modes and reliability of components can be obtained through studying the population of components in service. Conversely, the majority of civil UAS employ COTS hardware and software, which are not designed, manufactured, nor tested to defined standards. The rapid pace of technology development further compounds the situation, with COTS components constantly being updated to remain commercially competitive. As a consequence, it is difficult to develop heritage in a particular component and in turn, system baseline configuration.
- Dynamic system baselines – The system certification baseline is a description of the configuration of the entire system at a particular point in time. The description includes a specification of the system architecture and its constituent components, and is a key input to a system safety assessment for any aircraft. For CPA the system baseline is relatively static, allowing safety data to be quickly compiled for a single aircraft type or across the entire fleet of a particular aircraft type. For civil UAS the system baseline is dynamic, largely due to the rapid pace of technology development and the need for a flexible and commercially competitive UAS that remain at the forefront of current capability. In addition, many UAS are designed to be “plug-and-play” systems to meet the demand for flexible mission capability. It is difficult to develop safety heritage in the system without a static baseline. This also challenges the use of existing reliability models typically used in the system safety assessment process, which assume mature systems exhibiting constant failure rates.

Uncertainty in the inputs and models used will lead to uncertainty in relation to all of the outputs from the system safety assessment process. With reference to Equation (2) through to (4), these uncertainties can include:

- *F* – Whether all failure conditions have been correctly identified, and whether each identified failure condition (f_n), is correctly specified in terms of its modes of failure and its effects;
- *C* – Uncertainty in relation to the estimate of the magnitude of consequential effects and in turn, the severity condition category (c_n) assigned to each failure condition f_n;
- Λ – Uncertainty in relation to the estimate of λ_n for each failure condition f_n;
- *FPO* – Whether the correct o_n is selected for each identified failure condition f_n.

It is important to note that these uncertainties are not independent. For example, uncertainty in the choice of o_n will incorporate the uncertainty associated with the assignment of c_n. Typically, a number of people and organisations are involved in the system safety compliance process. As such, the outcomes of the system safety assessment process are also subject to communication uncertainty (*e.g.*, trust, certitude, *etc.*).

System safety guidance material (FAA, 2011, 1988; SAE ARP 4754A, 2010; SAE ARP 4761, 1996; SAE ARP 5150, 2013) make no explicit mention of uncertainty, its measurement or treatment as part of the system safety assessment process. However, it is acknowledged that a failure mode can potentially have a range of negative impacts on the safety of flight. In such cases, the recommended practice is to assign c_n to the highest potential severity category. Guidance material (SAE ARP 5150, 2013) also suggests the use of sensitivity analysis to determine the “upper bounds” on quantitative estimates of λ_n. Such conservative approaches, whilst arguably defensible, do not comprehensively address the uncertainties present in the system safety assessment process, particularly knowledge/model uncertainty. Such conservative assumptions can compound and result in the impost of unnecessary cost.

3.5.2. Uncertainty in the compliance assessment and finding processes

As described in Section §2.1.3, the current compliance assessment process is a deterministic binary process. No account of the uncertainty in the input sets *F*, *C*, Λ and *O* is taken into consideration in the evaluation of Equation (7). As such, there is no objective means for expressing the resulting uncertainty in the output state of compliance, H_S. The output assessment can be either *TRUE* or *FALSE*. As such, decision makers are unable to objectively account for uncertainty in decision-making.

Uncertainty is inherent to the entire process illustrated in Fig. 1; its inescapable existence gives rise to six possible outcomes from compliance decision-making, namely:

1. Certifying a UAS as compliant when it is in fact compliant; a desirable outcome;
2. Certifying the system as compliant when it is in fact non-compliant. This is the least desirable outcome, which can lead to the operation of a UAS that does not meet the minimum safety standards;
3. Not certifying a UAS as compliant when it is in fact compliant. This is a less than desirable outcome where an unnecessary cost is borne by the system manufacturer;
4. Not certifying a UAS as compliant when it is in fact non-compliant; a desirable outcome;
5. Requiring further data and analysis to be undertaken when the UAS is in fact compliant. This is a less than desirable outcome where an unnecessary cost is borne by the system manufacturer;
6. Requiring further data and analysis when the UAS is in fact non-compliant; this is a less than desirable outcome where an unnecessary cost is borne by the system manufacturer in undertaking additional assessment on a non-compliant system.

As described above, the consequences of various decision actions vary, and there is currently no objective means for decision makers to take these into consideration. A decision maker uses a subjective and somewhat “black box” process for making compliance findings.

3.6. Summary

The uncertainty inherent to the SSPR compliance process can lead to inconsistent, subjective, and potentially erroneous regulatory outcomes. This situation arises due the absence of a systematic and objective means for representing uncertainty to decision makers, and a framework that enables decision makers to make rational, logical, transparent, and consistent decisions when faced with uncertainty.

4. A new system safety performance requirement compliance process

A revised system safety performance requirement compliance process is illustrated in Fig. 4 and further described in the following sub-sections. Inspiration for the revised approach comes from (Perez, 2015, 2013, Perez et al., 2013, 2012a, 2012b). At its foundation, is the premise that the compliance finding process can be viewed as a problem of decision-making under uncertainty. Improved decision-making in the presence of uncertainty requires comprehensive assessments of the uncertainty. As discussed by Aven and Zio (2011) “the bottom line concern with respect to uncertainty in decision making is to provide the decision makers with a clearly informed picture of the problem upon which they can confidently reason and deliberate”.

In this paper we address only the uncertainty associated with the assessment of λ_n. Discussion on how the framework can be readily extended to represent other uncertainties in the system safety performance requirement process is presented in §5.4.

4.1. The system safety assessment process

The system safety assessment process remains a systematic process of determining *F*, *C*, Λ and *O*. However, the set Λ is now denoted Λ^* and no longer comprises point-value assessments of the average probability of failure, λ_n, but *N* conditional probability distributions describing the uncertainty (or degree of belief) in λ_n, denoted $p(\lambda_n|D,I)$, Equation (9).

$$\Lambda^* = \{p(\lambda_n|D,I) : n \in Q\} \tag{9}$$

In contrast to the traditional system safety assessment process, the outputs are measures of the uncertainty associated with the assessment of the APFH for the particular failure condition, given all of the available failure data, *D*, and knowledge and information, *I*. The conditional probability distribution, $p(\lambda_n|D,I)_n$, representing our uncertainty in λ_n is determined using Equation (10).

$$p(\lambda_n|D,I) = \frac{p(D|\lambda_n,I) \times p(\lambda_n|I)}{P(D|I)} \tag{10}$$

Equation (10) can be readily recognised as Bayes' Theorem, with $p(\lambda_n|D,I)$ corresponding to the posterior distribution, $p(D|\lambda_n,I)$ corresponding to the likelihood (or sampling) distribution, $p(\lambda_n|I)$ the prior distribution, and $P(D|I)$ the marginal or unconditional probability of observing failure condition data, *D*. $p(\lambda_n|D,I)$ is the distribution describing the uncertainty in the parameter of interest (λ_n) based on our prior state of knowledge and any new evidence provided by *D*. $p(\lambda_n|I)$ describes the uncertainty in our current knowledge; the model parameter λ_n (epistemic uncertainty), based on all previous available information, *I*. This is the analysts' state of knowledge about the hypothesis (Dezfuli et al., 2009) before taking into account *D*. $p(D|\lambda_n,I)$ is a distribution representing the likelihood of observing *D* and represents the aleatory uncertainty in the modelled system. $P(D|I)$ is a constant and serves as a normalisation factor.

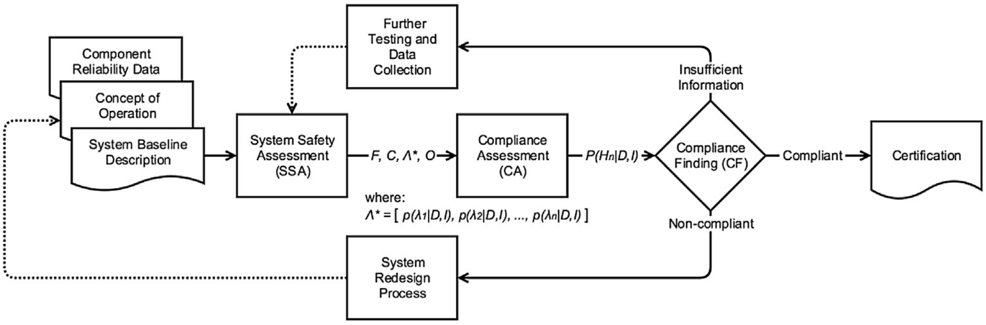

Component Reliability Data
Concept of Operation
System Baseline Description
Further Testing and Data Collection
System Safety Assessment (SSA)
F, C, Λ*, O
Compliance Assessment (CA)
P(Hn|D,I)
Insufficient Information
Compliance Finding (CF)
Compliant
Certification
Non-compliant
where:
Λ* = [p(λ1|D,I), p(λ2|D,I), ..., p(λn|D,I)]
System Redesign Process

Fig. 4. New SSPR compliance process.

4.1.1. The likelihood distribution

The likelihood distribution, $p(D|\lambda_n,I)$, represents the aleatory uncertainty in the observed/measured λ_n for the n^{th} identified failure condition, f_n. It is a statistical model describing the occurrence of the failure condition. There are a number of different models that are readily used in system safety assessment failure modelling. These include the Poisson, Exponential, Gamma, Weibull, Bernoulli and Binomial (Covello and Merkhofer, 1993). The particular likelihood distribution chosen will depend on the data and the fundamental physical phenomenon being observed; hence the distribution is conditioned on implicit information, I. The reader is directed to Covello and Merkhofer (1993) for further discussion on the selection of reliability distributions. A common choice used within the system safety assessment of most aviation systems is the Poisson, which assumes the failure condition, f_n, occurs at a constant rate. Discussion on the suitability of this model for describing the probability of UAS failures is presented in Section §5.1.2.

4.1.2. The prior distribution

There is uncertainty associated with the choice of $p(D|\lambda_n,I)$. This epistemic uncertainty is encoded through the choice of the prior distribution, $p(\lambda_n|,I)$. The prior distribution represents our current degree of belief in the model parameter, in this case λ_n. It describes an initial state of knowledge (Covello and Merkhofer, 1993) and reflects either what one believes or a summary of all one allows oneself to believe initially (Bolstad, 2007). Priors can be broadly classified as either informative or non-informative. Informative priors contain substantive information about the possible values of the unknown parameter (*i.e.*, λ_n), while non-informative priors are intended to let the data dominate the posterior distribution (Dezfuli et al., 2009). The prior could be any distribution that best represents the state of knowledge and will depend on the assessor. Expert judgement and historical failure data could be used to inform the choice of prior. A conjugate prior can also be used to simplify the evaluation of Equation (10). A conjugate prior permits solved analytical solution to Equation (10), removing the need to determine the posterior distribution through numerical integration (Bolstad, 2007; Dezfuli et al., 2009).

4.1.3. The posterior distribution

The marginal probability, $P(D|I)$, is obtained by integrating the numerator of Equation (10) over all the possible values of λ_n (for continuous distributions). Depending on the choice of distributions, Equation (10) can then be solved analytically or numerically, through Markov Chain Monte-Carlo (MCMC) simulation. The resulting posterior distribution, $p(\lambda_n|D,I)$, represents our updated state of knowledge in λ_n. This distribution can be used to make probabilistic inferences as to the value of λ_n.

To summarise, the output from the revised system safety assessment processes are the sets F, C, Λ^* and O. However, Λ^* contains a set of N distributions describing the uncertainty on the N estimates of APFH as opposed to point estimates of the APFH, as given in Equation (9).

4.2. The compliance assessment process

Input to the compliance assessment process is the set of posterior distributions, Λ^*, and the associated set of failure probability objectives, O. A moment (*e.g.*, mean) or the maximum likelihood estimator (MLE) of $p(\lambda_n|D,I)$ could be used to obtain representative point values of λ_n needed to evaluate Equation (7). However, this approach would discard the information captured in the uncertainty distribution (Perez, 2015).

Following (Perez, 2013; Perez et al., 2013, 2012a, 2012b), we redefine compliance assessment as the process of determining the degree of belief as to whether the candidate system satisfies all of its relevant failure probability objectives. Equation (7) is recast as a proposition (or hypothesis), for which we assign a probability representing the degree of belief in its state (*i.e.*, H_n being *TRUE* or *FALSE*). We begin by defining the set of N sub-propositions, S, as given in Equation (11).

$$S = \{H_n : n \in Q\} \tag{11}$$

Each sub-proposition, H_n, is *TRUE* if and only if λ_n is less than its relevant failure probability objective, O_n. We do not know the value of λ_n with certainty and hence can only determine a probability representing our uncertainty in each sub-proposition being *TRUE* (or not). This probability is denoted as $P(H_n|D,I)$. Each conditional probability $P(H_n|D,I)$ can be thought of as our degree of belief in the compliance of each failure condition, f_n, in meeting its required failure probability objective, O_n. There are a number of ways we can infer $P(H_n|D,I)$ from the posterior distributions $p(\lambda_n|D,I)$. One means for determining $P(H_n|D,I)$ is through the one-sided integration of $p(\lambda_n|D,I)$, Equation (12).

$$P(H_n|D,I) = \int_0^{O_n} p(\lambda_n|D,I).d\lambda \tag{12}$$

Alternatively, Bayesian Prediction can be used to determine the predicted probability of compliance taking full account of the uncertainty in λ_n. The predicted probability is calculated using Equation (13) (Bolstad, 2007) through marginalisation of the parameter λ_n (Hamada et al., 2008; Perez, 2015).

$$\begin{aligned} P(O_n|D,I) &= \int_{\Lambda} p(O_n,\lambda_n|\ D,\ I)\ .d\lambda \\ &= \int_0^{O_n} p(O_n|\ \lambda_n)p(\lambda_n|D,\ I)\ .d\lambda \end{aligned} \tag{13}$$

The predicted uncertainty in compliance can be found by combining Equations (10) and (13), as given in Equation (14).

$$P(H_n|D,I) = \int_0^{O_n} p(O_n|\lambda_n)\frac{p(D|\lambda_n,I)p(\lambda_n|I)}{P(D|I)}.d\lambda \tag{14}$$

In effect, Equation (14) averages the model uncertainty through integration of the sampling distribution $p(O_n|\lambda_n)$ over the posterior distribution $p(\lambda_n|D,I)$ (Hamada et al., 2008). The outcome is a predictive probability representing the uncertainty in compliance for the particular failure condition. Once $P(H_n|D,I)$ has been determined for all H_n in S and assuming the assessments are independent, Equation (8) can be recast to express our overall degree of belief in the compliance of the system $P(H_s|D,I)$ as follows:

$$\begin{aligned} P(H_s|D,I) &= \bigcap_{n=1}^{N} P(H_n|\ D,I) \\ &= P(H_1|D,I) \cap P(H_2|D,I) \cap \ldots \cap P(H_N|D,I) \end{aligned} \tag{15}$$

Unlike the original SSPR compliance assessment process, which provided a TRUE or FALSE statement to decision makers, the revised framework provides a conditional probability $P(H_0|D,I)$ representing the uncertainty in the system being compliant with the system safety performance requirement. This enables systematic consideration of uncertainty in the proceeding compliance process.

4.3. The compliance finding process

Following Perez et al. (2013), the compliance finding process can be considered as a problem of decision making under uncertainty. In so doing, it is explicitly acknowledged that the state of system compliance with the SSPR, H_s, cannot be known with absolute certainty. Instead, regulators can only pose a hypothesis as to the state of compliance of the system, and then look to reason, in some rational way, on the basis of its plausibility.

Input to the compliance finding process is the measure $P(H_s|D,I)$ describing the degree of belief in the state of compliance of the system with the system safety performance requirement. Based on this information, and as described in Section §3.5.2, decision makers can make one of three decision actions:

1. Deem the system to be compliant;
2. Deem the system to be non-compliant; or
3. Regulators request further data, testing, and analysis before they can have confidence to make a compliance finding.

A range of decision-making approaches can then be applied to assist decision makers in choosing between the above three options. A normative decision making approach is advocated by Perez et al. (2013). A normative decision making approach (refer to (Peterson, 2009) and Chapter 13 (Jaynes, 2003)) provides a means for rational and objective decision making. An individual's behaviour is likely to vary over time and across cultures, however the use of a normative theory can be expected to withstand the test of time and cultural differences (Peterson, 2009). In addition to this, the normative decision theory is a simple, transparent and pragmatic approach that is capable of accounting for the consequences that follow from a decision. It is a theory on how decisions should be made, rather than how they are actually made, thus serving as a prerequisite for rational decision making (Hansson, 2005). This latter point is important. Whilst simple and objective, normative decision-making is not intended to replace human decision-making. Rather, the authors consider it to be a useful input to human decision-making to encourage more rational, consistent and objective outcomes from what is an inherently subjective process. An area of future work would be in exploring a formulation of the decision space that better meets the information needs of human decision-making.

The compliance finding process can be formulated using a normative decision making approach as follows. Following Perez et al. (2013), the compliance finding decision problem can be considered to comprise of three components:

$$\Pi = \langle \mathscr{A}, \mathscr{X}, \mathscr{W} \rangle \tag{16}$$

$$\mathscr{A} = \{A_1, A_2, \ldots A_i\} \tag{17}$$

$$\mathscr{X} = \{X_1, X_2, \ldots X_y\} \tag{18}$$

$$\mathscr{W} = \{W_{uv}\} \quad \textit{for } u = 1, 2, \ldots i \textit{ and } v = 1, 2, \ldots y \tag{19}$$

where, $\mathscr{A}$ describes the set of decision options or actions, $\mathscr{X}$ describes the set of states of nature about which there is uncertainty, and $\mathscr{W}$ describes the set of decision outcomes. The uncertainty in the state of nature is denoted $P_k = P(X_k)$.

Specifying a loss with each decision action facilitates consideration of risk in decision-making. A loss function describing the consequences associated with pursuing each of the decision outcomes in $\mathscr{W}$ needs to be defined. The loss function L maps the states of nature $\mathscr{X}$ and the decision options $\mathscr{A}$ to measures of the consequences of outcomes (Perez et al., 2013):

$$L : A_u, X_v \mapsto L_{uv}(W_{uv}) \tag{20}$$

where L_{uv} measures the consequence of taking the decision $\mathscr{A}_u$, where X_v is the true state of nature. A decision criterion can then be applied, which selects the preferred decision option based on the consequences of the outcomes and the uncertainty in the state of nature [54]:

$$Z : \{L_{uv}, P_k\} \mapsto A^* \tag{21}$$

Applying the above to the compliance finding process, $\mathscr{A}$ has three elements representing the three possible decision options described above:

$$A_1 \equiv \textit{Compliant}$$
$$A_2 \equiv \textit{Non} - \textit{Compliant}$$
$$A_3 \equiv \textit{More information required}$$

The states of nature of interest corresponds to the state of system compliance, H_s, and its complement:

$$X_1 = H_s \quad X_2 = \overline{H_s} \tag{22}$$

The uncertainty in the states of nature P_k are provided by the compliance assessment process (Equation (12)):

$$\begin{aligned} P_1 &= P(X_1) = P(H_s|D, I) \\ P_2 &= P(X_2) = 1 - P_1 \end{aligned} \tag{23}$$

The six potential outcome states contained in $\mathscr{W}$ are described in Section §3.5.2 and are indexed as follows:

$\mathscr{W}_{11}$: *The UAS is deemed to be compliant when it is actually compliant;*
$\mathscr{W}_{12}$: *The UAS is deemed to be compliant but it is actually non-compliant;*
$\mathscr{W}_{21}$: *The UAS is deemed to be non-compliant but it is actually compliant;*
$\mathscr{W}_{22}$: *The UAS is deemed to be non-compliant when it is actually non-compliant;*
$\mathscr{W}_{31}$: *There is insufficient information in the state of compliance when the UAS is actually compliant;*
$\mathscr{W}_{32}$: *There is insufficient information in the state of compliance when the UAS is actually non-compliant.*

The decision/loss matrix providing the mapping between the loss function L_{uv}, decision options A_u and states of nature X_v is given in Table 1.

A negative loss value corresponds to a gain or reward, and a positive value represents a loss or cost. A qualitative description of the losses associated with the six outcome states in $\mathscr{W}$ was provided in Section §3.5.2. The loss values L_{11} and L_{22} would be assigned negative values reflecting desirable decision-making behaviour. Similarly, the loss values L_{12}, L_{21}, L_{31} and L_{32} would be assigned positive values reflecting less than desirable decision-making behaviour. It is important to note that the measurement of loss and the assigned values are subjective; reflecting the preferences and risk appetite of the regulator. With that said, same rational relationships between the assigned loss values can be hypothesised, with some examples summarised in Table 2.

Table 1
Compliance decision matrix.

	X_1 Compliant	X_2 Non-compliant
A_1 – Compliant	L_{11}	L_{12}
A_2 – Non-Compliant	L_{21}	L_{22}
A_3 – More information required	L_{31}	L_{32}

Table 2
Relationship between various loss functions.

Relationship	Description
$L_{12} = \max\limits_{\forall u,v}\{L_{u,v}\}$	It would be expected that the highest loss value would be assigned to $\mathscr{W}_{12}$ as it describes the outcome where a potentially unsafe UAS is certified as safe for operation.
$L_{22} = \min\limits_{\forall u,v}\{L_{u,v}\}$	It would be expected that the lowest assigned loss (or highest reward) would be assigned to $\mathscr{W}_{22}$ as it describes the outcome where a potentially unsafe UAS is deemed non-compliant.
$L_{22} \leq L_{11}$	From a safety perspective, deeming a system as non-compliant when it is in fact non-compliant ($\mathscr{W}_{22}$), is as desirable, if not more desirable, than deeming the UAS as compliant when it is actually compliant ($\mathscr{W}_{11}$).
$L_{31} < L_{21}$	It would be more preferable to seek further information before making a decision on whether or not a compliant system is actually compliant ($\mathscr{W}_{31}$) than deeming the compliant system to be not compliant ($\mathscr{W}_{21}$).
$L_{22} < L_{31}$	From a safety perspective, deeming a system as non-compliant when it is actually non-compliant ($\mathscr{W}_{22}$), would be more desirable than seeking further information before making a decision on whether or not a compliant system is compliant ($\mathscr{W}_{31}$)

It is now possible to take into consideration the risk associated with the decision outcomes. Decision risk is the composite of uncertainty and consequence for each decision outcome/action. The measure of uncertainty is given by the probabilities P_1 and P_2 (Equation (23)) and the values of loss as assigned inTable 1.

There are numerous ways in which a measure of risk can be found from its component measures of uncertainty and consequence. In aviation risk management frameworks, a risk matrix is used to provide a measure of risk. The matrix provides a Cartesian mapping between the component measures of consequence and uncertainty and risk. More simplistic approaches use multiplicative or additive operations.

For the purposes of providing a simple illustration of the approach, it is assumed that a measure of risk can be found through the multiplication of the measures of loss and probability. On this basis, a measure of the decision risk can be described as the expected loss over the posterior distribution of the uncertain states of nature at the time of making the decision (Perez et al., 2013; Singpurwalla, 2006). The risk for each of the three decision actions in $\mathscr{A}$ can be found using Equation (24).

$$\begin{aligned} R(A_1) &= L_{11}P_1 + L_{12}P_2 \\ R(A_2) &= L_{21}P_1 + L_{22}P_2 \\ R(A_3) &= L_{31}P_1 + L_{32}P_2 \end{aligned} \tag{24}$$

Following Perez et al. (2013) the decision criterion that satisfies Jaynes (2003) desiderata of consistency and rationality is the decision action A^* that minimises the Bayesian risk, as given in Equation (25).

$$A* = \arg\min_{A \in \mathscr{A}}\{R(A)\} \tag{25}$$

The decision option A^* determined through the use of Equation (25) represents the "objective" compliance decision option, given all available data and information. As mentioned, this does not reflect the subjective process of human decision-making. Rather, A^* would input to such a subjective decision making process, helping to foster more objective, consistent and rational compliance finding.

4.4. Summary

The proposed framework provides one means for fostering more robust, systematic, rational, objective, and transparent compliance decision making in the presence of uncertainty. Uncertainty in the estimates of the APFH is represented through the use of Bayesian probabilities. The normative decision making approach reduces the subjectivity of compliance findings in the presence of uncertainty and allows decision makers to take into account the risk associated with pursuing various decision actions. The revised system safety performance requirement compliance process is suited to UAS, which lack the data and knowledge needed to provide estimates of the APFH with certainty.

5. Case study

A hypothetical case study is presented to exemplify the features of the refined compliance process. The case study is for a manufacturer undertaking type certification of a new UAS. The certification activity includes the requirement to demonstrate compliance to the system safety performance requirement contained within sub-part 1309 of the respective civil aviation safety regulations. For the purposes of this case-study, the draft Part 1309 regulations presented in EASA (2015a) are used. The simple case study presented herein illustrates the general process for a single failure condition. It is important to note that a safety analysis and compliance assessment would need to consider numerous failure conditions and the potential dependencies between them (as discussed in Section §4.2).

5.1. System safety assessment process

Following standard failure identification and effects analysis processes (as described in Hayhurst et al. (2007)), one component of the UAS was identified as having a failure condition (f_1) and assigned the severity category (c_1) of *Minor*. The appropriate FPO for a failure condition of *Minor* severity as defined in EASA (2015a) is:

$$O_1 = 10^{-3}.hr^{-1} \tag{26}$$

5.1.1. Available data

The manufacturer has a fleet of six identical prototype UAS. The fleet has undergone extensive hardware in the loop (HIL) simulation and flight testing; collectively accummulating a total of 7500 hours of operation. f_1 was observed only five times during HIL and flight testing of the prototypes. This represents available data, *D*.

5.1.2. Choice of likelihood distribution

As stated previously, there are numerous mathematical models that can be used to describe discrete events such as the failure of a

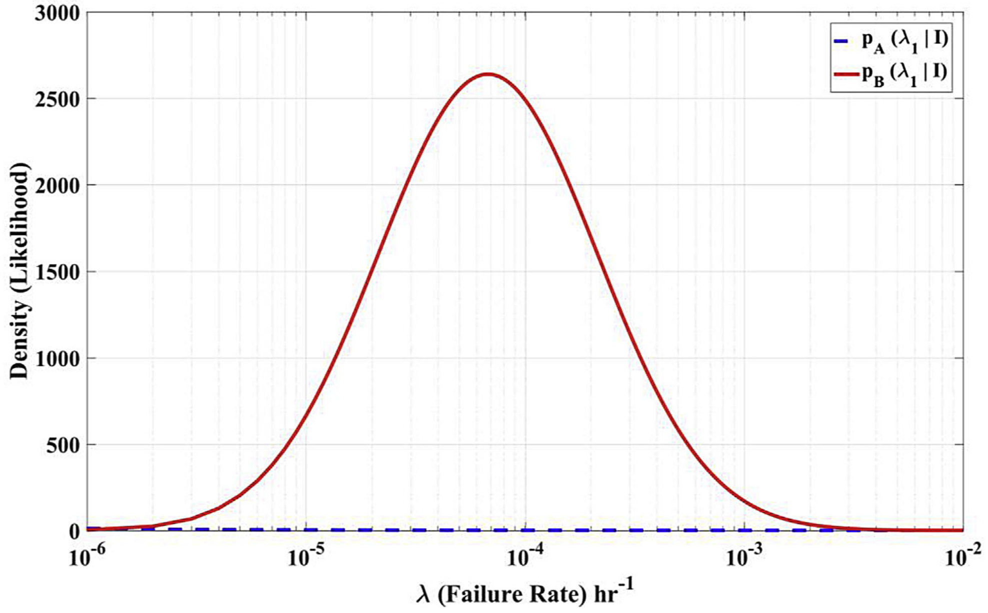


Fig. 5. Comparison of the prior distributions input by Analyst A and Analyst B.

component. Both Weibull and Poisson distributions could be considered appropriate choices for the likelihood distribution for this case study. One of the major limitations of the Poisson distribution is that it assumes a constant failure rate (Covello and Merkhofer, 1993), an assumption not made in the Weibull model. Given the characteristics of UAS described in Section §3.5.1, the Weibull distribution is potentially a more appropriate failure distribution, however, in keeping with Part 1309 Guidance Material, a Poisson likelihood distribution is assumed for this case study, Equation (27).

$$p(D|\lambda_1, I) = \frac{(\lambda_1 t)^D e^{-\lambda_1 t}}{D!} \tag{27}$$

where, *p(D|λ_1,I)* is the likelihood distribution, *D* is the observed number of failures (a positive integer), λ_1 is the APFH, *I* is the information known prior to *D*, *t* is the time period over which the failures were observed.

5.1.3. *Choice of prior distribution*

Two analysts were tasked with determining λ_1. *Analyst A* had no prior knowledge or information as to the value of λ_1, and thus adopted a non-informative prior. While there are a number of non-informative priors that can be used, a conjugate Jeffrey's Prior was selected for this case. The selection of this prior, not only lets the data speak for itself, but being a conjugate prior, the posterior distribution can be solved analytically.

There are different Jeffrey's priors for different distributions; for the Poisson distribution, it is a gamma distribution with shape parameter (α) equal to 0.5 and rate parameter (β) equal to zero (Equation (28)). It is important to note that this distribution is not a proper distribution as the integral over all possible values of λ_1 is not finite. The posterior distribution that it yields is a proper distribution with updated parameters (Dezfuli et al., 2009) as given in Equation (28), where Γ is the gamma function.

$$p_A(\lambda_1|I) \propto \frac{\beta^\alpha}{\Gamma(\alpha)} \lambda_1^{\alpha-1} e^{-\beta\lambda_1} \tag{28}$$

Analyst B undertakes a fault tree analysis (FTA) incorporating component reliability data and expert judgement. *Analyst B* is able to provide an estimate of the mean and standard deviation of λ_1. Thus, the prior distribution of λ_1 determined by *Analyst B* is taken to follow a lognormal distribution with parameters $\mu = -8.275$ and $\sigma = 1.151$ substituted into Equation (29). The corresponding mean and standardard deviation of the lognormal distribution is equal to 4.94×10^{-4} and 8.21×10^{-4} respectively. The two candidate prior distributions are illustrated in Fig. 5.

$$p_B(\lambda_1|I) = \frac{1}{\lambda_1 \sigma \sqrt{2\pi}} e^{-(ln(\lambda_1)-\mu)^2} \tag{29}$$

5.1.4. *Calculation of the posterior distribution*

Due to the choice of a conjugate prior distribution, *Analyst A* can determine the posterior distribution, *p_A(λ_1|D,I)*, analytically. In this case, *p_A(λ_1|D,I)* follows the same form as the prior distribution but with updated shape and rate parameters α and β as given in Equation (30).

$$p_A(\lambda_1|D, I) \propto \frac{\beta^\alpha + D}{\Gamma(\alpha + D)} \lambda_1^{(\alpha+D-1)} e^{-(\beta+D)\lambda_1} \tag{30}$$

where *D* is the number of observed failures in the time period *t* (the data) and Γ is a gamma function. As per Equation (10), the resulting distribution must be normalised by the marginal probability (summation of the gamma distributions for all values of λ_1) to obtain a proper posterior distribution. For Analyst B, numerical integration is needed to determine the posterior distribution *p_B(λ_1|D,I)*. The likelihood distribution *p(D|λ_1,I)* (Equation (27)) and the prior distribution *p_B(λ_1|I)* (Equation (29)) were substituted into Equation (10) and then solved using MCMC simulation. The

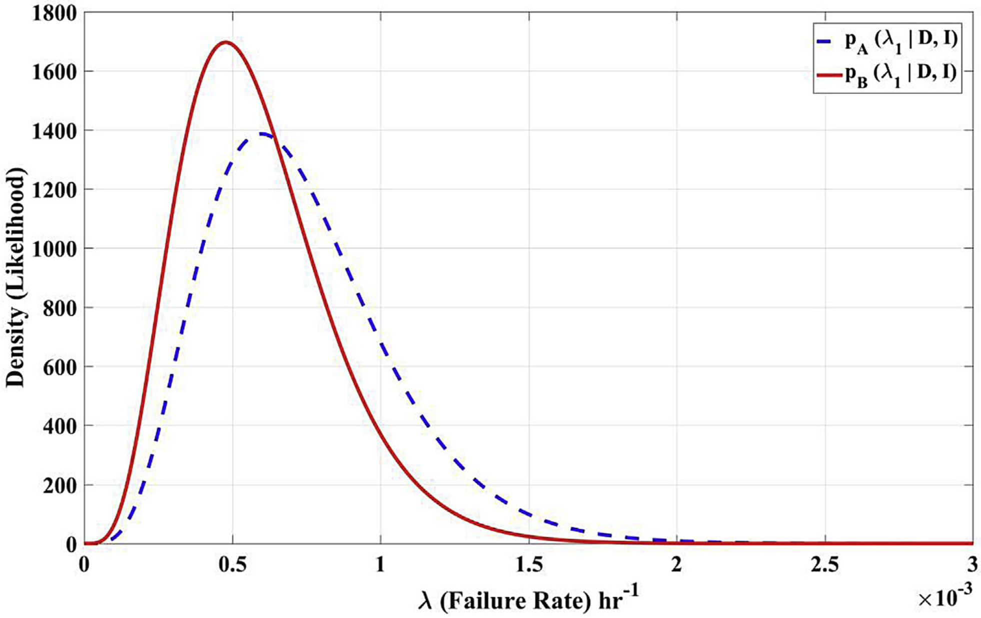


Fig. 6. Posterior distribution for *Analyst A* and *Analyst B*.

resulting posterior distributions are given in Fig. 6.

The effect of the additional prior information can be observed in the outcome posterior distributions illustrated in Fig. 6. The posterior distribution provided by *Analyst B* is slightly narrower compared to that of *Analyst A*, with *Analyst A*'s posterior distribution more strongly representing the available data, D. The non-informative prior has the effect of spreading the likelihood function. Taking this into consideration, if information is limited, as would currently be the case in the UAS industry, choosing a non-informative prior is not likely to adversely impact the posterior distribution. However, as more information becomes available, the Bayesian approach allows for it to be taken into consideration thus providing the regulator with additional information to aid in the decision making process. The tuples describing the output from the system safety assessment process are given in Equations (31) and (32), for *Analyst A* and *B*, respectively.

$$< f_1, Minor, p_A(\lambda_1|D, I), 10^{-03} > \quad (31)$$

$$< f_1, Minor, p_B(\lambda_1|D, I), 10^{-03} > \quad (32)$$

5.1.5. *What if point estimates were required?*

The output assessments are distributions describing the uncertainty in λ_n. However, estimates of the value of λ_n may also be required to support the quantitative analysis of other failure conditions. Direct statistical estimates on the value of the parameter

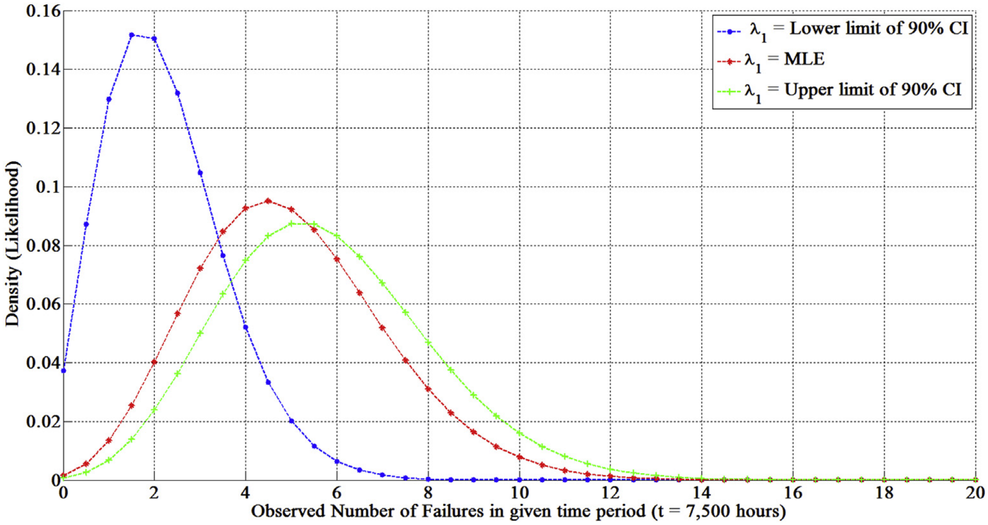


Fig. 7. Comparison of failure distributions for the MLE and upper and lower limits for the 90% Bayesian credibility interval.

Table 3
Proposition probabilities for *Analyst A* and *Analyst B*.

	Analyst A	Analyst B
$P(H_1\|D, I)$	0.8190	0.9296

Table 4
Compliance decision matrix for case study.

	X_1 – Compliant	X_2 – Non-Compliant
A_1 – Compliant	−3	3
A_2 – Non-Compliant	2	−3
A_3 – Uncertain	1	1

can be taken from the posterior distribution, for example, by computing the MLE. Bayesian credibility intervals (CI) (Covello and Merkhofer, 1993) can also be defined, which describe an interval on the domain of λ_n with probability α that it contains the true value λ_n, given all data and information available. These estimates of λ_n can be incorporated into the likelihood distribution to provide a "family of models" of the reliability of the system. For example, illustrated in Fig. 7 are three Poisson failure models for λ_n equal to the MLE and the lower and upper limits of the 90% CI for λ_n, taken from the posterior distribution $p_A(\lambda_1|D, I)$. Analysts could use the three cases as representative worst, likely, and best case failure distributions given all available data and information at hand. As described by Paté-Cornell (1996), the presentation of alternate models to decision makers represents the highest treatment of uncertainty. An advantage of this approach is that there is no need to aggregate expert opinions or to deal with the fundamental assumptions made by each expert. Information can be represented exactly as it was coded (Paté-Cornell, 1996).

5.2. Compliance assessment

From EASA (2015a), a failure condition classified as having *Minor* severity must have an APFH of *Probable* or less, which corresponds to the quantitative failure probability objective of 10^{-3} failures per flight hour. The compliance sub-proposition for the particular failure condition, H_1, can be defined as:

$$H_1 : \lambda_1 \leq 10^{-3} \tag{33}$$

As described in Section §4.2, the conditional probability describing our uncertainty in the proposition H_1 can be determined through integrating the posterior distribution for the appropriate bounds (Equation (12)) or through calculation of the predictive probability (Equation (14)). For the purposes of this case study, Equation (12) is used to determine the uncertainty in H_1 with the results for the two analysts summarised in Table 3. The probability of the hypothesis of compliance is the area under the curve to the left of the proposition as given in Fig. 8.

As we are only analysing a single failure condition (*i.e.*, $N = 1$), our uncertainty in the overall state of system compliance (as given by Equation (15)) simplifies to:

$$P(H_s|D, I) = P(H_1|D, I) \tag{34}$$

Thus the proposition probabilities given in Table 3 can be directly interpreted as the output compliance probabilities $P_A(H_s|D,I)$ and $P_B(H_s|D,I)$ input to the compliance finding process.

5.3. Compliance finding

The normative decision making approach as described in Section §4.3 is adopted for this case study. A loss matrix is defined in Table 4 following the qualitative relationships described in Section §4.3. The assigned loss values are subjective; with a loss scale ranging from −3 to +3 used in this case study. The loss value of −3 represents the most desirable outcome and +3 represents the least

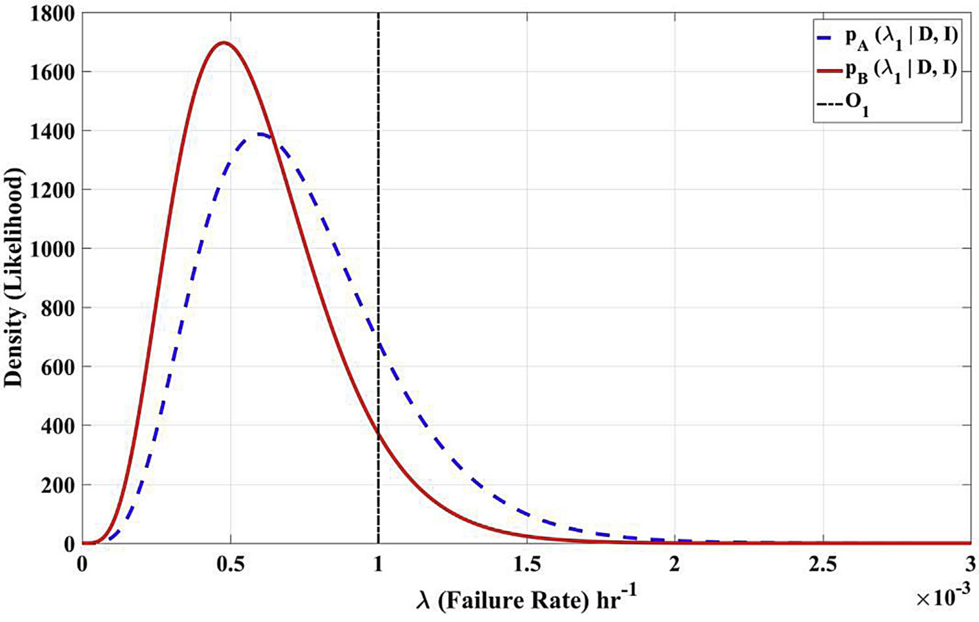


Fig. 8. Posterior distribution showing the uncertainty relating to H_1 for *Analyst A* and *Analyst B*.

Table 5
Probabilities characterising the uncertainty in the state of compliance.

	Analyst A	Analyst B
P_1	0.819	0.930
P_2	0.181	0.070

Table 6
Risk for each decision action.

	Analyst A	Analyst B
$R(A_1)$	−1.914	−2.578
$R(A_2)$	1.095	1.648
$R(A_3)$	1.000	1.000

desirable outcome. The compliance probabilities $P_A(H_1|D,I)$ and $P_B(H_1|D,I)$ correspond to $P_{A,1}$ and $P_{B,1}$ and their complements, as given in Table 5. Finally, the risk associated with each decision option can be obtained using Equation (24), with the results presented in Table 6. Applying Equation (25), the decision action with the minimum decision risk (A^*) for both analysts can be determined.

The recommended decision action is A_1, which corresponds to the decision to certify the failure condition as being compliant with the system safety performance requirement. The recommended decision action is the same for both analysts despite the differences in the prior knowledge held by each analyst. However, the value of having additional prior knowledge (*i.e.*, the use of an informed prior) is evident in the posterior probabilities and decision risks presented in Tables 5 and 6, respectively, where the additional information available to *Analyst B* leads to a much more distinct decision action.

The system safety assessment process typically involves a diverse range of data and expert judgement. As illustrated in the case study, the new framework provides an objective and mathematically defensible means for combining the various sources of data and information in the assessment process.

5.4. Discussion

With reference to Paté-Cornell's "levels of treatment of uncertainty" (Paté-Cornell, 1996); the revised framework provides for the highest treatment of the uncertainty associated with estimates of the average probability of failure, λ. Such an approach is necessary where there are situations of high uncertainty, such as the system safety assessment of civil UAS, which lack the data and knowledge that comes with extensive operational experience. Such knowledge and experience is gained incrementally. The posterior models can be progressively updated as data becomes available, allowing the regulator and manufacturer to objectively refine estimates of safety performance with time.

The revised approach does not take into consideration the uncertainty associated with the input data, D. Such uncertainty may arise through, for example, a lack of fidelity in the HIL simulation environment, or inaccurate, censored, or missing flight test records. A number of approaches can be used to account for data uncertainty and are presented in Chapter 10 of Kelly and Smith (2011). Extensions to this framework will look to account for the uncertainty associated with the assignment of the failure condition severities (c_n), and in turn selection of failure probability objectives (o_n).

In accordance with system safety assessment guidelines, this paper adopted a simple Poisson failure rate model, which assumes a constant failure rate. Currently, most commercial UAS do not exhibit the constant failure rates typical of mature aviation systems. For small UAS, their changing configuration may mean that they never achieve a stable failure rate. This brings into question the validity of the assumption of a constant failure rate model. A more appropriate model is likely to be the Weibull model, which can be used to characterise the reliability of immature, mature, and aging systems.

Existing system safety modelling techniques such as FTA can be readily incorporated into the proposed framework (see, for example, (Guarro, 2012)). An area requiring further research is in the extension of the current framework to include consideration of the uncertainty in the assignment of failure severities and input data. Further, advancements could be made through exploring likelihood distributions that more accurately characterise the failure characteristics of different types of sub-systems, including those associated with the remote pilot.

The risk measures are not immediately usable within existing aviation risk management frameworks. Future work would look to represent the decision risk within a standard risk matrix and incorporate existing risk evaluation and treatment decision-making frameworks (*i.e.*, the As Low As Reasonably Practicable (ALARP) framework) commonly used in aviation risk management.

6. Conclusion

The general lack of data and experience in the operation of civil UAS gives rise to uncertainty in relation to all aspects of their performance. This poses a particular problem when it comes to certifying such systems against airworthiness regulations. The existing system safety compliance process does not take uncertainty into consideration, and accounting for uncertainty in compliance decision-making is a subjective process. This paper proposes a fundamentally new approach to the aviation system safety performance requirement compliance process that could account for the uncertainty inherent in the system safety assessment of any aircraft system, manned or unmanned. The overall aim is to facilitate more transparent, rational, and systematic compliance decision-making.

Whilst applied to UAS and compliance to the Part 1309 regulations, the same fundamental approach could be readily adopted for any regulatory compliance process or aircraft system. The approach proposes a significant change to how aviation safety practitioners currently undertake regulatory compliance activities. Whilst the theoretical principles of the approach are not new, their application to aviation represents a significant advancement over current aviation regulatory practice. The proposed approach brings aviation system safety practices in line with the more contemporary (and well established) approaches adopted by other safety critical industries.

Acknowledgements

This research was supported, in part by, the Australian Government Research Training Program Scholarship, provided by the Australian Government.

Appendix A. Failure condition severity scales.

	JARUS (JARUS Working Group 6-Safety and Risk Assessment, 2015)	EASA (EASA, 2015a)	Hayhurst (Hayhurst et al., 2007)	NATO (NATO Standardization Agency, 2014)	RTCA (RTCA DO-344, 2013)*
No Safety Effect	Failure conditions that would have no effect on safety. For example, failure conditions that would not affect the operational capability of the RPAS or increase remote crew workload.	Failure conditions that would have no effect on safety. For example, failure conditions that would not affect the operational capability of the RPAS or increase the remote crew workload.	Failure Conditions that would have no effect on safety (that is, Failure Conditions that would not affect the operational capability of the airplane or increase flight crew workload).	None defined.	UAS failure condition(s) that have negligible effects to people on the ground. (Referred to as Minimal)
Minor	Failure conditions that would not significantly reduce RPAS safety and that involve remote crew actions that are within their capabilities. Minor failure conditions may include a slight reduction in safety margins or functional capabilities, a slight increase in remote crew workload, such as flight plan changes.	Failure conditions that would not significantly reduce RPAS safety and that involve remote crew actions that are well within their capabilities. Minor failure conditions may include a slight reduction in safety margins or functional capabilities, a slight increase in remote crew workload, such as flight plan changes.	Failure Conditions that would not significantly reduce UAS safety and involve flight crew actions that are well within their capabilities. Minor Failure Conditions may include a slight reduction in safety margins or functional capabilities or a slight increase in flight crew workload (such as routine flight plan changes).	Failure conditions that do not significantly reduce UA safety and involve UA crew actions that are well within their capabilities. These conditions may include a slight reduction in safety margins or functional capabilities, and a slight increase in UA crew workload.	UAS failure condition(s) that could result in minor injuries to one or more people on the ground.
Major	Failure conditions that would reduce the capability of the RPAS or the ability of the remote crew to cope with adverse operating conditions to the extent that there would be a significant reduction in safety margins, functional capabilities or separation assurance. In addition, the failure condition has a significant increase in remote crew workload or impairs remote crew efficiency.	Failure conditions that would reduce the capability of the RPAS or the ability of the remote crew to cope with adverse operating conditions to the extent that there would be a significant reduction in safety margins, functional capabilities or separation assurance. In addition, the failure condition has a significant increase in remote crew workload or impairs remote crew efficiency.	Failure conditions that would reduce the capability of the UAS or the ability of the flight crew to cope with adverse operating conditions to the extent that there would be: a significant reduction in safety margins or functional capabilities; a significant increase in flight crew workload or in conditions impairing flight crew efficiency; a discomfort to the flight crew; or a potential for physical discomfort to persons	Failure conditions that either by themselves or in conjunction with increased crew workload, are expected to result in an emergency landing of the UA on a predefined site where it can be reasonably expected that a serious injury will not occur. Or Failure conditions which could potentially result in injury to UA crew or ground staff.	UAS failure condition(s) that could result in moderate injuries to one or more people on the ground.
Hazardous	Failure conditions that would reduce the capability of the RPAS or the ability of the remote crew to cope with adverse operating conditions to the extent that there would be the following; i. Loss of the RPA where it can be reasonably expected that a fatality will not occur, or ii. A large reduction in safety margins or functional capabilities, or iii. High workload such that the remote crew cannot be relied upon to perform their tasks accurately or completely.	Failure conditions that would reduce the capability of the RPAS or the ability of the remote crew to cope with adverse operating conditions to the extent that there would be the following: i. Loss of the RPA where it can be reasonably expected that one or more fatalities will not occur, or ii. A large reduction in safety margins or functional capabilities or separation assurance, or iii. Excessive workload such that the remote crew cannot be relied upon to perform their tasks accurately or completely.	Failure Conditions that would reduce the capability of the UAS or the ability of the flight crew to cope with adverse operating conditions to the extent that there would be the following: i. A large reduction in safety margins or functional capabilities; ii. Physical distress or higher workload such that the UAS flight crew cannot be relied upon to perform their tasks accurately or completely; or iii. Physical distress to persons, possibly including injuries.	Failure conditions that either by themselves or in conjunction with increased crew workload, are expected to result in a controlled trajectory termination or forced landing potentially leading to the loss of the UA where it can be reasonably expected that a fatality will not occur. Or Failure conditions for which it can be reasonably expected that a fatality to UA crew or ground staff will not occur.	UAS failure condition(s) that could result in serious injuries to one or more people on the ground.
Catastrophic	Failure conditions that could result in one or more fatalities	Failure conditions that are expected to result in one or more fatalities.	Failure conditions that are expected to result in one or more fatalities or serious injury to persons, or the persistent loss of the ability to control the flight path of the aircraft normally with the loss of the aircraft.	Failure conditions that are expected to result in at least uncontrolled flight (including flight outside of pre-planned or contingency flight profiles/areas) and/or uncontrolled crash. Or Failure conditions which may result in a fatality to UA crew or ground staff.	UAS failure condition(s) that could result in a fatality to one or more people on the ground

*Additional safety effects on UAS crew, airspace users, air traffic control and UAS systems provided in reference.

References

ADF, 2016. Australian Air Publication 7001.054, Electronic Airworthiness Design Requirements Manual (eADRM).

Ancel, E., Shih, A.T., 2015. Bayesian Safety Risk Modeling of Human-flightdeck Automation Interaction.

Ancel, E., Shih, A.T., Jones, S.M., Reveley, M.S., Luxhøj, J.T., Evans, J.K., 2014. Predictive safety analytics: inferring aviation accident shaping factors and causation. J. Risk Res. 18, 1–24. http://dx.doi.org/10.1080/13669877.2014.896402.

Apostolakis, G., 1990. The concept of probability in safety assessments of technological systems. Science 250, 1359–1364. http://dx.doi.org/10.1126/science.2255906.

Apostolakis, G., 1981. Bayesian methods in risk assessment. In: Advances in Nuclear

Science and Technology. Springer, US, pp. 415–465.

Aven, T., 2010. Some reflections on uncertainty analysis and management. Reliab. Eng. Syst. Saf. 95, 195–201. http://dx.doi.org/10.1016/j.ress.2009.09.010.

Aven, T., 2003. Foundations of Risk Analysis: A Knowledge and Decision-oriented Perspective. John Wiley and Sons.

Aven, T., Zio, E., 2011. Some considerations on the treatment of uncertainties in risk assessment for practical decision making. Reliab. Eng. Syst. Saf. 96, 64–74. http://dx.doi.org/10.1016/j.ress.2010.06.001.

Ayyub, B.M., 2014. In: Chapman, Hall (Eds.), Risk Analysis in Engineering and Economics, second ed. CRC.

Ayyub, B.M., 2001. Experts, opinions, and elicitation methods. In: Elicitation of Expert Opinions for Uncertainty and Risks. CRC Press.

Bolstad, W.M., 2007. Introduction to Bayesian Statistics, second ed. John Wiley and Sons, Inc http://dx.doi.org/10.1080/10543406.2011.589638.

CAA, 2015. CAP-722, Unmanned Aircraft System Operations in UK Airspace - Guidance, sixth ed. London UK Civil Aviation Authority (CAA), Department of Transport (DfT), London, UK.

Clothier, R.A., Palmer, J.L., Walker, R.A., Fulton, N.L., 2011. Definition of an airworthiness certification framework for civil unmanned aircraft systems. Saf. Sci. 49, 871–885. http://dx.doi.org/10.1016/j.ssci.2011.02.004.

Clothier, R.A., Williams, B.P., Coyne, J., Wade, M., Washington, A., 2015. Challenges to the development of an airworthiness regulatory framework for unmanned aircraft systems. In: 16th Australian Aerospace Congress.

Clothier, R.A., Wu, P., 2012. A review of system safety failure probability objectives for unmanned aircraft systems. In: 11th International Probabilistic Safety Assessment and Management (PSAM11) Conference and the Annual European Safety and Reliability(ESREL 2012) Conference, Helsinki.

Clothier, R., Walker, R., 2006. Determination and evaluation of UAV safety objectives. In: 21st International Unmanned Air Vehicle Systems Conference. Bristol, UK, pp. 18.1–18.16.

Covello, V.T., Merkhofer, M.W., 1993. Risk Assessment Methods, Approaches for Assessing Health and Environmental Risks. Springer Science + Business Media, New York.

Dezfuli, H., Kelly, D., Smith, C., Vedros, K., Galyean, W., 2009. Bayesian Inference for NASA Probabilistic Risk and Reliability Analysis. NASA/SP-2009-569.

EASA, 2015a. Special Condition: Equipment, Systems, and Installations.

EASA, 2015b. Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes CS-25 / Amendment 17.

EASA, 2005. Policy for Unmanned Aerial Vehicle (UAV) certification, Advance–Notice of Proposed Amendment (NPA) No 16 / 2005.

Ellison, A.M., 1996. An introduction to Bayesian inference for ecological research and environmental decision-making. Ecol. Soc. Am. 6, 1036–1046.

EUROCAE, 2013. UAS/RPAS Airworthiness Certification “1309” System Safety Objectives and Assessment Criteria. MALAKOFF, France.

FAA, 2011. AC 23.1309-1E-System Safety Analysis and Assessment for Part 23 Airplanes. Advisory Circular 23.1309-1E.

FAA, 1988. AC 25.1309-1A-System Design and Analysis. Advisory Circular 25.1309-1A.

Guarro, S., 2012. Risk assessment of new space launch and supply vehicles, 2012, 11th Int. Probabilistic Saf. Assess. Manag. Conf. and the Annu. Eur. Saf. Reliab. Conf, PSAM11 ESREL 2012 6, 5157–5164.

Guikema, S.D., Pate-Cornell, M.E., 2004. Bayesian analysis of launch vehicle success rates. J. Spacecr. Rockets 41, 93–102. http://dx.doi.org/10.2514/1.9268.

Hamada, M.S., Wilson, A.G., Reese, C.S., Martz, H.F., 2008. Bayesian Reliability. Springer-Statistics. http://dx.doi.org/10.1007/978-0-387-77950-8.

Hansson, S.O., 2005. Decision Theory, a Brief Introduction. http://www.infra.kth.se/~soh/decisiontheory.pdf.

Hayhurst, K.J., Maddalon, J.M., Miner, P.S., Szatkowski, G.N., Ulrey, M.L., DeWalt, M.P., Spitzer, C.R., 2007. Preliminary Considerations for Classifying Hazards of Unmanned Aircraft Systems, NASA TM-2007–21439.

Huang, H.Z., Zuo, M.J., Sun, Z.Q., 2006. Bayesian reliability analysis for fuzzy lifetime data. Fuzzy Sets Syst. 157, 1674–1686. http://dx.doi.org/10.1016/j.polymdegradstab.2005.12.004.

JAA/EUROCONTROL, 2004. UAV Task-force Final Report: a Concept for European Regulations for Civil Unmanned Aerial Vehicles (UAVs).

JARUS Working Group 6-Safety and Risk Assessment, 2015. Safety Assessment of Remotely Piloted Aircraft Systems. AMC RPAS.1309.

Jaynes, E.T., 2003. Probability Theory: the Logic of Science. Cambridge University Press. http://dx.doi.org/10.1017/CBO9781107415324.004.

Kelly, D., Smith, C., 2011. Bayesian Inference for Probabilistic Risk Assessment: a Practitioners Guidebook. Springer, London.

Kelly, D.L., Smith, C.L., 2008. Risk Analysis of the Space Shuttle : Pre- Challenger Bayesian Prediction of Failure. NASA Space Systems Engineering & Risk Management Symposium.

Lindsey, N.J., Rackley, N., Brali, A., Mosleh, A., 2013. Reliability Prediction Using Bayesian Updating of On-Orbit Performance. NASA Technical Reports Server (NTRS).

Luxhøj, J.T., Matthew, H., 2015. An Object-Oriented Bayesian Network (OOBN) Prototype for Modeling the Safety Risk of an Unmanned Rotorcraft, in: IIE Annual Conference. Proceedings. pp. 183–192.

Mallick, B.K., Gold, D.L., Baladandayuthapani, V., 2009. Bayesian Analysis of Gene Expression Data. John Wiley and Sons. Ltd.

Maranzano, C.J., Krzysztofowicz, R., 2008. Bayesian reanalysis of the challenger O-ring data. Risk Anal. 28, 1053–1067. http://dx.doi.org/10.1111/j.1539-6924.2008.01081.x.

Marcot, B.G., Holthausen, R.S., Raphael, M.G., Rowland, M.M., Wisdom, M.J., 2001. Using Bayesian belief networks to evaluate fish and wildlife population viability under land management alternatives from an environmental impact statement. For. Ecol. Manage 153, 29–42. http://dx.doi.org/10.1016/S0378-1127(01)00452-2.

McCann, R.K., Marcot, B.G., Ellis, R., 2006. Bayesian Belief Networks: applications in ecology and natural resource management. Can. J. For. Res. 36, 3053–3062.

Moller, N., 2012. The concepts of risk and safety. In: Roeser, S., Hillerbrand, R., Sandin, P., Peterson, M., Trautmann, T., Vieider, F.M. (Eds.), Handbook of Risk Theory. Springer, pp. 56–85. http://dx.doi.org/10.1007/978-94-007-1433-5.

Morris, A.T., Beling, P.A., 2001. Space shuttle RTOS Bayesian Network. In: 20th DASC. 20th Digit. Avion. Syst. Conf. (Cat. No.01CH37219). http://dx.doi.org/10.1109/DASC.2001.963378.

NATO Standardization Agency, 2014. AEP-83, Light Unmanned Aircraft Systems Airworthiness Requirements.

NATO Standardization Agency (NSA), 2009. STANAG 4671 (Edition 1) - Unmanned Aerial Vehicles Systems Airworthiness Requirments (USAR) (Brussels, Belgium).

Nilsen, T., Aven, T., 2003. Models and model uncertainty in the context of risk analysis. Reliab. Eng. Syst. Saf. 79, 309–317. http://dx.doi.org/10.1016/S0951-8320(02)00239-9.

US DoD, 2007. Unmanned Systems Roadmap 2007-2032. United States Department of Defense.

Ozbay, K., Noyan, N., 2006. Estimation of incident clearance times using Bayesian Networks approach. Accid. Anal. Prev. 38, 542–555. http://dx.doi.org/10.1016/j.aap.2005.11.012.

Paté-Cornell, M.E., 1996. Uncertainties in risk analysis: six levels of treatment. Reliab. Eng. Syst. Saf. 54, 95–111. http://dx.doi.org/10.1016/S0951-8320(96)00067-1.

Perez, T., 2015. Ship seakeeping operability, motion control, and autonomy - a Bayesian perspective. In: 10th IFAC Conference on Manoeuvring and Control of Marine Craft. Elsevier, Copenhagen, pp. 217–222.

Perez, T., 2013. A Bayesian approach to seakeeping operability computations. In: Pacific 2013 International Maritime Conference: the Commercial, Maritime and Naval Defence Showcase for the Asia Pacific. Engineers Australia, Barton, ACT, pp. 572–581.

Perez, T., Clothier, R.A., Williams, B., 2013. Risk-management of UAS robust autonomy for integration into civil aviation safety frameworks. In: Cant, T. (Ed.), Australian System Safety Conference (ASSC 2013).

Perez, T., Williams, B., Lamberterie, P. de, 2012a. Evaluation of robust autonomy and implications on UAS certification and design. In: 28th International Congess of the Aeronautical Sciences.

Perez, T., Williams, B., Lamberterie, P. de, 2012b. Computational aspects of probabilistic assessment of UAS robust autonomy. In: 28th International Congess of the Aeronautical Sciences.

Peterson, M., 2009. An Introduction to Decision Theory. Cambridge University Press, New York.

Punt, A.E., Hilborn, R., 1997. Fisheries stock assessment and decision analysis: the Bayesian approach. Rev. Fish. Biol. Fish. 7, 35–63. http://dx.doi.org/10.1023/A:1018419207494.

Riesch, H., 2013. Levels of uncertainty. In: Roeser, S., Hillerbrand, R., Sandin, P., Peterson, M. (Eds.), Essentials of Risk Theory. Springer, pp. 29–56. http://dx.doi.org/10.1007/978-94-007-1433-5.

RTCA DO-344, 2013. Operational and Functional Requirements and Safety Objectives (OFRSO) for Unmanned Aircraft Systems (UAS) Standards, vol. 2.

SAE ARP 4754A, 2010. Guidelines for Development of Civil Aircraft and Systems.

SAE ARP 4761, 1996. Guidelines and Methiods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment.

SAE ARP 5150, 2013. Safety Assessment of Transport Airplanes in Commercial Service.

Singpurwalla, N.D., 2006. Reliability and Risk: a Bayesian Perspective. John Wiley & Sons Ltd, New York 2006.

Spiegelhalter, D.J., Riesch, H., 2011. Don't know, can't know: embracing deeper uncertainties when analysing risks. Philos. Trans. R. Soc. A Math. Phys. Eng. Sci. 369, 4730–4750. http://dx.doi.org/10.1098/rsta.2011.0163.

United States Nuclear Regulatory Commission, 1975. Reactor Safety Study. An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants. WASH-1400 (NUREG-75 / 014).

Wade, P.R., 2000. Bayesian methods in conservation biology. Conserv. Biol. 14.

Wieland, P., Lustosa, L.J., 2009. Modeling operational risks of the nuclear industry with Bayesian networks. In: International Nuclear Atlantic Conference - INAC 2009. Rio de Janerio.

Zio, E., Pedroni, N., 2013. Methods for Representing Uncertainty: A Literature Review. Foundation for an Industrial Safety Culture.

5. Managing Uncertainty in the System Safety Assessment of Unmanned Aircraft Systems

Figure 11: Concept image of an unmanned aircraft operation over Melbourne City, Australia
Image Copyright © Achim Washington

"If you are looking for perfect safety, you will do well to sit on the fence and watch the birds"

Wilbur Wright (1867-1912)

This chapter titled, "Managing Uncertainty in the System Safety Assessment of Unmanned Aircraft Systems" extends the framework developed in Chapter 4 to address certain additional uncertainties in the system safety process (Research Question 2.1 and Research Question 2.2). It demonstrates how certain types of model uncertainty, such as those arising from the assumption of a constant failure rate, can be accounted for in the assessment and compliance processes. This paper only focuses on the SSA process and how the variable failure rate can be incorporated into this model. It does not explore the impact of this modification on the remaining components of the SSPR compliance framework.

5.1. Statement of Authorship

The authors listed in Table 9 have certified* that:

1. They meet the criteria for authorship (refer to Appendix B: Definition of Authorship) in that they have participated in the conception, execution, or interpretation, of at least that part of the publication in their field of expertise;
2. They take public responsibility for their part of the publication, except for the responsible author who accepts overall responsibility for the publication;
3. There are no other authors of the publication according to these criteria;
4. Potential conflicts of interest have been disclosed to (a) granting bodies, (b) the editor or publisher of journals or other publications, and (c) the head of the responsible academic unit; and
5. They agree to the use of the publication in the student's thesis and its publication on the Australian Digital Thesis database consistent with any limitation set by publisher requirements.

Table 9: Statement of authorship – paper three

Title of Paper:	Managing Uncertainty in the System Safety Assessment of Unmanned Aircraft Systems			
Contributor	**Area of Contribution and percentage contribution to paper: ***			
	(i)	(ii)	(iii)	(iv)
	Conception and Design	Analysis and Interpretation	Drafting Sections	Critically Revising
Mr Achim Washington	90%	90%	90%	10%
Dr Reece Clothier	10%	10%	10%	50%
Mr Brendan Williams				10%
Dr Jose Silva				30%

Principal Supervisors confirmation

I have email or other correspondence from all co-authors confirming their certifying authorship

Dr Reece Clothier	25th August 2018
Name	**Date**
Dr Jose Silva	25th August 2018
Name	**Date**

** for further details refer to Appendix B: Definition of Authorship*

Managing Uncertainty in the System Safety Assessment of Unmanned Aircraft Systems

Achim Washington[a], Reece A. Clothier[a,b], Brendan P. Williams[b], Jose Silva[a]

s3270338@student.rmit.edu.au, reece.a.clothier@boeing.com, brendan.p.williams@boeing.com, jose.silva@rmit.edu.au

[a]School of Engineering, RMIT University, Melbourne, Australia

[b]Boeing Research & Technology – Australia, Brisbane, Australia

Abstract

There is much debate over the development of suitable system safety requirements for Unmanned Aircraft Systems (UAS). A particular point of contention is the approach for determining the allowable average probability per flight hour of failure conditions. For UAS, there is limited knowledge and data to inform the assessment of the average probability of failure conditions. This leads to uncertainty in the system safety assessment (SSA) process. Current literature provides no discussion as to how this uncertainty can be managed in the system safety certification (SSC) of a UAS. In addition to this, uncertainty in the average probability of failure conditions is not accounted for in compliance findings, which can result in subjective certification decision-making. This research proposes a new framework for system safety certification under conditions of uncertainty. The new framework is briefly introduced, with the focus of this paper being on the characterisation of uncertainty within the SSA process. A Bayesian approach to the modelling of the average probability of failure conditions is adopted. The traditional assumption of a constant failure rate model is challenged; with a Weibull distribution proposed as a more appropriate representation of UAS failure occurrence.

Keywords: Unmanned Aircraft Systems, System Safety Assessment, Airworthiness

Introduction

Unmanned Aircraft Systems (UAS) are the fastest growing sector of the aviation industry. However, as with any new technology, there is a considerable amount of risk and uncertainty associated with the operation of these systems. At present, the default stance taken by regulatory authorities the world over is to manage these risks through the imposition of a significant amount of restrictions on the operation of these systems [1]–[4]. Uncertainty, while mentioned is not taken into consideration by any of the regulatory bodies. And while this is implicitly recognised when dealing with manned aircraft operations, the same cannot be said for UAS operations. In order to ease these restrictions, it is of paramount importance to provide a greater degree of assurance in the airworthiness of these systems taking both the risks and uncertainties associated with them into consideration.

A central component of airworthiness regulations are system safety regulations. System safety regulations supplement prescriptive design requirements and are put in place to ensure that an aircraft or system is capable of continued safe flight and landing following a failure or multiple failures of systems [5]. The current method for assessing the system safety of civilian aviation systems [6], [7] does not comprehensively address uncertainty in the input data, models, and assessment processes. The model developed in [8] addresses some of these shortcomings by providing a means of incorporating uncertainty in the system safety assessment and compliance finding process. The approach, however, assumes systems fail at a constant rate; a poor assumption for new and complex systems such as UAS. This paper builds on the approach presented in [8] through relaxing this assumption. The failure rate of the system is considered an uncertain parameter. Subsequently, the output of the system safety assessment process is no longer a point estimate of the failure rate of the system but a probability distribution representing the uncertainty inherent in the system.

System Safety Regulations

Part 1309 regulations are intended to supplement prescriptive standards on the design, manufacture, and installation of aircraft components. A complete description of the Part 1309 regulations can be found in [5], [9]–[13] and associated guidance material [14], [15]. Guidelines on the system safety assessment (SSA) process and accepted assessment tools and techniques can be found in [6], [10], [12], [16]. The primary focus of this paper is showing compliance to the system safety performance requirements (SSPR). The main objective for which is to demonstrate (through a documented qualitative or quantitative analysis) that the expected frequency of failure of equipment and systems, when considered separately and in relation to other systems, is inversely-related to the severity of its effect on the safe operation of the system.

System Safety Assessment Process

The current SSA process can be carried out at the component, sub system and system level and requires the component reliability data, concept of operations and system baseline description as input. Output from this process is a set *F*, which contains a description of the various ways the component, system or sub system can fail; the associated set *C* describing the assigned failure severity categories for each failure condition identified in *F*; and the set *Λ*, which contains the estimate of the Average Probability of failure per Flight Hour (APFH) of these failure conditions being realised. The APFH estimates are then compared to a set of failure probability objectives (*O*) to determine if the system is compliant or not with the SSPR. The net output from the SSA process are thus the four related sets: *F, C, Λ* and *O*. The index variable *n* can be used to reference the assessment for each identified failure mode; describing the tuple given in Eqn 1. Further details on the system SSA process and the tools used in performing an assessment are provided in [6], [16].

The focus of this paper is on the uncertainty associated with the estimates of the failure rate (APFH). The APFH is assessed on qualitative or quantitative “failure probability scales” defined in Part 1309 regulations for each category of failure condition in *F*. The qualitative description can include extremely improbable, extremely remote, remote (or improbable), probable or frequent and the quantitative description ranges from an APFH of 10^{-9} per hour to 10^{-0} per hour. Example failure probability scales are summarised in [8]. Estimates of the APFH can be determined through a combination of data from testing, modelling and simulation, expert judgement, and structured analysis techniques as detailed in [6]. The output of the assessment is the specification of the set *Λ* as given in Eqn 2. *Λ* comprises *N* assessed point estimates of the APFHs; one associated with each of the failure conditions defined in *F*.

$$< f_n, c_n, \lambda_n, o_n > \qquad where \quad n \in Q; \tag{1}$$

$$\Lambda \quad = \quad \{\lambda_n : n \in Q\} \tag{2}$$

Incorporating Variable Failure Rates into System Safety Assessment

The current SSPR assessment process does not comprehensively account for uncertainty associated in the assessments of the APFH. The approach proposed in [8] recognises this shortcoming and provides an objective, transparent and rational means to show compliance with the SSPR in those cases where there is uncertainty in the SSA process. A Bayesian approach is adopted that facilitates a more comprehensive treatment of the uncertainties inherent to all SSA. Following SSA guidance material, the approach described in [8] assumes that the failure rate of the system is constant. This paper explores the impact of substituting the constant failure rate assumption with variable failure rates.

Failure Rate Modelling

A “bathtub curve” is typically used to model the failure rate of a system (or population of systems). It is divided into three main phases, the “Infant Mortality” phase, the “Useful Life” phase and the “Wear-out” phase, each of which are associated with a different failure rate [17]. A typical distribution used in the industry to model this is a Weibull distribution. A Weibull distribution is a general two-parameter distribution. By adjusting the scale parameter α and the shape parameter υ a variety of shapes can be obtained to fit experimental data [18]. The Weibull distribution can be used to represent each of the phases of the “bathtub” curve by varying υ. The “Infant Mortality” phase represents the initial phase of the lifecycle of the family of systems and has $\upsilon < 1$. The failure rate of the family of systems is reducing during this period. It encompasses the latent design faults and errors inherent in the design, production, and operation of any new system. These “failures” tend to be identified and addressed with increasing operational experience of the system, leading to a reduction in the failure rate with accumulated operational time. The second phase, the “Useful Life” phase, represents the plateau in these safety improvement measures. The family of systems in the Useful Life phase is generally said to exhibit a constant failure rate corresponding to the random failures that occur during the life of a system. This phase can be modelled using the Weibull function with $\upsilon = 1$. The final phase, the “Wear-out” phase, is associated with the increasing failure rate of the family of systems, which can come with, for example, aging systems. The Wear-out phase can be modelled using the Weibull distribution with values of $\upsilon > 1$.

UAS Failure Rates

Existing SSA guidance material assume mature aircraft systems exhibiting stable failure rates (*i.e.*, in its Useful Life phase). This may not be an appropriate assumption for UAS, particularly small commercial UAS, due to the rapid pace of technology development and the use of Commercial-off-the-shelf (COTS) components, which create a constantly changing system baseline. This in turn means it is difficult to build heritage in a particular configuration of a system. Components are not designed or manufactured to accepted standards. Further, many small UAS are not subject to routine maintenance. The rapid evolution of technology may mean that many UAS types may never achieve a constant failure rate. On this basis, this paper assumes the failure rate of UAS follows a Weibull distribution.

Accounting for Uncertainty in UAS Failure Rates

In [8], uncertainty (or the degree of belief) in the estimates of the APFH is captured through the use of conditional probability distributions, denoted $p(\lambda_n|D,I)$. Where, λ_n is an estimate of the APFH for a particular failure condition f_n. $p(\lambda_n|D,I)$ is determined through the use of Bayes’ equation (as given in Eqn 3) taking into consideratoin all of the available data, D, and knowledge and information, I. The posterior distribution, $p(\lambda_n|D,I)$ is the distribution describing the uncertainty in the parameter of interest (λ_n) based on our prior state of knowledge and any new evidence provided by D. $p(\lambda_n|I)$ describes the uncertainty in our current knowledge; the model parameter λ_n (epistemic uncertainty), based on all previous available information, I. $p(D|\lambda_n,I)$ is a distribution representing the likelihood of observing D and represents the aleatory uncertainty in the modelled system. $P(D|I)$ is a constant and serves as a normalisation factor. For more details on each of these components, the reader is directed to [8]. It is important to note that the output from the SSA is no longer a point estimate of λ_n but distributions representing our uncertainty in λ_n.

$$p(\lambda_n|D,I) \quad = \quad \frac{p(D|\lambda_n,I) \times p(\lambda_n|I)}{P(D|I)} \qquad 3$$

Accounting for Uncertainty in Non-constant UAS Failure Rates

As discussed, it is assumed the likelihood distribution can be modelled using the Weibull distribution given in Eqn 4.

$$p(D|\tau,\nu,I) = \nu\tau D^{\nu-1}\, exp\,[-\tau D^{\nu}] \qquad 4$$

Where, *p(D|τ,υ,I)* is the likelihood distribution, *D* is the observed time period or time to failure (positive rational number), *τ* is the scale parameter[1] (positive rational number) and υ is the shape parameter (positive rational number), and *I* is the information known prior to *D*. The Weibull distribution represents the mean time to failure (MTTF) of the system. The failure rate of the system for varying time periods can be calculated from the parameters *τ* and *v* using the hazard function provided in Eqn 5.

$$\boldsymbol{\lambda(t) = \nu\tau t^{\nu-1}} \qquad 5$$

Where λ(t) represents the varying failure rate of the system and τ and υ are the scale and shape parameters of the posterior distribution respectively. The choice of priors can be broadly classified into two distinct categories, informative priors and non-informative priors. Informative priors contain substantive information about the possible values of the unknown parameter (*i.e., τ, v*), while non-informative priors are intended to let the data dominate the posterior distribution [19]. While data on the failure rate is known from historical data, a distribution of the scale and shape parameters for the systems operations is not readily available for the case study example. Taking this into consideration a non-informative prior, in the form of a gamma distribution was selected as the prior distributions for both the shape and scale parameter. A gamma distribution is ideal for those events that occur in a purely random fashion [20], and being non-informative, it allows the data dominate the posterior distribution [19]. The general form of the equation is presented in Eqn 6. Where *A* can be substituted with *τ* and *υ* to represent the scale and shape parameters for the Weibull distribution that are to be evaluated and *a* and *b* are respectively the scale and rate parameters of the gamma distribution (both set to 0.0001, to serve as a non-informative prior).

$$p(A|I) = \frac{b^a}{\Gamma(a)}\, A^{a-1}\, e^{-bA} \qquad 6$$

The marginal probability, *P(D|I)*, is obtained by integrating the numerator of Eqn 3 over all the possible values of τ and υ. The posterior distribution is then calculated using Eqn 3. This can be done numerically for simpler models (through MATLAB) or through Markov Chain Monte-Carlo (MCMC) simulation (through OpenBUGS) for more complex examples such as that presented in this paper. The resulting posterior distributions, *p(τ|D,I*) and *p(υ|D,I*), represent our updated state of knowledge in the Weibull parameters *τ* and *υ*. This distribution can be used to make probabilistic inferences as to the value of *τ* and *υ* and, from that, inferences as to the APFH (through the use of the hazard function given in Eqn 5).

Case Study Application

In order to exemplify the features of the model a simple case study example based on the RQ-2 (Pioneer) UAS is presented. The Class A mishap data for the RQ-2 from 1986 to 2002 were taken from [21]. A Class A mishap is defined as those aircraft accidents resulting in loss of

[1] It is important to note here that the scale parameter is often defined using α and is equal to $\tau^{-1/\upsilon}$. The equations used here have been modified to take this into consideration.

the aircraft (in naval parlance "strike"), human life, or causing over $1,000,000 in damage [21]. A mishap can result from a range of technical, operational factors. For the purposes of this example, it is assumed that all of the recorded mishaps were the result of technical failures. The MTTF were calculated from the data using the equations given in [21]. It is assumed that all the mishaps presented were for non-repairable systems or components, thus making the MTTF equivalent to the Mean Time Between Failures (MTBF). Taking this into consideration the following MTTF (in hours) based on the failure rates for the 17 years of operation were observed: 11, 86, 124, 259, 122, 361, NA, NA, 174, 1752, 222,692, NA, 187, 423, 1091, NA. These represent the input data, *D*, in Eqn. 3 and 4.

As described in the previous section, $p(\tau|I)$ and $p(\upsilon|I)$ were modelled using uniformed Gamma priors. MCMC software was then used to determine the posterior distributions $p(\tau|D,I)$ and $p(\upsilon|D,I)$.

Results

The posterior distributions $p(\tau|D,I)$ and $p(\upsilon|D,I)$ output from the MCMC simulations are presented in Fig 1 and Fig 2. The mean and lower and upper limits of the 90% Credible Interval (CI) for both parameters were then calculated and presented in Table 1. The posterior distribution showing the MTTF for the RQ-2 UAS unconditional upon τ and υ is presented in *Fig 3*. This has a mean value of 488.5 hours with the lower and upper limit of the 90% CI being 13.2 hours and 1574 hours respectively. The failure rate of the system for varying time periods determined using Eqn 5 is presented in Fig 4. It is important to note that only the mean τ value of 0.0074 (corresponding to mean α of 192.4) has been used in Fig 4, Fig 5 and consequently the results presented in Table 2.

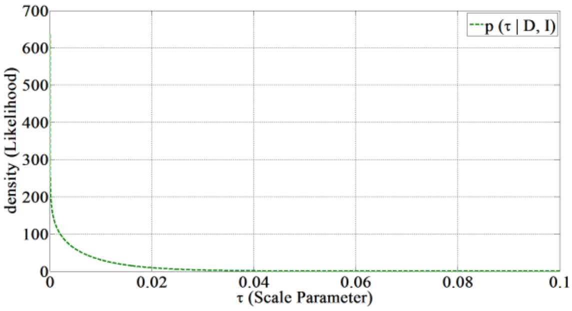


Fig 1: Posterior distribution for τ

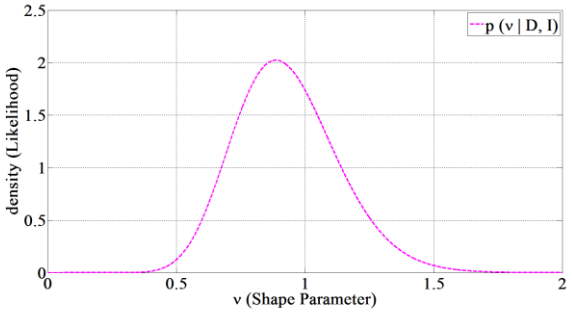


Fig 2: Posterior distribution for υ

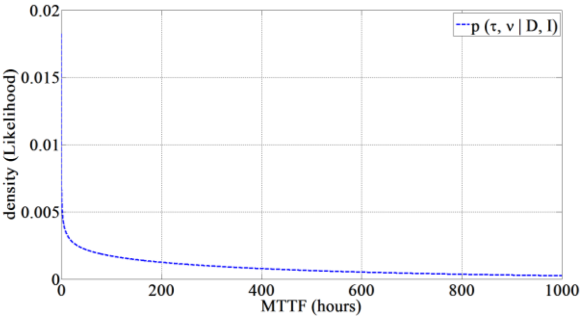


Fig 3: Posterior distribution for MTTF unconditional on τ and υ

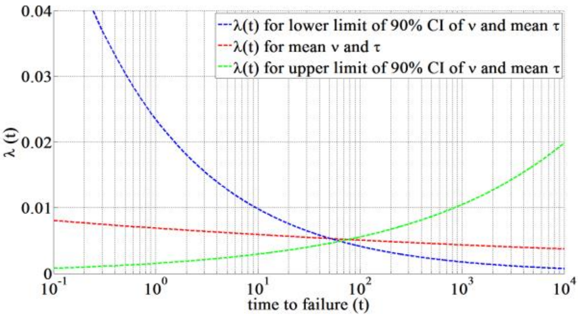


Fig 4: Failure rate distribution of the system for varying time periods

Table 1: Scale and Shape parameter for mean and 90% Credible Interval (CI)

	Scale (τ)	**Shape (υ)**
Lower limit of 90% CI	0.0003	0.6234
Mean	0.0074	0.9328
Upper limit of 90% CI	0.0266	1.2770

Using the mean τ value and the mean, lower, and upper limits of the 90% CI for υ, the reliability function can be plotted (Fig 5) using Eqn 7. The MTTF can be determined by integrating the reliability function. The failure rate can then be calculated by taking the inverse of the MTTF with the results presented in Table 2.

$$\boldsymbol{R(t) = exp\,[-\tau t^{\nu}]} \qquad 7$$

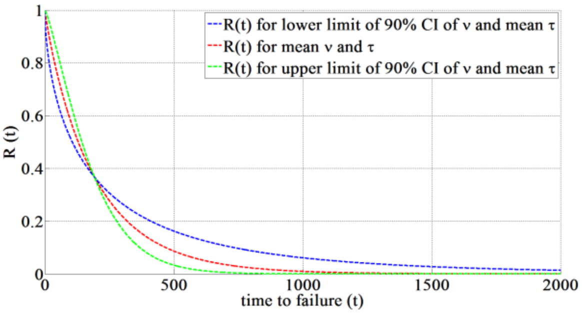


Fig 5: Reliability distribution for mean τ and varying υ values from 90% CI

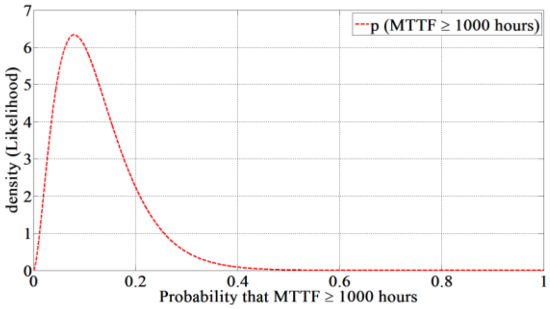


Fig 6: Probability that the mean time to failure is at least 1000 hours

Table 2: Outputs from System Safety Assessment Process

	MTTF (hours)	**Failure Rate (Failures/hour)**
Lower limit of 90% CI	278.29	0.0036
Mean	202.02	0.0050
Upper limit of 90% CI	180.99	0.0055

Uncertainty in the RQ-2 meeting System Safety Objectives

For the three MTTF obtained in Table 2 the probability of each MTTF for varying shape and scale parameters can be calculated from the reliability function presented in Eqn 7. This provides not only the probability that the MTTF is greater than or equal to a prescribed system safety objective (for illustrative purposes, a system safety objective of 1x10^{-3} flight hours is used) but also the uncertainty surrounding this information. One such example of this is provided in Fig 6. Here the probability that the MTTF is at least 1000 hours is provided. This corresponds to an APFH of no more than 10^{-3} failures/hour. The mean probability obtained from this is estimated to be 0.1251 with a 90% CI of (0.0319, 0.2692), indicating that we are 12.51% certain that the APFH of the system will satisfy the failure probability objective (FPO) of 10^{-3} failures per flight hour.

Discussion

There are a number of advantages to the incorporation of uncertainty into the SSA process. The approach provided allows for uncertainty to be taken into consideration into the compliance finding process rather than the traditional “point” assessments of APFH. Decision makers can also draw additional inferences on the predicted failure performance of the system that reflect the risk appetite of the regulator (*e.g.*, choosing to use the upper 90% CI values on the APFH as opposed to the mean value of the APFH).

The most significant advantage of the approach is that it provides decision makers with a measure of the uncertainty in the system meeting a given system safety failure probability objective as opposed to binary “pass / fail” comparison. In the case study, there was 0.1251 probability that the RQ-2 met the 10^{-3} per flight hour FPO. Confidence in this finding is reflected in the 90% CI defined about this value.

Additional information can be provided to the decision maker in relation to the uncertainty in the model. For example, in the case study provided, the posterior distribution of the shape parameter υ can be used to provide insight into the particular phase of the bathtub curb the RQ-2 fleet is in. A value of υ greater than one indicates an increasing failure rate (infant mortality phase), equal to one indicates a constant failure rate (useful life phase), and less than one indicates a reducing failure rate (wear-out phase). From Fig 2, the mean of the shape parameter is 0.9328[2], indicating that the RQ-2 fleet is still in the "infant mortality" phase but approaching the "useful life" phase. The area under the curve to the left of one in Fig 2, provides a measure of the degree of confidence that the failure rate is in fact reducing. From this we can see that, given the available data and prior knowledge, there is a probability of 0.657 that the RQ-2 failure rate is reducing or constant ($\upsilon \leq 1$). This means there is also 34.3% chance that the RQ-2 is in the wear-out phase ($\upsilon > 1$).

Forward inferences (predictions) on the future failure performance of the fleet can also be made as described in [22]. Further, if new mishap data becomes available, the existing analysis can be readily updated using Bayes' formula (Eqn. 3).

Conclusion

The general lack of data and experience in the operation of civil UAS gives rise to uncertainty in relation to their safety performance. This poses a particular problem when it comes to certifying UAS against airworthiness regulations, and in particular, system safety requirements. The existing system safety assessment process does not take uncertainty into consideration. The work presented in [8] provided a mathematical framework for incorporating uncertainty into this process. This work extends this framework through relaxing the modelling assumption that UAS exhibit constant failure rates. The case study highlights the power of the approach, with system safety decision makers measures of the probability of compliance. Additional inferences in relation to the model and the future performance of the system can also be made. Further work still needs to be undertaken to take other sources and types of uncertainty into consideration. In particular, how to represent uncertainty in the input mishap data and in the assignment of failure severity conditions.

References

[1] CAA, "CAP-722, Unmanned Aircraft System Operations in UK Airspace - Guidance," London UK Civil Aviation Authority (CAA), Department of Transport (DfT), London, UK, 2015.

[2] OSD, *Unmanned Systems Roadmap 2007-2032*. Office of Secretary of Defense, Washington D.C., USA, 2007.

[3] JAA/EUROCONTROL, "UAV Task-Force Final Report: A concept for European regulations for civil unmanned aerial vehicles (UAVs)," Brussels, Belgium, 2004.

[4] R. A. Clothier, J. L. Palmer, R. A. Walker, and N. L. Fulton, "Definition of an airworthiness certification framework for civil unmanned aircraft systems," *Saf. Sci.*, vol. 49, no. 6, pp. 871–885, 2011.

[5] JARUS Working Group 6, "Safety Assessment of Remotely Piloted Aircraft Systems," *AMC RPAS.1309*, no. 2, 2015.

[6] SAE ARP 4761, "Guidelines and Methiods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment." SAE International, 1996.

[7] SAE ARP 5150, "Safety Assessment of Transport Airplanes in Commercial Service," 2013.

[8] A. Washington, R. A. Clothier, and B. P. Williams, "A Bayesian Approach to System

[2] Measures other than the mean of the distribution could also be taken, for example, the upper limit of the 90% CI.

Safety Assessment and Compliance Assessment for Unmanned Aircraft Systems," 2017.

[9] EASA, "Policy for Unmanned Aerial Vehicle (UAV) certification," *Advance - Notice of Proposed Amendment (NPA)*, no. 16. 2005.

[10] NATO Standardization Agency (NSA), "STANAG 4671 (Edition 1) - Unmanned Aerial Vehicles Systems Airworthiness Requirments (USAR)," Brussels, Belgium, 2009.

[11] K. Hayhurst, J. Maddalon, and P. Miner, "Preliminary considerations for classifying hazards of unmanned aircraft systems," *Tech. Rep. NASA TM-2007-21439*, 2007.

[12] NATO Standardization Agency, *AEP-83, Light Unmanned Aircraft Systems Airworthiness Requirements*. 2014.

[13] RTCA DO-344, "Operational and Functional Requirements and Safety Objectives (OFRSO) for Unmanned Aircraft Systems (UAS) Standards, Volume 2," 2013.

[14] FAA, "Advisory Circular 23.1309-1E, System Safety Analysis and Assessment for Part 23 Airplanes.," 2011.

[15] FAA, "Advisory Circular 25.1309-1A, System Design and Analysis," 1988.

[16] SAE ARP 4754A, "Guidelines for Development of Civil Aircraft and Systems." SAE International, 2010.

[17] B. J. de O. M. Franco and L. C. S. Góes, "Managing the Reliability of Unmanned Aerial System," *20th Int. Congr. Mech. Eng.*, 2009.

[18] R. Ramakumar, *Engineering Reliability Fundamentals and Applications*. Oklahoma: Prentice Hall Engineering/Science/Mathematics, 1993.

[19] H. Dezfuli, D. Kelly, C. Smith, K. Vedros, and W. Galyean, "Bayesian Inference for NASA Probabilistic Risk and Reliability Analysis," *NASA/SP-2009-569*, 2009.

[20] V. T. Covello and M. W. Merkhofer, *Risk Assessment Methods, Approaches for Assessing Health and Environmental Risks*. New York: Springer Science + Business Media, 1993.

[21] Department of Defense, "Unmanned Aerial Vehicle Reliability Study," United States of America, 2003.

[22] W. M. Bolstad, *Introduction to Bayesian Statistics*, Second edi. Wiley, 2007.

6. Adoption of a Bayesian Belief Network for the System Safety Assessment of Remotely Piloted Aircraft Systems

Figure 12: Concept image of an unmanned aircraft operation over New York City Skyline
Image Copyright © Achim Washington

"Take calculated risks. This is quite different from being rash"

George S. Patton (1885 – 1945)

This chapter titled *"Adoption of a Bayesian Belief Network for the System Safety Assessment of Remotely Piloted Aircraft Systems"* extends the framework developed in Chapter 4 to address certain additional uncertainties in the system safety process, thus helping address Research Question 2.1 and Research Question 2.2. It develops a general template for high level classification of functions and failures which can be applied to any aircraft system. It also allows for the application of BBN as a valid approach for capturing uncertainty in the assessed compliance scenario. Instead of assessing single credible (often worst-case) scenarios, this allows for multiple assessments of compliance scenarios. It is the first to apply a BBN within an aviation regulatory System Safety "Part 1309" context. By showing how the risk and uncertainty measures obtained from the regulatory safety risk assessment process can be represented to the decision makers, the research also addresses elements of Research Question 1.3.

6.1. Statement of Authorship

The authors listed in Table 10 have certified* that:

1. They meet the criteria for authorship (refer to Appendix B: Definition of Authorship) in that they have participated in the conception, execution, or interpretation, of at least that part of the publication in their field of expertise;
2. They take public responsibility for their part of the publication, except for the responsible author who accepts overall responsibility for the publication;
3. There are no other authors of the publication according to these criteria;
4. Potential conflicts of interest have been disclosed to (a) granting bodies, (b) the editor or publisher of journals or other publications, and (c) the head of the responsible academic unit; and
5. They agree to the use of the publication in the student's thesis and its publication on the Australian Digital Thesis database consistent with any limitation set by publisher requirements.

Table 10: Statement of authorship – paper four

Title of Paper:	Adoption of a Bayesian Belief Network for the System Safety Assessment of Remotely Piloted Aircraft Systems

Contributor	**Area of contribution and percentage contribution to paper: ***			
	(i)	(ii)	(iii)	(iv)
	Conception and Design	Analysis and Interpretation	Drafting Sections	Critically Revising
Mr Achim Washington	85%	80%	85%	10%
Dr Reece Clothier	15%	10%	15%	40%
Dr Natasha Neogi		10%		20%
Dr Jose Silva				20%
Dr Kelly Hayhurst				5%
Mr Brendan Williams				5%

Principal Supervisors confirmation

I have email or other correspondence from all co-authors confirming their certifying authorship

Dr Reece Clothier	25th August 2018
Name	**Date**
Dr Jose Silva	25th August 2018
Name	**Date**

**for further details refer to Appendix B: Definition of Authorship*

Safety Science 118 (2019) 654–673

Contents lists available at ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/safety

Adoption of a Bayesian Belief Network for the System Safety Assessment of Remotely Piloted Aircraft Systems

Achim Washington[a,*], Reece Clothier[b], Natasha Neogi[c], Jose Silva[a], Kelly Hayhurst[c], Brendan Williams[b]

[a] School of Engineering, RMIT University, Melbourne, Australia
[b] Boeing Research & Technology – Australia, Brisbane, Australia
[c] NASA Langley Research Centre, VA, USA

ARTICLE INFO

Keywords:
Remotely Piloted Aircraft Systems
Bayesian Belief Networks
System Safety Regulations
Failure rate
Uncertainty

ABSTRACT

There can be significant uncertainty as to the safety of novel or complex aviation systems, such as Remotely Piloted Aircraft Systems (RPAS). Current aviation safety assessment and compliance processes do not adequately account for uncertainty. The aim of this research is to support more objective, transparent, systematic and consistent regulatory outcomes in relation to the safety assessment of such systems. The objective of this work is to provide a systematic means of accounting for the various uncertainties inherent to any System Safety Assessment (SSA) process. The paper first defines the system safety compliance process and its modification to account for uncertainty. The SSA process, its various outputs, and associated uncertainties are defined and then applied to a generic RPAS. A Bayesian Belief Network (BBN) is adopted that facilitates a more comprehensive treatment of the uncertainty in each of the outputs of a typical SSA process. A case study of a generic RPAS is used to illustrate the features of the new approach. The adoption of the *Proposed* SSA approach would allow for the high uncertainty associated with the safety assessment of novel or complex aviation systems, such as RPAS, to be taken into consideration. Such an approach would enable the risk-based regulation of the sector.

1. Introduction

A new set of airworthiness regulations for RPAS is emerging. It is now broadly recognised that this set of regulations should be tailored to different RPAS types and their Concepts of Operations (CONOPs), and that this tailoring should be governed by the associated safety risk. The European Aviation Safety Agency (EASA) has proposed a risk-based regulatory framework that divides RPAS into the three regulatory categories of *Open*, *Specific*, and *Certified* (EASA, 2016). RPAS in the *Specific* or *Certified* categories must demonstrate a minimum level of assurance in their airworthiness. For RPAS in the *Certified* category, this assurance is provided through compliance to a comprehensive code of airworthiness requirements.

A key component of airworthiness regulations are System Safety Regulations (SSR), also referred to as Part 1309 regulations (FAA, 1988, 2011). SSR supplement prescriptive standards on specific equipment or sub-systems, with the intent of ensuring the integrated system, across its spectrum of intended missions and operational environments, satisfies minimum safety objectives. The SSR describe a number of requirements; the most important to this work being the System Safety Performance Requirements (SSPR). They are considered to be “fundamental to the safety of UAS” but are also “an area of evolution and disagreement” (ADF, 2017). Discussion on the challenges to defining SSR for RPAS are presented in Clothier and Wu (2012), EUROCAE

Abbreviations: RPAS, Remotely Piloted Aircraft Systems (RPAS); SSA, System Safety Assessment; BBN, Bayesian Belief Networks; CONOPs, Concept of Operations; EASA, European Aviation Safety Agency; SSR, System Safety Regulations; COTS, Commercial Off The Shelf; SSPR, System Safety Performance Requirement; CA, Compliance Assessment; CF, Compliance Findings; FHA, Functional Hazard Assessment; ETA, Event Tree Analysis; FTA, Fault Tree Analysis; APFH, Average Probability of Failure per Flight Hour; FPOs, Failure Probability Objectives; FHA, Functional Hazard Assessment; ATSB, Australian Transport Safety Bureau; RPS, Remote Pilot Station; RPA, Remotely Piloted Aircraft; UDS, Unpremeditated Descent Scenario; LOC, Loss of Control; CFIT, Controlled Flight into Terrain; DOJC, Dropped or Jettisoned Components (DOJC); LOSS, Loss of Safe Separation; RP, Remote Pilot; NPT, Node Probability Table; KE, Kinetic Energy; FAA, Federal Aviation Administration; ADF, Australian Defence Force; NSA, NATO Standardization Agency; JARUS, Joint Authorities for Rulemaking of Unmanned Systems

* Corresponding author.

E-mail addresses: s3270338@student.rmit.edu.au (A. Washington), reece.a.clothier@boeing.com (R. Clothier), natasha.neogi@nasa.gov (N. Neogi), jose.silva@rmit.edu.au (J. Silva), kelly.hayhurst@nasa.gov (K. Hayhurst), brendan.p.williams@boeing.com (B. Williams).

https://doi.org/10.1016/j.ssci.2019.04.040
Received 16 August 2018; Received in revised form 12 March 2019; Accepted 27 April 2019

(2013), Washington et al. (2018). There are also challenges in how to ensure compliance with the SSR. In particular, managing the uncertainty in the SSA of RPAS is a challenge, which, in part, arises due to (Washington et al., 2017):

- limited operational data and experience;
- use of commercial off the shelf (COTS) components; and
- dynamic system configurations.

A more comprehensive means for treating and managing uncertainty in the SSA of RPAS is needed to ensure objective, transparent, systematic and consistent compliance findings against the SSR (Apostolakis, 1990; Paté-Cornell, 1996). A new system safety compliance process, based on the adoption of Bayesian methods, was proposed by Washington et al. (2017a, 2017b). Taking inspiration from Perez et al. (2012a, 2012b, 2013), Perez (2013), the new approach reframed the system safety compliance process as a problem of decision making under uncertainty, and showed how Bayesian analysis techniques and simple normative decision theory could be used to more comprehensively address uncertainty in the assessed failure rate of a system. The result was a risk-based process, which represented a paradigm shift in standard aviation processes.

The new process presented in Washington et al. (2017a, 2017b) addressed only the uncertainty in the assessed failure rate. Uncertainty in relation to the identification of the failure conditions was not taken into consideration. In addition to this, uncertainty in relation to the specification of the assessed failure scenario, in particular, the possible failure condition severity categories assigned to a failure condition, and in turn, compliance with multiple associated safety objectives, were not addressed. In *Traditional* SSAs this uncertainty is accounted for by assuming the "worst case" consequential outcome from a failure scenario (NSA, 2009), which can lead to the imposition of overly conservative safety objectives. This, in turn, results in additional costs in the design, production, testing, and certification of the system. Identified failure conditions are assessed and treated independently, with compliance only shown against the assigned "worst case" safety objective (NSA, 2009). As a result, overall compliance of the RPAS (as a whole) with its system-level safety objective is never shown. This assumption was also made in the models developed in Washington et al. (2017a, 2017b).

Building on the framework developed in Washington et al. (2017a, 2017b), this paper proposes the use of a BBN as a means for more comprehensively capturing the uncertainty in the SSA process. BBNs have been used in the past for a number of applications including environmental (e.g. Marcot et al., 2001; Cain, 2001; Uusitalo, 2007; Borsuk et al., 2004; Bromley et al., 2005), nuclear (e.g. Kang and Golay, 1999; Beaumont et al., 2015; Lee and Lee, 2006), space (e.g. Morris and Beling, 2001; Mengshoel et al., 2008; Guikema and Paté-Cornell, 2004), aviation (e.g. Ale et al., 2009; Luxhøj et al., 2003; Kardes and Luxhøj, 2005; Ancel and Shih, 2015; Ancel et al., 2015; Ministry of Transport and Water Management, 2009; Luxhøj and Coit, 2006; Luxhøj and Harrell, 2015) and even UAS (e.g. Luxhoj, 2016; Luxhøj et al., 2017; Luxhøj, 2015) applications. BBNs have also been previously applied to aviation safety assessments (*e.g.*, Ale et al., 2009, 2013; Ancel et al., 2017; Barr et al., 2017; Kevorkian, 2016; Kumar et al., 2014) but have not been previously integrated within the formal structure of the SSPR compliance process. The *Proposed* BBN SSA approach takes into consideration the uncertainty in the consequential outcomes assigned to a set of identified failure conditions, removing the need for "worst case" assumptions. System safety compliance assessments can also be made at different levels of abstraction of the system (*i.e.*, from an individual failure condition through to a set of all identified failure conditions, representative of the overall system), providing a means of assessing the compliance of the overall system with its top-level safety objectives.

The body of this paper is structured as follows. A brief introduction to SSR and the modelling of the SSPR compliance process is provided in Section 2, with the various sources of uncertainty and their representation within the SSPR compliance process presented in Section 2.2. The general approach is applied to a generic RPAS in Section 3. The SSA of a generic RPAS using a BBN is described in Section 4. Following this, a case-study is used to illustrate various aspects of the new approach in Section 5, with discussion and areas for future research presented in Section 6.

2. System Safety Regulations

SSR supplement prescriptive standards on specific equipment or sub-systems, with the intent of ensuring the integrated system, across its spectrum of intended missions and operational environments, satisfies minimum safety objectives. System safety "Part 1309" regulations can be found in NSA (2009), JARUS (2015), EASA (2005), Hayhurst et al. (2007), NATO (2014), RTCA Special Committee (2013), and further information is contained in associated guidance material (FAA, 1988, 2011). Guidelines on the SSA process and accepted assessment tools and techniques can be found in NSA (2009), NATO (2014), SAE (1996, 2010). At a high level, SSR include requirements for (Clothier and Wu, 2012):

1. A documented analysis showing that equipment and systems perform as intended under foreseeable operating and environmental conditions;
2. The adoption of principles from fail-safe and fault-tolerant design (FAA, 1988); and
3. The demonstration (through a documented qualitative or quantitative analysis) that the expected frequency of failure of equipment and systems, when considered separately and in relation to other systems, is inversely-related to the severity of its effect on the safe operation of the system. This is commonly referred to as the System Safety Performance Requirement (SSPR).

The focus of this paper is on the assessments and compliance findings against the SSPR.

2.1. SSPR Compliance Process

The SSPR defines the minimum acceptable level of reliability of aviation equipment and components (Clothier and Wu, 2012). It comprises the three sub-processes of: (1) System Safety Assessment (SSA), (2) Compliance Assessment (CA), and (3) Compliance Finding (CF), as illustrated in Fig. 1. The scope of this paper is restricted to the SSA and CA sub-processes. The CF sub-process is not further discussed (refer to Washington et al. (2017)).

2.1.1. System Safety Assessment Process

The SSA process involves the use of a variety of tools (*e.g.*, Functional Hazard Assessment (FHA), Failure Mode, Effects and Criticality Analysis (FMECA), Event Tree Analysis (ETA) and Fault Trees Analysis (FTA), *etc.*), data, and expert judgment to determine: (1) the various ways in which a system or sub-system can fail (referred to as failure conditions); (2) the potential consequential impacts of these failure conditions on the safety of the aircraft (referred to as failure condition severity categories); (3) the Average Probability per Flight Hour (APFH) of these failure conditions occurring, and (4) the maximum permissible APFH (referred to as Failure Probability Objectives (FPOs)). These outputs are illustrated in Fig. 2. The set notations described in Eq. (1) through to Eq. (10) are based on Washington et al. (2017) but reiterated here for the sake of completeness.

The first output is the set F containing descriptions f_n of the N identified failure conditions, as given in Eq. (1), where Q is an integer set used to index the various outputs from the SSA process, as shown in Eq. (2).

$$F = \{f_n : n \in Q\} \tag{1}$$

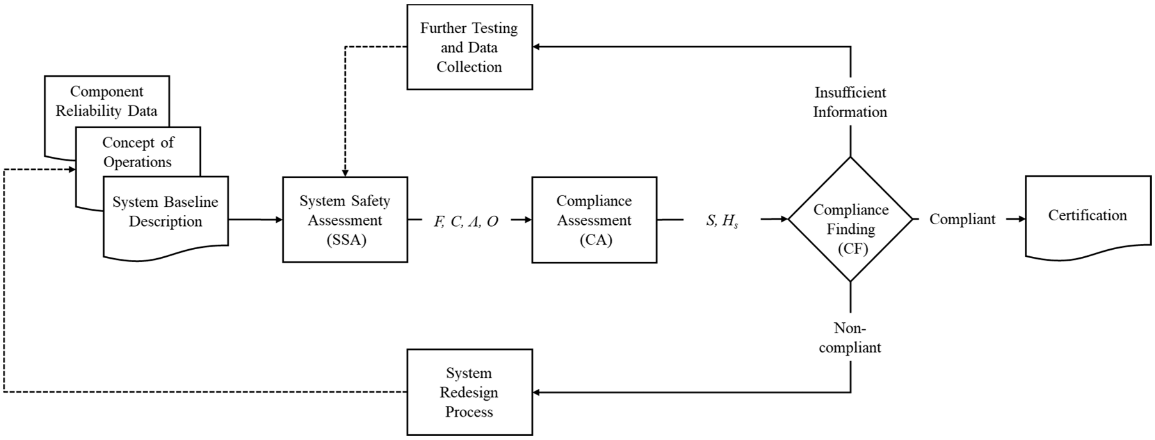

Further Testing and Data Collection
Component Reliability Data
Concept of Operations
System Baseline Description
System Safety Assessment (SSA)
F, C, Λ, O
Compliance Assessment (CA)
S, H_s
Insufficient Information
Compliance Finding (CF)
Compliant
Certification
Non-compliant
System Redesign Process

Fig. 1. Overview of Traditional SSPR compliance process (adapted from Washington et al. (2017)).

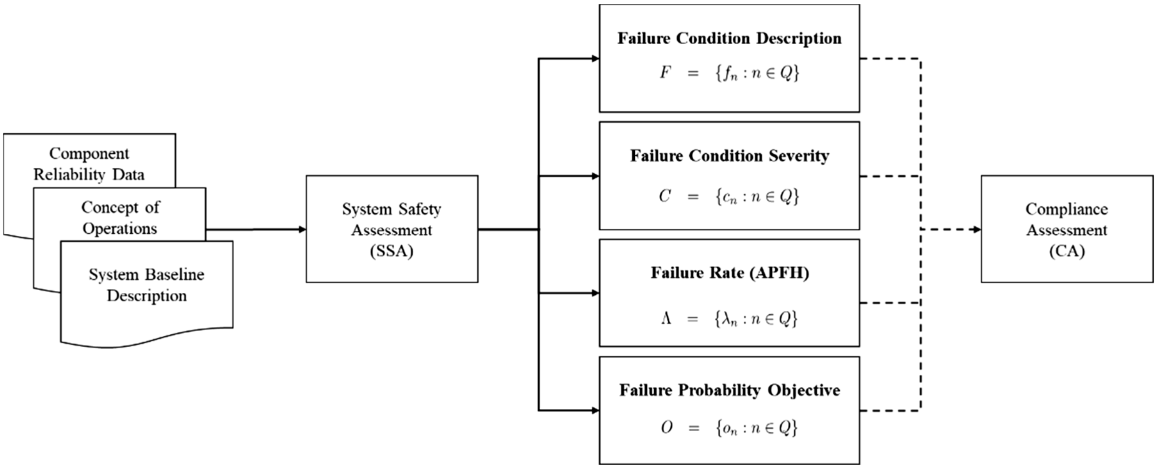

Component Reliability Data
Concept of Operations
System Baseline Description
System Safety Assessment (SSA)
Failure Condition Description
F = {f_n : n ∈ Q}
Failure Condition Severity
C = {c_n : n ∈ Q}
Failure Rate (APFH)
Λ = {λ_n : n ∈ Q}
Failure Probability Objective
O = {o_n : n ∈ Q}
Compliance Assessment (CA)

Fig. 2. Principal outputs of a Traditional SSA process.

$$Q = \{n | n \in \mathbb{Z}^+, n \le N\} \tag{2}$$

Associated with the set *F* are the sets *C, Λ,* and *O* as given in Eqs. (3)–(5). The set *C* contains the failure condition severities assigned to each failure condition identified in *F*. Typically a FMECA is used to determine the failure condition severity c_n assigned to a given failure condition f_n. Various scales that are used in the assessment of the failure condition severity are summarised in Table 3 in the Appendix.

$$C = \{c_n: n \in Q\} \tag{3}$$

A qualitative or quantitative estimate of the APFH for each failure condition is then determined through a combination of data from testing, modelling and simulation, expert judgement, and structured analysis techniques (as detailed in SAE (1996)). The APFH is defined as "the probability of occurrence, normalised by the flight time of a failure condition during a single flight[1]" (FAA, 2011). Fig. 15 in the Appendix, summarises different scales used in the assessment of the APFH. The output is the set *Λ*, comprising *N* assessed APFHs; one associated with each of the failure conditions in *F*, as given in Eq. (4).

$$\Lambda = \{\lambda_n: n \in Q\} \tag{4}$$

The final output from the SSA process is the set *O,* which contains *N* FPOs, one for each identified failure condition in *F*. The FPO specifies the maximum APFH permissible for a given failure condition. The specific FPO to be assigned to the failure conditions of different failure condition severity levels is defined in the SSR. Example descriptions of FPOs can be found in EASA (2015a). An illustration of the assignment of FPOs can be found in Fig. 16 in the Appendix. Traditionally, a single FPO, o_n, is assigned to each failure condition, f_n, in accordance with the SSR, with the resulting set of *N* FPOs contained in *O*, as given in Eq. (5).

$$O = \{o_n: n \in Q\} \tag{5}$$

The index variable *n* can be used to reference the output of the SSA for each identified failure condition; describing the tuple:

$$<f_n, c_n, \lambda_n, o_n> \ where\ n \in Q \tag{6}$$

For further details on the SSA process and tools used in performing the assessment refer to SAE (1996, 2010).

2.1.2. Compliance Assessment Process

As illustrated in Figs. 1 and 2 the outputs of the SSA process are input to a CA process, with each tuple (Eq. (6)) representing an independent compliance assessment. In a *Traditional* SSPR compliance process the CA process follows a simple deterministic binary "pass or fail" process. The state of the compliance for the n^{th} identified failure condition, H_n, is determined to be *True* when the assessed APFH, λ_n, is shown to be less than the applicable FPO, o_n, as shown in Eq. (7).

$$H_n = \begin{cases} True & if\ |\lambda_n| \le o_n \\ False & \text{otherwise} \end{cases} \tag{7}$$

This CA process is undertaken for all *N* failure conditions in *F* with the output state of compliance for each of the *N* failure conditions, f_n, summarised in the set *S,* given in Eq. (8).

[1] By definition, the APFH is not a probability but the expected frequency of occurrence per hour.

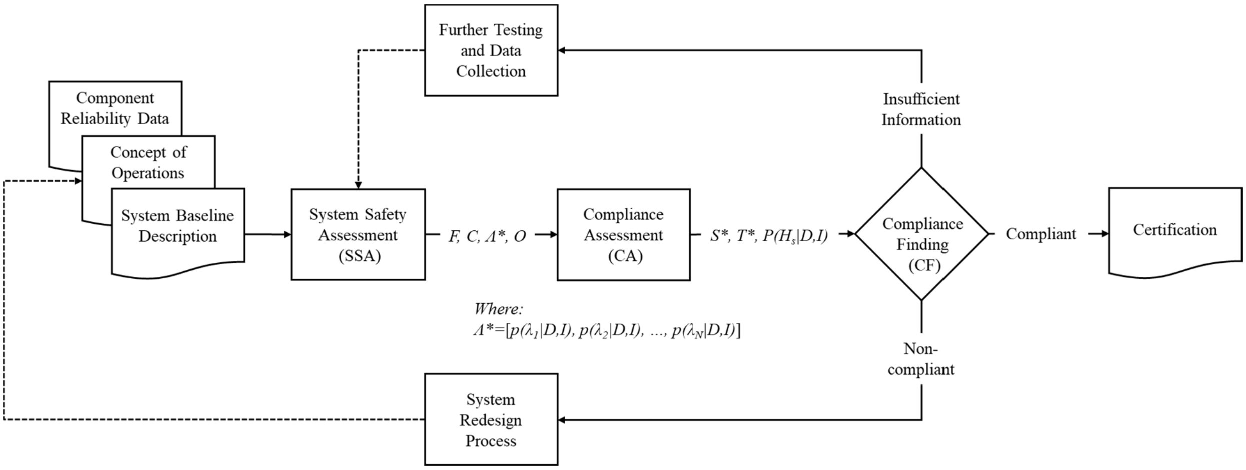

Further Testing and Data Collection
Component Reliability Data
Concept of Operations
System Baseline Description
System Safety Assessment (SSA)
F, C, Λ*, O
Compliance Assessment (CA)
S*, T*, P(H_s|D,I)
Insufficient Information
Compliance Finding (CF)
Compliant
Certification
Non-compliant
System Redesign Process
Where:
Λ*=[p(λ_1|D,I), p(λ_2|D,I), ..., p(λ_N|D,I)]

Fig. 3. Extended SSPR compliance process (adapted from Washington et al. (2017)).

$$S = \{H_n\colon n \in Q\} \tag{8}$$

The overall state of compliance of the system, H_s, is determined to be *True,* if it can be shown that all the assessed APFH satisfy their applicable FPO, as shown in Eq. (9).

$$H_S = \begin{cases} True & if \quad H_n = True \quad \forall \ n \in Q \\ False & otherwise \end{cases} \tag{9}$$

2.2. Accounting for Uncertainty in the SSA Process

Washington et al. (2017a) explore how the *Traditional* SSPR compliance process (as described in the previous sub-section) can be modified to better account for uncertainties inherent to the SSA process. They identify how uncertainty arising from a lack of knowledge and data on a system can manifest in relation to each of the outputs from the SSA process, specifically:

1. ***F*** – Whether all failure conditions have been correctly identified, and whether each identified failure condition, f_n, is correctly specified in terms of its operational failure modes and its effects;
2. ***C*** – Uncertainty in relation to the estimate of the magnitude of consequential effects and in turn, whether the correct failure condition severity category, c_n, is assigned to a particular failure condition f_n;
3. ***Λ*** – Uncertainty in relation to the estimate of λ_n for each failure condition f_n;
4. ***O*** – Whether the correct o_n is selected for each identified failure condition f_n.

2.2.1. Accounting for Uncertainty in the SSA Process (Extended Framework)

Washington et al. (2017a, 2017b) then went on to show how the uncertainty in relation to the quantitative assessments contained in the set Λ can be represented, proposing the *Extended* SSPR compliance process shown in Fig. 3.

A Bayesian approach was used to represent uncertainty in the assessments of λ_n. The resulting output being a set, Λ^*, of N conditional probability distributions describing the uncertainty (or degree of belief) in λ_n; one associated with each failure condition in F. The modified SSA output Λ^* is given in Eq. (10), where D represents the available failure data, and I represents the available knowledge and information. The remaining outputs from the SSA process, namely, F, C and O remained the same.

$$\Lambda^* = \{p(\lambda|\ D,\ I)_n\colon n \in Q\} \tag{10}$$

Washington et al. (2017) then went on to show how the updated output from the SSA process can be used within the CA and CF processes to support more objective, transparent, systematic and consistent SSPR compliance findings under uncertainty. This *Extended* framework was later modified to take into consideration variable failure rates (Washington et al., 2017).

2.2.2. Accounting for Uncertainty in the SSA Process (Proposed Framework)

A given failure can have multiple operational failure modes, and in turn, potential consequential impacts in relation to the safety of an RPAS operation (*i.e.*, there can be more than one applicable failure condition severity assigned to an identified failure condition). There can be considerable uncertainty in the specification of the scenarios for which an APFH needs to be assessed. The *Traditional* SSA approach does not account for this uncertainty, with guidance stating that "worst case" assumptions should be used to identify the single failure scenario for assessment (NSA, 2009). This can lead to the imposition of overly conservative safety objectives. This, in turn, results in additional costs in the design, production, testing, and certification of the system. Identified failure conditions are assessed independently. The potential for multiple consequential outcomes, and the dependencies between assessments for such outcomes, are not addressed. A new structure is needed, one which facilitates consideration for uncertainty in the modelling of the specification of the assessment scenario; and one which provides a means of assessing the compliance of the overall system with its top-level safety objectives.

The *Extended* SSA structure presented in Washington et al. (2017a, 2017b) can be further modified to facilitate consideration of the uncertainty in the specification of the scenario for assessment (*i.e.*, uncertainty in the specification of the remaining sets F, C, and O). The proposed structure showing the primary outputs from the SSA process is illustrated in Fig. 4. This framework provides a means of assessing the compliance of the overall system with its top-level safety objectives.

As can be seen in Fig. 4, the output of the *Proposed* SSA process is still a tuple of related sets as given in Eq. (11). The description of each of the elements in the tuple are however updated.

$$<F^{**},\ C^{**},\ \Lambda^{**},\ O^{**}> \tag{11}$$

The *Traditional* SSA had a failure condition severity (c_n), APFH (λ_n) and FPO (o_n) associated with each identified failure condition (f_n), as shown in Eq. (6). The *Extended* framework had a similar relationship, with the APFH (λ_n) being replaced with a probability distribution describing the uncertainty in the APFH ($p(\lambda|D,I)_n$). In the *Proposed* framework, the SSA process is being conducted at the system level, taking the dependencies between different failure conditions into consideration. Under the *Proposed* framework, the updated sets C^{**}, Λ^{**} and O^{**}

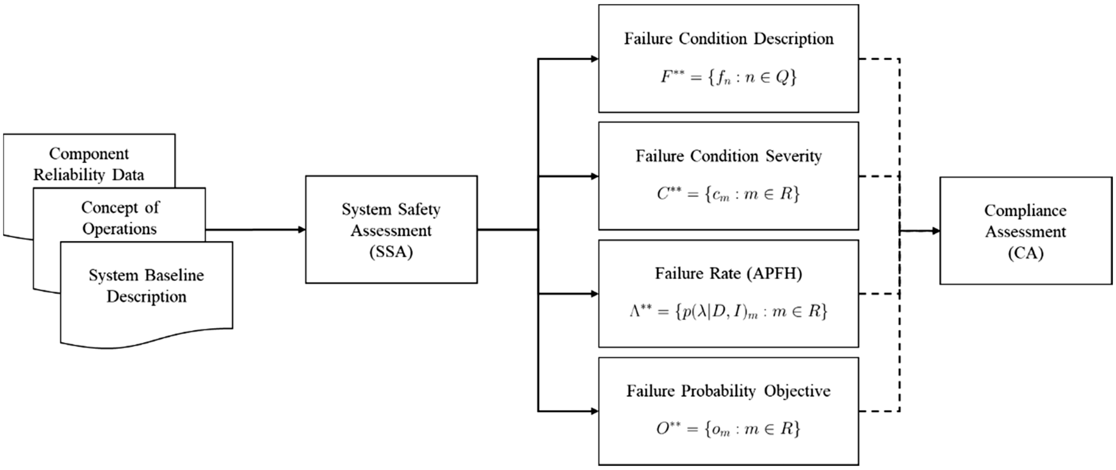

Component Reliability Data
Concept of Operations
System Baseline Description
System Safety Assessment (SSA)
Failure Condition Description
$F^{**} = \{f_n : n \in Q\}$
Failure Condition Severity
$C^{**} = \{c_m : m \in R\}$
Failure Rate (APFH)
$\Lambda^{**} = \{p(\lambda|D,I)_m : m \in R\}$
Failure Probability Objective
$O^{**} = \{o_m : m \in R\}$
Compliance Assessment (CA)

Fig. 4. Proposed SSA framework showing primary outputs from the model.

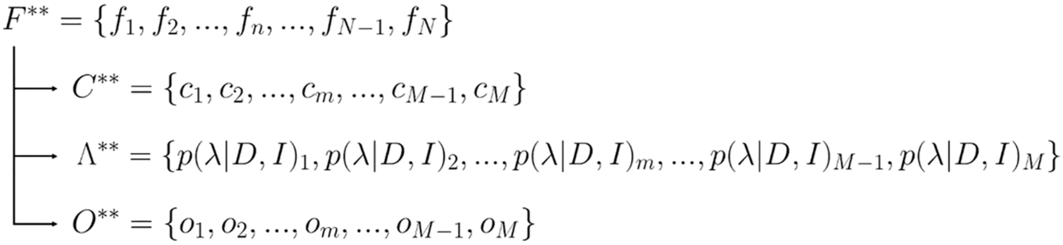

$F^{**} = \{f_1, f_2, \dots, f_n, \dots, f_{N-1}, f_N\}$
$C^{**} = \{c_1, c_2, \dots, c_m, \dots, c_{M-1}, c_M\}$
$\Lambda^{**} = \{p(\lambda|D,I)_1, p(\lambda|D,I)_2, \dots, p(\lambda|D,I)_m, \dots, p(\lambda|D,I)_{M-1}, p(\lambda|D,I)_M\}$
$O^{**} = \{o_1, o_2, \dots, o_m, \dots, o_{M-1}, o_M\}$

Fig. 5. Relationship between defined sets F^{**}, C^{**}, Λ^{**} and O^{**}

are now related to the set of failure conditions, F^{**}, and not a single failure condition. The relationship between the sets described in the tuple is depicted graphically in Fig. 5.

The set of failure conditions F^{**} is described using Eq. (12). The uncertainty in the failure conditions is taken into consideration by accounting for the potential for multiple outcomes (multiple operational failure modes) from a failure in a given system function and the dependencies between assessments for such outcomes.

$$F^{**} = \{f_n : n \in Q\} \tag{12}$$

While this is equivalent to Eq. (1), each of the elements (f_n) are now more clearly described by the relationship between a given system function (u_x) and operational failure mode (v_y), Eq. (13).

$$u_x \overset{f_n}{\rightarrow} v_y \tag{13}$$

The original output set C given in Eq. (3) is modified to be a set, C^{**}, given in Eq. (14). Where m is the index to one of the M unique failure condition severity categories associated with the given set of failure conditions, F^{**}, as defined in Eq. (15).

$$C^{**} = \{c_m : m \in R\} \tag{14}$$

$$R = \{m|\ m \in \mathbb{Z}^+,\ for \quad m = 1, 2, \cdots, M\} \tag{15}$$

Following this, assessments of the uncertainty in the APFH for each of the M potential failure condition severities associated with the set F^{**} is needed. The process used to estimate the APFH and the uncertainty associated with it is detailed in Section 4. The set described in Eq. (10) was updated to take this into consideration. The set Λ^{**}, Eq. (16) is a set of M conditional probability distributions describing the uncertainty (or degree of belief) in each λ_m.

$$\Lambda^{**} = \{p(\lambda|\ D, I)_m : m \in R\} \tag{16}$$

Associated with each assessed failure condition severity, c_m, is the relevant FPO assigned in accordance with the relevant Part 1309 regulation. The output set O is now modified to be a set, O^{**}, as given in Eq. (17), representing the set of FPOs relevant to a specific set of failure conditions F^{**}.

$$O^{**} = \{o_m : m \in R\} \tag{17}$$

In summary, the proposed mathematical specifications of the outputs of the SSA allow each identified set of failure conditions F^{**} to be assessed against all of its potential relevant FPOs and no longer just the FPO corresponding to the “worst case” (and potentially least likely) failure condition severity category. The practical application of the *Proposed* framework to a generic RPAS is described in the next section.

The *Proposed* framework enables consideration of the uncertainty in the specification of F, C, and O. Specifically, for a given set failure conditions, F^{**} containing N failure conditions, there can now be a set of M possible failure condition severity categories, C^{**}, reflecting the uncertainty in the exact consequential outcome. Associated with each potential failure condition severity category, c_m is a corresponding FPO, o_m and assessments of the uncertainty in the APFH, $p(\lambda|D,I)_m$. The overall *Proposed* SSPR compliance framework can be seen in Fig. 6.

It is important to note that, the set descriptions provided in this subsection for F^{**}, C^{**}, Λ^{**} and O^{**} and the relationship between them (Fig. 5) is for a system level assessment (e.g. for an RPAS). This allows the overall compliance of the system (e.g. RPAS) as a whole to be shown with respect to its system-level safety objectives, something lacking from the *Traditional* and *Extended* frameworks. If an assessment is to be undertaken for each system function or each failure condition independently, then an updated description for the sets can be provided.

3. Application of Framework to Generic Remotely Piloted Aircraft Systems

3.1. Specification of the Set of Failure Conditions (F^{**})

A Functional Hazard Assessment (FHA) and high-level FMECA are common techniques used in an SSA process to determine a system level set of failure conditions. Input to these techniques are a system-level

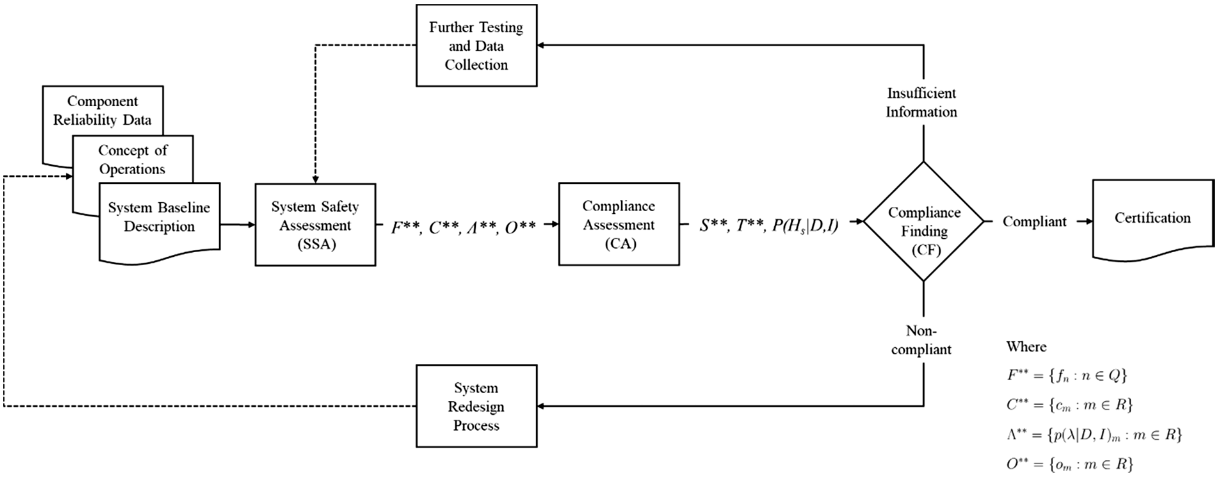

Further Testing and Data Collection
Component Reliability Data
Concept of Operations
System Baseline Description
System Safety Assessment (SSA)
F^{**}, C^{**}, Λ^{**}, O^{**}
Compliance Assessment (CA)
S^{**}, T^{**}, $P(H_s|D,I)$
Insufficient Information
Compliance Finding (CF)
Compliant
Certification
Non-compliant
System Redesign Process
Where
$F^{**} = \{f_n : n \in Q\}$
$C^{**} = \{c_m : m \in R\}$
$\Lambda^{**} = \{p(\lambda|D,I)_m : m \in R\}$
$O^{**} = \{o_m : m \in R\}$

Fig. 6. Proposed SSPR compliance process.

functional decomposition of a generic RPAS and the identification of a set of operational failure modes.

3.1.1. *Specification of System-Level Functions for a Generic RPAS*

A set of top-level operational system functions need to be defined for a generic RPAS. Arriving at a set of generic system functions requires a proper understanding of the workings of an RPAS and all the systems necessary to achieve the four core functions of any aviation system, namely, to aviate, navigate, communicate and mitigate (Hayhurst et al., 2007). The functional decomposition proposed herein is based on a review and consolidation of existing system functional breakdowns proposed in the literature (Hayhurst et al., 2007; Burke, 2010; RTCA, 2007). The resulting eight top-level system functions identified were:

1. **Structure –** The provision, at a minimum, of a level of structural integrity necessary to maintain controlled flight and continued functionality of the system across a defined envelope of operational conditions;
2. **Propulsion –** The provision, at a minimum, of a sufficient amount of thrust to maintain controlled flight;
3. **Power –** The provision, at a minimum, of a sufficient amount of electrical energy to support systems necessary for continued flight. This includes the provision of power to off-board components of the RPAS (*e.g.*, Remote Pilot Station (RPS), communication repeaters, *etc*.);
4. **Control –** The ability to determine and execute changes necessary to achieve or maintain a desired Remotely Piloted Aircraft (RPA) state (e.g., position, attitude, and airspeed) within minimum requirements;
5. **Guidance –** The generation of a trajectory, plan, or sequence of changes to the current system state necessary to meet mission objectives under constraints (*e.g.*, system performance limitations, airspace requirements, terrain clearance, *etc*.);
6. **Navigation –** The determination of the current state (*e.g.*, position, speed) of the RPA in relation to the desired state;
7. **Communication –** The provision of a means to exchange flight critical command and control data and information critical for flight between the RPA, the RPS, other elements of the RPAS, and external elements (*e.g.*, Air Traffic Control, other aircraft, etc.);
8. **Mitigation –** The ability to detect and predict hazardous states (internal and external), generate warnings and alerts, and take the necessary actions to mitigate the risk.

It is important to note that the substantiation of functions is intentionally not prescribed (*e.g.*, whether functions are performed by human or machine components of the RPAS). It should also be made clear that these functions are not independent, that is, a failure in one function can impact multiple other functions.

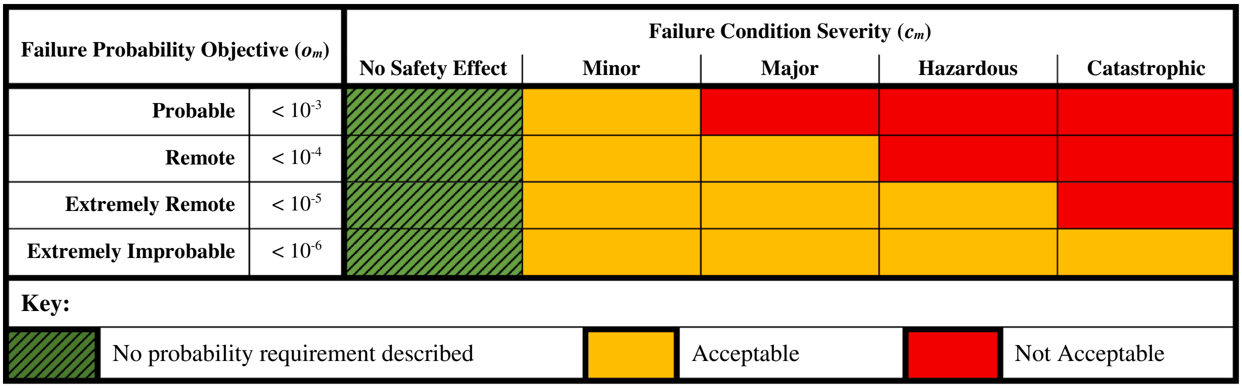
A review of RPAS incident and accident data (provided by Belcastro et al. (2017) along with other incident and accident reports relating to RPAS from the Australian Transport Safety Bureau (ATSB)) was undertaken to validate the completeness of the proposed set of functions. The objective of this review was to determine if previously observed RPAS incidents and accidents could be described in relation to losses or degradations of at least one of the system functions identified above. A number of incident and accident data points provided in the existing databases lacked the information necessary to assign a loss or degradation of a particular system function. However, the ones that had sufficient information (37 data points out of the 110 data points) could have loss or degradation events clearly described using the set of eight identified system functions.

To put this component of the model into context, consider the following scenario. A pre-flight check failed to identify contamination of fuel. This failure can be related to the potential loss of the high level system function of *Propulsion*. Therefore, the top-level system function of interest in this case is the *Propulsion* system. This scenario will be further elaborated in each of the following sub-sections.

3.1.2. *Specification of Operational Failure Mode Classifications for a Generic RPAS*

Clothier et al. (2015) identify three high level operational failure modes referred to as operational 'threats' based on a review of existing classifications proposed in the literature (ADF, 2017; Williams et al., 2014; EASA, 2009). In a later paper, Clothier et al. (2018) go on to define a fourth threat, that of "Dropped or Jettisoned Components" (DOJC). These four operational threats can be used to describe the possible impact of a failure at the operational level of a system and are described below. Each of these operational threats relate to the potential to cause harm to third party individuals on the ground. In addition to these states, are operational states that have the potential to result in consequences to people on-board other aircraft. Hence, we define a fifth operational failure mode as a Loss of Safe Separation (LOSS) between aircraft. Combined with the 'threat' definitions outlined in Clothier et al. (2015, 2018), the set of possible operational failure modes for a generic RPAS are defined as:

1. **Unpremeditated descent scenario (UDS)** – a failure (or combination of failures), which results in the inability of the RPA to maintain a safe altitude above the surface or distance from objects and structures;
2. **Loss of control (LOC)** – a failure (or combination of failures), which



Failure Probability Objective (o_m)		Failure Condition Severity (c_m)				
		No Safety Effect	Minor	Major	Hazardous	Catastrophic
Probable	$< 10^{-3}$	▨	🟧	🟥	🟥	🟥
Remote	$< 10^{-4}$	▨	🟧	🟧	🟥	🟥
Extremely Remote	$< 10^{-5}$	▨	🟧	🟧	🟧	🟥
Extremely Improbable	$< 10^{-6}$	▨	🟧	🟧	🟧	🟧

Key:

▨	No probability requirement described	🟧	Acceptable	🟥	Not Acceptable

Fig. 7. Failure Probability Objectives for JARUS (2015).

results in loss of control of the RPA and may lead to impact at high velocity;

3. **Controlled flight into terrain (CFIT)** – when an airworthy RPA is flown, under the control of a qualified Remote Pilot (RP) or certified autopilot system, unintentionally into terrain (water, structures, or obstacles);
4. **Dropped or jettisoned components (DOJC) –** failures that result in a component of the RPA (including its payload or stores) being dropped or jettisoned from the RPA; and
5. **Loss of Safe Separation (LOSS) –** failures that result in the RPA failing to remain safely separated from, or colliding with, aircraft in the air or on the ground.

Loss or degradation of each of the eight top-level system functions should be traceable to one or more of the five operational failure modes described above. The association of a loss or degradation of a high-level system function with a particular operational failure mode defines one unique failure condition, f_n, to be further assessed (as seen in Eq. (13)).

Continuing our example, the loss of *Propulsion* as a result of contaminated fuel is likely to result in UDS and potentially a LOC (e.g., due to aerodynamic stall). Thus, F^{**} contains the two failure conditions as given in Eq. (18).

$$F^{**} = \{\text{"}\mathit{Propulsion\ resulting\ in\ UDS}\text{"},\quad \text{"}\mathit{Propulsion\ resulting\ in\ LOC}\text{"}\} \tag{18}$$

The incident and accident data provided by Belcastro et al. (2017) and the ATSB were also used as a form of partial validation of the defined set of operational failure modes. With the exception of the DOJC operational failure mode, it was found that all previously documented incidents and accidents (where sufficient information was available) could be classified using the set of identified operational failure modes. The absence of the DOJC operational failure mode could be attributed to the lack of recorded data in these data sets. Numerous cases of payloads (*e.g.*, cameras) falling from RPA have been reported in public media sources, providing a partial validation for the DOJC operational failure mode as well.

3.2. Specification of the Set of Failure Condition Severity Categories (C^{**})

SSR and associated guidance materials describe the range of possible failure condition severity scales that can be used to assess the failure condition severity categories contained in C^{**}. These existing scales are summarised in Table 3 of the Appendix. In this paper, we adopt the more recent failure condition severity scale developed by JARUS (2015), specifically:

1. **No Safety Effect –** Failure conditions that would have no effect on safety. For example, failure conditions that would not affect the operational capability of the RPAS or increase remote crew workload can be classified as no safety effect;
2. **Minor –** Failure conditions that would not significantly reduce RPAS safety and that involve remote crew actions that are within their capabilities. *Minor* failure conditions may include a slight reduction in safety margins or functional capabilities, and/or a slight increase in remote crew workload, such as flight plan changes;
3. **Major –** Failure conditions that would reduce the capability of the RPAS or the ability of the remote crew to cope with adverse operating conditions, to the extent that there would be a significant reduction in safety margins, functional capabilities or separation assurance. In addition, the failure condition has a significant increase in remote crew workload or impairs remote crew efficiency;
4. **Hazardous** – Failure conditions that would reduce the capability of the RPAS or the ability of the remote crew to cope with adverse operating conditions to the extent that there would be the following:
   o Loss of the RPA, where it can be reasonably expected that a fatality will not occur, or
   o A large reduction in safety margins or functional capabilities, or
   o High workload such that the remote crew cannot be relied upon to perform their tasks accurately or completely;
5. **Catastrophic –** Failure conditions that could result in one or more fatalities**.**

In the context of the example scenario involving the loss of *Propulsion*, if the RPAS operation is taking place near a populous area, then the set of potential failure condition severities for the set of failure conditions, F^{**} can include "*Hazardous*" and "*Catastrophic*". We could consequently specify C^{**} as given in Eq. (19).

$$C^{**} = \{\text{"}\mathit{Hazardous}\text{"},\quad \text{"}\mathit{Catastrophic}\text{"}\} \tag{19}$$

3.3. Specification of the Set of Failure Probability Objectives (O^{**})

The potential values of the set O^{**} can be determined directly from the applicable Part 1309 Regulation. Maintaining consistency with the JARUS framework, these are described in Fig. 7.

Applying this to our example scenario, we can identify the applicable FPOs (qualitative and quantitative) for each of the failure condition severities contained in C^{**}, Eq. (19). These are assigned to the set O^{**} as shown in Eq. (20).

$$O^{**} = \{\text{"}\mathit{Extremely\ Remote}\ (10^{-5})\ \ \text{"},\quad \text{"}\mathit{Extremely\ Improbable}\ (10^{-6})\text{"}\} \tag{20}$$

3.4. Summary

This section has described how the existing outcomes from the SSA can be extended. The *Proposed* framework facilitates the representation, and in turn assessment of, the uncertainty associated with (1) the identification of failure conditions, (2) the assignment of failure severities, and (3) the assignment of the FPO. Under the *Proposed* framework it is now possible to associate multiple possible failure condition severities with a given set of failure conditions, and in turn, explore the compliance of the system as a whole in relation to all of its potential consequential outcomes.

A generic system level framework which can be applied to any RPAS was presented. Assessments using the *Proposed* framework can be performed using existing techniques, namely FHA, FMEA, FTA, *etc*. and the applicable SSR, to specify the sets F^{**}, C^{**}, and O^{**} for a given RPAS and concept of operation. The modified sets presented in Eqs. (14) and (17) can be used to update the general framework outlined by Washington et al. (2017a, 2017b) to take the uncertainty in each of these outputs into consideration.

What has yet to be addressed is how to quantitatively assess Λ^{**} within the *Proposed* framework. The modified set to take the uncertainty in the APFH for each of the M potential failure condition severities associated with a given set of failure conditions, F^{**}, is provided in Eq. (16). An appropriate model would need to be able to account for the various dependencies between identified failure conditions and propagate the uncertainty throughout the model. This would require the ability to combine the uncertainty in the APFH for each of the M potential failure condition severities associated with a given failure condition, f_n. One such method, which has not previously been applied in the SSA process, is a Bayesian Belief Network (BBN). The following section explores the application of BBNs as a new modelling method for assessing the set Λ^{**} as part of the SSA process.

4. Bayesian Belief Networks – Assessing Λ^{**}

BBNs are graphical structures that make use of probabilistic reasoning to ascertain information about the unknown (Kevorkian, 2016) and are beneficial when expert judgement is ambiguous, incomplete or uncertain (Jensen and Nielsen, 2007). In contrast to other approaches (e.g. ETA, FTA, FMEA, etc.) that are either deductive or inductive, BBNs are abductive (Kevorkian, 2016), that is they seek to find the simplest and most likely explanation to an observation. Given evidence of failure at the top or intermediate events, we can diagnose which of the primary, or other, events are the most likely cause of this failure. BBNs can thus also be used for fault finding and accident investigation (Fenton and Neil, 2013). Furthermore, unlike classic FTA, a BBN does not assume independence between primary events, and as such is more representative of real systems.

BBNs have a number of advantages compared to other standard modelling techniques. They explicitly model causal factors; allow for reasoning from effect to cause and vice versa; reduce the burden of parameter acquisition; allow for previous beliefs to be overturned in light of new evidence; make predictions with incomplete data; and can combine diverse types of evidence including both subjective beliefs and objective data to arrive at decisions based on visible, auditable reasoning (Fenton and Neil, 2013).

In the context of the SSA process, BBNs are particularly useful in the modelling of complex relationships with multiple dependencies. They are capable of being used in the presence of scarce data and can easily combine objective data available for a system with subjective judgment provided by the assessors.

BBNs have been extensively used in risk modelling in a number of industries as outlined previously. In the context of aviation safety, BBNs have been used in studies such as those that relate to the estimation of the failure rates of the system and the evaluation of the potential impact locations (*e.g.*, Ale et al., 2009, 2013; Ancel et al., 2017; Barr et al., 2017; Kevorkian, 2016; Kumar et al., 2014). They have however not been integrated within the formal structure of a system safety compliance process.

4.1. Structure of a Bayesian Belief Network

A detailed description of the theoretical mathematical principles of a BBN and methods for their construction can be found in Fenton and Neil (2013), Charniak (1991), Jensen (1996), Press (1989), Pearl (1997) and Lauritzen and Spiegelhalter (1988). Only a brief introduction based on Fenton and Neil (2013) is provided here. A BBN is a directed acyclic graph comprising of nodes and arcs. Nodes represent stochastic variables of interest, and the arcs represent the direct dependencies between the nodes (Fenton and Neil, 2013).

Associated with each node in a BBN is a Node Probability Table (NPT) describing the probability distribution given the set of parents of the node. For a node without parents, also called a root node, the NPT is simply the probability distribution of that node. In most real-world risk applications, the variables of interest are not likely to be labelled, Boolean or ranked, but rather numeric (discrete or continuous) variables that require an infinite number of states (Fenton and Neil, 2013). A major advantage of numeric nodes (as opposed to a labelled or ranked node) is that we are able to use a wide range of pre-defined mathematical and statistical functions instead of having to manually define NPTs (Fenton and Neil, 2013), which can prove to be a complex task as the number of nodes increases.

The arcs between nodes represent the causal or influential dependencies. The direction of the arcs is of utmost importance. The arc should always be in the direction of cause to effect rather than in the direction implied by the deductions one might wish to make (Fenton and Neil, 2013). However, it is important to note that taking the latter approach does not necessarily lead to an invalid BBN. The process of determining what evidence will update which node is determined by the conditional dependency structure (Fenton and Neil, 2013). For more details refer to Fenton and Neil (2013). The varying impact of a given node on one or more of the other nodes, can also be taken into consideration through the introduction of different weighting factors.

For a BBN consisting of n variables $A_1, A_2, \ldots, A_n$, the simplified full joint probability distribution of the BBN is shown in Eq. (21), where the parents for a node A_i are given as *Parents*(A_i) (Fenton and Neil, 2013).

$$P(A_1, A_2, A_3, \cdots, A_n) = \prod_{i=1}^{n} P(A_i|Parents(A_i)) \tag{21}$$

4.2. Application of BBNs within the SSA Process

A high-level BBN can be developed using the SSA framework proposed in Section 3. The various outputs from the SSA can be used to form the basis of the nodes of a BBN, as illustrated in Fig. 8. The set of failure conditions (F^{**}) are defined by the set of generic system functions and the set of potential operational failure modes (see Eq. (13)). The set of failure condition severities (C^{**}) are defined by the failure severity scales outlined by the regulatory bodies.

4.2.1. Substantiation of the Arcs

The connections between the nodes are specific to a particular RPAS and its CONOPs and therefore, Fig. 8 shows all potential connections and arcs that could exist for any generic RPAS. Traditional SSA tools such as FHA, FMECA, FTA, ETA, *etc*., accident and incident data, and expert judgment can all be used to substantiate the network for a specific RPAS CONOPs. Arcs (relationships) that are not feasible or deemed extremely unlikely, can be removed. Alternatively, such arcs could be preserved and assigned a low weighting factor reflecting its low relative probability. By doing so, we preserve the possibility of the arc's occurrence. The arcs relating system functions to operational failure modes are primarily determined by the characteristics of the RPAS, whereas the arcs relating operational failure modes to failure condition severities are heavily influenced by the characteristics of the operation and environment (e.g., whether the RPA is operating over a populous

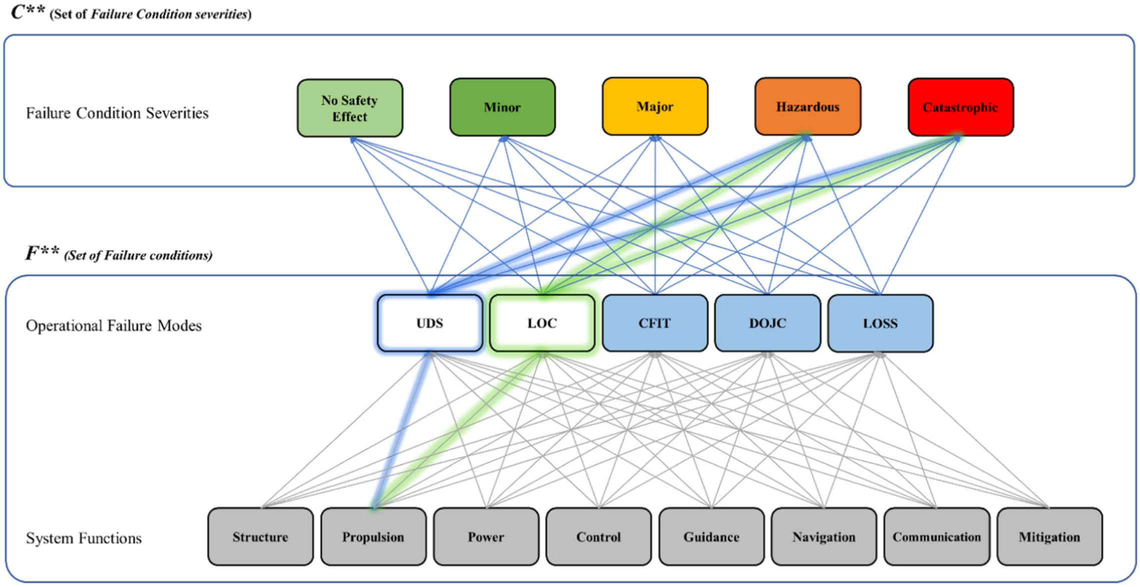


Fig. 8. General structure of BBN showing outputs from SSA process.

area). Also shown in Fig. 8 is the illustrative example of a *Propulsion* failure, used throughout Section 3, with the two scenarios for quantitative assessment highlighted.

4.2.2. Quantifying the NPTs

The first level of nodes (the system function nodes) can be described using a wide variety of probability distribution functions that are characteristic of the failure rate associated with each respective system function. The use of point value estimates of the failure rate to determine these inputs, would not account for the uncertainty in the input estimate (e.g., due to limited failure data). In order to account for this input uncertainty, an additional Bayesian analysis process can be undertaken for each of the identified system function nodes. This requires the specification of a likelihood distribution and a prior distribution for the APFH. A standard Bayesian update process can then be used to determine the posterior distribution of the APFH for each of the identified system function nodes, which forms the input to the BBN. For further details on the Bayesian analysis process, the reader is directed to Washington et al. (2017). The Bayesian input is illustrated as Step 1 in Fig. 9, which shows the *Proposed* SSA process using a BBN.

The nodes in level two of the model (seen in Fig. 8) have arcs joining the system functions to the operational failure modes, while those nodes in level three have arcs joining the operational failure modes to the failure condition severity categories. This makes the NPT associated with each of these nodes significantly more complicated as they are dependent on the nodes from the previous level. As these nodes are numeric, mathematical expressions or probability distributions can be used to describe them as well, negating the need to describe complex NPTs (Fenton and Neil, 2013) (Step 2 in Fig. 9). For more details on the different mathematical expressions or probability distributions that can be used the reader is directed to Fenton and Neil (2013).

4.2.3. Output Assessments of APFH

Once the Bayesian analysis process for each of the relevant root

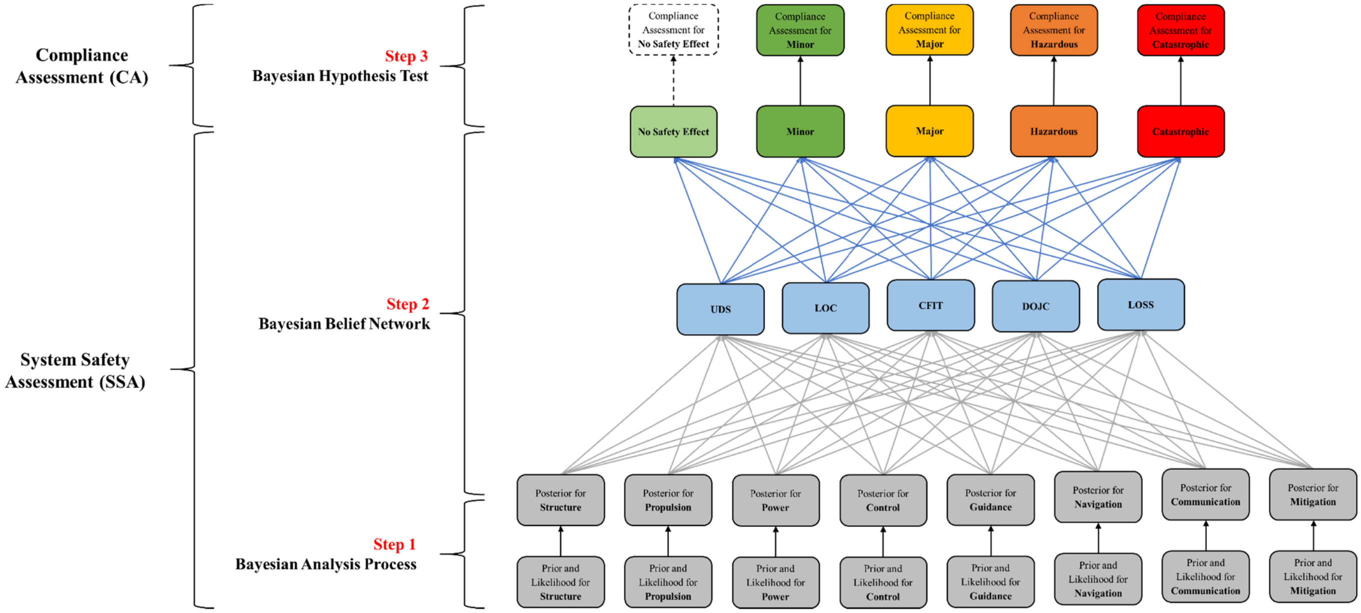

Compliance Assessment (CA)
Step 3
Bayesian Hypothesis Test
System Safety Assessment (SSA)
Step 2
Bayesian Belief Network
Step 1
Bayesian Analysis Process
Compliance Assessment for No Safety Effect
Compliance Assessment for Minor
Compliance Assessment for Major
Compliance Assessment for Hazardous
Compliance Assessment for Catastrophic
No Safety Effect
Minor
Major
Hazardous
Catastrophic
UDS
LOC
CFIT
DOJC
LOSS
Posterior for Structure
Posterior for Propulsion
Posterior for Power
Posterior for Control
Posterior for Guidance
Posterior for Navigation
Posterior for Communication
Posterior for Mitigation
Prior and Likelihood for Structure
Prior and Likelihood for Propulsion
Prior and Likelihood for Power
Prior and Likelihood for Control
Prior and Likelihood for Guidance
Prior and Likelihood for Navigation
Prior and Likelihood for Communication
Prior and Likelihood for Mitigation

Fig. 9. Overall framework for model showing Bayesian analysis process (Step 1), BBN (Step 2) and Bayesian hypothesis test (Step 3) for generic RPAS.

nodes is undertaken, and a posterior distribution for them is obtained, the BBN can be used to combine these distributions to determine the APFH (and the uncertainty surrounding the APFH) associated with each of the remaining nodes in the network. The weighting factors associated with the arcs, along with the mathematical expressions used for each of the nodes, determine how these distributions combine. The end result is an APFH (and the uncertainty surrounding the APFH) associated with each of the relevant operational failure modes and failure condition severity categories defined in the network. The assessments of the APFH can be updated as more data and information is gained through operational experience or analysis.

4.3. Using the Output from the BBN within Compliance Assessment

For completeness, we briefly explain how the updated output distributions from the BBN are used within the CA process (Step 3 in Fig. 9). The CA process described in this sub-section is based on that developed in Washington et al. (2017) for the *Extended* SSPR framework.

Instead of assessing whether a particular system is compliant against the identified "worst case" failure condition severity category, a strength of the *Proposed* framework is that a failure in the system can now be assessed for compliance against all of its possible consequential outcomes and corresponding FPOs. This allows for the relaxation of some of the overly conservative safety objectives imposed on these systems, thereby reducing the costs in the design, production, testing, and certification of the system.

Input to the CA process is a set of failure conditions, F^{**} and the associated set of failure condition severity categories, C^{**}, uncertainties (or degree of beliefs) in each λ_m, Λ^{**}, and FPOs, O^{**}. Following (Perez et al., 2012a, 2012b, 2013; Perez, 2013), the CA process is redefined as the process of determining the degree of belief as to whether the candidate system satisfies all of its relevant FPOs. The CA process for the identified set of failure conditions (F^{**}) is undertaken for each of the M identified failure condition severity categories (for which a relevant FPO exists) contained in the set C^{**}. Instead of being a simple deterministic binary process, the state of compliance for each of the M identified failure condition severity categories is recast as a proposition (or hypothesis), against which a probability representing the degree of belief in its state (i.e., H_m being *True* or *False*) is assigned. Each of the sub-propositions, H_m, can be defined using Eq. (22). These M sub-propositions are then collected in the set, S^{**}, described in Eq. (23).

$$H_m\colon \lambda_m \le o_m \quad \text{where } m \in R \tag{22}$$

$$S^{**} = \{H_m \ \forall \ \ m \in R\} \tag{23}$$

Each sub-proposition, H_m is *True* if λ_m is less than its relevant FPO, o_m. We do not know the value of λ_m with certainty and hence can only determine a probability representing our uncertainty in the state of compliance, i.e. the probability of each sub-proposition being *True* (or not). This probability is denoted as $P(H|D,I)_m$, which can be thought of as a measure of our degree of belief in the compliance of the system, against the FPO, o_m, associated with the relevant failure condition severity category, c_m. Each of the M probabilities, $P(H\ |D,I)_m$, associated with the M sub-propositions can be contained in the set T^{**}, described in Eq. (24).

$$T^{**} = \{P(H|D,\ I)_m\colon m \in R\} \tag{24}$$

There are a number of ways we can infer $P(H|D,I)_m$ from the posterior distributions $p(\lambda|D,I)_m$. One means for determining $P(H|D,I)_m$ is through the one-sided integration of $p(\lambda|D,I)_m$, as seen in Eq. (25).

$$P(H|D,\ I)_m = \int_0^{o_m} p(\lambda|\ D,\ I)_m{\cdot}d\lambda \tag{25}$$

Another approach that can be used to this accord is that of Bayesian Prediction. For more details on this, the reader is directed to Washington et al. (2017a). Once $P(H|D,I)_m$ has been determined for all H_m in S^{**} and assuming the assessments are independent, Eq. (9) can be recast to express our overall degree of belief in the compliance of the system $P(H|D,I)_S$. For more details on this, the reader is once again directed to Washington et al. (2017a).

In summary, the *Traditional* CA process did not account for uncertainty, providing *True* or *False* statements to decision makers. The *Proposed* CA process acknowledges the uncertainty inherent in the assessment and presents decision makers with measures of uncertainty in the state of compliance (i.e., system, function or failure condition meeting all of its relevant FPOs). This enables a more objective, transparent, systematic and consistent certification decision making process on the basis of risk.

4.4. Validation of the Structure of the BBN Model

Existing RPAS incident and accident databases such as that provided by Belcastro et al. (2017) and ATSB were reviewed to help validate the structure of the BBN model developed in this paper. These databases provided limited (but useful) information on the system functions, operational failure modes and failure condition severity categories associated with each failure. Each data point was compared to the set of system functions, operational failure modes and failure condition severity categories arrived at in this study. Any data points that did not fall under this set were then re-evaluated for inclusion. Standard CONOPs, FMEA and FMECA were further used to help validate the model.

4.5. Summary

This section has shown how a BBN could be used within the SSA process to provide assessments of the APFH under situations of uncertainty. The resulting framework is illustrated in Figs. 8 and 9. The generic framework enables the assessment of multiple outcomes for a given system (e.g. RPAS), system function (e.g. *Propulsion*), or failure condition (e.g. *Propulsion* leading to UDS).

Fig. 9 provides the overall framework of the developed model, showing how each of the steps described above, relate to the SSA and CA process. In the following section, the new approach is applied to a simple case study to highlight various aspects of the framework that provide improved insights to the assessors compared to existing frameworks.

5. Case Study

A hypothetical case study example is presented to illustrate the practical features of the *Proposed* BBN approach and modified SSA and CA processes described in this paper. The case study chosen is for an RPAS manufacturer who is developing the compliance case for a new RPAS type design. For the purposes of this case study, the draft Part 1309 regulations presented in JARUS (EASA, 2015b) are used as the certification basis. The analysis and results are purely illustrative, based on available data and expert judgement and are not necessarily representative of a real system. The output from this analysis is used only to highlight the practical aspects of the *Proposed* approach and is not an accurate representation of an analysis for RPAS of a similar type. The characteristics of the RPAS, environmental conditions and operational environment all play an important role in determining the relationships that exist in the model, and consequently, have been described below.

5.1. System, Mission and Environment

The manufacturer intends to mass produce a small quadrotor RPA with a maximum take-off mass of less than 2.0 kg for commercial applications in Europe. It is fitted with failure detection, warning, and recovery/mitigation devices, automatic recovery parachutes and has engine restart capabilities. The RPA falls under the open category[2] of RPA, and as such adheres to the corresponding regulations associated with open category RPA as detailed by EASA (2017).[3] The flight tests involve the RP conducting routine operations over a predetermined area to gather flight test data. Operations are conducted in clear weather conditions during the day, in keeping with the restrictions and regulations imposed on these systems. The chosen case study RPAS and application is representative of commonly used COTS RPAS.

5.2. Available Data

Data from 500 hours of flight testing were collected over a six-month period. Seven incidents relating to a failure in the *Propulsion* function were observed during this period. This represents the available data, *D*. A summary of the APFH data for the *Propulsion* function are provided in Table 4 in the Appendix. Two of the incidents resulted in the RPA being unable to maintain a safe altitude (i.e., UDS operational failure mode) and the remaining five resulted in the RP completely losing control of the RPA (i.e., LOC operational failure mode). In each instance the RPA impacted the ground, and while no one was injured, the RPA sustained irreparable damage.

The manufacturer was also able to draw upon existing datasets to supplement the limited data from flight testing. The dataset compiled by Belcastro et al. (2017) and ATSB were available. This data, along with expert judgement, can be used to determine the weighting factors within the BBN model. The datasets contain information on 110 distinct incidents and accidents involving RPAS, of which only 37 were related to multi-rotor RPAS. Of these 37, only 22 data records contained sufficient information and were used to assign the weighting factors in the model. The limited data were supplemented by a simple high level FMECA, to help tune the appropriate weighting factors within the BBN model. The FMECA process involved exploring the different ways a failure in the *Propulsion* system could eventuate and what operational failure modes and failure condition severity could materialise from this. In addition to this, the RPA CONOPS played an important role in determining the likely consequence severities (and hence weighting factors) assigned to each operational failure mode. Tables 6 and 7 in the Appendix provide a summary of the weighting factors used to substantiate the model.

It is important here to note that historically reported incident and accident data are inherently skewed to *Catastrophic* and *Hazardous* events owing to the mandatory reporting nature of these safety occurrences. Such data needs to be supplemented with predictive analysis and the results of a preliminary SSA. The uncertainty associated with these various information and data sources is not taken into consideration and marks an area of future research extension.

5.3. Defining the Structure of the BBN

The BBN for the case study is illustrated in Fig. 10. The BBN approach allows for multiple concurrent failures in different system functions to be evaluated simultaneously. However, in order to keep the case study as simple as possible, only failures in the single system function, *Propulsion,* are evaluated. The remaining system function nodes have consequently been removed from the BBN shown in Fig. 10. The set notation provided in Section 2.2.2, can be updated to take this into consideration.

Through the existing data and FMECA, a complete, partial or intermittent loss of the *Propulsion* function was determined as having two primary operational failure modes: UDS and LOC. Other operational failure modes may be possible. However, taking the characteristics of the case study and the limitations of the software for evaluating the BBN into consideration, the remaining operational failure mode nodes have also been removed from the BBN depicted in Fig. 10.

The five failure condition severity categories of interest span "*No Safety Effect*", "*Minor*", "*Major*", "*Hazardous*" and "*Catastrophic*". Taking the operational environment into consideration, it is evident that fatal injuries are unlikely, and consequently the "*Catastrophic*" failure condition severity category can potentially be removed. However, to ensure completeness in the assessment process, all five categories have been included in this case study.

In any real-world application, these additional nodes (faded nodes in Fig. 10) would not be removed. Instead, they would be assigned a low weighting factor. While this would increase the complexity of the model, it would ensure that no credible scenario (despite never being observed in data) was inadvertently ignored. An example of this can be seen in the inclusion of the "*Catastrophic*" failure condition severity category. This link was preserved as, even though the operations would be limited to non-populous areas, there is always the chance that third party individuals might inadvertently enter the flight test area. In addition to this, based on the stress model, it was clear that the RPA had sufficient Kinetic Energy (KE) to cause a fatality on impact (refer to Ball et al. (2012), Burke (2011), Dalamagkidis et al. (2012)) for examples of energy cut-off limits), in the event any recovery mechanisms failed.

5.3.1. Quantification of the NPTs

Based on the fundamental theory of BBNs outlined previously, each of the nodes representing the system functions, operational failure modes and failure condition severity categories, are numeric and hence require continuous variables to represent them.

The first step (Step 1 in Fig. 9) is to determine the posterior distribution of the *Propulsion* failure. This is achieved through a Bayesian analysis process. Following Washington et al. (2017) and Barr et al. (2017), the failure rate was assumed constant, and a standard Poisson distribution was selected for the likelihood distribution (refer to Washington et al. (2017) for the limitations of this assumption). From the choice of a Poisson distribution, it is clear that the time between successive failures is an independent and identically distributed random variable. An uninformed prior in the form of a Gamma distribution was also selected for the prior distribution based on Washington et al. (2017a). Being uninformed, it lets the data dominate the posterior distribution (Dezfuli et al., 2009). For more information on the rationale for the choice of the prior and likelihood functions, refer to Washington et al. (2017a). These probability distributions, along with the incident and accident data available on the system (seven incidents in 500 hours) were input into the AgenaRisk™ software to obtain the posterior distribution, representing the uncertainty in the estimate of the APFH of the *Propulsion* system function. For further details on the Bayesian analysis process, the reader is directed to Washington et al. (2017a).

The distributions associated with the nodes for each operational failure mode were obtained by multiplying the posterior distribution for the *Propulsion* function with the appropriate weighting factors. If two or more system functions were being evaluated, then an appropriate mathematical function would have been used to estimate the distributions associated with the operational failure mode nodes. As can be seen in Fig. 10 each of the failure condition severity category nodes have two associated arcs, one from each of the operational failure mode nodes. Thus, a mathematical function was required to combine the distributions (and the relevant weighting factors) from each of the operational failure mode nodes. In this case study, a dynamic OR gate was used to obtain the distributions for each of the failure condition severity nodes (Step 2 in Fig. 9). For more details on this and other mathematical functions that could be used, the reader is directed to Fenton and Neil (2013).

Once the model is developed, it needs to be executed. The AgenaRisk™ software conducts the necessary analysis associated with a BBN to empirically determine the output probability distributions

[2] The open category defined by EASA is similar to the excluded category defined by CASA.

[3] RPA in the open or excluded categories are not typically required to undergo certification against prescriptive standards such as those included under subpart 1309. The case study is illustrative only (but potentially applicable to operations over persons unconnected to the operation, which is similar to many commercial operations).

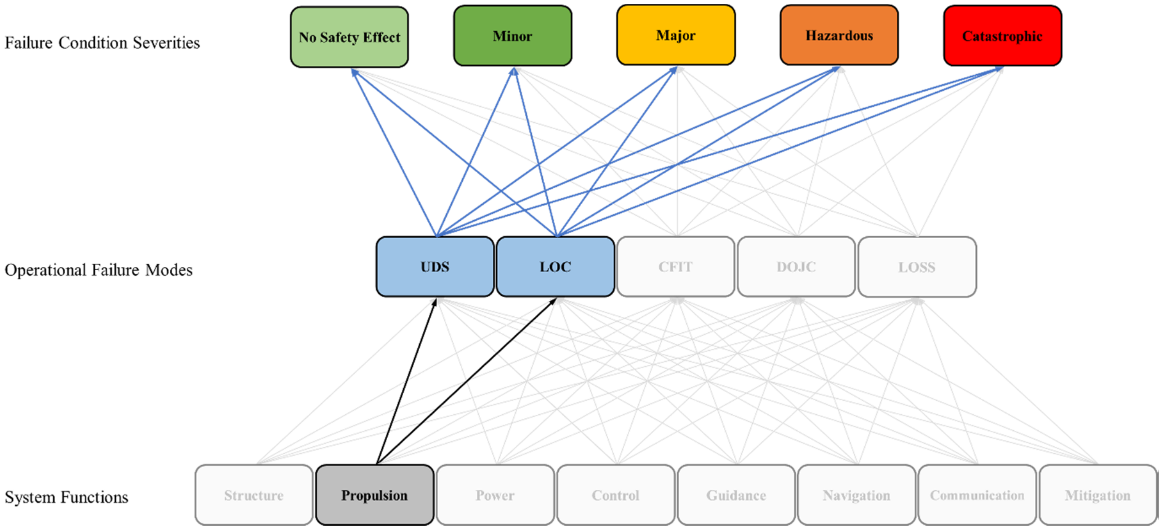


Fig. 10. BBN for case study highlighting relevant nodes and relationships.

representing the uncertainty in the APFH associated with each of the nodes in the model. For further details, the reader is directed to Fenton and Neil (2013).

5.4. Using the Outputs from the BBN within the Compliance Assessment Process

The resulting five output distributions associated with the failure condition severity nodes, describe the uncertainty associated with a *Propulsion* failure resulting in a given failure condition severity (e.g., *No Safety Effect* through to *Catastrophic*). The probability distributions themselves represent the uncertainty associated with the APFH for the *Propulsion* system given a particular failure condition severity category. The CA process (Step 3 in Fig. 9), involves the comparison of these output distributions with the relevant FPO to determine the uncertainty in the state of compliance. The FPOs defined in JARUS (EASA, 2015b) are used for the purposes of this case study, with the resulting compliance sub-propositions for each c_m associated with F^{**} given in Table 1.

As described in Section 4.3, the conditional probability describing the uncertainty in the sub-proposition H_m can be determined by integrating the posterior distributions for each of the failure condition severity category nodes over the appropriate bounds (from zero to the relevant FPO), as given in Eq. (25). The probability of compliance for each relevant sub-proposition is the area under the curve to the left of the relevant FPO (Washington et al., 2017a, 2017b). The resulting outputs representing the *certainty* in each sub-proposition (i.e., compliance with each respective FPO) are summarised in Table 1. The BBN, with associated probability distributions and outputs is depicted graphically in Fig. 11.

Whilst the quantitative results are purely hypothetical, they illustrate the nature of the outputs from the BBN model and their use within the CA process. These values correspond to the degree of *certainty* (or *uncertainty*) of the *Propulsion* system function satisfying the various FPOs, given all available data and information. For example, the probability (representing uncertainty) that the *Propulsion* function meets the minimum FPO for a *Major* failure condition severity category is 0.893. This assessment represents the state of knowledge from available data and information. An advantage of the BBN SSA approach is that the analysis can be quickly updated as new data or information become available.

At this point it is interesting to compare the outputs and results from the *Proposed* model with those obtained through following the *Traditional* SSA and CA processes. Under standard SSA guidelines, a “worst case” credible consequential outcome must be assumed for all failures. Thus, for this case study RPAS, only a single failure condition severity category of *Catastrophic* would be assessed under the *Traditional* approach. The resulting assessment of the APFH would be 1.4×10^{-2} (total number of failures divided by the total number of flight hours). This point value assessment of the APFH does not meet the corresponding FPO of 1×10^{-6}, and the system would consequently be deemed non-compliant.

In contrast to this, the *Proposed* SSPR compliance framework described in this paper would have determined that the probability of the system meeting the FPO (for the *Catastrophic* failure condition severity category) was 0.976. That is, there is an 97.6% certainty that the APFH, was in fact less than the relevant FPO. Based on a CF process (refer to Washington et al. (2017a)), this would have potentially resulted in a positive state of compliance against the *Catastrophic* failure condition severity category. It is important here to note that under the *Proposed* framework, the CA process would need to be conducted for each failure condition severity category before an overall state of compliance can be made.

5.5. Additional Analysis

An advantage of the BBN modelling approach is that it enables further analysis as new data and information becomes available. For example, an analyst can pose questions such as, given an incident of specific consequential outcome, what is the most likely operational failure mode and subsequently, system functional failure that results in this consequence? This is an example of deductive reasoning.

To illustrate, consider the situation where new data, obtained through an additional 100 hours of operational testing, becomes

Table 1
Compliance probabilities for each failure condition severity categories.

Failure condition severity (c_m)	*No Safety Effect*	*Minor*	*Major*	*Hazardous*	*Catastrophic*
Sub-Proposition (H_m)	H_1: N/A	H_2: $\lambda_2 \le 10^{-3}$	H_3: $\lambda_3 \le 10^{-4}$	H_4: $\lambda_4 \le 10^{-5}$	H_5: $\lambda_5 \le 10^{-6}$
Compliance probability ($P(H\|D,I)_m$)	N/A	0.963	0.893	0.856	0.976

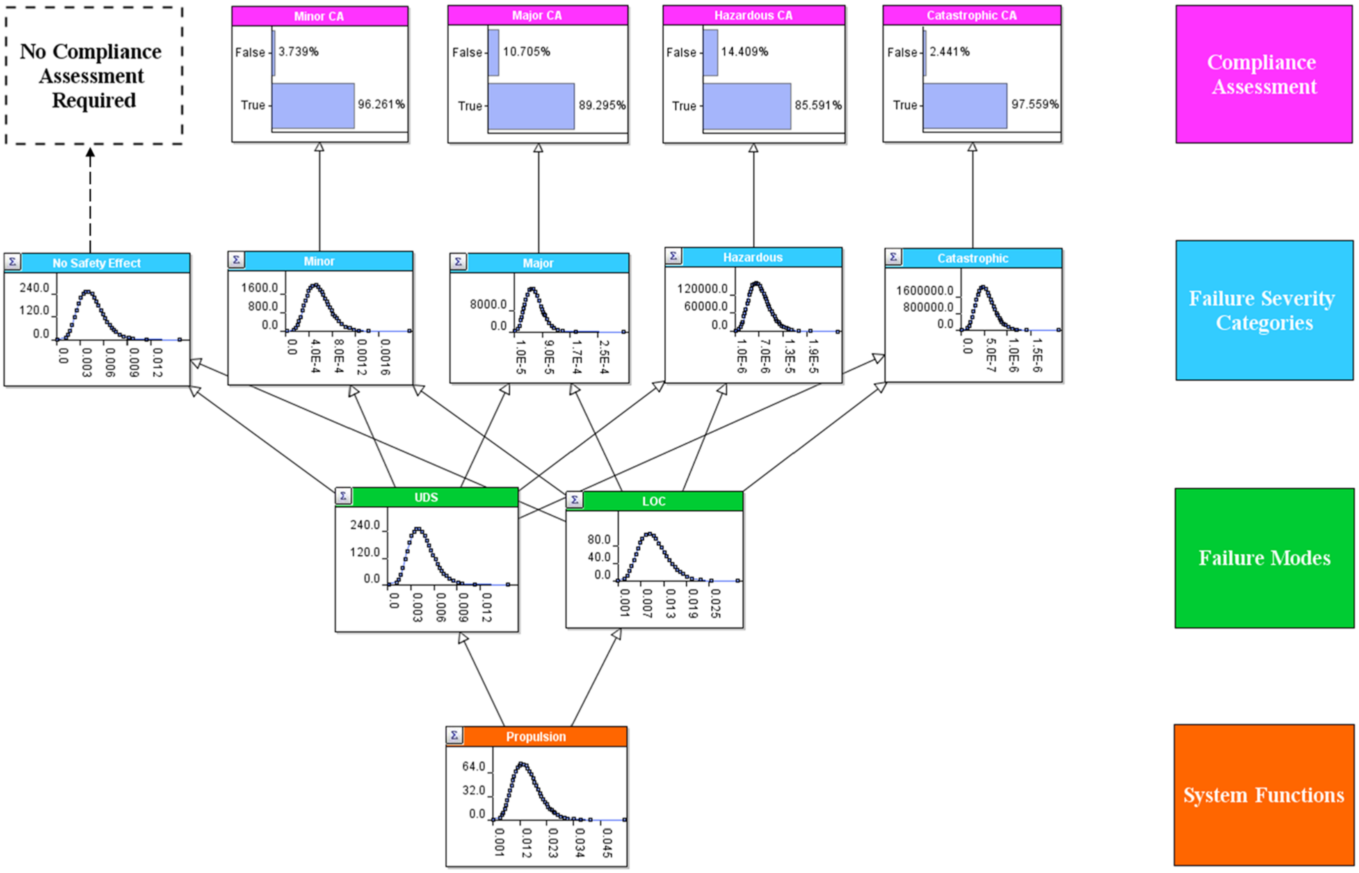


Fig. 11. BBN for case study showing probability distributions (failure rate-*hr*$^{-1}$ vs. density/likelihood) and compliance probabilities.

available. During this period, another four incidents classified as *Major* are observed. Using the AgenaRisk™ software, these data can be added to the top-level *Major* failure severity condition consequence node as observations. The model can then be executed again, resulting in an update to the probability distributions associated with each node. The updated probability distributions compared to the original probability distributions are shown in Fig. 12. The updated compliance probabilities for each of the failure condition severity category nodes are also presented in Table 2. Looking at the compliance probability for the *Major* failure condition severity category for example, it can be seen that the new data resulted in a reduced confidence in the state of compliance. A similar behaviour can be seen for each of the remaining failure condition severity categories as well.

From Fig. 13, the mean APFH of the *Propulsion* system can be seen to increase from 1.500×10^{-2} to 2.35×10^{-2} and the standard deviation from 5.556×10^{-3} to 7.5×10^{-3}. The added data relating to the *Major* failure condition severity category updated all the remaining nodes in the BBN, highlighting its dynamic nature. This behaviour is particularly useful to new systems, where data and expert knowledge is being progressively accumulated. As can be seen in Fig. 12, the certainty in the state of compliance for each failure condition severity is also updated. This directly affects the overall CF process.

6. Discussion

The evolution in the outputs from the SSA process achieved by this research is illustrated in Fig. 14. The *Traditional* SSA process, as described in Section 2.1.1, does not account for uncertainty in the SSA, CA and CF processes. The output of the SSA process is a point assessment of the APFH resulting from a series of cascading conservative assumptions as illustrated in Fig. 14(a). The work presented in Washington et al. (2017a, 2017b), extended this approach to account for uncertainty in the assessment of the APFH, as illustrated in Fig. 14(b). In so doing, the *Extended* SSA approach enabled the basis for risk-based compliance findings, thus evolving the CA and CF processes as well.

A more comprehensive treatment of uncertainty within the SSA process has been proposed in this paper. Specifically, a BBN is used to take into account the uncertainties in relation to the specification of the failure scenario (i.e., the failure conditions and failure condition severities) and the associated FPO against which compliance needs to be assessed. Uncertainty in the assessment of the APFH is also still taken into consideration. The output of the SSA process is now a family of distributions, each describing the uncertainty in the assessed APFH associated with each possible failure condition severity category, as shown in Fig. 14(c). This thus negates the need for the conservative "worst case" consequential outcome assumption and allows for the uncertainty in the failure condition severities to be considered. The approach provides regulators with a more comprehensive picture of the state of knowledge in relation to the APFH for input to CA and CF processes. With reference to Paté-Cornell's "six levels of treatment of uncertainties" (Paté-Cornell, 1996); the *Proposed* framework provides for the highest treatment of uncertainty associated with each of the four outputs from the SSA process. An updated CA process (still based on the Bayesian hypothesis test) that is capable of taking this added data and information into consideration is also proposed in this paper.

In addition to providing a more comprehensive means of treating the uncertainty associated with each of the outputs of the SSA process, the *Proposed* approach has a number of other advantages. It provides a more mathematically robust means for combining objective data with expert judgement and updating the state of knowledge as new data and information is gained. By accounting for the uncertainty in the failure condition severity categories, the *Proposed* approach negates the need for making conservative "worst case" assumptions in relation to the consequential outcomes. Finally, it also supports more justifiable and systematic compliance findings, thus allowing for airworthiness

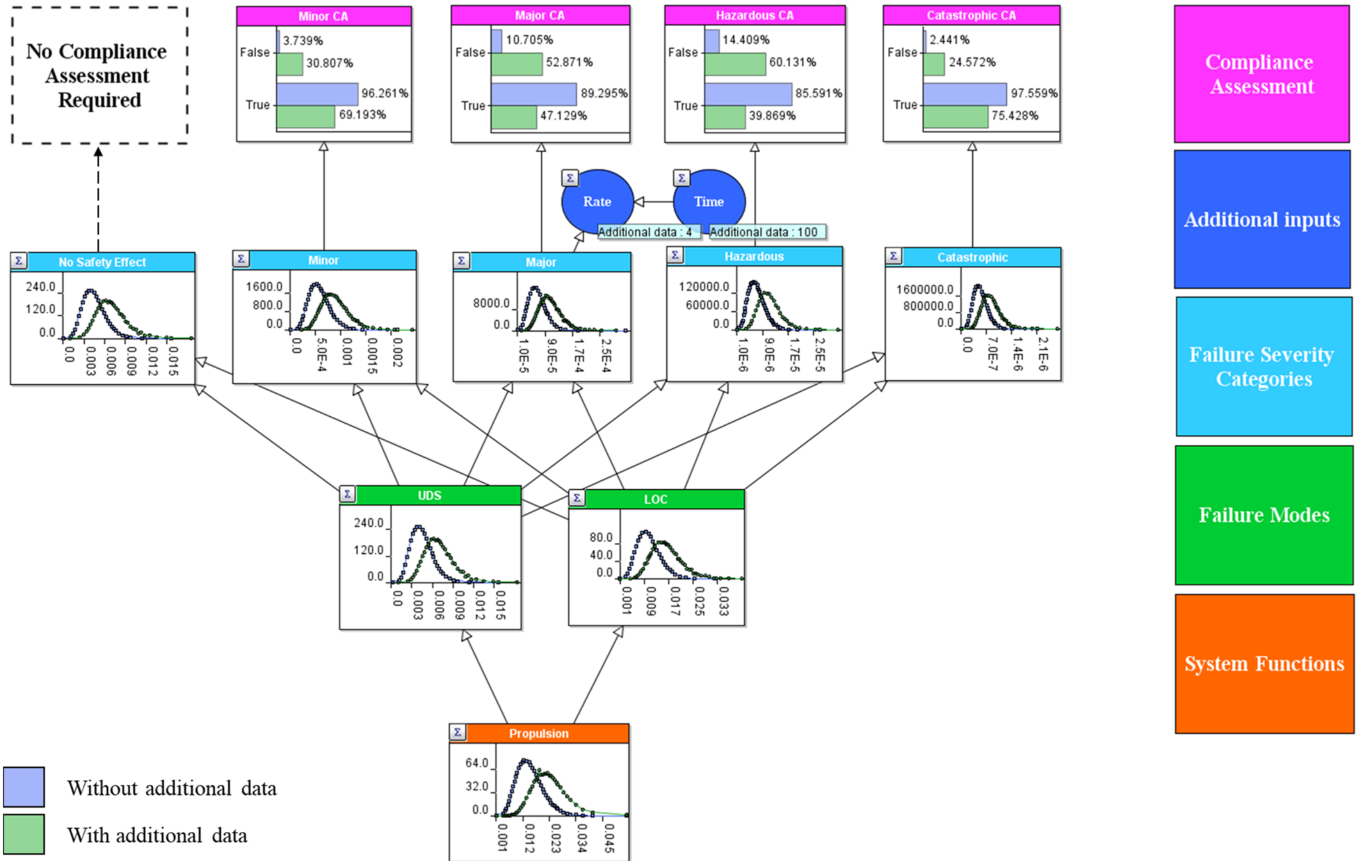


Fig. 12. BBN for case study showing comparison of outputs (with and without additional failure condition severity data).

Table 2
Updated compliance probabilities for each failure condition severity category.

Failure condition severity (c_m)	*No Safety Effect*	*Minor*	*Major*	*Hazardous*	*Catastrophic*
Sub-Proposition (H_m)	H_1: N/A	H_2: $\lambda_2 \leq 10^{-3}$	H_3: $\lambda_3 \leq 10^{-4}$	H_4: $\lambda_4 \leq 10^{-5}$	H_5: $\lambda_5 \leq 10^{-6}$
Compliance probability ($P(H\|D,I)_m$)	N/A	0.692	0.471	0.399	0.754

compliance decisions to be made based on compliance risk. In conjunction with the *Extended* approach developed previously in Washington et al. (2017), the research undertaken in this paper shows how the concept of risk-based regulation can be extended to include a risk-based approach to compliance assessment and compliance finding.

The *Proposed* BBN framework can be developed based on data and information from a number of different sources. Simple FTA, FHA, FMEA and FMECA can be used to help identify the set of system functions and failure modes, while regulatory material can help specify the set of possible failure condition severity categories. In terms of substantiating the

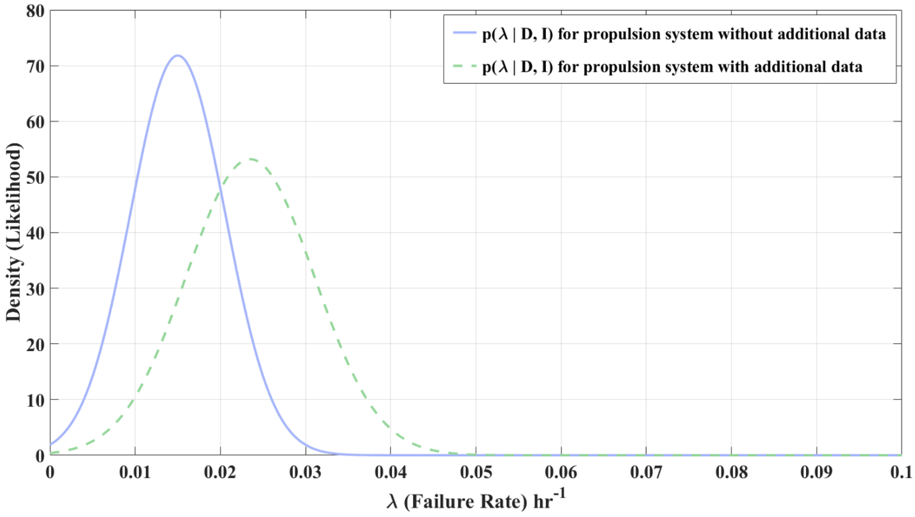


Fig. 13. Comparison of the output probability distributions for the Propulsion function.

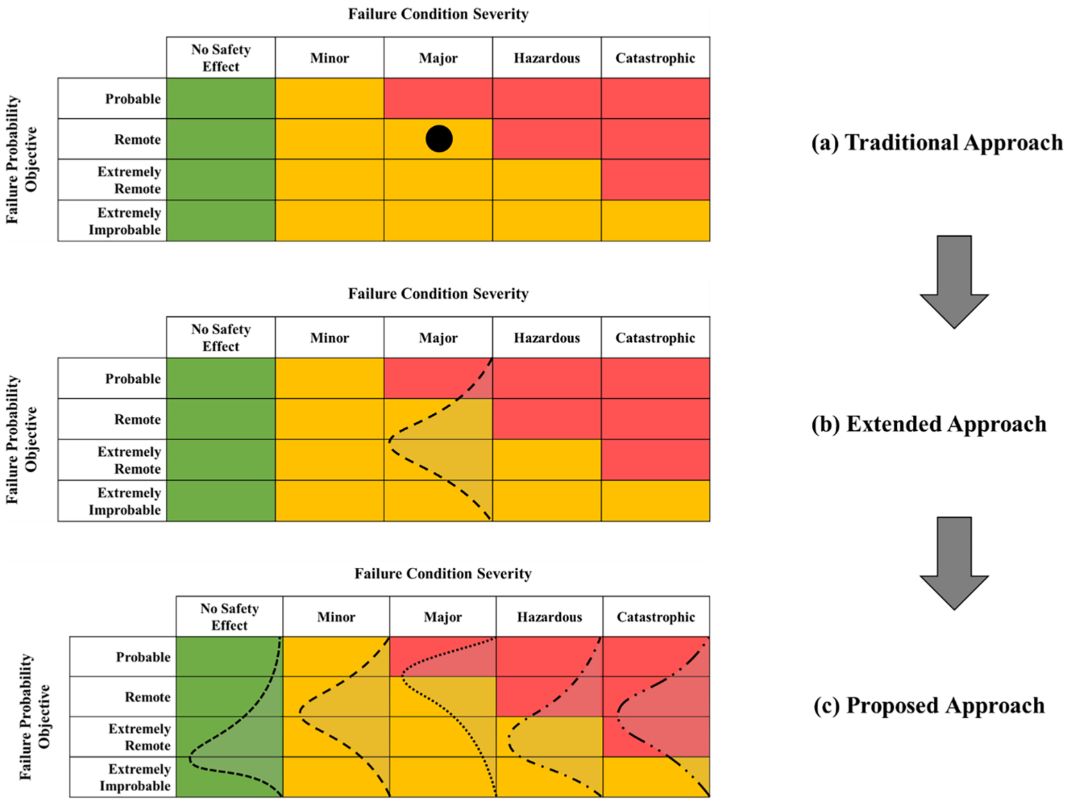


Fig. 14. Incorporating uncertainty in the failure condition severity categories of the SSA process (Extended Approach based on Washington et al. (2017)).

arcs similar tools such as FTA, FHA, FMEA and FMECA along with accident and incident data and expert judgement can all be used to help substantiate the network. The weighting factors used in the proposed model were based on the limited data available and expert judgement. Future work will look at where additional data and information can be obtained from and how to better specify these weighting factors taking the additional data and information into consideration.

In accordance with the system safety assessment guidelines, and previous work undertaken by the authors, this paper makes use of a simple Poisson model to represent the likelihood distribution while evaluating the APFH of the system function. This inherently makes the assumption that the failure rate associated with the system function is constant. As discussed in Washington et al. (2017), this can be extremely limiting as most commercial UAS do not exhibit a constant failure rate. Consequently, a Weibull model is recommended as a suitable alternative to characterise the reliability of these systems. While this was an important extension to make, the authors felt that this would add to the complexity of the BBN model developed and as such would take away from the novelty of the current research. Future work will look at incorporating this into the *Proposed* approach, thus allowing for the variable failure rate associated with these systems to be taken into consideration.

In addition to this, future work will look also to revise the CF process to make best use of the additional data and information output from the SSA and CA processes proposed in this paper. Additional work is also needed to represent the uncertainty associated with the data input to the SSA process (i.e., the data that are input into the BBN). Chapter 10 of Kelly and Smith (2011) proposes a number of approaches to account for data uncertainty, and future research will look to incorporate this into the proposed framework.

7. Conclusion

Regulatory bodies the world over are advocating for the need to move towards a risk-based approach to the regulation of the rapidly emerging RPAS sector. This requires a clear understanding of the risks and uncertainty posed by these systems. The general lack of data and experience associated with the operation of civil RPAS gives rise to a considerable uncertainty associated with all aspects of their operation. *Traditional* system safety analysis approaches do not adequately address the high uncertainty associated with novel or complex systems such as RPAS. Building on previous work (Washington et al., 2017a, 2017b), this paper has shown how the uncertainty associated with each of the outputs of the SSA process can be taken into consideration. Through the adoption of a BBN, the framework presented in this paper provides an approach for capturing the uncertainty in the potential consequential outcomes of an identified failure. This removes the need for conservative "worst case" assumptions and allows for compliance to be assessed for all possible failure condition severities. This in turn allows for the relaxation of overly conservative safety objectives, thereby reducing undue burden (in terms of costs in the design, production, testing, and certification of the system) on manufactures and operators and promoting a more risk-based approach to certification. The overall compliance of the system (e.g. RPAS) as a whole, with its system-level safety objectives is shown. The network can be updated as data from testing and operational experience becomes available, facilitating updated compliance reasoning on the output distributions. The novelty of the *Proposed* model lies in the application of this framework to the airworthiness certification and in particular to the Part 1309 regulations. The adoption of the *Proposed* SSA approach would allow for the high uncertainty associated with the safety assessment of new aviation systems, such as RPAS, to be taken into consideration. Such an approach would enable the risk-based regulation of the sector. This work is part of an ongoing program seeking to develop tools that support risk-based regulation, and in so doing, assist regulators in making more objective, transparent, systematic and consistent decisions regarding regulation of new and emerging aviation systems.

Acknowledgements

This research was supported, in part by, the Australian Government Research Training Program Scholarship, provided by the Australian Government.

Appendix

Table 3
Failure condition severity scales.

	JARUS (JARUS, 2015)	EASA (Agency, 2015)	Hayhurst (Hayhurst et al., 2007)	NATO (Atlantic, 2014)	RTCA (Special, 2013)*
No Safety Effect	Failure conditions that would have no effect on safety. For example, failure conditions that would not affect the operational capability of the RPAS or increase remote crew workload.	Failure conditions that would have no effect on safety. For example, failure conditions that would not affect the operational capability of the RPAS or increase the remote crew workload.	Failure Conditions that would have no effect on safety (that is, Failure Conditions that would not affect the operational capability of the airplane or increase flight crew workload).	None defined.	UAS failure condition(s) that have negligible effects to people on the ground. (Referred to as Minimal)
Minor	Failure conditions that would not significantly reduce RPAS safety and that involve remote crew actions that are within their capabilities. Minor failure conditions may include a slight reduction in safety margins or functional capabilities, a slight increase in remote crew workload, such as flight plan changes.	Failure conditions that would not significantly reduce RPAS safety and that involve remote crew actions that are well within their capabilities. Minor failure conditions may include a slight reduction in safety margins or functional capabilities, a slight increase in remote crew workload, such as flight plan changes.	Failure Conditions that would not significantly reduce UAS safety and involve flight crew actions that are well within their capabilities. Minor Failure Conditions may include a slight reduction in safety margins or functional capabilities or a slight increase in flight crew workload (such as routine flight plan changes).	Failure conditions that do not significantly reduce UA safety and involve UA crew actions that are well within their capabilities. These conditions may include a slight reduction in safety margins or functional capabilities, and a slight increase in UA crew workload.	UAS failure condition(s) that could result in minor injuries to one or more people on the ground.
Major	Failure conditions that would reduce the capability of the RPAS or the ability of the remote crew to cope with adverse operating conditions to the extent that there would be a significant reduction in safety margins, functional capabilities or separation assurance. In addition, the failure condition has a significant increase in remote crew workload or impairs remote crew efficiency.	Failure conditions that would reduce the capability of the RPAS or the ability of the remote crew to cope with adverse operating conditions to the extent that there would be a significant reduction in safety margins, functional capabilities or separation assurance. In addition, the failure condition has a significant increase in remote crew workload or impairs remote crew efficiency.	Failure conditions that would reduce the capability of the UAS or the ability of the flight crew to cope with adverse operating conditions to the extent that there would be: a significant reduction in safety margins or functional capabilities; a significant increase in flight crew workload or in conditions impairing flight crew efficiency; a discomfort to the flight crew; or a potential for physical discomfort to persons	Failure conditions that either by themselves or in conjunction with increased crew workload, are expected to result in an emergency landing of the UA on a predefined site where it can be reasonably expected that a serious injury will not occur. Or Failure conditions which could potentially result in injury to UA crew or ground staff.	UAS failure condition(s) that could result in moderate injuries to one or more people on the ground.
Hazardous	Failure conditions that would reduce the capability of the RPAS or the ability of the remote crew to cope with adverse operating conditions to the extent that there would be the following; i. Loss of the RPA where it can be reasonably expected that a fatality will not occur, or ii. A large reduction in safety margins or functional capabilities, or iii. High workload such that the remote crew cannot be relied upon to perform their tasks accurately or completely.	Failure conditions that would reduce the capability of the RPAS or the ability of the remote crew to cope with adverse operating conditions to the extent that there would be the following: i. Loss of the RPA where it can be reasonably expected that one or more fatalities will not occur, or ii. A large reduction in safety margins or functional capabilities or separation assurance, or iii. Excessive workload such that the remote crew cannot be relied upon to perform their tasks accurately or completely.	Failure Conditions that would reduce the capability of the UAS or the ability of the flight crew to cope with adverse operating conditions to the extent that there would be the following: i. A large reduction in safety margins or functional capabilities; ii. Physical distress or higher workload such that the UAS flight crew cannot be relied upon to perform their tasks accurately or completely; or iii. Physical distress to persons, possibly including injuries.	Failure conditions that either by themselves or in conjunction with increased crew workload, are expected to result in a controlled trajectory termination or forced landing potentially leading to the loss of the UA where it can be reasonably expected that a fatality will not occur. Or Failure conditions for which it can be reasonably expected that a fatality to UA crew or ground staff will not occur.	UAS failure condition(s) that could result in serious injuries to one or more people on the ground.
Catastrophic	Failure conditions that could result in one or more fatalities	Failure conditions that are expected to result in one or more fatalities.	Failure conditions that are expected to result in one or more fatalities or serious injury to persons, or the persistent loss of the ability to control the flight path of the aircraft normally with the loss of the aircraft.	Failure conditions that are expected to result in at least uncontrolled flight (including flight outside of pre-planned or contingency flight profiles/areas) and/or uncontrolled crash. Or Failure conditions which may result in a fatality to UA crew or ground staff.	UAS failure condition(s) that could result in a fatality to one or more people on the ground

Table 4
Evaluation of the failure rate of the system functions showing prior, likelihood and posterior distribution.

S. No.	System Function	Prior distribution	Likelihood distribution	Time	Parameters for Prior*		Parameters for Time		Observations		Posterior distribution	
					α (shape parameter)	β (rate parameter)	Lower Bound	Upper Bound	Failures	Time (hours)	Mean	Standard Deviation
1	Propulsion	Gamma distribution	Poisson distribution	Uniform Distribution	0.5	10^6	0	10^6	7	500	1.500×10^{-2}	5.556×10^{-3}

* The parameters of the Gamma distribution are characteristic of an uninformed Gamma distribution.

Table 5
Evaluation of the failure rate of the failure condition severity categories showing prior, likelihood and posterior distribution.

S. No.	Failure Condition Severity Category	Prior distribution	Likelihood distribution	Time	Parameters for Prior		Parameters for Time		Observations		Posterior distribution	
					Mean	Standard Deviation	Lower Bound	Upper Bound	Failures	Time (hours)	Mean	Standard Deviation
1	*Major*	Normal distribution	Poisson distribution	Uniform Distribution	6.8168×10^{-5}	2.5731×10^{-5}	0	10^6	4	100	1.0702×10^{-4}	3.5142×10^{-5}

Table 6
Weighting factors used for evaluating Operational Failure Modes.

S no.	System function	Operational failure mode	
		UDS	LOC
1	Propulsion	0.3	0.7

Table 7
Weighting factors used for evaluating Failure Condition Severity Categories.

S no.	Operational failure modes	Failure condition severity category				
		No Safety Effect	*Minor*	*Major*	*Hazardous*	*Catastrophic*
1	UDS	1	0.127	0.0151	0.0016	0.00012
2	LOC	1	0.181	0.0213	0.00298	0.00025

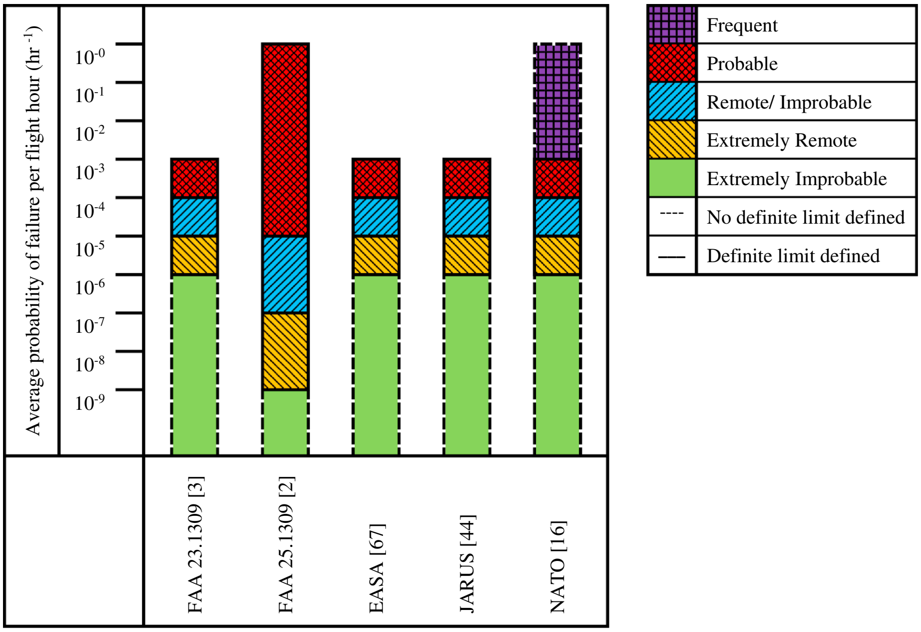
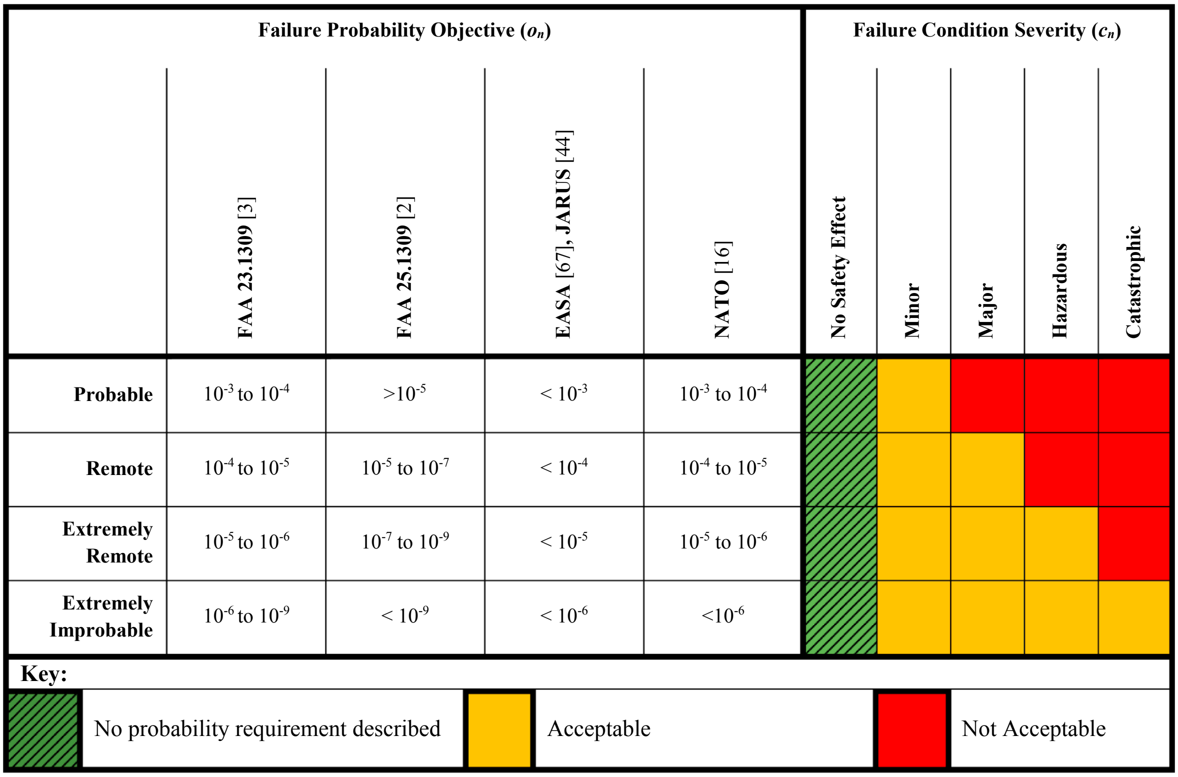


Fig. 15. Comparison of quantitative failure probability objective scales.



	Failure Probability Objective (o_n)				Failure Condition Severity (c_n)				
	FAA 23.1309 [3]	**FAA 25.1309 [2]**	**EASA [67], JARUS [44]**	**NATO [16]**	**No Safety Effect**	**Minor**	**Major**	**Hazardous**	**Catastrophic**
Probable	10^{-3} to 10^{-4}	$>10^{-5}$	$< 10^{-3}$	10^{-3} to 10^{-4}	▨	🟨	🟥	🟥	🟥
Remote	10^{-4} to 10^{-5}	10^{-5} to 10^{-7}	$< 10^{-4}$	10^{-4} to 10^{-5}	▨	🟨	🟨	🟥	🟥
Extremely Remote	10^{-5} to 10^{-6}	10^{-7} to 10^{-9}	$< 10^{-5}$	10^{-5} to 10^{-6}	▨	🟨	🟨	🟨	🟥
Extremely Improbable	10^{-6} to 10^{-9}	$< 10^{-9}$	$< 10^{-6}$	$<10^{-6}$	▨	🟨	🟨	🟨	🟨

Key:

▨	No probability requirement described	🟨	Acceptable	🟥	Not Acceptable

Fig. 16. Comparative illustration of the Part 1309 safety objectives/failure probability objectives.

References

Australian Defence Force (ADF), 2017. Australian Air Publication 7001.054, Electronic Airworthiness Design Requirements Manual (eADRM). Australia.

Ale, B.J.M., Bellamy, L.J., van der Boom, R., Cooper, J., Cooke, R.M., Goossens, L.H.J., Hale, A.R., Kurowicka, D., Morales, O., Roelen, A.L.C., Spouge, J., 2009. Further development of a Causal model for Air Transport Safety (CATS): Building the mathematical heart. Reliab. Eng. Syst. Saf. 94 (9), 1433–1441.

Ale, B.J.M., Van Gulijk, C., Hanea, D., Hudson, P., Lin, P.H., Sillem, S., Steenhoek, M., Ababei, D., 2014. Further development of a method to calculate frequencies of loss of control including their uncertainty. In: Safety, Reliab. Risk Anal. Beyond Horiz. - Proc. Eur. Saf. Reliab. Conf. ESREL 2013, Amsterdam, Netherlands, pp. 1839–1846.

Ancel, E., Shih, A.T., 2015. Bayesian Safety Risk Modeling of Human-Flightdeck Automation Interaction: NASA/TM-2015-218791. National Aeronautics and Space Administration (NASA), Langley Research Centre. Hampton Virginia.

Ancel, E., Shih, A.T., Jones, S.M., Reveley, M.S., Luxhøj, J.T., Evans, J.K., 2015. Predictive safety analytics: inferring aviation accident shaping factors and causation. J. Risk Res. 18 (4), 428–451.

Ancel, E., Capristan, F.M., Foster, J.V., Condotta, R.C., 2017. Real-time risk assessment framework for unmanned aircraft system (UAS) traffic management (UTM). In: 17th AIAA Aviation Technology, Integration, and Operations Conference. Denver, Colorado.

Apostolakis, G., 1990. The concept of probability in safety assessments of technological systems. Science 250 (4986), 1359–1364.

Australian Transport Safety Bureau (ATSB). Aviation Safety Investigations and Reports: Online Database. [Online]. < https://www.atsb.gov.au/publications/safety-investigation-reports/?mode=Aviation > .

Ball, J.A., Knott, M., Burke, D., 2012. Crash Lethality Model: Technical Report no. NAWCADPAX/TR-2012/196. Naval Air Warfare Centre Aircraft Division, Maryland, USA.

Barr, L.C., Newman, R.L., Ancel, E., Belcastro, C.M., Foster, J.V., Evans, J.K., Klyde, D.H., 2017. Preliminary risk assessment for small unmanned aircraft systems. In: 17th AIAA Aviation Technology, Integration, and Operations Conference. Denver, Colorado.

Beaumont, P., Evans, N., Huth, M., Plant, T., 2015. Confidence analysis for nuclear arms control: SMT abstractions of Bayesian belief networks. In: Computer Security – ESORICS 2015. pp. 521–540.

Belcastro, C.M., Newman, R.L., Evans, J., Klyde, D.H., Barr, L.C., Ancel, E., 2017. Hazards identification and analysis for unmanned aircraft system operations. In: 17th AIAA Aviation Technology, Integration, and Operations Conference. Denver, Colorado.

Borsuk, M.E., Stow, C.A., Reckhow, K.H., 2004. A Bayesian network of eutrophication models for synthesis, prediction, and uncertainty analysis. Ecol. Model. 173 (2–3), 219–239.

Bromley, J., Jackson, N.A., Clymer, O.J., Giacomello, A.M., Jensen, F.V., 2005. The use of Hugin® to develop Bayesian networks as an aid to integrated water resource planning. Environ. Model. Softw. 20 (2), 231–242.

Burke, D.A., 2010. System Level Airworthiness Tool: A Comprehensive Approach to Small Unmanned Aircaft System Airworthiness. North Carolina Sate University, Raleigh, North Carolina.

Burke, D.A., 2011. System-level airworthiness tool: a comprehensive approach to small unmanned aircraft system airworthiness. J. Aircr. 48 (3), 777–785.

Cain, J., 2001. Planning Improvements in Natural Resources Management - Guidelines for Using Bayesian Networks to Support the Planning and Management of Development Programmes in the Water Sector and Beyond. Centre for Ecology and Hydrology, Crowmarsh Gifford, Wallingford, Oxon, UK.

Charniak, E., 1991. Bayesian networks without tears. AI Magazine 12 (4), 50–63.

Clothier, R.A., Wu, P.P., 2012. A review of system safety failure probability objectives for unmanned aircraft systems. In: 11th International Probabilistic Safety Assessment and Management (PSAM11) Conference and the Annual European Safety and Reliability (ESREL 2012) Conference, Helsinki.

Clothier, R.A., Williams, B.P., Washington, A., 2015. Development of a template safety case for unmanned aircraft operations over populous areas. In: SAE 2015 AeroTech Congress & Exhibition, 22–24 September, Seattle, Washington, USA.

Clothier, R.A., Williams, B.P., Hayhurst, K.J., 2018. Modelling the risks remotely piloted aircraft pose to people on the ground. Saf. Sci. 101, 33–47.

Dalamagkidis, K., Valavanis, K.P., Piegl, L.A., 2012. On Integrating Unmanned Aircraft Systems into the National Airspace System, second ed. Springer.

Dezfuli, H., Kelly, D., Smith, C., Vedros, K., Galyean, W., 2009. Bayesian Inference for NASA Probabilistic Risk and Reliability Analysis, NASA/SP-2009-569. National Aeronautics and Space Administration (NASA).

European Aviation Safety Agency (EASA), 2005. Advance -Notice of Proposed Amendment (NPA) No. 16/2005, Policy for Unmanned Aerial Vehicle (UAV) Certification.

European Aviation Safety Agency (EASA), 2009. Policy Statement Airworthiness Certification of Unmanned Aircraft Systems (UAS), E.Y013-01, pp. 1–17.

European Aviation Safety Agency (EASA), 2015. Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes CS25.

European Aviation Safety Agency (EASA), 2015. Special Condition: Equipment, systems, and installations. SC-RPAS. 1309-01, No. 2.

European Aviation Safety Agency (EASA), 2016. Explanatory note on ‘Prototype’ Commission Regulation on Unmanned Aircraft Operations.

European Aviation Safety Agency (EASA), 2017. NPA 2017-05 (A): Introduction of a Regulatory Framework for the Operation of Drones, vol. 05, pp. 1–128.

The European Organisation for Civil Aviation Equipment (EUROCAE), 2013. UAS/RPAS Airworthiness Certification ‘1309’ System Safety Objectives and Assessment Criteria,” MALAKOFF, France.

Federal Aviation Administration (FAA), 1988. Advisory Circular 25.1309-1A, System Design and Analysis. US Department of Transportation, Washington, DC, United States of America.

Federal Aviation Administration (FAA), 2011. Advisory Circular 23.1309-1E, System Safety Analysis and Assessment for Part 23 Airplanes. U.S. Department of Transportation, Washington, DC, United States of America.

Fenton, N., Neil, M., 2013. Risk Assessment and Decision Analysis with Bayesian Networks. CRC Press, Taylor and Francis Group.

Guikema, S.D., Paté-Cornell, M.E., 2004. Bayesian analysis of launch vehicle success rates. J. Spacecr. Rockets 41 (1).

Hayhurst, K.J., Maddalon, J.M., Miner, P.S., Szatkowski, G.N., Ulrey, M.L., DeWalt, M.P., Spitzer, C.R., 2007. NASA TM-2007-21439. Preliminary considerations for classifying hazards of unmanned aircraft systems. National Aeronautics and Space Administration (NASA), Langley Research Centre. Hampton Virginia.

Joint Authorities for Rulemaking of Unmanned Systems (JARUS) Working Group 6-Safety and Risk Assessment, 2015. Safety Assessment of Remotely Piloted Aircraft Systems. AMC RPAS.1309, no. 2.

Jensen, F.V., 1996. An Introduction to Bayesian Networks. UCL Press, London.

Jensen, F.V., Nielsen, T.D., 2007. Bayesian Networks and Decision Graphs, second ed. Springer Science & Business Media.

Kang, C.W., Golay, M.W., 1999. A Bayesian belief network-based advisory system for operational availability focused diagnosis of complex nuclear power systems. Expert Syst. Appl. 17 (1), 21–32.

Kardes, E., Luxhøj, J.T., 2005. A hierarchical probabilistic approach for risk assessments of an aviation safety product portfolio. Air Traffic Control Q. 13 (3), 279–308.

Kelly, D., Smith, C., 2011. Bayesian Inference for Probabilistic Risk Assessment: A Practitioners Guidebook. Springer, London.

Kevorkian, C.G., 2016. UAS Risk Analysis using Bayesian Belief Networks : An Application to the Virginia Tech ESPAARO.

Kumar, V., Toussaint, S., Luxhoj, J., Wieland, F., 2014. Unmanned Aerial System (UAS) safety analysis model. In: 14th AIAA Aviation Technology, Integration and Operations Conference , Atlanta, CA, pp. 1–10.

Lauritzen, S.L., Spiegelhalter, D.J., 1988. Local computations with probabilities on graphical structures and their application to expert systems. J. R. Stat. Soc. Ser. B 50 (2), 157–194.

Lee, C.J., Lee, K.J., 2006. Application of Bayesian network to the probabilistic risk assessment of nuclear waste disposal. Reliab. Eng. Syst. Saf. 91 (5), 515–532.

Luxhøj, J.T., 2015. A conceptual Object-Oriented Bayesian Network (OOBN) for modeling aircraft carrier-based UAS safety risk. J. Risk Res. 18 (10), 1230–1258.

Luxhoj, J.T., 2016. System safety modeling of alternative geofencing configurations for small UAS. Int. J. Aviat. Aeronaut. Aerosp. 3 (1).

Luxhøj, J.T., Coit, D.W., 2006. Modelling low probability/high consequence events: an aviation safety risk model. RAMS ’06 Annual Reliability and Maintainability Symposium 23–26 Jan 2006.

Luxhøj, J.T., Jalil, M., Jones, S.M., 2003. A risk-based decision support tool for evaluating aviation technology integration in the national airspace system. In: Proceedings of the AIAAs Third Annual Aviation Technology, Integration, and Operations (ATIO) Technical Forum Denver, Colorado, November 17–19.

Luxhøj, J.T., Harrell, M.B., 2015. An Object-Oriented Bayesian Network (OOBN) prototype for modeling the safety risk of an unmanned rotorcraft. In: IIE Annual Conference and Expo 2015, pp. 183–192.

Luxhøj, J.T., Joyce, W., Luxhøj, C., 2017. A ConOps derived UAS safety risk model. J. Risk Res. 9877, 1–23.

Marcot, B.G., Holthausen, R.S., Raphael, M.G., Rowland, M.M., Wisdom, M.J., 2001. Using Bayesian belief networks to evaluate fish and wildlife population viability under land management alternatives from an environmental impact statement. For. Ecol. Manage. 153 (1–3), 29–42.

Mengshoel, O.J., Darwiche, A., Cascio, K., Chavira, M., Poll, S., Uckun, S., 2008. Diagnosing faults in electrical power systems of spacecraft and aircraft. In: IAAI’08 20th national conference on Innovative applications of artificial intelligence, no. 3. pp. 1699–1705.

Ministry of Transport and Water Management. Causal Model for Air Transport Safety. Delft, Amsterdam, London; 2009.

Morris, A.T., Beling, P.A., 2001. Space Shuttle RTOS Bayesian Network. In: 20th DASC. 20th Digit. Avion. Syst. Conf. (Cat. No.01CH37219).

North Atlantic Treaty Organization (NATO), 2014. NATO Standard AEP-83. Light Unmanned Aircraft Systems Airworthiness Requirements.

NATO Standardization Agency (NSA), 2009. STANAG 4671 - Unmanned Aerial Vehicles Systems Airworthiness Requirments (USAR). Brussels, Belgium.

Paté-Cornell, M.E., 1996. Uncertainties in risk analysis: Six levels of treatment. Reliab. Eng. Syst. Saf. 54 (2–3), 95–111.

Pearl, J., 1997. Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference. Morgan Kaufmann Publishers.

Perez, T., Williams, B., de Lamberterie, P., 2012. Computational aspects of probabilistic assessment of UAS robust autonomy. In: 28th International Congess of the Aeronautical Sciences, Brisbane, Australia.

Perez, T., Williams, B., de Lamberterie, P., 2012. Evaluation of robust autonomy and implications on UAS certification and design. In: 28th International Congess of the Aeronautical Sciences, Brisbane, Australia.

Perez, T., Clothier, R.A., Williams, B., 2013. Risk-management of UAS robust autonomy for integration into civil aviation safety frameworks. In: Australian System Safety Conference (ASSC 2013), Adelaide, Australia. pp. 37–45.

Perez, T., 2013. A Bayesian approach to seakeeping operability computations. In: Pacific 2013 International Maritime Conference: The Commercial, Maritime and Naval Defence Showcase for the Asia Pacific, Barton, ACT, Australia. pp. 572–581.

Press, S.J., 1989. Bayesian Statistics: Principles, Models, and Applications. John Wiley & Sons Inc, New York.

RTCA Special Committee 203 (SC-203), 2013. RTCA DO-344. Operational and Functional Requirements and Safety Objectives (OFRSO) for Unmanned Aircraft Systems (UAS) Standards, vol. 2. Washington D.C.

RTCA, 2007. Guidance Material and Considerations for Unmanned Aircraft Systems. Stand. RTCA DO-304.

SAE ARP4761, 1996. Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment. SAE International.

SAE ARP4754A, 2010. Guidelines for Development of Civil Aircraft and Systems. SAE International.

Uusitalo, L., 2007. Advantages and challenges of Bayesian networks in environmental modelling. Ecol. Modell. 203 (3–4), 312–318.

Washington, A., Clothier, R.A., Williams, B.P., 2017a. A bayesian approach to system safety assessment and compliance assessment for unmanned aircraft systems. J. Air Transp. Manage. 62, 18–33.

Washington, A., Clothier, R.A., Williams, B.P., Silva, J., 2017. Managing uncertainty in the system safety assessment of unmanned aircraft systems. In: 17th Australian International Aerospace Congress: AIAC 17, Melbourne, Vic, Australia, pp. 611–618.

Washington, A., Clothier, R., Silva, J., 2018. Managing uncertainty in unmanned aircraft system safety performance requirements compliance process. In: ICUAS 2018, Amsterdam, Netherlands.

Williams, B.P., Clothier, R., Fulton, N., Lin, X.G., Johnson, S., Cox, K., 2014. Building the safety case for UAS operations in support of natural disaster response. In: 14th AIAA Aviation Technology, Integration, and Operations Conference, Atlanta, USA.

7. Managing Uncertainty in Unmanned Aircraft System Safety Performance Requirements Compliance Process

Figure 13: Concept image of an unmanned aircraft operation over Amsterdam, Europe
Image Copyright © Achim Washington

"A ship in the harbor is safe, but that is not what ships are for"

Admiral Grace Hopper (1906-1992)

This chapter entitled, "Managing Uncertainty in Unmanned Aircraft System Safety Performance Requirements Compliance Process" looks at the challenges and advantages of adopting the proposed risk-based framework for UAS and presents current and envisaged research aimed at addressing these challenges. It focuses on Research Question 2.3 and develops the overall concept for risk-based assessment and compliance regulatory processes which allows for a more comprehensive treatment of uncertainty. This in turn has the potential to result in more rational, transparent and systematic outcomes from the regulatory process, particularly for new or novel aviation systems.

7.1. Statement of Authorship

The authors listed in Table 11 have certified* that:

1. They meet the criteria for authorship (refer to Appendix B: Definition of Authorship) in that they have participated in the conception, execution, or interpretation, of at least that part of the publication in their field of expertise;
2. They take public responsibility for their part of the publication, except for the responsible author who accepts overall responsibility for the publication;
3. There are no other authors of the publication according to these criteria;
4. Potential conflicts of interest have been disclosed to (a) granting bodies, (b) the editor or publisher of journals or other publications, and (c) the head of the responsible academic unit; and
5. They agree to the use of the publication in the student's thesis and its publication on the Australian Digital Thesis database consistent with any limitation set by publisher requirements.

Table 11: Statement of authorship – paper five

Title of Paper:	Managing Uncertainty in Unmanned Aircraft System Safety Performance Requirements Compliance Process			
Contributor	**Areas of contribution and percentage contribution to paper: ***			
	(i)	(ii)	(iii)	(iv)
	Conception and Design	Analysis and Interpretation	Drafting Sections	Critically Revising
Mr Achim Washington	90%	90%	90%	10%
Dr Reece Clothier	10%	10%	10%	60%
Dr Jose Silva				30%
Principal Supervisors confirmation				
I have email or other correspondence from all co-authors confirming their certifying authorship				
Dr Reece Clothier			25th August 2018	
Name			**Date**	
Dr Jose Silva			25th August 2018	
Name			**Date**	
**for further details refer to Appendix B: Definition of Authorship*				

World Academy of Science, Engineering and Technology
International Journal of Mechanical and Mechatronics Engineering
Vol:12, No:5, 2018

Managing Uncertainty in Unmanned Aircraft System Safety Performance Requirements Compliance Process

Achim Washington, Reece Clothier, Jose Silva

International Science Index, Mechanical and Mechatronics Engineering Vol:12, No:5, 2018 waset.org/Publication/10008962

Abstract—System Safety Regulations (SSR) are a central component to the airworthiness certification of Unmanned Aircraft Systems (UAS). There is significant debate on the setting of appropriate SSR for UAS. Putting this debate aside, the challenge lies in how to apply the system safety process to UAS, which lacks the data and operational heritage of conventionally piloted aircraft. The limited knowledge and lack of operational data result in uncertainty in the system safety assessment of UAS. This uncertainty can lead to incorrect compliance findings and the potential certification and operation of UAS that do not meet minimum safety performance requirements. The existing system safety assessment and compliance processes, as used for conventional piloted aviation, do not adequately account for the uncertainty, limiting the suitability of its application to UAS. This paper discusses the challenges of undertaking system safety assessments for UAS and presents current and envisaged research towards addressing these challenges. It aims to highlight the main advantages associated with adopting a risk based framework to the System Safety Performance Requirement (SSPR) compliance process that is capable of taking the uncertainty associated with each of the outputs of the system safety assessment process into consideration. Based on this study, it is made clear that developing a framework tailored to UAS, would allow for a more rational, transparent and systematic approach to decision making. This would reduce the need for conservative assumptions and take the risk posed by each UAS into consideration while determining its state of compliance to the SSR.

Keywords—Part 1309 regulations, unmanned aircraft systems, system safety, uncertainty.

I. Introduction

THE UAS industry is the fastest growing sector of the commercial aviation industry. However, the integration of UAS into the ultra-safe aviation sector poses some challenges. All technologies have associated safety risks. Currently, the majority of UAS do not exhibit the same high reliability shown by conventionally piloted aircraft. A recent study conducted by the Australian Transport Safety Bureau (ATSB) showed that the number of reported Remotely Piloted Aircraft Systems (RPAS) occurrences between January 2012 and December 2016 was approximately 180. The models used to forecast the number of reported occurrences also saw a 60% increase in this number in 2017 when compared with 2016 [1]. To date, the safety risks associated with civil/commercial UAS operations are largely managed through restrictions on their operation [2]. These restrictions include prohibiting their flight over populated regions or in close proximity to people. This can impede the utility of UAS in a wide range of civil and commercial applications.

The risks presented to people and property overflown can be managed through the implementation of a range of technical and operational risk controls [3]. One such control is ensuring a higher degree of airworthiness, and in turn reliability, in the operated system. Airworthiness can be defined as, “the condition of an item (aircraft, aircraft system, or part) in which that item operates in a safe manner to accomplish its intended function” [4]. The item (aircraft, aircraft system, or part) is defined as airworthy if it is certified against the appropriate set of airworthiness regulations. For example, STANAG 4671 establishes the baseline set of airworthiness standards in relation to the design and construction of military UAS [5].

It is now broadly recognised that airworthiness regulations should be tailored to the different UAS types and their Concepts of Operations (CONOPs), and that this tailoring should be governed by the level of risk posed. Further, not all UAS types may be required to meet prescriptive codes of airworthiness requirements in order to be safe for operation. EASA has proposed a risk-based airworthiness regulatory framework that divides airworthiness of UAS into the three categories of: 1) Open, 2) Specific, and 3) Certified [6]. UAS in the Specific and Certified categories are likely to require certification against prescriptive codes of airworthiness requirements (or parts of). These requirements are likely to include compliance to SSR, also referred to as “Part 1309 regulations”.

Compliance with the SSR is a central component to the airworthiness of any aviation system. SSR supplement prescriptive requirements on the design and testing of an aviation system and are, in part, put in place “to ensure that an aircraft is capable of continued safe flight and landing following a failure or multiple failures of systems” [7]. The regulations can be applied to installed sub-systems or an aircraft system as a whole. SSR are briefly discussed in Section II.

There is ongoing debate on the setting of appropriate SSR for UAS [8]. Putting this debate aside, the next challenge lies

Achim Washington is a PhD candidate at the School of Engineering, RMIT University, Melbourne, Australia (corresponding author, e-mail: s3270338@student.rmit.edu.au).

Reece Clothier is a Principal Researcher at Boeing Research & Technology- Australia and Adjunct Associate Professor at RMIT University, Melbourne, Australia (e-mail: reece.a.clothier@boeing.com).

Jose Silva is a Senior Lecturer with the School of Engineering, RMIT University, Melbourne, Australia (e-mail: jose.silva@rmit.edu.au).

International Science Index, Mechanical and Mechatronics Engineering Vol:12, No:5, 2018 waset.org/Publication/10008962

in how to apply the system safety assessment and compliance process to UAS. These challenges are discussed further in Section III. Addressing these challenges is critical to the eventual airworthiness certification of UAS, and subsequently, to enabling UAS operations in increasing populous areas.

There is continuing research into addressing these challenges [9], [10]. This research has focused on how to better account for uncertainty in the System Safety Assessment (SSA) process (as currently used for conventional civil aviation systems) and how to improve compliance findings and decision making in the presence of uncertainty. The revised system safety process described in [9], [10], enables a fundamentally new approach to regulatory decision making, that of making compliance decisions on the basis of risk. The process is particularly suited to UAS and any other aviation system or sub-system where there is limited knowledge and data to base assessments of safety performance.

Section III of this paper summarises the broader research endeavour of existing research [9], [10] and future research. The advantages of these modified frameworks, and application to the SSA of civil/commercial UAS are also described in Section IV.B. The limitations of current research and avenues for extension are presented in Section III.C, with concluding remarks outlined in Section IV.

II. System Safety Regulations (SSR)

SSR are contained in sub-part 1309 of conventionally piloted aircraft airworthiness certification regulations (e.g. CS/FAR 23.1309 [11] for aeroplanes in the normal, utility, acrobatic or commuter category and CS/FAR 25.1309 [12] for aeroplanes in the transport category). They supplement prescriptive standards on the design, manufacture, and installation of aircraft components, and at a high level, specify the requirements for [13]:

- A documented analysis showing that equipment and systems perform as intended under foreseeable operating and environmental conditions;
- The adoption of principles from fail-safe and fault-tolerant design [12]; and
- The demonstration (through a documented qualitative or quantitative analysis) that the expected frequency of failure of equipment and systems, when considered separately and in relation to other systems, is inversely-related to the severity of its effect on the safe operation of the system.

The latter requirement is commonly referred to as the SSPR and is the particular element of SSR that this research is focused on.

The SSPR establishes a minimum acceptable level of reliability of aviation equipment and components. It comprises of three sub-processes, namely the SSA, Compliance Assessment (CA), and Compliance Finding (CF) sub-processes [9]. The sub-processes and the interactions between them are illustrated in Fig. 1 and are discussed further in the following three sub-sections. The limitations of the overall SSPR compliance process are outlined in Subsection II.D.

A. System Safety Assessment Process

The purpose of the SSA process is to identify potential system failures and their safety effect, determine the likelihood of their occurrence, and assign a relevant safety objective. Inputs to the SSA process include component reliability data, expert knowledge, concept of operations, and system baseline description.

The SSA process includes a number of sub-processes that can be applied at different stages of a product lifecycle. Detailed in the SAE ARP 4761 are a range of recommended supporting tools and techniques that can be used within the process, including Fault Tree Analysis (FTA), Failure Modes and Effects Analysis (FMEA), Common Mode Analysis (CMA), etc. [4]. Further details on the SSA process and the tools used in a SSA can be found in [4], [9], [14].

Outputs from the SSA process include:

- a description of identified failure conditions,
- associated assessments of the failure severity category,
- associated assessments of the average probability of failure per flight hour (APFH) of the failure conditions being realised, and
- an assignment of applicable failure probability objective (FPO).

These outputs can be represented by the four sets *F, C, Λ* and *O*, respectively (1)-(4).

$$F = \{f_n : n \in Q\} \tag{1}$$

$$C = \{c_n : n \in Q\} \tag{2}$$

$$\Lambda = \{\lambda_n : n \in Q\} \tag{3}$$

$$O = \{o_n : n \in Q\} \tag{4}$$

The integer set *Q*, given in (5), is used to index an assessment for a specific failure condition (f_n), where N corresponds to the total number of unique failure conditions identified within the SSA process. The output assessment for a specific failure condition (f_n) is described by the tuple given in (6).

$$Q = \{n | n \in \mathbb{Z}^+, n \leq N\} \tag{5}$$

$$< f_n, c_n, \lambda_n, o_n > \qquad where \;\; n \in Q; \tag{6}$$

System safety advisory materials (e.g., [11], [12]) define the qualitative and quantitative scales to be used for the assessment of the failure severity category and APFH. An example of these scales, based on those provided in airworthiness regulations for UAS [7] and manned systems [11], are provided in Tables I-III in the Appendix. The FPO is qualitatively described in the SSR and depends on the particular certification category of the aircraft or component. It is often represented graphically as shown in Fig. 8 of the Appendix.

International Science Index, Mechanical and Mechatronics Engineering Vol:12, No:5, 2018 waset.org/Publication/10008962

B. Compliance Assessment Process

CA can be thought of as a process of determining the degree to which a candidate system meets relevant requirements. Inputs to the CA process are the *N* tuples described in (6). For each assessment, a simple deterministic binary "pass or fail" process is applied, whereby, λ_n (the APFH assessed for a specific failure condition f_n) is compared to its corresponding FPO (o_n) to determine the state of compliance. The state of compliance for the n^{th} identified failure mode, h_n, is true if λ_n is less than o_n, as given in (7):

$$h_n = \begin{cases} True & if\ |\lambda_n| \leq o_n \\ False & otherwise \end{cases} \quad (7)$$

The CA process is undertaken for all *N* assessed failure conditions, with the resulting compliance state assessments contained in the set *H*.

$$H = \{h_n :\ n \in Q\} \quad (8)$$

An overall compliance state of the system, H_S, is determined as *True* if it can be shown that all the assessed APFH satisfy their FPOs (*i.e.*, all h_n are *True*), (9).

$$H_s = \begin{cases} True & if\ h_n = True\ \forall_n \in Q \\ False & otherwise \end{cases} \quad (9)$$

C. Compliance Finding Process

The CF process is a simple deterministic decision-making process. The system is deemed compliant to the Part 1309 SSPR if the following conditions hold:

- H_s is *True*; and
- All necessary documentation on the assessment outcomes, people, tools, and data used as part of the SSA and compliance processes is provided.

If the system is determined to be non-compliant (*i.e.*, H_s = *False*) then an iterative engineering process is usually undertaken to reduce the APFH and/or the failure condition severity, as shown by the dotted line in Fig. 1. It is possible for regulators to declare a system as non-compliant based on insufficient evidence of compliance. In such cases, further information or a reassessment is required (shown as a feedback path in Fig. 1). A system is then deemed as compliant (or not) with the SSPR, with the outcome forming part of its case for certification.

D. Limitation of Current SSPR Compliance Process

The SSA process can be conducted at the component, sub-system, or system level. Each assessment results in a set of outputs described by the tuple defined in (6). These assessments are however conducted independently of each other. Therefore, the interactions and dependencies between these components or sub-systems are not taken into consideration. While the current approach is simple and easy to implement, such dependencies would need to be taken into consideration in order to address the complexity of the overall problem and move towards a risk based approach to regulations.

Another major limiting assumption of the current SSA process is that it assumes a constant failure rate when providing an estimate of the APFH of the system. This essentially implies that the system is a mature system and as such is in the useful life phase of its operational life cycle, which is characterised by a constant failure rate. For new systems like UAS, owing to a number of factors described in the following section, the failure rate is not constant. The inability of the current SSA approach to take the reducing or increasing failure rate of the UAS into consideration is another limiting factor of the approach.

While the current SSPR compliance process does recognise that multiple failure scenarios are possible, it takes the worst-case scenario into account [14], thus failing to take the uncertainty associated with the other scenarios into consideration.

Uncertainty is inherent in every stage of the SSPR compliance process illustrated in Fig. 1. However, the current process does not comprehensively capture this uncertainty. Uncertainty manifests as uncertainty in the SSA process outputs, specifically:

1. *F* – Uncertainty in relation to whether all failure conditions have been identified (completeness), and whether each identified failure condition (f_n), is correctly specified in terms of its modes of failure and potential effects;
2. C – Uncertainty in relation to the estimate of the magnitude of consequential effects and in turn, the severity condition category (c_n) assigned to each of the identified failure conditions in *F*;
3. *Λ* – Uncertainty in relation to the estimate of the APFH (λ_n) for each failure condition;
4. *O* – Whether the correct FPO (o_n) is assigned to each identified failure condition.

The CA decision process described in (9) has no means for accounting for these uncertainties, with the CA output being a binary comparison with two possible outcomes: *True* or *False*. There is no objective means of expressing the resulting uncertainty in the output state of compliance. Consequently, decision makers are unable to objectively account for uncertainty when making compliance findings.

The uncertainty in the SSA process and CA process carries forward to the CF process. Its inescapable existence gives rise to six possible outcomes from the compliance decision making process as described in [9]. These range from certifying a UAS as compliant when it is in fact compliant (desirable outcome) to requiring further data and analysis when the UAS is in fact non-compliant (less than desirable outcome). There is currently no objective and mathematical means for a decision maker to decide between these outcomes. Decision makers use a subjective and somewhat "black box" process to make compliance findings and as such the process lacks the transparency and objectivity required of regulatory decision making.

International Science Index, Mechanical and Mechatronics Engineering Vol:12, No:5, 2018 waset.org/Publication/10008962

III. Challenges in the Application of the SSPR Process to UAS

There are numerous on-going efforts to define suitable SSR for UAS. These include those specified by NATO [5], [15], EASA [16] and EUROCONTROL [17]. There are various points of contention between specifications [8]. Whilst the focus of this debate has been on the specification of the SSR, there has been limited research to date exploring the challenges associated with the application of the traditional SSPR compliance process to UAS; specifically, how to show compliance with the SSR.

UAS are fundamentally different from conventionally piloted aircraft (CPA), not only in the nature of their physical systems and how they are operated but also in the underlying philosophy and engineering processes used in their design and manufacture. These differences lead to unique challenges when it comes to their airworthiness certification. Some of the challenges described in [18], [19] include:

- Challenge associated with the regulatory surveillance enforcement;
- Accounting for the human system interaction in the assessment process;
- Need to certify the UAS based on both the function of the system and properties of the intended operational environment as opposed to just certifying the CPA based on the intended function of the system.
- Need to account for mitigation measures as part of the safety case when certifying the UAS as opposed to looking at the mitigation measures on a case by case basis when evaluating a CPA.

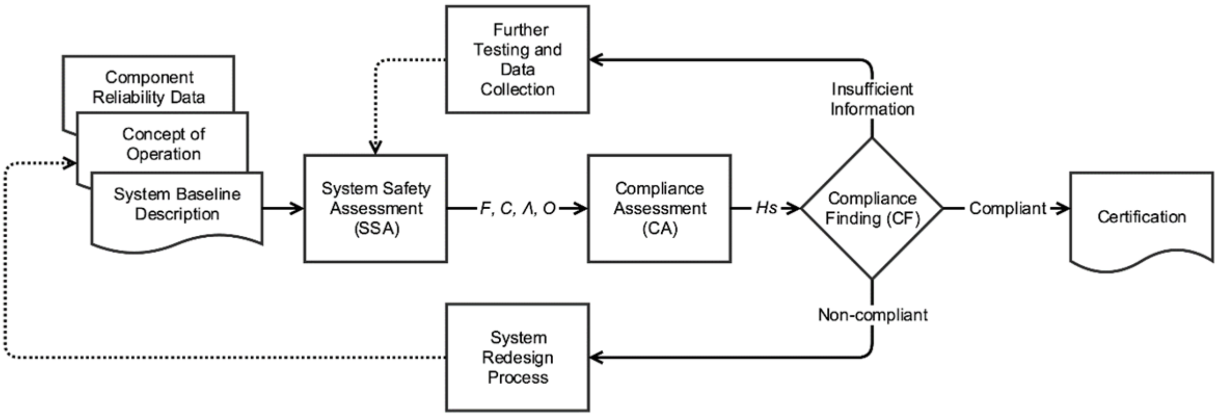

Component Reliability Data
Concept of Operation
System Baseline Description
System Safety Assessment (SSA)
F, C, Λ, O
Compliance Assessment (CA)
Hs
Compliance Finding (CF)
Compliant
Certification
Further Testing and Data Collection
Insufficient Information
Non-compliant
System Redesign Process

Fig. 1 Overview of the SSPR Compliance Process [9]

Further to the general challenges described in [18], [19], there are a number of important differences between UAS and CPA that can impact their certification:

- **Design philosophy** – many UAS have a different design trade space than CPA. For many UAS, system reliability can be determined by a trade-off between capability, cost, and restrictions on their operation. For manned aircraft, there is always a hard limit to this trade, dictated by the minimum reliability and system performance required to ensure the safety of those on-board. Some of the main issues in adopting new technologies such as UAS that impact this trade space are described in [20].
- **Engineering processes** – currently, many civil/commercial UAS are designed and manufactured in non-traditional aviation engineering environments. Many small UAS are designed by hobbyist, modelling and remote control flying enthusiasts. As a consequence, many UAS lack the supporting documentation, and systems engineering rigour that would be expected in the engineering of a CPA. This body of evidence is a key input to the SSPR process.
- **Technology refresh rate** – UAS types are rapidly evolving. A study conducted in [21] shows how technologies that are central to UAS have improved at a rapid pace over the years. This is driven by the need to 1) keep pace with new capability in component technologies (*e.g.*, new battery, sensing, autopilot, and communications sub-systems), 2) meet new and emerging requirements of new customers, and 3) to ensure that their product-offering is at the forefront of current capability. The high refresh rate coupled with the use of Commercial Off the Shelf (COTS) components makes it difficult to collect reliability data on systems and components.
- **Changing certification baseline** – Many UAS lack a static design baseline against which a certification case can be established. This stems from the high technology refresh rate and the customer demand for flexible and reconfigurable systems capable of performing a variety of missions. As a consequence, it can be difficult to develop significant safety heritage in a particular system configuration. In contrast, CPA have a relatively static system baseline. This allows safety data to be gathered for a single aircraft type or across the entire fleet of a particular aircraft type.
- **Unassured components** – UAS make extensive use of COTS components. COTS components are generally not designed, manufactured, or tested to an approved standard and therefore lack the necessary assurance of normal aviation components. These standards are an important input to the SSA process.

- **Lack of knowledge** – In general there is a lack of domain expertise in the design and operation of civil/commercial UAS when compared to CPA. This is owing to the relative infancy of the sector and restrictions on their operation. Expert judgment in relation to UAS design and operations is a key input to the SSA process. The lack of knowledge gives rise to uncertainty in the SSA process. This uncertainty can be in relation to known parameters or even unknown parameters (parameters that can impact the model but have not been taken into consideration owing to the lack of information available on them). Currently there is no means of representing this knowledge uncertainty in the SSA process.
- **Heterogeneity of fleet and operations** – There is significant diversity in the types, configurations, performance, and operational profiles of civil/commercial UAS. A study conducted in [19] shows that the Maximum Take-Off Weight (MTOW) of the UAS fleet ranged from a few grams to hundreds of tonnes, whereas for the CPA fleet, the MTOW ranged from a few hundred kilograms through to thousands of tonnes. Similarly, as can be seen from Fig. 2, there is significant diversity in the type of operations of the UAS as well. The heterogeneity of the UAS fleet and their operations makes it difficult to base assessments and develop knowledge through comparison.

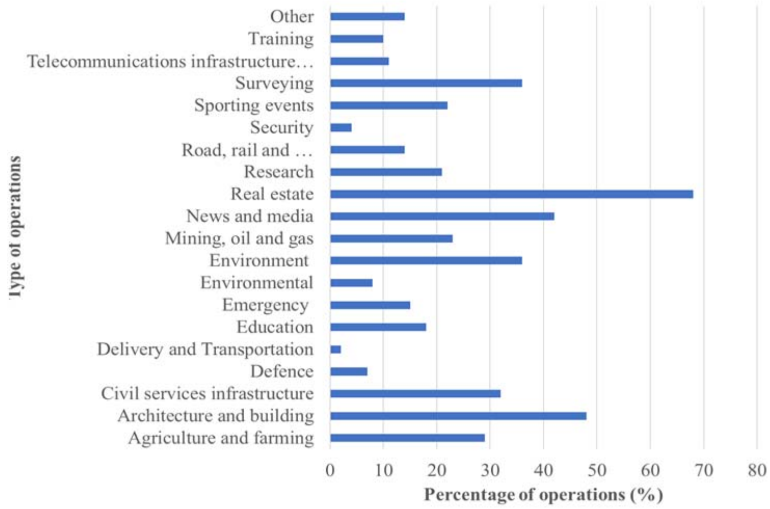


Fig. 2 Diversity in types of UAS operations, based on [22]

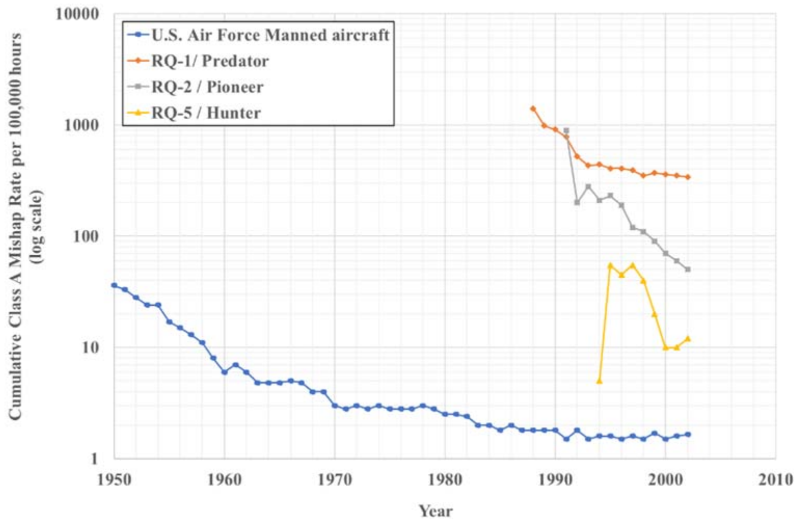


Fig. 3 Comparison of cumulative mishap rate based on [23]

- **Changing failure rate-** The current SSPR compliance process assumes a constant failure rate as CPA are mature systems that are in the useful life phase of their life-cycle. This assumption cannot be made for UAS as these systems are still relatively new and are in the infant mortality phase of their life-cycle. Factors like the design philosophy, technology refresh rate, use of COTS all contribute to systems with a dynamic baseline. Thus, the failure rate of many systems might never reach a stable/constant value. An example of the mishap rate for

UAS compared to manned systems based on [23] is shown in Fig. 3. From this, it can be seen that the mishap rate of the UAS has still not reached a constant value, while that for manned aircraft has become relatively stable. The limited data available on UAS compared to manned aircraft can also be seen here.

As a result of these differences, there is a general lack of knowledge and operational data, and a lack of trust in the data and knowledge that is available, to support airworthiness assessment and compliance finding processes for UAS. There can be considerable uncertainty associated with the certification of civil/commercial UAS, which in turn can lead to high certification risk (i.e., the risk associated with certifying a UAS as compliant, and therefore safe for operation, when indeed it is not).

The SSPR compliance process as used for the certification of CPA does not adequately account for the high uncertainty inherent to the SSA of UAS. System safety guidance materials [4], [11], [12], [14], [24] make no explicit mention of uncertainty, its measurement or treatment as part of a SSA. Reference [14] acknowledges that a failure mode can potentially have a range of negative impacts on the safety of flight. In such cases, the recommended practice is to assign the highest potential severity category c_n. In so doing, uncertainty in the set of potential consequential outcomes is discarded and can result in an overly conservative failure probability objective being assigned to the system. While this may not adversely impact the safety of the general public, it does result in the imposition of unnecessarily stringent restrictions on the design of UAS. This in turn comes at the cost of capability and system cost.

The reliability of a UAS can be improved in a number of ways including, investing in more advanced and expensive components that have been designed to higher standards and installation of redundant systems to use in case of emergencies. While it is important to have a UAS with components that are designed to a certain level of reliability and with redundant systems put in place, this needs to be balanced with the cost (both in terms of monetary costs and costs in terms of added weight, volume and power consumption to the system) involved in installing these components and the risk posed by having systems with lower reliability. The added components would result in a reduced payload capacity, range and endurance, thus limiting the potential applications.

Taking all of this into consideration, it is clear that research needs to be conducted into improving the current SSPR compliance process so that it is capable of taking the unique characteristics associated with UAS into consideration.

IV. Improving the SSPR Compliance Process

A new approach to regulatory compliance is to consider it as a problem of decision making under uncertainty. Jaynes [25] describes the desiderata of rationality and consistency for plausible reasoning in the presence of uncertainty. Based on this, decision makers can only make inferences (or propositions) about the state of the world based on the uncertain knowledge and information at hand. Bayesian inference provides a means for measuring uncertainty in relation to these hypotheses by producing information based on models, data, and other information [26]. In addition to this, Bayesian inference also allows for the state of knowledge (degree of belief in the hypothesis) to be progressively updated as new data or experience in the operation of the system is gained. Decisions are made on the basis of objective measures of uncertainty (or by extension, measures of risk) as opposed to binary statements of compliance. This approach to safety compliance has been explored for autonomous ships [27] and for showing assurance in autonomous UAS performance [28]. Within a safety assessment context, Bayesian approaches have been extensively used in the probabilistic risk assessment of space launch activities [29], [30] and nuclear power generation [31]. Such assessments are characterised as complex and based on sparse data; characteristics common to the SSA of UAS.

A. Extended SSPR Compliance Process

References [9] and [10] have begun to apply this general approach to the SSPR compliance process for UAS. The research to date has focused on addressing only the uncertainty in relation to the assessment of the APFH for individual failure conditions. The modified approach is illustrated in Fig. 6 and briefly described in this section. For further details the reader is directed to [9].

The principle modification lies in the SSA process, specifically, the quantification of the APFH. As described in Section II, the output set Λ contains point value assessments of λ_n of the APFH for each failure. This is depicted graphically in Fig. 4. Under the extended approach of [9], Bayesian methods are used to characterise the state of knowledge in each assessment of APFH as opposed to the value of λ_n. The modified output from the SSA process is the set Λ^*, which comprises N conditional probability distributions describing the uncertainty (or degree of belief) in λ_n. The probability distributions obtained replace the point-value assessments of the APFH originally output from the SSA process, as illustrated in Fig. 5. Each probability distribution, denoted by $p(\lambda_n|D,I)$ and given in (10) represents the state of knowledge in APFH for the given failure condition, where D represents data and I the knowledge and information available.

$$\Lambda^* = \{p(\lambda_n|D,I) : n \in Q\} \tag{10}$$

As shown in Fig. 6, these distributions are input to the CA process. Various inference approaches (hypothesis testing and Bayesian prediction) can be used to provide a measure of the uncertainty in the state of compliance with the FPO. The simple deterministic *True* or *False* output of the CA process is replaced by measures describing the degree of certainty in the state of compliance (*i.e.*, system failure meets its assigned FPO, o_n). Referring to Fig. 5, this can be visualised as the area under the curve that resides in the "acceptable" region.

As shown in Fig. 6, the CA uncertainty measures are then input to the CF process, which, in [9], has been structured as a simple normative decision-making problem. Whilst many possible decision making formulations could be adopted, the normative approach ensures an objective, transparent, and systematic input to decision making. From [9], there are six possible outcomes from the CF process:

- The UAS is deemed to be compliant when it is actually compliant;
- The UAS is deemed to be compliant but it is actually non-compliant;
- The UAS is deemed to be non-compliant but it is actually compliant;
- The UAS is deemed to be non-compliant when it is actually non-compliant;
- There is insufficient information in the state of compliance when the UAS is actually compliant;
- There is insufficient information in the state of compliance when the UAS is actually non-compliant.

A loss/benefit function can be assigned to each possible outcome and combined with the uncertainty measures to provide measures of the compliance risk. A range of objective decision utility functions can then be applied to aid the regulator in making the best compliance decision (Reference [9] applied a simple minimum-risk decision selection function).

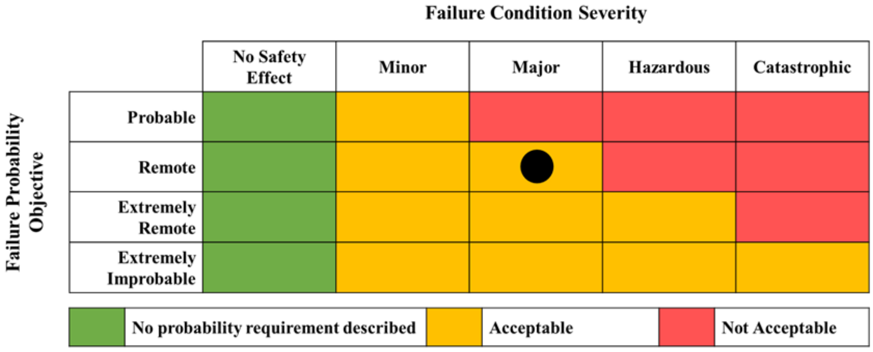


Fig. 4 Output from traditional SSA approach

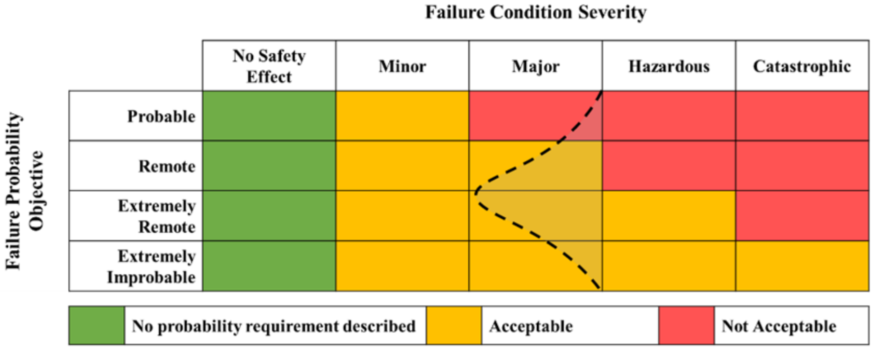


Fig. 5 Output from extended SSA approach

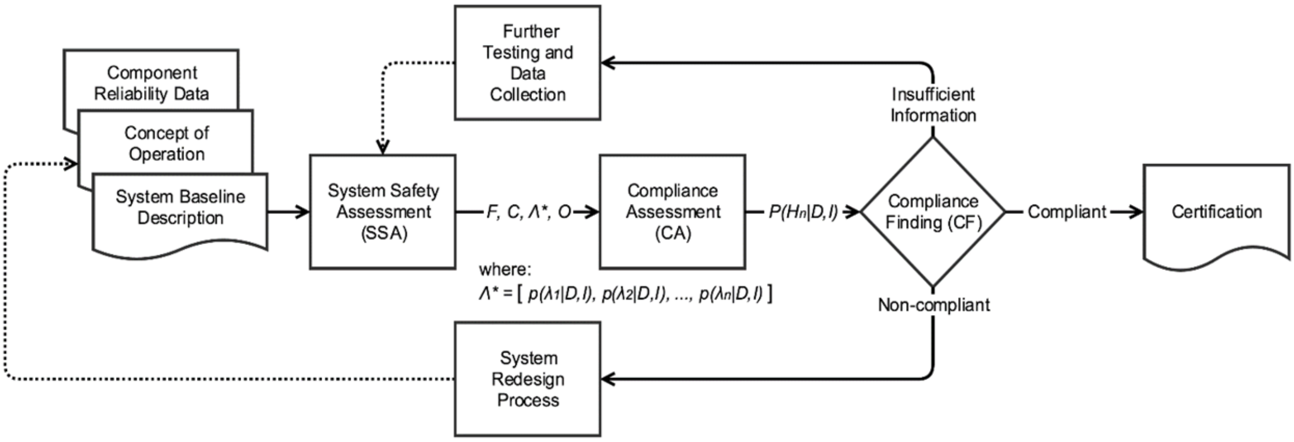

Component Reliability Data
Concept of Operation
System Baseline Description
Further Testing and Data Collection
System Safety Assessment (SSA)
F, C, Λ*, O
where:
Λ* = [p(λ1|D,I), p(λ2|D,I), ..., p(λn|D,I)]
Compliance Assessment (CA)
P(Hn|D,I)
Insufficient Information
Compliance Finding (CF)
Compliant
Certification
Non-compliant
System Redesign Process

Fig. 6 Overview of the extended SSPR Compliance Process [9]

International Science Index, Mechanical and Mechatronics Engineering Vol:12, No:5, 2018 waset.org/Publication/10008962

B. General Advantages

The approach provides a more transparent, rational, and systematic compliance decision-making process. It proposes a significant change to how aviation safety practitioners currently undertake regulatory compliance activities. The application of such an approach provides a:

- more comprehensive means for assessing and treating uncertainties inherent to the SSA of an aviation system;
- mathematically robust means for combining data with expert judgement in safety assessments;
- means to support inductive and deductive reasoning in relation to the system safety of UAS (e.g., predictive assessments or incident analysis);
- framework that is compatible with existing system safety modelling and analysis tools (e.g., Functional Hazard Assessments (FHA), Failure Mode Effects and Criticality Analysis (FMECA), Fault Tree Analysis (FTA), etc.);
- mathematically robust means for updating the state of knowledge as new data or operational experience is gained (a useful feature for rapidly evolving systems such as UAS);
- framework that supports more justifiable and systematic compliance findings;
- method for making airworthiness compliance decisions based on compliance risk;
- means for ensuring more transparent, objective, and consistent compliance findings in the presence of uncertainty; and
- means to reduce the need for conservative assumptions and the subsequent impost of unnecessary costs on the UAS industry.

C. Further Evolutions of the SSPR Compliance Process

The revised SSPR compliance process represents a paradigm shift in regulatory compliance. However, there remain a number of opportunities to further enhance the process to take better account of the issues identified in Section III.

The traditional SSA process assumes that failures occur at a constant rate. The same assumption was made in the approach developed in [9] through the use of a Poisson likelihood distribution. The assumption of a constant failure rate fails to account for the variable failure rate characteristic of most new systems like UAS (as described in Section III). The model presented in [10] addresses this shortcoming by adopting a Weibull distribution as the likelihood distribution.

There is also a need to extend the SSPR process to account for the uncertainty in the remaining outputs of the SSA process. For example, a single failure can have more than one failure mode, and in turn, different consequential effects. The uncertainty in relation to these different scenarios can also differ. This in turn can lead to uncertainty in the assignment of the correct FPO. This uncertainty has traditionally been addressed through the assignment of the worst case consequential outcome, which, as described previously, can lead to overly conservative requirements on the reliability of the system. This is a consequence driven as opposed to a risk driven regulatory approach. A means for capturing and representing all potential consequential outcomes (and in turn risk) associated with potential failure conditions is needed. The output for a single failure condition would thus be a set of assessments, conceptually shown in Fig. 7.

SSA processes make use of a wide range of data sources. From component reliability test data, incident, and accident reports, through to expert judgment based on operational experience or technical knowledge. Data uncertainty has yet to be fully accounted for in the current SSA approach. Current SSA guidelines recommend the use of sensitivity analysis, which does not account for biases, missing, or erroneous data. There are various techniques for accounting for input data uncertainty within a Bayesian context, which could be adopted and applied to the specific problem of UAS failure modelling.

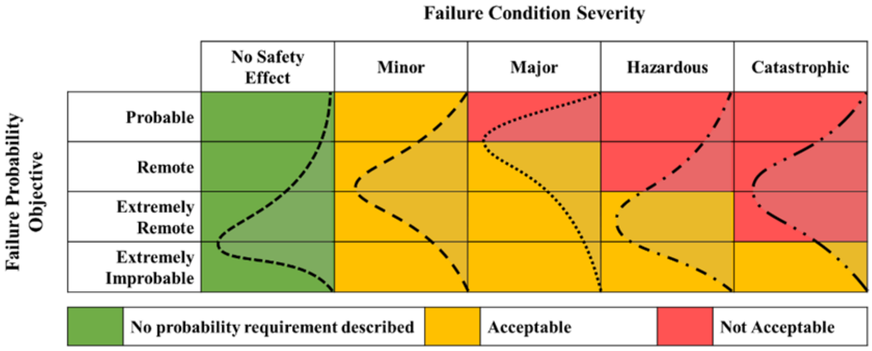


Fig. 7 Desired output from SSA approach

The current SSPR framework assumes independence in failure conditions and their management. This is largely necessitated by the need to manage complexity. The FPOs are derived from an apportionment of a system-level acceptable failure rate to individual failure conditions. Implicit to this apportioning is the assumption of independence. Common mode failures are considered in current SSA processes, however, the combined assessment and management of all failure conditions accounting for the dependencies between them, is not undertaken at the system level. Consequently, there is no guarantee the overall system-level safety objective is met.

More advanced modelling approaches are required to address these challenges. One such approach is through the use of Bayesian Belief Networks (BBN), which are particularly suited to higher level system modelling. Examples of the application of BBN to aviation operational risk modelling include [32]−[34]. These techniques have yet to be applied within the framework of a formal SSA within the SSPR compliance process.

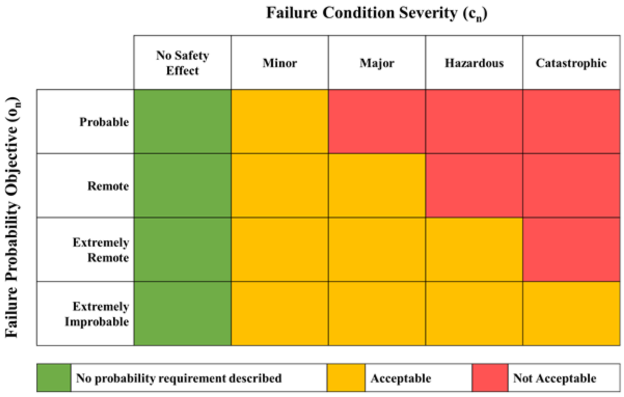
V. Conclusion

System safety is a critical component of the airworthiness certification of UAS. Assurance in the airworthiness of UAS is needed to enable greater freedom of their operation in non-segregated airspace and over increasingly populous areas. Whilst research to date has focused on the specification of the SSR for UAS, there has been little effort directed towards understanding the suitability of existing regulatory compliance processes.

This paper has highlighted a number of challenges to the application of existing system safety compliance process to UAS. It is found that a more comprehensive treatment of the uncertainties inherent to the SSA of UAS is needed. Potential approaches for achieving this are presented.

UAS are revolutionising all aspects of aviation – the introduction of new technology, autonomy, operations, and airspace design and manufacturing processes. This evolution extends to the fundamental philosophy and approach to the safety regulation of aviation. Through UAS, there is the opportunity to reassess and evolve longstanding regulatory practices; potentially bringing them in line with more contemporary principles for safety management and decision making. An example of this is the move towards risk-based regulation for the UAS sector, a regulatory development principle that has equal applicability to all aviation sectors. With this in mind, the fundamental theory, process, and techniques explored within this paper have broader applicability to the aviation sector.

Appendix



Failure Probability Objective (o_n)	No Safety Effect	Minor	Major	Hazardous	Catastrophic
Probable	🟩	🟨	🟥	🟥	🟥
Remote	🟩	🟨	🟨	🟥	🟥
Extremely Remote	🟩	🟨	🟨	🟨	🟥
Extremely Improbable	🟩	🟨	🟨	🟨	🟨

Fig. 8 Risk matrix showing FPO based on [7]

TABLE I
Qualitative Description of Failure Severity Categories for UAS Based on [7]

No Safety Effect

Failure conditions that would have no effect on safety.
For example, failure conditions that would not affect the operational capability of the RPAS or increase remote crew workload.

Minor

Failure conditions that would not significantly reduce RPAS safety and that involve remote crew actions that are within their capabilities. Minor failure conditions may include a slight reduction in safety margins or functional capabilities, a slight increase in remote crew workload, such as flight plan changes.

Major

Failure conditions that would reduce the capability of the RPAS or the ability of the remote crew to cope with adverse operating conditions to the extent that there would be a significant reduction in safety margins, functional capabilities or separation assurance. In addition, the failure condition has a significant increase in remote crew workload or impairs remote crew efficiency.

Hazardous

Failure conditions that would reduce the capability of the RPAS or the ability of the remote crew to cope with adverse operating conditions to the extent that there would be the following;

- Loss of the RPA [Remotely Piloted Aircraft] where it can be reasonably expected that a fatality will not occur, or
- A large reduction in safety margins or functional capabilities, or
- High workload such that the remote crew cannot be relied upon to perform their tasks accurately or completely.

Catastrophic

Failure conditions that could result in one or more fatalities

TABLE II
Qualitative Description of Failure Probability Objectives for Manned Aircraft [11]

Probable

Those failure conditions anticipated to occur one or more times during the entire operational life of each airplane. These failure conditions may be determined on the basis of past service experience with similar components in comparable airplane applications.

Remote

Those failure conditions that are unlikely to occur to each airplane during its total life but that may occur several times when considering the total operational life of a number of airplanes of this type.

Extremely Remote

Those failure conditions not anticipated to occur to each airplane during its total life, but which may occur a few times when considering the total operational life of all airplanes of this type.

Extremely Improbable

For commuter category airplanes, those failure conditions so unlikely that they are not anticipated to occur during the entire operational life of all airplanes of one type. For other classes of airplanes, the likelihood of occurrence may be greater.

TABLE III
Quantitative Description of FPO for UAS[1] [7]

FPO	Quantitative value (APFH)
Probable	$< 10^{-3}$ hr^{-1}
Remote	$< 10^{-4}$ hr^{-1}
Extremely Remote	$< 10^{-5}$ hr^{-1}
Extremely Improbable	$< 10^{-6}$ hr^{-1}

Acknowledgment

This research was supported, in part by, the Australian Government Research Training Program Scholarship, provided by the Australian Government.

[1] FPO described using Average Probability per Flight Hour

REFERENCES

[1] ATSB, "A safety analysis of remotely piloted aircraft systems," 2017.

[2] CAA, "CAP-722, Unmanned Aircraft System Operations in UK Airspace - Guidance," London UK Civil Aviation Authority (CAA), Department of Transport (DfT), London, UK, 2015.

[3] R. A. Clothier, B. P. Williams, and K. J. Hayhurst, "Modelling the Risks Remotely Piloted Aircraft Pose to People on the Ground," *Saf. Sci.*, vol. 101, pp. 33–47, 2018.

[4] SAE ARP 4761, "Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment." SAE International, 1996.

[5] NATO Standardization Agency (NSA), "STANAG 4671 - Unmanned Aerial Vehicles Systems Airworthiness Requirments (USAR)," Brussels, Belgium, 2009.

[6] EASA, "'Prototype' Commission Regulation on Unmanned Aircraft Operations - Explanatory Note," 2016.

[7] JARUS Working Group 6, "Safety Assessment of Remotely Piloted Aircraft Systems," *AMC RPAS.1309*, no. 2, 2015.

[8] EUROCAE, "UAS / RPAS Airworthiness Certification '1309' System Safety Objectives and Assessment Criteria," MALAKOFF, France, 2013.

[9] A. Washington, R. A. Clothier, and B. P. Williams, "A Bayesian Approach to System Safety Assessment and Compliance Assessment for Unmanned Aircraft Systems," *J. Air Transp. Manag.*, vol. 62, pp. 18–33, 2017.

[10] A. Washington, R. A. Clothier, B. P. Williams, and J. Silva, "Managing Uncertainty in the System Safety Assessment of Unmanned Aircraft Systems," in *17th Australian International Aerospace Congress: AIAC 17, Melbourne, Vic, Australia*, 2017, pp. 611–618.

[11] FAA, "Advisory Circular 23.1309-1E, System Safety Analysis and Assessment for Part 23 Airplanes.," 2011.

[12] FAA, "Advisory Circular 25.1309-1A, System Design and Analysis," US Department of Transportation, Federal Aviation Administration, 1988.

[13] R. A. Clothier and P. P. Wu, "A Review of System Safety Failure Probability Objectives for Unmanned Aircraft Systems," in *11th International Probabilistic Safety Assessment and Management (PSAM11) Conference and the Annual European Safety and Reliability (ESREL 2012) Conference, Helsinki*, 2012.

[14] SAE ARP 4754A, "Guidelines for Development of Civil Aircraft and Systems." SAE International, 2010.

[15] NATO Standardization Agency, "AEP-83, Light Unmanned Aircraft Systems Airworthiness Requirements," 2014.

[16] EASA, "E.Y013-01 Policy Statement Airworthiness Certification of Unmanned Aircraft Systems (UAS)," 2009. (Online). Available: https://easa.europa.eu/system/files/dfu/E.Y013-01_ UAS_ Policy.pdf. (Accessed: 23-Oct-2015).

[17] JAA/EUROCONTROL, "UAV Task-Force Final Report: A concept for European regulations for civil unmanned aerial vehicles (UAVs)," 2004.

[18] R. Clothier, B. P. Williams, J. Coyne, M. Wade, and A. Washington, "Challenges to the Development of an Airworthiness Regulatory Framework for Unmanned Aircraft Systems," in *16th Australian International Aerospace Congress (AIAC 16)*, 2015, pp. 87–98.

[19] R. A. Clothier, J. L. Palmer, R. A. Walker, and N. L. Fulton, "Definition of an airworthiness certification framework for civil unmanned aircraft systems," *Saf. Sci.*, vol. 49, no. 6, pp. 871–885, 2011.

[20] R. A. Clothier, N. L. Fulton, and R. A. Walker, "Pilotless aircraft: the horseless carriage of the twenty-first century?," *Journal of Risk Research*, vol. 11, no. 8. pp. 999–1023, 2008.

[21] M. Elbanhawi, A. Mohamed, R. Clothier, J. L. Palmer, M. Simic, and S. Watkins, "Enabling technologies for autonomous MAV operations," *Prog. Aerosp. Sci.*, vol. 91, pp. 27–52, 2017.

[22] R. Clothier, "Turning Hype into Reality: Unmanned Aircraft Systems and the Challenges Ahead." AAUS, 2016.

[23] Department of Defense, "Unmanned Aerial Vehicle Reliability Study," United States of America, 2003.

[24] SAE ARP 5150, "Safety Assessment of Transport Airplanes in Commercial Service," 2013.

[25] E. T. Jaynes, *Probability Theory: The Logic of Science*. Cambridge University Press, 2003.

[26] H. Dezfuli, D. Kelly, C. Smith, K. Vedros, and W. Galyean, "Bayesian Inference for NASA Probabilistic Risk and Reliability Analysis," *NASA/SP-2009-569*, 2009.

[27] T. Perez, "Ship seakeeping operability, motion control, and Autonomy - A Bayesian Perspective," *IFAC -PapersOnline*, pp. 217–222, 2015.

[28] T. Perez, R. A. Clothier, and B. Williams, "Risk-management of UAS Robust Autonomy for Integration into Civil Aviation Safety Frameworks," in *Australian System Safety Conference (ASSC 2013)*, 2013, pp. 37–45.

[29] S. Guarro, "Risk assessment of new space launch and supply vehicles," in *11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012, PSAM11 ESREL 2012*, 2012, pp. 5157–5164.

[30] S. D. Guikema and M. E. Pate-Cornell, "Bayesian Analysis of Launch Vehicle Success Rates," *J. Spacecr. Rockets*, vol. 41, no. 1, pp. 93–102, 2004.

[31] United States Nuclear Regulatory Commission, "Reactor safety Study. An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," 1975.

[32] E. Ancel, F. M. Capristan, J. V. Foster, and R. C. Condotta, "Real-time Risk Assessment Framework for Unmanned Aircraft System (UAS) Traffic Management (UTM)," in *17th AIAA Aviation Technology, Integration, and Operations Conference,Denver, Colarado*, 2017.

[33] L. C. Barr, R. L. Newman, E. Ancel, C. M. Belcastro, J. V. Foster, J. K. Evans, and D. H. Klyde, "Preliminary Risk Assessment for Small Unmanned Aircraft Systems," in *17th AIAA Aviation Technology, Integration, and Operations Conference, Denver, Colarado*, 2017.

[34] B. J. M. Ale, L. J. Bellamy, R. van der Boom, J. Cooper, R. M. Cooke, L. H. J. Goossens, A. R. Hale, D. Kurowicka, O. Morales, A. L. C. Roelen, and J. Spouge, "Further development of a Causal model for Air Transport Safety (CATS): Building the mathematical heart," *Reliab. Eng. Syst. Saf.*, vol. 94, no. 9, pp. 1433–1441, 2009.

8. Discussion and Conclusions

Figure 14: Boeing X-45 model in National Air and Space Museum, Washington, DC
Image Copyright © Achim Washington

This chapter aims to summarise the main findings made in relation to each of the publications contained in Chapter 3 to Chapter 7, and relate this to the overall aim, objectives and research questions outlined previously in this thesis. Section §8.1 provides an in-depth discussion highlighting the main contributions of the chapters, how they relate to each other and how they relate to the overall thesis. Section §8.2 then summarises the novel contributions of the overall thesis, with avenues of future research highlighted in Section §8.3. Closing remarks are then provided in Section §8.4

8.1. Discussion

Over the course of this thesis, the individual papers presented in Chapter 3 through to Chapter 7 address different elements of the overall research questions that were identified in Section §1.2. Each chapter on its own makes a number of novel contributions to theory and when viewed in conjunction with each other they help address the overall aim of the thesis, which is to "improve regulatory outcomes under the new paradigm of risk-based regulation, through providing a conceptual framework for the rational, transparent and systematic treatment of uncertainty in the risk assessment and regulatory decision-making process”. This section will provide a summary of the contributions of each chapter, highlighting the differences that exist between them and relating them to the overall research questions and objectives of the thesis. The novel contributions, while summarised in Section §8.2, have been outlined here on a chapter by chapter basis to provide a clear indication of how they were achieved.

8.1.1. Chapter 3: A Review of Unmanned Aircraft Systems Ground Risk Models

A risk-based approach to the regulation of the industry requires a risk-based approach to rule-making, compliance assessment and compliance finding. Focusing on the risk-based approach to rule-making, it was clear that a means of capturing the risks posed by UAS to people and property on the ground (primary hazard of interest) and a means of relating this risk to different components of the regulation was needed. Based on a review of the literature it was evident that GRM are commonly used in the industry to identify and characterise these risks. This chapter summarised the current state of the art with respect to GRM, identifying the various component models that go into defining these GRM. A review was undertaken for each of the component models, which provides: a detailed description of the component model; a review of the literature highlighting the current state of the art with respect to the component model; a summary of how the component model is substantiated in the literature; a detailed analysis of the sources of uncertainty and how they are taken into consideration (including the level of uncertainty) with respect to each component model; and finally a clear linkage between the component model and the component of the regulations that they impact, highlighting the implications of the level of treatment of uncertainty with respect to these component models. The conceptual framework developed in this chapter provides the theoretical basis which can be used to help support the development of GRM.

In developing this conceptual framework and analysing the models identified in the literature, a number of high-level findings were made. Firstly, it was seen that there exists a significant amount of diversity in the GRM (and component sub-models). The diversity amongst these models can lead to a lack of consensus and variability in the risk assessment outputs that are input into the regulatory decision-making process and can thus impact the risk-based approach to compliance assessment and compliance finding as well. Secondly, it was observed that a majority of these GRM (and component sub-models) are based on a number of conservative assumptions, the cascading impact of which have not been evaluated in the context of these GRM. These assumptions are mostly implicit and undocumented, and where explicit, their impact on the resulting assessments of risk are not explored. A series of conservative assumptions can lead to overly conservative risk estimates, and in turn, impose unnecessary regulatory costs on the industry. Finally, it was evident that there exists a considerable amount of diversity in the level of uncertainty taken into consideration by each of the component sub-models, with a majority of the models only taking lower levels of uncertainty into consideration. When considered in the context of supporting the development of regulations for UAS, this diversity and limited treatment of uncertainty in each of the component sub-models of the GRM can hamper objective decision-making in relation to the regulations. This can thus prevent the adoption of a more transparent, systematic and consistent regulatory decision-making process, something necessary for the development of justifiable regulations that have a clear and traceable relationship to the safety risks they are intended to manage. In developing a GRM it is imperative to take these factors into consideration.

The focus of this chapter was thus on Research Question 1. It clearly identifies the sources of uncertainty associated with the safety risk assessment process, detailing how they are being characterised and represented in existing models using Paté-Cornell's [33] "six levels of treatment of uncertainties in risk analysis" framework (Research Question 1.1). By relating the uncertainty associated with each of these component models to the regulations and seeing how the different levels of uncertainty can impact these regulations, the research highlighted the need to apply a Level 5 (displaying uncertainties about fundamental hypotheses by a family of risk curves) treatment of uncertainty to the existing aviation safety risk management and regulatory development processes (Research Question 1.2). The six levels of treatment of uncertainty identified by Paté-Cornell [33] clearly show how the risk and uncertainty measures obtained from the regulatory safety risk assessment processes can be represented to decision makers (Research Question 1.3). While it is evident that a Level 5 treatment of uncertainty is most beneficial, discussion relating to which of these levels best supports regulatory decision-making was provided in the later chapters.

By answering these research questions, this chapter partially addresses the first research objective which was to "identify and characterise the various sources of uncertainty inherent in risk assessment and decision-making processes and determine how this is currently managed, with application to the aviation regulatory framework".

The paper presented in this chapter is one of the first of its kind, not only providing an in-depth review of the component sub-models but also showing how they take uncertainty into consideration and how this impacts the associated regulations. In addition, based on the extensive literature review undertaken, a set of generic component sub-models that need to be taken into consideration in developing a GRM were identified. Future research can look at how to relate each of these component sub-models to different risk metrics (e.g. Failure Metric, Hazard Metric, Economic Risk Metric, Individual Risk Metric, Collective Risk Metric and Societal Risk Metric) to see how they can impact the overall SRMP and consequently how they can be used to help the adoption of a risk-based approach to compliance assessment and compliance finding. By clearly outlining the component sub-models and describing how they relate to each other, this paper provides a conceptual framework for describing the component sub-models of GRM, and in turn, providing a general theoretical basis for the systematic development and analysis of models proposed in the literature. Taking the overall objectives of the thesis into consideration, in undertaking the review, it was considered important to see how each of the component sub-models accounted for uncertainty. The paper thus identifies various sources of uncertainty with respect to each of the component sub-models and shows how failing to account for such uncertainties can impact different elements of the regulation. For example, looking at the failure model it was observed that there is significant uncertainty (epistemic and aleatory) in the identification and modelling of failures for UAS. This uncertainty arises due to several factors including a lack of reliability data, the changing system configurations, use of non-certified components, and limited operational experience. This often results in the imposition of conservative restrictions on these systems, more stringent failure probability objectives and conservative design performance criteria for components. This in turn can have implications on the design, production, testing, and certification of these systems. Similar findings were made in relation to each of the remaining component sub-models as well. This was an important component of the research as it directly feeds into the risk management process which in itself is the focus of the remaining chapters.

8.1.2. Chapter 4: A Bayesian Approach to System Safety Assessment and Compliance Assessment for Unmanned Aircraft Systems

While the previous chapter focused on the models used to help identify and characterise the risk, this chapter (as well as the following chapters) focused on how to make compliance findings based on compliance risk, taking uncertainty into consideration. Using the case study of the SSR, the paper aimed to identify the various sources of uncertainty associated with the Traditional SSPR compliance process and look at how some of these sources of uncertainty were taken into consideration to support more objective, transparent and rational compliance findings in those cases where there is uncertainty associated with the assessment of the system. The paper outlines the structure of the Traditional SSPR compliance process, identifies the sources of uncertainty associated with this process, shows how some of these sources of uncertainty can be taken into consideration (using Bayesian analysis, Bayesian hypothesis testing and normative Decision theory) and proposes an Extended SSPR compliance process that takes this uncertainty into consideration. Avenues for future research (some of which are undertaken in the proceeding chapters) were also identified in this chapter.

The general lack of data and experience in the operation of civil UAS gives rise to uncertainty in relation to all aspects of their performance. The Traditional SSPR compliance process does not provide a means of taking this uncertainty into consideration in either the SSA or the CA and CF decision-making processes that follow. A comprehensive treatment of uncertainty is required for more rational, objective and consistent compliance decision-making. Focusing on the SSPR compliance process, this chapter provides a means of capturing the uncertainty in not only the SSA process (through the adoption of a Bayesian analysis approach) but also the CA process (through the adoption of a

Bayesian hypothesis test) and the CF process (through the adoption of normative decision theory) that follow. While this marks a significant step forward compared to traditional approaches, there were a number of assumptions made and a number of areas where future research effort could be directed. Firstly, the extended framework presented in this chapter does not provide a means of taking the uncertainty in the data input to the model into consideration. Secondly, looking at the SSA process, it is clear that the extended framework only allows for uncertainty in one of the outputs (*i.e.* APFH) to be taken into consideration. The uncertainty in the remaining outputs (*i.e.* failure condition descriptions, failure condition severities and failure probability objectives) have not been addressed. Finally, focusing on the SSA process, in accordance with the system safety guidelines, a common Poisson failure rate model (which assumes a constant failure rate) is adopted. While such an assumption might be suitable for well-established and mature aviation systems, it may not be suitable for small UAS owing to a number of factors such as the changing system-baseline. This brings into question the validity of the assumption of a constant failure rate model. Future research would need to look at how these additional sources of uncertainty can be considered and what alternate models are able to characterise the reliability of such systems. The same fundamental theory and approach developed in this chapter could readily be adopted to any other regulatory compliance process or aviation system. This marks another potential avenue for future research.

The focus of this chapter was thus on answering Research Question 2, though elements of Research Question 1 are also addressed. In relation to the first research question, the chapter clearly shows how the identified sources of uncertainty can be incorporated into the SSPR compliance process (Research Question 1.2). It highlights the benefits of adopting a Level 5 treatment of uncertainty by providing a means of displaying multiple risk curves to the decision maker (though at this point they are all in relation to the failure rate associated with the worst-case consequential outcome) through the adoption of various Bayesian analysis techniques (Research Question 1.3). In relation to the second research question, the chapter clearly identifies the sources of uncertainty in not just the SSA process but also the CA and CF processes and shows how they are currently managed in each of these sub-processes (Research Question 2.1). By developing the Extended SSPR compliance process, the research undertaken in this chapter directly shows how some of the identified sources of uncertainty in the Traditional SSPR compliance process can be represented and accounted for to support more objective and consistent regulatory outcomes, using Bayesian analysis, Bayesian hypothesis testing and normative decision theory (Research Question 2.2).

By answering these research questions, this chapter clearly focuses on addressing the second and third research objectives, that is, "drawing on contemporary risk and uncertainty theory, to develop a new compliance assessment and compliance finding decision-making process that incorporates the varying sources of uncertainty inherent in them" and applying "the above to the regulation of UAS, in particular, the system safety "Part 1309" regulations". Elements of the first research objective are however also addressed. While this chapter in conjunction with the previous chapter essentially addresses each of the research objectives and answers most of the research questions, work still needs to be done to further improve the Extended SSPR compliance process and achieve the overall aim of the thesis. These improvements are made in the following two chapters, with the summary of findings and overall advantages outlined in Chapter 7.

The Extended SSPR compliance process developed in this chapter clearly shows how uncertainties in the SSA, CA and CF processes can be taken into consideration. This allows the framework to be applied to new and novel technologies such as UAS. The research has thus helped show how the concept of risk-based regulation can be extended to include a risk-based approach to compliance assessment and compliance finding and how the uncertainty associated with these three processes can be taken into consideration. In addition to this, the research proposes a new risk-based approach to the regulatory compliance process, through reframing it as a problem of decision making under uncertainty. By adopting the Bayesian hypothesis test and normative decision theory in the Extended SSPR compliance process, the research developed and demonstrated a mathematically robust approach for accounting for uncertainty in performance/compliance assessments; and allowed for the systematic treatment of uncertainty in the aviation regulatory compliance assessment and compliance finding processes.

8.1.3. Chapter 5: Managing Uncertainty in the System Safety Assessment of Unmanned Aircraft Systems

One of the assumptions made in the Extended SSPR compliance process provided in the previous chapter was in relation to the APFH and the use of a constant failure rate model (in the form of a Poisson model) to account for the uncertainty in this parameter. While this assumption may be suitable for more established technologies such as CPA that are in the "useful life" phase of their lifecycle and was in keeping with the requirements outlined in the guidelines, it did not take the relative infancy of UAS into consideration. When dealing with new and evolving technologies such as UAS that make use of COTS components and have a continuously changing system baseline, it is evident that these systems will potentially never reach the "useful life" phase of their lifecycle. They are more likely to be in the "infant mortality" phase of their lifecycle. This chapter thus looks to refine the extended framework developed in the previous chapter by addressing this limitation and providing a model that is capable of taking the variable failure rates associated with UAS into consideration. The chosen model was a Weibull model. In addition to providing a means of taking the variable failure rate associated with these UAS into consideration the model also provided the decision maker with a number of different outputs which could be used to help support more risk-informed decisions. For example, the posterior distribution of the shape parameter (one of the input parameters for the Weibull model) can be used to provide insight into the particular phase of operation of the system (*i.e.* infant mortality phase, useful life phase or wear-out phase). Forward inferences (predictions) on the future failure performance of the fleet can also be made using various Bayesian inference techniques. While this directly addresses some of the limitations of the extended framework by relaxing the modelling assumption that the UAS exhibit constant failure rates, there are still certain limitations with the extended framework that have yet to be addressed. The most significant of which being the inability of the extended framework to take the uncertainty in the remaining outputs of the SSA process into consideration. Uncertainty in the input mishap data is another area where future research efforts need to be directed.

As this research is directly building off the research undertaken in the previous chapter, it is evident that the main focus of this chapter is on the second research question. By clearly describing the limitations associated with not taking the variable failure rate of the system into consideration and identifying the uncertainties introduced with this assumption, the research helps identify additional uncertainties and shows how they are currently managed in the aviation safety compliance assessment and compliance finding processes (Research Question 2.1). By advocating the need to evolve the framework and take this uncertainty into consideration through the adoption of a Weibull failure rate model and showing how this can further support more objective and consistent regulatory outcomes, the research further helps answer the second part of this research question (Research Question 2.2).

By helping answer these research questions and extending the framework further, the research again focuses on the second and third research objectives that is, “drawing on contemporary risk and uncertainty theory, to develop a new compliance assessment and compliance finding decision-making process that incorporates the varying sources of uncertainty inherent in them” and applying “the above to the regulation of UAS, in particular, the system safety “Part 1309” regulations”.

As this research focuses on a particular limitation of the Extended SSPR compliance process (*i.e.* the limitation associated with the use of a constant failure rate model), its novel contributions are focused on addressing this limitation. In particular, it shows how types of model uncertainty can be accounted for in the assessment and compliance processes, something fundamental to the application of a risk-based approach to the regulation of the UAS industry. In doing so, it evolves the Extended SSPR compliance process further.

8.1.4. Chapter 6: Adoption of a Bayesian Belief Network for the System Safety Assessment of Remotely Piloted Aircraft Systems

Another limitation of the Extended SSPR compliance process presented in Chapter 4 is in relation to the inability of the framework to account for the uncertainty associated with the remaining outputs from the SSA process. In keeping with traditional frameworks, the extended framework assumed a worst-case consequential outcome from the failure scenario. This has the potential to lead to overly conservative safety objectives as well as operational constraints. This, in turn, results in additional costs in the design, production, testing, and certification of the system. Identified failure conditions are assessed and treated independently, with compliance only shown against the assigned worst-case safety objective. As a result, overall compliance of the RPAS (as a whole) with its system-level safety objective is never shown. This chapter aims to address this assumption and the associated limitations, thus evolving the Extended SSPR compliance process even further.

The chapter starts by reintroducing the Traditional SSPR compliance process and outlining the sources of uncertainty associated with this process. The Extended SSPR compliance process is then presented to show how previous work looked to extend this framework by providing a rational, transparent and systematic means of accounting for uncertainty in this process, thus supporting a risk-based approach to the regulation of the industry. The major limitation of this extended framework which would then be addressed is highlighted, with the research developing a Proposed SSPR compliance process. This framework outlines the general set notation that would be needed to take the additional sources of uncertainty into consideration. It then relates the framework to a generic RPAS to see how the sets could be substantiated, thus showing how the uncertainty in the remaining outputs could be accounted for from a theoretical perspective. A BBN is then introduced as a suitable tool to model the SSA process and relate its outputs to the CA process. Details regarding the substantiation of the arcs and quantification of the NPTs are then provided, with the revised outputs clearly identified. A case study example is used to exemplify the features of the developed model.

As mentioned above, the chapter proposes the use of a BBN as a means for more comprehensively capturing the uncertainty in the SSA process. The proposed BBN SSA approach takes into consideration the uncertainty in the consequential outcomes assigned to a set of identified failure conditions, removing the need for worst-case assumptions. System safety compliance assessments can also be made at different levels of abstraction of the system (*i.e.*, from an individual failure condition through to a set of all identified failure conditions, representative of the overall system), providing a means of assessing the compliance of the overall system with its top-level safety objectives. The output of the SSA process is now a family of distributions describing the uncertainty in the assessed APFH. This provides the regulator with a more comprehensive picture of the state of knowledge in relation to the APFH for input to the CA and CF processes. It is important here to note that, while the BBN has its advantages, there are still certain challenges that can impact the overall output from the SSA process. For example, each of the input parameters that are represented by probability distributions have uncertainty surrounding them. On using the BBN to combine these distributions, the uncertainty has the tendency to compound. The impact of this on the resulting distribution has not been explored. While this discussion is beyond the scope of this research it does highlight a potential avenue for research.

The proposed framework still does not take uncertainty in the data input to the model into consideration. Future work needs to look at how this data uncertainty can be taken into consideration in the proposed framework. In addition to this, while the adoption of a risk matrix is standard practice in industry, it is evident that there is potential uncertainty associated with the application of this risk matrix, which is being propagated throughout the SRMP. While addressing the limitations associated with this uncertainty is beyond the scope of this thesis, it is important to understand the uncertainty associated with these risk-matrices and how they can potentially impact the overall output from the SRMP. Future research can look to study the impact of this on the overall outputs from the framework. While the proposed SSA process allows for additional sources of uncertainty to be taken into consideration, the CA and CF processes have not been further updated from the extended framework, to account for these additional outputs. Future research needs to look at how these additional sources of data and information can be used within these decision-making processes, perhaps through the adoption of alternate decision theories within the CF process. Future research can also look at how this theory can be applied to represent the decision risk within a standard risk matrix and incorporate existing evaluation and treatment decision-making frameworks (e.g. ALARP and SFARP decision-making frameworks) commonly used in aviation risk management.

As this research is again directly building off the research undertaken in Chapter 4, it is evident that the main focus of this chapter was on the second research question, though elements of the first research question are also addressed. The framework supports a Level 5 treatment of uncertainty, and clearly shows how these additional outputs in the form of multiple probability curves can be used to improve regulatory outcomes. The research highlights the advantages of the Level 5 treatment of uncertainty and shows how the risk and uncertainty measures obtained from the regulatory safety risk assessment processes can be represented to decision makers (Research Question 1.3). The paper clearly shows how the uncertainties associated with these remaining outputs are managed (Research Question 2.1) and then shows how these uncertainties can be represented and accounted for to support more objective and consistent regulatory outcomes, through the adoption of a BBN (Research Question 2.2).

By answering these research questions, it is evident that this research can directly be used in conjunction with the previous chapters to address the overall aim of the thesis, that is “to improve regulatory outcomes under the new paradigm of risk-based regulation, through providing a conceptual framework for the rational, transparent and systematic treatment of uncertainty in the risk assessment and regulatory decision-making process” by providing additional information which can be used to further strengthen the Extended SSPR compliance process, thus addressing the second and third research objectives.

While the Extended SSPR compliance process marked a significant step change over the Traditional SSPR compliance process, further work needed to be undertaken to incorporate the uncertainties associated with the remaining outputs of the SSA process. The chapter develops the Proposed SSPR compliance process, which provides a means of taking these additional sources of uncertainty into consideration. In addition to being one of the first research endeavours to apply a BBN within an aviation SSR "Part 1309" system safety context, the research makes a number of additional novel contributions to theory. By relating the outputs of the SSA process to a generic RPAS, it develops a general template for high level classification of functions and failures which can be applied to any aircraft system. This can be used in the context of other regulatory processes as well. The research advocates the adoption of a BBN as a valid approach for capturing uncertainty in the assessed compliance scenario. This removes the requirement for assessing single credible (often worst-case) scenarios, thus extending compliance scenarios to multiple assessments and addressing one of the major limitations associated with current approaches.

8.1.5. Chapter 7: Managing Uncertainty in Unmanned Aircraft System Safety Performance Requirements Compliance Process

The research presented in Chapter 4 to Chapter 6 looked to evolve the Traditional SSPR compliance process so that it could be applied to new and evolving systems such as UAS, that are characterised by limited data and high uncertainty. Focusing on the SSA process, this chapter looks to highlight some of the main challenges associated with the application of the traditional framework to new and evolving systems such as UAS and see how this impacts the CA and CF decision-making processes that follow. A summary of current and envisaged research towards addressing these challenges is also presented. Based on the research undertaken, it was seen that the main challenges include: the challenge associated with the regulatory surveillance enforcement; accounting for the human system interaction in the assessment process; the need to certify the UAS based on both the function of the system and properties of the intended operational environment as opposed to just certifying the CPA based on the intended function of the system; and the need to account for mitigation measures as part of the safety case when certifying the UAS as opposed to looking at the mitigation measures on a case by case basis when evaluating a CPA. In addition to these challenges, it was also seen that there are a number of differences between UAS and CPA that can impact their certification. These differences are in relation to the: design philosophy; engineering processes; technology refresh rate; changing certification baseline; unassured components; lack of knowledge; heterogeneity of fleet and operations; and changing failure rate.

Taking these challenges and inherent differences into consideration it is evident that there is a general lack of knowledge and operational data, and a lack of trust in the data and knowledge that is available to support airworthiness assessment and compliance finding processes for UAS. There can be considerable uncertainty associated with the certification of civil/commercial UAS, which in turn can lead to high certification risk (*i.e.*, the risk associated with certifying a UAS as compliant, and therefore safe for operation, when indeed it is not). The Traditional SSPR compliance process as used for the certification of CPA does not adequately account for this high uncertainty inherent to the SSA, CA and

CF process of UAS. Developing a framework tailored to UAS, would allow for a more rational, transparent and systematic approach to decision-making. This would reduce the need for conservative assumptions and take the risk posed by each UAS into consideration while determining its state of compliance to the SSR.

This chapter links all of the work undertaken in Chapter 4 to Chapter 6 and highlights the challenges associated with applying the Traditional SSPR compliance process to UAS. The advantages of the Extended and Proposed SSPR compliance processes are also discussed. The difference between UAS and CPA were highlighted, further supporting the need for a more rational, transparent and systematic treatment of uncertainty in the adoption of a risk-based approach to the regulation of the industry.

While elements of Research Question 2.1 and Research Question 2.2 were discussed at a high-level, the main focus of the work was in linking the previous research and highlighting the limitations and advantages of the identified approaches. In doing so it directly answers Research Question 2.3 by highlighting some of the potential benefits of the risk-based philosophy in the aviation sector.

By answering the above research questions, it is evident that the research was focused on the second and third research objectives. The high-level discussion provided clearly shows how the extensive research undertaken in each of the chapters relates to each other and how this directly helps achieve the overall aim of the thesis. By clearly identifying the advantages of the Extended and Proposed SSPR compliance process, the research supports the adoption of such frameworks for new and evolving technologies such as UAS.

8.1.6. Summary

The aim of this thesis is to improve regulatory outcomes under the paradigm of risk-based regulation, through providing a conceptual framework for the rational, transparent and systematic treatment of uncertainty in the risk assessment and regulatory decision-making processes. The review of literature identified that the definition of risk is moving towards one that considers uncertainty. Thus, in moving towards a risk-based approach to regulation, it is imperative to take the uncertainty associated with the process into consideration. To achieve the overall aim of this thesis, the research objectives outlined in Section §1.3 were identified.

Under a risk-based approach to regulation, the SRMP drives not only the rule-making process but also the regulatory processes of compliance assessment and compliance finding. Uncertainty is inherent to all the elements of the SRMP. However, a review of aviation safety guidance and safety management practices found that aviation safety literature does not adequately address the uncertainty associated with the SRMP. For example, when measuring risk, only the likelihood and severity are taken into consideration, with uncertainty generally not mentioned. Where uncertainty is mentioned, it is addressed through the use of conservative worst-case assumptions. This has the potential to result in the imposition of overly stringent restrictions on the operation of the systems where there is uncertainty in the safety risk, such as UAS. Subsequently, providing a more comprehensive treatment of uncertainty in the aviation SRMP is essential to the uptake of a risk-based approach to rule-making. Further, it follows that if assessments of performance are uncertain, then these uncertainties are also inherent in the assessments required to show compliance to regulations. It was found that the current aviation compliance process does not provide an objective means for accounting for uncertainty. As a consequence, compliance assessments can be subjective and inconsistent, with regulators lacking the tools and processes to be able to make objective compliance findings on the basis of compliance risk. A means to enable NAA to account for uncertainty in regulatory compliance processes is needed. Taking this into consideration, this thesis aimed at answering two main research questions:

1. **What are the uncertainties associated with the safety risk assessment process and how are they addressed within the current aviation safety risk management and regulatory development processes?**

2. **How can uncertainty associated with the SRMP be accounted for in existing aviation rule-making and compliance processes?**

The papers presented in Chapter 3 through to Chapter 7 addressed each of these research questions. Taking the case study example of UAS into consideration, Chapter 3 provided an in-depth review of the state of the art in UAS GRM used to evaluate the risks posed by the operation of UAS to people and property on the ground. Based on the review, the various sources of uncertainty inherent in the safety risk assessment process were identified (Research Question 1.1). The GRM and component sub-models were then related to the regulations to show how the uncertainty in these sub-models and the conservative assumptions used to manage them, impact different components of the regulations (Research Question 1.2). The six level of treatment of uncertainty identified clearly show the risk and uncertainty measures obtained from the regulatory safety risk assessment processes can be represented to decision makers (Research Question 1.3). Chapter 0 explored how this uncertainty can be taken into consideration in the SRMP, highlighting the benefits of adopting a Level 5 treatment of uncertainty (Research Question 1.2, Research Question 1.3 and Research Question 2.1). Looking at the case study of the SSR, the paper presented in Chapter 4 extended the concept of risk-based regulation to include a risk-based approach to the processes of compliance assessment and compliance finding (Research Question 2.2). This allows for compliance decisions to be made based on compliance risk. The papers presented in Chapter 5 and Chapter 6 further extends this framework to show how additional uncertainties in the system safety process can be taken into consideration (Research Question 2.1 and Research Question 2.2). Chapter 6 also further helps highlight the advantages of adopting a Level 5 treatment of uncertainty (Research Question 1.3). Finally, Chapter 7 looked at the challenges and advantages associated with adopting such a risk-based framework for UAS and presented current and envisaged research towards addressing these challenges (Research Question 2.3).

The focus of this thesis has been on providing a conceptual framework for the rational, transparent and systematic treatment of uncertainty in the risk assessment and regulatory decision-making process. The overall research and developed framework have been presented to military airworthiness authorities and received positive feedback (refer to [139]). In developing this framework every effort was taken to validate its structure through referencing the use of accepted tools, practices and definitions; as is evidenced by the discussion provided in the individual chapters. This is however only a partial validation, and it is recognised that this effort does not validate the outcomes or claimed benefits of use of the model. According to Dalamagkidis et al. [140], "a thorough model validation would require a wealth of experimental results, some of which are difficult if not impossible to obtain". In the absence of such data, as is the case with UAS, one approach of validating the outcomes or claimed benefits of use of the model is through the use of data from alternate sources, such as General Aviation data, as inputs to the model. This approach was adopted by Melnyk et al. [141], Waggoner [142] and Lum and Waggoner [143] to name a few, to validate their risk models. This marks an avenue for potential future research for this thesis. A limitation associated with the use of such an approach is the inherent differences that exist between UAS and General Aviation systems. This is potential source of uncertainty that would need to be taken into consideration. Another approach to the validation of the posited benefits of the proposed framework can be through its application to a real-world certification case. Such a validation exercise would require the collaboration of both an industry applicant and NAA. The analysis would however be system or product specific and consequently the outputs and posited benefits would not be able to be disclosed due to commercial sensitivities (especially when dealing with military systems). While such a validation exercise has yet to be undertaken, follow on research projects have been planned with military airworthiness authorities to further help validate parts of the proposed framework. As described by Clothier et al. [144], "Decision makers must have a high degree of confidence in the modelling approach employed before the results are of any use in the decision-making process. Model verification and validation becomes an essential component of the risk analysis process". These future research endeavours thus mark an important step in the adoption of the frameworks proposed in this thesis.

8.2. Summary of Novel Contributions

This thesis has made a number of novel contributions to theory. The specific case study of UAS and SSPR has been used to illustrate the more general novel theoretical contributions made in this thesis. The majority of these contributions are applicable to any aviation sector, rule or regulation. The novel contributions include:

- Development of a conceptual framework for describing the component-models of GRM, and in turn, providing a general theoretical basis for the systematic development and analysis of models proposed in the literature;
- Identification of the various sources of uncertainty with respect to each of the component-models and showing how failing to account for such uncertainties can impact various elements of the regulation;
- Development of an overall concept for risk-based assessment and compliance processes, showing how the theoretical concepts described evolve towards a more comprehensive treatment of uncertainty. The potential benefits and challenges associated with this process are also highlighted;
- Proposing a new risk-based approach to regulatory compliance process, through reframing it as a problem of decision making under uncertainty. This approach:
    - Developed and demonstrated a mathematically robust approach for accounting for uncertainty in performance/compliance assessments;
    - Allowed for the systematic treatment of uncertainty in the aviation regulatory compliance assessment and compliance finding processes by the application of a normative decision theory, combined with assessments of the consequence of the different compliance finding outcomes, to provide NAA with a systematic basis for making compliance decisions (findings) on the basis of compliance risk;
- Demonstrating how types of model uncertainty can be accounted for in the assessment and compliance processes;
- Development of a general template for high level classification of functions and failures which can be applied to any aircraft system;
- Application of a BBN as a valid approach for capturing uncertainty in the assessed compliance scenario. This removes the requirement for assessing single credible (often worst-case) scenarios, thus extending compliance scenarios to multiple assessments;
- Being the first to apply a BBN within an aviation SSR “Part 1309” system safety context.

8.3. Future Research

There are numerous opportunities to extend the initial theoretical contributions provided in this thesis. These include:

- Further developing sub-models of the GRM to address identified deficiencies and enhance treatment of uncertainties where a knowledge gap is present (e.g. recovery model, stress model).

These sub-models are identified as important areas for advancement and will directly influence the overall GRM and the regulations they impact;

- Providing a theoretical approach for accounting for data uncertainty (e.g., inaccurate, censored or missing, etc.) input to assessment processes (e.g., failure rate data);
- Identify and characterise the uncertainties within the ALARP and SFARP decision-making frameworks;
- Determine how a normative decision-making approach can be adapted to account for ALARP and SFARP decision making principles, and the uncertainties inherent to them;
- Exploring how to represent decision risk within a standard risk matrix taking the uncertainty associated with the likelihood and severity into consideration
- Application of the general approach to other aviation sectors (e.g., space launch, UAM, *etc*.), and regulations;
- Working in partnership with an industry applicant and NAA, validate posited benefits of the approach through its use as an alternate means of compliance.

8.4. Closing Remarks

The proposed conceptual framework has the potential to significantly change how NAA approach rule-making and compliance activities for new or novel aviation systems such as UAM concepts, personal air mobility vehicles, reusable space launch vehicles, and UAS. The implementation of the proposed framework enables NAA to account for uncertainty implicit to regulatory compliance assessment and compliance finding processes. This enables NAA with a systematic and objective means of making compliance findings on the basis of "compliance risk". In the context of risk-based rule-making, the more comprehensive treatment of uncertainty means regulations need not be based on conservative or worst-case assumptions; ensuring regulations are more proportionate to the operational safety risks they are intended to manage.

This page is intentionally left blank.

9. Appendices

9.1. Appendix A: Supporting Publications

A complete list of published papers, conference papers and presentations completed during this candidature are presented in Table 12 and Table 13.

Table 12: Supporting journal and conference publications

Title of Paper	*A Review of Unmanned Aircraft Systems Ground Risk Models*
Authors	Achim Washington, Reece Clothier, Jose Silva
Journal	Progress in Aerospace Sciences
Status	Published
Impact Factor	6.814
Link	https://www.sciencedirect.com/science/article/pii/S0376042117301392
Title of Paper	*A Bayesian Approach to System Safety Assessment and Compliance Assessment for Unmanned Aircraft Systems*
Authors	Achim Washington, Reece Clothier, Brendan Williams
Journal	Journal of Air Transport Management
Status	Published
Impact Factor	2.412
Link	https://www.sciencedirect.com/science/article/pii/S0969699716304768
Title of Paper	*Managing Uncertainty in the System Safety Assessment of Unmanned Aircraft Systems*
Authors	Achim Washington, Reece Clothier, Brendan Williams, Jose Silva
Conference	17th Australian International Aerospace Congress (AIAC 17), Melbourne, Australia, 27th and 28th February, 2017
Status	Published in proceedings (full paper peer reviewed)
Link	https://search.informit.com.au/documentSummary;res=IELENG;dn=739801934595508
Title of Paper	*Adoption of a Bayesian Belief Network for the System Safety Assessment of Remotely Piloted Aircraft Systems*
Authors	Achim Washington, Reece Clothier, Natasha Neogi, Jose Silva, Kelly Hayhurst, Brendan Williams
Journal	Safety Science
Status	Published
Impact Factor	3.619
Link	https://www.sciencedirect.com/science/article/pii/S0925753518312670
Title of Paper	*Managing Uncertainty in Unmanned Aircraft System Safety Performance Requirements Compliance Process*
Authors	Achim Washington, Reece Clothier, Jose Silva
Conference	International Conference on Unmanned Aircraft Systems (ICUAS 2018, Amsterdam), 10th and 11th May, 2018
Status	Published in proceedings (full paper peer reviewed)
Link	https://waset.org/publications/10008962/managing-uncertainty-in-unmanned-aircraft-system-safety-performance-requirements-compliance-process

Title of Paper	*Challenges to the Risk-based Regulation of Unmanned Aircraft Systems*
Authors	Achim Washington, Reece Clothier, Jose Silva
Conference	18th Australian International Aerospace Congress (AIAC 18), Melbourne, Australia, 24th to 26th February, 2019
Status	Published in proceedings (full paper peer reviewed)
Link	https://search.informit.com.au/documentSummary;dn=319803390521073;res=IELENG;type=pdf
Title of Paper	*Development of a Template Safety Case for Unmanned Aircraft Operations Over Populous Areas*
Authors	Reece Clothier, Brendan Williams, Achim Washington
Conference	SAE International AeroTech Congress & Exhibition (SAE 2015, Seattle, USA), 22-24 September 2015
Status	Published in proceedings (full paper peer reviewed)
Link	http://papers.sae.org/2015-01-2469/
Title of Paper	*Challenges to the development of an airworthiness regulatory framework for unmanned aircraft systems*
Authors	Reece Clothier, Brendan Williams, James Coyne, Mark Wade, Achim Washington
Conference	16th Australian International Aerospace Congress (AIAC16), Barton, ACT, Australia, 24-26 February 2015
Status	Published in proceedings (full paper peer reviewed)
Link	https://trove.nla.gov.au/work/212667555?q&versionId=233541550
Title of Paper	*Practical Considerations in the Design of an Obstacle Detection, Mapping and Path Planning System for Small Unmanned Aircraft Systems*
Authors	Achim Washington, Willem van Deventer, Reece Clothier
Journal	International Journal of Unmanned Systems Engineering (IJUSEng)
Status	Published
Link	https://search.proquest.com/openview/102213a14896b7e1e89358043ddcc4de/1?pq-origsite=gscholar&cbl=2032535

Table 13: Supporting industry presentations

Title of Presentation	*Accounting for Uncertainty in System Safety Assessments*
Authors	Dr Reece Clothier, Mr Achim Washington, Mr Brendan Williams, Ms Kelly Cox
Conference	DGTA System Safety and Software Conference, Sept, RAAF Laverton, Melbourne, Australia.
Status	Presented on 11th September 2016
Title of Presentation	*Higher Level Treatment of Uncertainty in Aviation Risk Management with Applications to the Regulation of Unmanned Aircraft Systems*
Authors	Mr Achim Washington, Dr Reece Clothier
Conference	NASA Langley Research Centre, Virginia
Status	Presented on 2nd November 2016
Title of Presentation	*Risk-based Regulation of Unmanned Aircraft Systems*
Authors	Mr Achim Washington, Dr Reece Clothier, Dr Jose Silva
Conference	Australian System Safety Conference 2019 (ASSC 2019)
Status	Presented on 24th May 2019

9.2. Appendix B: Definition of Authorship

In accordance with the **Australian Code for the Responsible Conduct of Research**, authorship is defined as being based on substantial contributions in a combination of:

i. Conception and design of the project;

ii. Analysis and interpretation of research data;

iii. Drafting significant parts of a work, or

iv. Critically revising it so as to contribute to the interpretation.

9.3. Appendix C: Reference Tables for Literature Review

Table 14: Definitions of risk

S. No.	Definition	Source
	Probability Based Risk Definitions	
1	Risk is defined as the **possibility** that human actions or events lead to consequences that harm aspects of things that human beings value.	[107]
2	**Possibility** of loss, injury, disadvantage or destruction; to expose to hazard or danger; to incur risk of danger.	[82]
3	**Probability** of an adverse event amplified or attenuated by degrees of trust, acceptance of liability and/or share of benefit.	[82]
4	Risk is the combination of the **probability** of an event and its consequences.	[145]
5	Risk is a measure of the **probability** and severity of adverse effects.	[51]
6	Risk "is" the set of triplets. R= {<$s_i, p_i. c_i$>}, where s_i is a scenario identification or description; p_i is the **probability** of that scenario; and x_i is the consequence or evaluation measure of that scenario, *i.e.*, the measure of damage.	[38]
7	Combination of the **likelihood** of harm and the severity of that harm.	[42]
8	A combination of the severity of the mishap and the **probability** that the mishap will occur	[47]
9	More common today is the definition of risk as the **probability** of occurrence for an undesirable outcome.	[52]
10	The defining of risk as the product of **probability** and consequence magnitude is slightly more common than the defining of risk as **probability** or as magnitude of consequence.	[52]
11	A combination of the **likelihood** of a hazard occurring and the severity of the accident that could result; e.g. the higher the risk, the more likely the accident will occur and/or the more severe will be the consequence.	[31]
12	Safety risk is defined as the assessment, expressed in terms of predicted **probability** and severity, of the consequences of a hazard, taking as reference the worst foreseeable situation.	[25]
13	The composite of predicted severity and **likelihood** of the potential effect of a hazard.	[26]
14	The chance of something happening that will have an impact on objectives. A risk is often specified in terms of an event or circumstance and any consequence that might flow from it. Risk is measured in terms of a combination of the consequences of an event, and its **likelihood**. Risk can have a positive or negative impact.	[27], [28]
15	The combination of the **likelihood** and severity that is associated with a non-compliance as part of the certification basis.	[32]

S. No.	Definition	Source
	Uncertainty Based Risk Definitions	
1	The notion of risk involves some kind of loss or damage that might be received by a target and the **uncertainty** of its transformation in an actual loss or damage.	[49], [83]
2	Risk should be associated with a system and commonly defined as the potential loss resulting from an **uncertain** exposure to a hazard or resulting from an **uncertain** event that exploits the system's vulnerability	[34]
3	Effect of **uncertainty** on objectives	[146]
4	A measure of **uncertainty** of an event happening times the severity of the outcome.	[77]
5	The notion of risk involves both **uncertainty** and some kind of loss or damage that might be received. Risk = **uncertainty** + damage	[38]
6	Risk is defined as, **uncertainty** of outcome, whether positive opportunity or negative threat, of actions and events. It is the combination of likelihood and impact, including perceived importance.	[147]
7	An **uncertain** consequence of an event or an activity with respect to something that humans value	[148]
8	Risk is equal to the two-dimensional combination of events/ consequences and associated **uncertainties.**	[149]
9	Risk is **uncertainty** about and severity of the consequences (or outcomes) of an activity with respect to something that humans value.	[150]
10	Risk is, at minimum, a two-dimensional concept involving (1) the possibility of an adverse outcome, and (2) **uncertainty** over the occurrence, timing, or magnitude of that adverse outcome. If either attribute is absent, then there is no risk.	[52]
11	A characteristic of a situation or action wherein two or more outcomes are possible, the particular outcome that will occur is unknown, and at least one of the possibilities is undesired	[52]
12	Risk is the future impact of a hazard that is not controlled or eliminated. It can be viewed as future uncertainty created by the hazard	[40]
13	Effect of uncertainty on objectives	[121]

S. No.	Definition	Source
	Other Risk Definitions	
1	Risks are the occurrence likelihood and occurrence consequences of an event.	[34]
2	Risk is a threat (or opportunity) that could affect adversely (or favourably) achievement of the objectives of a project and its outcomes.	[34]
3	Risk can be defined as the expected value of harm.	[62]
4	Risk refers to situations with objective probabilities for the randomness the decision-maker is faced with.	[151]
5	Risk has been defined as, the chance that someone or something that is valued will be adversely affected in a stipulated way by the hazard.	[65]
7	Risk is a combination of the consequences of an event, including changes in circumstances, and the associated likelihood of occurrence.	[34]
8	Risk is "the combination of the likelihood of harm and the severity of that harm.	[42]

Table 15: Measuring risk

S. No.	Equation		Description	Ref.
1	$Risk = \left(C_{1,}P_1\right), (C_2, P_2), \ldots, (C_n, P_n)$		C : Consequence P : Probability	[86]
2	$R = S \times P$		R : Risk S : Severity of harm P : Likelihood of occurrence of that harm	[53]
3	$R = \sum_{i=1}^{n} P_i C_i$		R : Risk P : Probability the event will occur C : Potential consequence n : Number of events	[109]
4	R = $\{< s_i, p_i, x_i >\}$,	*where i = 1, 2, 3… N*	R : Risk {} : Set s_i : Scenario identification p_i : Probability of the scenario measuring the likelihood of it happening x_i : Consequence or evaluation measure of that scenario	[38]
5	R = $\{< s_i, p_i, x_i >\}$,	*where i = 1, 2, 3… N+1*	R : Risk {} : Set s_i : Scenario identification p_i : Probability of the scenario measuring the likelihood of it happening x_i : Consequence of evaluation measure of that scenario	[38]
6	$R = \{< s_i\ , p_i(\emptyset_i\ , x_i) >\}$,	*where i = 1, 2, 3… N+!*	s_i : Scenario identification $Ø_i$: Measure of frequency with which the proposed scenario occurs x_i : Consequence of evaluation measure of that scenario $p_i\,(Ø_i, x_i)$: Probability curve which takes the uncertainty about the actual value of $Ø_i$ and the damage x_i into account	[38]

7	$\text{Risk} \equiv \{(l_1, o_1, u_1, cs_1, po_1), (l_2, o_2, u_2, cs_2, po_2), \ldots, (l_n, o_n, u_n, cs_n, po_n)\}$	l o u cs po n	: : : : : :	Likelihood Outcome Utility (or significance) Causal scenario Population affected by the outcome Number of outcomes	[34]
8	$\text{Risk} = (A, C, P_f)$	A C P_f	: : :	Activity Consequence Frequency interpreted probability of the event (A) occurring per unit of time	[110]
9	$\text{Risk} \ = (A, C, P_f^*, U\ (P_f^*), K)$	A C P_f^* $U(P_f^*)$ K	: : : : :	Activity Consequence Estimate of P_f Uncertainty description of P_f^* relative to P_f Background knowledge	[110]
10	$\text{Risk} \ = (A, C, P_f^*, P\ (P_f), K)$	A C P_f^* $P(P_f)$ K	: : : : :	Activity Consequence Estimate of P_f subjective probabilities[4] P used to express uncertainties about P_f Background knowledge	[110]
11	$\text{Risk} \ = (A, C, P_f^*, C\ (P_f), K)$	A C P_f^* $C(P_f)$ K	: : : : :	Activity Consequence Estimate of P_f Traditional confidence interval for P_f Background knowledge	[110]
12	$\text{Risk} = (A, C, U)$	A C U	: : :	Event Consequence Uncertainty	
13	$\text{Risk} \ = (A, C, U, P, K)$	A C U P K	: : : : :	Event Consequence Uncertainty in the risk description Subjective probability expressing *U* based on *K* Background knowledge	[110]

[4] a subjective probability is a measure of uncertainty seen through the eyes of the assessor

Table 16: Common definitions of the safety risk management process

S. No.	Definition	Ref.
1	A decision-making process designed to systematically identify hazards, assess the degree of risk, and determine the best course of action.	[40]
2	A systematic approach to managing safety, including the necessary organizational structures, accountabilities, policies and procedures.	[13]
3	Safety risk management encompasses the assessment and mitigation of safety risks. The objective of safety risk management is to assess the risks associated with identified hazards and develop and implement effective and appropriate mitigations. Safety risk management is therefore a key component of the safety management process at both the State and product/service provider level.	[122]
4	Safety risk management is a careful examination of what, in your work, could cause harm, so that you can weigh up whether you have taken enough precautions, or should do more to prevent harm.	[66]
5	The process of ensuring that hazards and potential accidents are identified and managed.	[42]
6	The process of reducing the risks to a level deemed acceptable by society.	[107]
7	The systematic application of management and engineering principles.	[48]

9.4. Appendix D: Bayesian Analysis – Concepts and Tools

This section looks to describe some of the concepts and tools that will be used in the individual chapters to take the identified sources of uncertainty into consideration. This review is only meant as a high-level description of these concepts and tools. For further details on these concepts and tools and how they have been applied in the context of this thesis, the reader is directed to the individual references and chapters.

9.4.1. Bayes Theorem

In probability theory and statistics, it is often required to calculate the probability of an event given that another event has occurred at some prior point in time [71]. Bayes' Theorem describes the probability of this event arising, given some prior data and information in relation to the event. It is based on conditional probabilities and along with the concept of subjective probabilities, forms the basis of Bayesian inference [71], [85], [152]. Bayesian inference itself is commonly used in PRA, which is fundamental to the research undertaken as part of this thesis.

According to Bayes' Theorem, for a sequence of disjoint events (*e.g.* $A_1, A_2, \ldots, A_n$) and any other given event (*e.g.* B) where the probability of that event is greater than zero (*i.e.* $Pr(B) > 0$), the posterior probability is equal to the likelihood probability of the observation times the prior probability divided by the normalisation constant [71]. This is described mathematically in Equation (1) below (based on [71], [85]):

$$P(A_i|B) = \frac{P(B \mid A_i) \times P(A_i)}{P(B)} \tag{1}$$

Here $P(A_i|B)$ is the posterior (or posteriori) probability for the event A_i; $P(A_i)$ is the prior (or a priori) probability of the event A_i before experimentation or observation; $P(B|A_i)$ is the probability of the observation given A_i is true; and $P(B)$ is the normalisation constant, which for disjoint events and discrete probability distributions can be calculated using Equation (2):

$$P(B) = \sum\nolimits_{j=1}^{n} P\left(B\middle|A_j\right) \times P(A_j) \tag{2}$$

While Equation (1) pertains to disjoint discrete events and discrete probability distributions, it cannot be directly applied to continuous probability distribution functions that are often used in many real-world applications. An analogous form of this equation is used for this application as outlined in Equation (3), based on [71].

$$p(\lambda_n|D,I) = \frac{p(D \mid \lambda_n, I) \times p(\lambda_n|I)}{P(D|I)} \tag{3}$$

Here $p(\lambda_n|D,I)$ corresponds to the posterior distribution and it describes the uncertainty in the parameter of interest (λ_n) based on the prior state of knowledge and new evidence provided by D. $p(D|\lambda_n,I)$ corresponds to the likelihood distribution and represents the aleatory uncertainty in the model.

$p(\lambda_n|I)$ corresponds to the prior distribution and describes the uncertainty in our current state of knowledge; the model parameter (epistemic uncertainty), based on previous information, *I*. Finally, *$P(D|I)$* corresponds to the normalisation factor and is the marginal or unconditional probability of observing the data, *D*. It is important here to note that, with the exception of the normalisation factor, all the other components are probability distributions as is evident from the nomenclature adopted.

Different probability distribution functions can be used for both the prior and likelihood distributions. In terms of the likelihood distribution, a range of distributions including the Poisson distribution, Exponential distribution, Gamma distribution and Weibull distribution can be used [52]. For a complete list of distributions and corresponding details the reader is directed to [52]. The choice of likelihood distribution is dependent on the data and the fundamental physical phenomenon being observed, hence it is conditioned on the implicit information, *I*. The choice of prior distribution can again vary significantly, with the distributions generally divided into two broad categories, informative and non-informative [71]. The prior distribution can be any distribution that best represents the state of knowledge and is dependent on the assessor. Conjugate priors can also often be used to represent the prior distributions. This negates the need for complex numerical integrations [71], [85]. Conjugate priors only exist when the observation distribution comes from the exponential family and they take the same functional form as the likelihood of the observation distribution [85]. There are a number of limitations associated with the use of conjugate priors, for details the reader is directed to [85]. It is important to note that a number of different software packages and tools were used throughout this thesis to conduct the Bayesian analysis, including: MATLAB, AgenaRisk and OpenBUGS. Hence, the choice of prior distribution did not need to be limited to a conjugate prior. Chapter 4 provides an example case study where a conjugate prior is used as part of the Bayesian analysis undertaken. The mathematics in relation to this are also explored in this chapter. For further details on the choice of conjugate priors and the challenges associated with them, the reader is directed to [71], [85], [153]–[156]. While additional information on the choice of distributions is provided in the individual chapters of this thesis, this has not been explored in detail as it is beyond the scope of the thesis.

9.4.2. Bayesian Credible Intervals and Bayesian Hypothesis Testing

From the preceding discussion, it is evident that the output from the Bayesian analysis process is a probability distribution representing the uncertainty about the parameter of interest (posterior distribution). Given this output, a number of additional tools and techniques can be used to infer further information from the outputs. Two types of inferences that are of interest are interval estimation and hypothesis testing. These inferences will be briefly outlined below, describing both the Frequentist and Bayesian approaches associated with them.

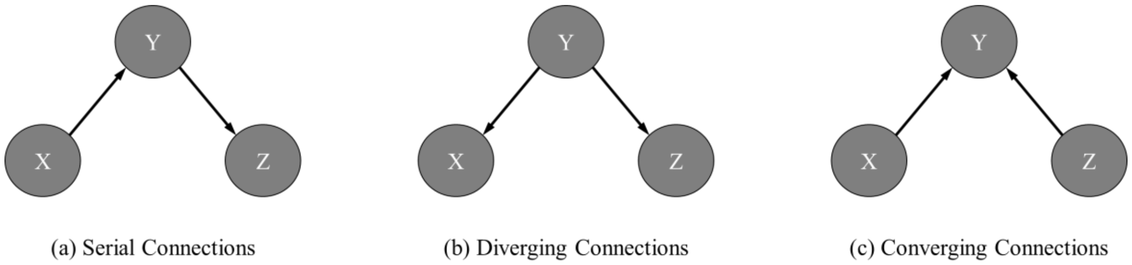
In terms of interval estimation, the interval that has a predetermined probability of containing the parameter needs to be determined [85]. Under the Frequentist interpretation, a traditional confidence interval is used. This is based on the sampling distributions of the statistic, *i.e.* how it varies over all possible samples [85]. These probabilities are not conditional on the actual sample that did occur [85]. The limitations of this approach are discussed in Ref. [85]. Under the Bayesian interpretation, Bayesian Credible Intervals are used. This makes use of the posterior distribution output from the Bayesian analysis process and has a direct (degree of belief) probability interpretation conditional on the observed sample data [85]. This provides more valuable information to the assessor, based upon which decisions can be made. This approach is used throughout the thesis, particularly in Chapter 4 where the Bayesian Credible Intervals are used to provide additional outputs from the SSA process to support a Level 5 treatment of uncertainty.

In terms of hypothesis testing (one-sided hypothesis test), we wish to provide a means of making claims that are justified by data. Two alternate hypotheses (null hypothesis and the alternative hypothesis) are described, that try to explain the discrepancy between the observed data and what would be expected under the null hypothesis [85]. Under the Frequentist approach the probability of the data given the null hypothesis is *true* is calculated. This is then compared to the threshold level (level of significance) and if it is below this level, the null hypothesis is rejected at that level of significance, and if it is more than the threshold level (level of significance) then it is accepted at that level of significance. Under the Bayesian approach the additional data and information that is provided as part of the posterior distribution is used to provide more informed decisions. The posterior probability of the null hypothesis being *true* is calculated by integrating over the correct regions (*i.e.* from zero to the threshold level). The null hypothesis is rejected if the posterior probability is less than the level of significance. This Bayesian approach is used throughout the thesis, particularly in Chapter 4 to Chapter 6, to support the risk-based approach to CA. This in turn allows for compliance findings to be made based on compliance risk, thus helping support the overall aims and objectives of this thesis. For further details the reader is directed to Ref. [85] and the individual chapters of this thesis.

9.4.3. Bayesian Belief Networks

BBN are graphical structures that make use of probabilistic reasoning to ascertain information about the unknown [157] and are beneficial when expert opinion is ambiguous, incomplete or uncertain [158]. There are two elements characteristic of any BBN, namely, the directed graphs and the node probability tables (NPT). The directed graphs comprise of two sub elements, the nodes (circles in Figure 15) which describe the variables of interest and the arcs (arrows in Figure 15) which represent the direct dependencies between the nodes. The nodes correspond to the variables and the arcs link directly dependent variables [152]. Looking at Figure 15 (a), an arc between any two nodes (*e.g.* node X to node Y) encodes an assumption that there is a direct causal or influential dependence of node X on node Y. Based on this, node X is then said to be a parent of node Y. It is important to note here that there are no cycles in the graph (so, for example, if we have an arc from X to Y and from Y to Z, then we cannot have an arc from Z to X). This avoids circular reasoning [152] and is important to take into consideration while developing a BBN. Each node of the BBN has an associated probability table, called the NPT. This is the probability distribution of the node (*e.g.* node Y in Figure 15 (a)) given the set of parents of the node (*e.g.* node X in Figure 15 (a)). For a node without parents (*e.g.* node X in Figure 15 (a)) also called a root node, the NPT of the node is simply the probability distribution of that node. It is important here to note that, when dealing with real-world risk applications, the nodes are numeric (discrete or continuous) and hence a range of pre-defined mathematical and statistical functions can be used instead of having to manually define the NPT [152].

From the preceding discussion, it was made evident that the arcs represent the causal or influential dependencies between the nodes. As such, the direction of the arrows/edges is of utmost importance. The arc directions should always be in the direction of cause to effect rather than in the direction implied by the deductions one might wish to make [152]. However, it is important to note that taking the latter approach does not necessarily lead to an invalid BBN. The process of determining what evidence will update which node is determined by the conditional dependency structure [152], examples for which are outlined in Figure 15 (a), (b) and (c). For more details on this, the reader is directed to Ref. [152].



(a) Serial Connections

(b) Diverging Connections

(c) Converging Connections

Figure 15: Structural properties of BBNs showing different conditional dependencies

For a BBN consisting of *n* variables A_1, A_2, ..., A_n, the full joint probability distribution can be represented using the chain rule as described in [152] and represented in Equation (4).

$$\begin{aligned} P(A_1, A_2, A_3, \cdots, A_n) &= P(A_1|A_2, A_3, \cdots, A_n)\, P(A_2|A_3, \cdots, A_n) \cdots P(A_{n-1}|A_n)P(A_n) \\ &= \prod_{i=1}^{n} P(A_i|A_{i+1}, \cdots, A_n) \end{aligned} \tag{4}$$

This may however prove to be overly complex, especially for larger networks and can thus be simplified using the knowledge of the parents for each node. Representing the parents for the node A_i as *Parents(A_i)* the full joint probability distribution of the BBN can be simplified as described in Ref. [152] and shown in Equation (5) below.

$$P(A_1, A_2, A_3, \cdots, A_n) = \prod_{i=1}^{n} P(A_i|Parents(A_i)) \tag{5}$$

In the context of this thesis, BBNs have been used in Chapter 6 to allow for additional sources of uncertainty associated with the remaining outputs of the SSA process to be taken into consideration.

For further details, the reader is directed to the individual chapter. It is important to note that while the BBN provide a means of capturing both epistemic and aleatory uncertainties associated with the system, there is still the concern of the uncertainties associated with the limited data available on the system. The less the data, the more the uncertainty that the sample mean and variance is actually representative of the population. This has the tendency to propagate, especially when multiplying distributions (as is done in the developed BBN) and this introduces further uncertainty in the output. The BBN allows this output to be updated as new data and information is gathered and this consequently addresses some of this uncertainty. Future research efforts will look to provide a means of capturing this data uncertainty in the model, thus allowing for more statistically significant results. At this point it is beyond the scope of this thesis, however it marks another potential area for future research. For further information on propagation of uncertainty, the reader is directed to [159]–[161].

This page is intentionally left blank.

10. Bibliography

[1] A. Washington, R. Clothier, and J. Silva, “Managing Uncertainty in Unmanned Aircraft System Safety Performance Requirements Compliance Process,” in *ICUAS 2018, Amsterdam, Netherlands*, 2018.

[2] A. Washington, R. A. Clothier, and B. P. Williams, “A Bayesian approach to system safety assessment and compliance assessment for Unmanned Aircraft Systems,” *J. Air Transp. Manag.*, vol. 62, 2017.

[3] International Civil Aviation Organization (ICAO), “Unmanned Aircraft Systems (UAS), Cir 328 AN/190,” Quebec, Canada, 2011.

[4] European Commission: Enterprise and Industry Directorate General, “Study Analysing the Current Activities in the Field of UAV, ENTR/2007/065,” 2007.

[5] The Joint JAA/EUROCONTROL initiative on UAVs, “UAV Task-Force Final Report: A concept for European regulations for civil unmanned aerial vehicles (UAVs),” 2004.

[6] R. A. Clothier, J. L. Palmer, R. A. Walker, and N. L. Fulton, “Definition of an airworthiness certification framework for civil unmanned aircraft systems,” *Saf. Sci.*, vol. 49, no. 6, pp. 871–885, 2011.

[7] R. A. Clothier, B. P. Williams, J. Coyne, M. Wade, and A. Washington, “Challenges to the Development of an Airworthiness Regulatory Framework for Unmanned Aircraft Systems,” in *16th Australian International Aerospace Congress (AIAC 16), Melbourne, Australia*, 2015, pp. 87–98.

[8] R. A. Clothier, N. L. Fulton, and R. A. Walker, “Pilotless aircraft: the horseless carriage of the twenty-first century?,” *Journal of Risk Research*, vol. 11, no. 8. pp. 999–1023, 2008.

[9] R. A. Clothier and R. A. Walker, “Determination and Evaluation of UAV Safety Objectives,” in *21st International Unmanned Air Vehicle Systems Conference, Bristol, United Kingdom*, 2006, pp. 18.1-18.16.

[10] European Aviation Safety Agency (EASA), “Concept of Operations for Drones A risk based approach to regulation of unmanned aircraft,” Cologne, Germany, 2015.

[11] Federal Aviation Administration (FAA), “Unmanned Aircraft Systems (UAS) Registration

Task Force (RTF) Aviation Rulemaking Committee (ARC) Task Force Recommendations Final Report," US Department of Transportation Washington D.C., United States of America, 2015.

[12] Joint Authorities for Rulemaking of Unmanned Systems (JARUS), "JARUS guidelines on Specific Operations Risk Assessment (SORA)," 2017.

[13] International Civil Aviation Organization (ICAO), "Manual on Remotely Piloted Aircraft Systems (RPAS)," Quebec, Canada, 2015.

[14] Civil Aviation Safety Authority (CASA), "Notice of Proposed Rule Making (NPRM 1309OS), Remotely Piloted Aircraft Systems," Canberra, Australia, 2014.

[15] Civil Aviation Safety Authority (CASA), "Advisory Circular AC 101-10v1.3, Remotely piloted aircraft systems – operation of excluded RPA," Canberra, Australia, 2018.

[16] R. A. Clothier, B. P. Williams, and A. Washington, "Development of a Template Safety Case for Unmanned Aircraft Operations Over Populous Areas," in *SAE 2015 AeroTech Congress & Exhibition, 22-24 Sept, Seattle, Washington, USA*, 2015.

[17] R. A. Clothier and R. A. Walker, "Safety Risk Management of Unmanned Aircaft Systems," in *Handbook of Unmanned Aerial Vehicles*, K. P. Valavanis and G. J. Vachtsevanos, Eds. Springer, Netherlands, 2015, pp. 2229–2275.

[18] European Aviation Safety Agency (EASA), "Explanatory note on 'Prototype' Commission Regulation on Unmanned Aircraft Operations," 2016.

[19] Joint Authorities for Rulemaking of Unmanned Systems (JARUS) Working Group 6: UAS System Safety Analysis (1309), "Remotely Piloted Aircraft Systems; Systems Safety Assessment," *Scoping Paper to AMC RPAS 1309*, no. 1. 2014.

[20] The European Organisation for Civil Aviation Equipment (EUROCAE), "UAS / RPAS Airworthiness Certification '1309' System Safety Objectives and Assessment Criteria," MALAKOFF, France, 2013.

[21] European Aviation Safety Agency (EASA), "Advance -Notice of Proposed Amendment (NPA) No. 16/2005, Policy for Unmanned Aerial Vehicle (UAV) certification," 2005.

[22] NATO Standardization Agency (NSA), "STANAG 4671 (Edition 1) - Unmanned Aerial Vehicles Systems Airworthiness Requirments (USAR)," Brussels, Belgium, 2009.

[23] Joint Authorities for Rulemaking on Unmanned Systems (JARUS) Working Group 6 (system safety), "AMC UAS.1309 development," Brussels, 2012.

[24] Australian Defence Force (ADF), "Australian Air Publication 7001.054, Electronic Airworthiness Design Requirements Manual (eADRM)," Australia, 2017.

[25] International Civil Aviation Organisation (ICAO), "Safety Management Manual (SMM),Doc 9859 (2nd Ed)," Quebec, Canada, 2009.

[26] Federal Aviation Administration (FAA), "FAA Order 8000.369B - Safety Management System," U.S. Department of Transportation, Washington, DC, United States of America., 2016.

[27] Civil Aviation Authority (CAA), "Safety Management Systems (SMS) guidance for organisations, CAP 795," London, United Kingdom, 2014.

[28] Civil Aviation Safety Authority (CASA), "SMS 3: Safety Risk Management: SMS for Aviation, A Practical Guide (2nd Ed)," Canberra, Australia, 2014.

[29] SAE ARP4761, "Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment." SAE International, 1996.

[30] SAE ARP 5150, "Safety Assessment of Transport Airplanes in Commercial Service," 2013.

[31] Civil Aviation Authority (CAA), "Guidance on the Conduct of Hazard Identification, Risk Assessment and the Production of Safety Cases, Cap 760," United Kingdom, 2010.

[32] European Aviation Safety Agency (EASA), "Notice of Proposed Amendment 2017-20," 2017.

[33] M. E. Paté-Cornell, "Uncertainties in risk analysis: Six levels of treatment," *Reliab. Eng. Syst. Saf.*, vol. 54, no. 2–3, pp. 95–111, 1996.

[34] B. M. Ayyub, *Risk Analysis in Engineering and Economics*, Second Ed. Chapman and Hall / CRC, 2014.

[35] Federal Aviation Administration (FAA), "Advisory Circular 23.1309-1E, System Safety Analysis and Assessment for Part 23 Airplanes.," U.S. Department of Transportation, Washington, DC, United States of America., 2011.

[36] B. M. Ayyub, "Experts, opinions, and elicitation methods," in *Elicitation of Expert Opinions for Uncertanty and Risks*, CRC Press, 2001.

[37] R. A. Clothier, "Decision Support for the Safe Design and Operation of Unmanned Aircraft

Systems," Queensland University of Technology, Queensland , Australia, 2012.

[38] S. Kaplan and B. J. Garrick, "On the quantitative definition of Risk," *Risk Anal.*, vol. 1, no. 1, pp. 11–27, 1981.

[39] B. Meacham, "Understanding Risk: Quantification, Perceptions, and Characterization.," *J. Fire Prot. Eng.*, vol. 14, no. 3, pp. 199–227, 2004.

[40] Federal Aviation Administration (FAA), "Risk Management Handbook," US Department of Transportation Washington D.C., United States of America, 2009.

[41] P. B. Ladkin, "Problems Calculating Risk Via Hazard," in *Causal System Analysis*, Springer London ltd, 2005.

[42] Ministry of Defence, "Defence Standard 00-56 Safety Management Requirements for Defence Systems Part 1 Requirements," United Kingdom, 2007.

[43] J. McDermid, "Software Hazard and Safety Analysis," in *Formal Techniques in Real-Time and Fault- Tolerant Systems.FTRTFT 2002*, W. Damm and E. R. Olderog, Eds. Springer, Berlin, Heidelberg, 2002, pp. 23–34.

[44] Department of Defense (DoD), "Standard Practice for System Safety," United States of America, 2000.

[45] D. R. Williams, *What is Safe? :Risks of living in a Nuclear Age*. Royal Society of Chemistry, 1998.

[46] N. Leveson, *Safeware: System Safety and Computers*. Massachusetts: Addison-Wesley, 1995.

[47] Department of Defense (DoD), "Department of Defense Standard Practice -System Safety- (MIL-STD-882E)," Unted States of America, 2012.

[48] Federal Aviation Administration (FAA), "Operational Risk Management (ORM)," in *System Safety Handbook*, US Department of Transportation Washington D.C., United States of America, 2000, pp. 1–23.

[49] E. Zio and N. Pedroni, *Risk Analysis - Uncertainty Characterization in Risk Analysis for Decision- Making Practice*. Foundation for an Industrial Safety Culture, Toulouse, France, 2012.

[50] T. Aven, *Foundations of Risk Analysis: A Knowledge and Decision-Oriented Perspective*. John

Wiley and Sons, 2004.

[51] W. W. Lowrance, *Of Acceptable Risk: Science and the Determination of Safety*. Los Altos, California: WIlliam Kaufmann Inc, 1976.

[52] V. T. Covello and M. W. Merkhofer, *Risk Assessment Methods, Approaches for Assessing Health and Environmental Risks*. New York: Springer Science + Business Media, 1993.

[53] J. M. Woodruff, "Consequence and likelihood in risk estimation: A matter of balance in UK health and safety risk assessment practice," *Saf. Sci.*, vol. 43, no. 5–6, pp. 345–353, 2005.

[54] P. L. Bernstein, *Against the Gods: the remarkable story of Risk*. John Wiley and Sons, 1998.

[55] International Civil Aviation Organization (ICAO), *International Standards and Recommended Practices: Annex 19 to the Convention on International Civil Aviation: Safety Management*, 1st ed. 2013.

[56] Federal Aviation Administration (FAA), "System Safety Handbook," US Department of Transportation Washington D.C.,United States of America, 2000.

[57] L. Wildman *et al.*, "Guidance for Def (Aust) 5679 Issue 2," in *13th Australian Workshop on Safety-Related Programmable Systems,Canberra, Australia*, 2008.

[58] P. B. Ladkin, "Definitions for system safety analysis," in *Causal System Analysis*, Springer-Verlag, Heidelberg and London, 2001.

[59] National Research Council Assembly of Engineering Committee on Flight Airworthiness Certification Procedures, "Improving aircraft safety: FAA certification of commercial passenger aircraft," Washington D.C., 1980.

[60] N. Moller, S. O. Hansson, and M. Peterson, "Safety is more than the antonym of risk," *J. Appl. Philos.*, vol. 23, no. 4, pp. 419–432, 2006.

[61] C. G. Jardine and S. E. Hrudey, "Mixed Messages in Risk Communication," *Risk Anal.*, vol. 17, no. 4, pp. 489–498, 1997.

[62] N. Moller, "The Concepts of Risk and Safety," in *Handbook of Risk Theory*, S. Roeser, R. Hillerbrand, P. Sandin, M. Peterson, T. Trautmann, and F. M. Vieider, Eds. Springer, 2012, pp. 56–85.

[63] Civil Aviation Authority (CAA), "CAP-722, Unmanned Aircraft System Operations in UK

Airspace - Guidance," London, UK, 2015.

[64] Defence Aviation Safety Authority (DASA), "Notice of Proposed Amendment NPA 04/2017, Defence Aviation Safety Regulations for Unmanned Aircraft Systems (DASR UAS)," Department of Defence, Australia, 2017.

[65] Health and Safety Executive (HSE), "Reducing risks, protecting people, HSE's decision-making process," Norwich, United Kingdom, 2001.

[66] Civil Aviation Safety Authority (CASA), "SMS 3:Safety risk management, SMS for Aviation - A Practical Guide," Australia, 2014.

[67] Department of Defence; Defence Aviation Safety Program, "Australian Air Publication 7001.048 Defence Aviation Safety Program Manual," Australian Government, 2012.

[68] Health and Safety Executive (HSE), "Principles and guidelines to assist HSE in its judgements that duty-holders have reduced risk as low as reasonably practicable," United Kingdom, 2001.

[69] R. A. Clothier, B. P. Williams, N. L. Fulton, and X. Lin, "ALARP and the risk management of civil unmanned aircraft systems," in *Australian System Safety Conference (ASSC 2013), Adelaide, 22-24 May*, 2013.

[70] D. Proske and P. van Gelder, *Safety of Historical Stone Arch Bridges*. Heidelberg: Springer-Verlag, 2009.

[71] H. Dezfuli, D. Kelly, C. Smith, K. Vedros, and W. Galyean, "Bayesian Inference for NASA Probabilistic Risk and Reliability Analysis, NASA/SP-2009-569," National Aeronautics and Space Administration (NASA), 2009.

[72] B. Wynne, "Uncertainty and environmental learning: Reconceiving science and policy in the preventive paradigm," *Glob. Environ. Chang.*, vol. 2, no. 2, pp. 111–127, 1992.

[73] F. H. Knight, *Risk, uncertainty and profit*. Houghton Mifflin Co., 1921.

[74] M. B. A. van Asselt and J. Rotmans, "Uncertainty in integrated assessment modelling: From positivism to pluralism," *Clim. Chang.*, vol. 54, no. 1, pp. 75–105, 2002.

[75] W. E. Walker, P. Harremoes, J. P. Van der Slujis, M. B. A. Van Asselt, P. Janssen, and K. von Krauss, "Defining uncertainty: A conceptual basis for uncertainty management in model based decision support," *Integr. Assess.*, vol. 4, no. 1, pp. 5–17, 2003.

[76] B. M. Ayyub, “Expressing and modeling expert opinions,” in *Elicitation of Expert Opinions for Uncertainty and Risks*, CRC Press LLC, Florida, 2001, pp. 125–206.

[77] H. Riesch, “Levels of Uncertainty,” in *Essentials of Risk Theory*, S. Roeser, R. Hillerbrand, P. Sandin, and M. Peterson, Eds. Springer, 2013, pp. 29–56.

[78] T. Aven, “Some reflections on uncertainty analysis and management,” *Reliab. Eng. Syst. Saf.*, vol. 95, no. 3, pp. 195–201, 2010.

[79] D. J. Spiegelhalter and H. Riesch, “Don’t know, can’t know: embracing deeper uncertainties when analysing risks,” *Philos. Trans. R. Soc. A Math. Phys. Eng. Sci.*, vol. 369, pp. 4730–4750, 2011.

[80] D. H. Rumsfield, “News transcript,” *U.S.Department of Defense (DoD)*, 2002. [Online]. Available: http://www.defense.gov/transcripts/transcript.aspx?transcriptid=2636. [Accessed: 18-Jul-2015].

[81] B. Ayyub, “Consensus and Aggregating expert opinions,” in *Elicitation of Expert Opinions for Uncertainty and Risks*, CRC Press LLC, 2001, pp. 207–232.

[82] S. M. Macgill and Y. L. Siu, “The nature of risk,” *J. Risk Res.*, vol. 7, no. 3, pp. 315–352, 2004.

[83] T. Aven and E. Zio, “Some considerations on the treatment of uncertainties in risk assessment for practical decision making,” *Reliab. Eng. Syst. Saf.*, vol. 96, no. 1, pp. 64–74, 2011.

[84] E. Zio and N. Pedroni, *Methods for representing uncertainty: A literature review*. Foundation for an Industrial Safety Culture, 2013.

[85] W. M. Bolstad, *Introduction to Bayesian Statistics*, 2nd ed. John Wiley & Sons, 2007.

[86] T. Nilsen and T. Aven, “Models and model uncertainty in the context of risk analysis,” *Reliab. Eng. Syst. Saf.*, vol. 79, no. 3, pp. 309–317, 2003.

[87] S. Guarro, “Risk assessment of new space launch and supply vehicles,” in *11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012, PSAM11 ESREL 2012*, 2012, pp. 5157–5164.

[88] S. D. Guikema and M. E. Pate-Cornell, “Bayesian Analysis of Launch Vehicle Success Rates,” *J. Spacecr. Rockets*, vol. 41, no. 1, pp. 93–102, 2004.

[89] A. T. Morris and P. A. Beling, “Space Shuttle RTOS Bayesian Network,” *20th DASC. 20th*

Digit. Avion. Syst. Conf. (Cat. No.01CH37219), 2001.

[90] N. J. Lindsey, N. Rackley, A. Brali, and A. Mosleh, “Reliability Prediction Using Bayesian Updating of On-Orbit Performance,” NASA Technical Reports Server (NTRS), 2013.

[91] D. L. Kelly and C. L. Smith, “Risk Analysis of the Space Shuttle : Pre- Challenger Bayesian Prediction of Failure,” in *NASA Space Systems Engineering & Risk Management Symposium*, 2008.

[92] C. J. Maranzano and R. Krzysztofowicz, “Bayesian reanalysis of the challenger O-ring data,” *Risk Anal.*, vol. 28, no. 4, pp. 1053–1067, 2008.

[93] US Nuclear Regulatory Commision, “Reactor safety study, An assessment of accident risks in U. S. commercial nuclear power plants,” 1975.

[94] H. Z. Huang, M. J. Zuo, and Z. Q. Sun, “Bayesian reliability analysis for fuzzy lifetime data,” *Fuzzy Sets Syst.*, vol. 157, no. 12, pp. 1674–1686, 2006.

[95] K. Ozbay and N. Noyan, “Estimation of incident clearance times using Bayesian Networks approach,” *Accid. Anal. Prev.*, vol. 38, no. 3, pp. 542–555, 2006.

[96] G. Apostolakis, “Bayesian Methods in Risk Assessment,” in *Advances in Nuclear Science and Technology*, Springer US, 1981, pp. 415–465.

[97] P. Wieland and L. J. Lustosa, “Modeling Operational Risks of the Nuclear Industry With Bayesian Networks,” in *nternational Nuclear Atlantic Conference - INAC 2009*, 2009.

[98] A. E. Punt and R. Hilborn, “Fisheries stock assessment and decision analysis: the Bayesian approach,” *Rev. Fish Biol. Fish.*, vol. 7, no. 1, pp. 35–63, 1997.

[99] A. M. Ellison, “An Introduction to Bayesian Inference for Ecological Research and Environmental Decision-Making,” *Ecol. Soc. Am.*, vol. 6, no. 4, pp. 1036–1046, 1996.

[100] R. K. McCann, B. G. Marcot, and R. Ellis, “Bayesian Belief Networks: applications in ecology and natural resource management.,” *Can. J. For. Res.*, vol. 36, pp. 3053–3062, 2006.

[101] B. G. Marcot, R. S. Holthausen, M. G. Raphael, M. M. Rowland, and M. J. Wisdom, “Using Bayesian belief networks to evaluate fish and wildlife population viability under land management alternatives from an environmental impact statement,” *For. Ecol. Manage.*, vol. 153, no. 1–3, pp. 29–42, 2001.

[102] Mallick B.K., D. Gold, and V. Baladandayuthapani, *Bayesian analysis of Gene expression data*. John Wiley & Sons, 2009.

[103] P. R. Wade, “Bayesian methods in conservation biology,” *Conserv. Biol.*, vol. 14, pp. 1308–1316, 2000.

[104] E. Ancel, A. T. Shih, S. M. Jones, M. S. Reveley, J. T. Luxhøj, and J. K. Evans, “Predictive safety analytics: inferring aviation accident shaping factors and causation,” *J. Risk Res.*, vol. 18, no. 4, pp. 428–451, 2015.

[105] E. Ancel and A. T. Shih, “Bayesian Safety Risk Modeling of Human-Flightdeck Automation Interaction: NASA/TM-2015-218791,” National Aeronautics and Space Administration (NASA), Langley Research Centre. Hampton Virginia, 2015.

[106] J. T. Luxhøj and M. B. Harrell, “An Object-Oriented Bayesian Network (OOBN) Prototype for Modeling the Safety Risk of an Unmanned Rotorcraft,” in *IIE Annual Conference and Expo 2015*, 2015, pp. 183–192.

[107] A. Klinke and O. Renn, “A new approach to risk evaluation and management: Risk-based, precaution-based, and discourse-based strategies,” *Risk Anal.*, vol. 22, no. 6, pp. 1071–1094, 2002.

[108] M. W. Merkhofer, *Decision Science and Social Risk Management: A Comparative Evaluation of Cost-Benefit Analysis, Decision Analysis, and Other Formal Decision-Aiding Approaches*. D. Reidel Publishing Company, Holland, 1987.

[109] M. H. Faber, “Statistics and Probability Theory in Pursuit of Engineering Decision Support,” in *Topics in Safety, Risk, Reliability and Quality*, vol. 18, A. V. Gheorghe, Ed. Springer, 2012.

[110] T. Aven, “On how to define, understand and describe risk,” *Reliab. Eng. Syst. Saf.*, vol. 95, no. 6, pp. 623–631, 2010.

[111] International Organization for Standardization (ISO), “Risk Management - Principles and Guidelines. ISO 31000:2009,” Geneva, 2009.

[112] M. Peterson, *An Introduction to Decision Theory*. Cambridge University Press, 2009.

[113] J. Black, N. Hashimzade, and G. Myles, *A Dictionary of Economics*, 5th ed. Oxford University Press, 2017.

[114] T. Hens and K. Bachmann, “Decision Thoery,” in *Behavioural Finance for Private Banking*,

John Wiley & Sons Ltd, 2008.

[115] S. O. Hansson, *Decision Theory, A Brief Introduction*. Royal Institute of Technology, 2005.

[116] E. Zio and N. Pedroni, *Risk-informed decision-making processes: An Overview*. Foundation for an Industrial Safety Culture, France, 2012.

[117] E. Zio, "Reliability Engineering: Old Problems and New Challenges," *Reliab. Eng. Syst. Saf.*, vol. 94, no. 2, pp. 125–141, 2009.

[118] National Aeronautics and Space Administration (NASA), "NASA Risk-Informed Decision Making Handbook, NASP/SP-2010-576, Version 1.0," Office of Safety and Misssion Assurance, NASA Headquarters, United States of America, 2010.

[119] E. T. Jaynes, *Probability Theory: The Logic of Science*. Cambridge University Press, 2003.

[120] J. Rasmussen, "Risk Management in a Dynamic Society: A Modelling Problem," *Saf. Sci.*, vol. 27, no. 2, pp. 183–213, 1997.

[121] International Organization of Standards (ISO), "International Standard: Risk management - Principles and guidelines ISO 31000:2018(E)," 2018.

[122] International Civil Aviation Organization (ICAO), "Safety Management Manual (SMM), Doc 9859 (3rd Ed)," Montreal, Canada, 2013.

[123] A. Lammerding and A. Fazil, "Hazard identification and exposure assessment for microbial food safety risk assessment.," *Int. J. Food Microbiol.*, vol. 58, no. 3, pp. 147–157, 2000.

[124] A. Mcfadyen, T. Martin, and T. Perez, "Low-level Collision Risk Modelling for Unmanned Aircraft Integration and Management," *IEEE Aerosp. Conf. MT, USA*, pp. 1–10, 2018.

[125] A. Mcfadyen, T. Martin, and L. Mejias, "Simulation and modelling tools for quantitative safety assessments of unmanned aircraft systems and operations," in *2016 IEEE Aerospace Conference, MT, USA*, 2016, pp. 1–12.

[126] K. M. Thompson and J. D. Graham, "Going beyond the single number: Using probabilistic risk assessment to improve risk management," *Hum. Ecol. Risk Assess. An Int. J.*, vol. 2, no. 4, pp. 1008–1034, 1996.

[127] H. J. Zimmermann, "An application-oriented view of modeling uncertainty," *Eur. J. Oper. Res.*, vol. 122, no. 2, pp. 190–198, 2000.

[128] R. L. Armacost and J. Pet-Edwards, "Integrative risk and uncertainty analysis for complex public sector operational systems," *Socioecon. Plann. Sci.*, vol. 33, no. 2, pp. 105–130, 1999.

[129] L. A. (Tony) Cox, "What ' s Wrong with Risk Matrices ?," *Risk Anal.*, vol. 28, no. 2, pp. 497–512, 2008.

[130] European Aviation Safety Agency (EASA), "EASA News Release: EASA presents new regulatory approach for Remotely Piloted Aircraft (RPAS)," 2015. [Online]. Available: https://www.easa.europa.eu/newsroom-and-events/news/easa-presents-new-regulatory-approach-remotely-piloted-aircraft-rpas. [Accessed: 15-Jul-2016].

[131] J. A. Ball, M. Knott, and D. Burke, "Crash Lethality Model: Technical Report no. NAWCADPAX/TR-2012/196," Naval Air Warfare Centre Aircraft Division, Maryland, USA, 2012.

[132] A. Washington, R. A. Clothier, and J. Silva, "A review of unmanned aircraft system ground risk models," *Prog. Aerosp. Sci.*, vol. 95, pp. 24–44, 2017.

[133] R. A. Clothier and P. P. Wu, "A Review of System Safety Failure Probability Objectives for Unmanned Aircraft Systems," in *11th International Probabilistic Safety Assessment and Management (PSAM11) Conference and the Annual European Safety and Reliability(ESREL 2012) Conference, Helsinki*, 2012.

[134] Federal Aviation Administration (FAA), "Advisory Circular 25.1309-1A, System Design and Analysis," US Department of Transportation, Washington, DC, United States of America., 1988.

[135] Joint Authorities for Rulemaking of Unmanned Systems (JARUS) Working Group 6 -Safety and Risk Assessment, "Safety Assessment of Remotely Piloted Aircraft Systems," *AMC RPAS.1309*, no. 2, 2015.

[136] K. J. Hayhurst *et al.*, "NASA TM-2007-21439. Preliminary considerations for classifying hazards of unmanned aircraft systems," National Aeronautics and Space Administration (NASA), Langley Research Centre. Hampton Virginia, 2007.

[137] North Atlantic Treaty Organization (NATO), "NATO Standard AEP-83. Light Unmanned Aircraft Systems Airworthiness Requirements," 2014.

[138] RTCA Special Committee 203 (SC-203), "RTCA DO-344. Operational and Functional Requirements and Safety Objectives (OFRSO) for Unmanned Aircraft Systems (UAS) Standards, Volume 2," Washington D.C., 2013.

[139] R. Clothier, A. Washington, B. Williams, and K. Cox, “Accounting for Uncertainty in System Safety Assessments,” in *DGTA System Safety and Software Conference, Sept, RAAF Laverton, Melbourne, Australia.*, 2016.

[140] K. Dalamagkidis, K. P. Valavanis, and L. A. Piegl, *On integrating unmanned aircraft systems into the national airspace system*, 2nd ed. Springer, 2012.

[141] R. Melnyk, D. Schrage, V. Volovoi, and H. Jimenez, “A third-party casualty prediction model for UAS operations,” Georgia Institute of Technology, 2013.

[142] B. Waggoner, “Developing a Risk Assessment Tool for Unmanned Aircraft System Operations,” University of Washington, 2010.

[143] C. W. Lum and B. Waggoner, “A Risk Based Paradigm and Model for Unmanned Aerial Systems in the National Airspace,” in *Proc. AIAA Infotech@Aerospace 2011 Conference, St. Louis, MO*, 2011, pp. 1–31.

[144] R. A. Clothier, R. A. Walker, N. Fulton, and D. A. Campbell, “A casualty risk analysis for unmanned aerial system (UAS) operations over inhabited areas,” in *AIAC12: Twelfth Australian International Aerospace Congress, Second Australasian Unmanned Air Vehicle Conference, Melbourne, Australia*, 2007, pp. 1–15.

[145] International Organization for Standardization (ISO), “ISO/IEC Guide 73:2002 - Risk management - Vocabulary - Guidelines for use in standards,” 2002.

[146] Standards Australia, “AS/NZS ISO 31000:2009- Risk Management - Principles and guidelines,” Australia, 2009.

[147] The Strategy Unit, “Risk: Improving government’s capability to handle risk and uncertainty. Summary Report,” Cabinet Office, United Kingdom, 2002.

[148] R. W. Kates, C. Hohememser, and J. X. Kasperson, *Perilous Progress: Managing the Hazards of Technology*. Westview Press, 1985.

[149] T. Aven, *Risk Analysis: Assessing Uncertainties beyond Expected Values and Probabilities*. John Wiley & Sons Ltd, 2008.

[150] T. Aven and O. Renn, “On risk defined as an event where the outcome is uncertain,” *J. Risk Res.*, vol. 12, no. 1, pp. 1–11, 2009.

[151] E. J. Douglas, “Managerial Economics: theory, practice and problems,” *Prentice Hall*, 1983.

[152] N. Fenton and M. Neil, *Risk Assessment and Decision Analysis with Bayesian Networks*. CRC Press, Taylor and Francis Group, 2013.

[153] L. Held and D. Sabanés Bové, *Applied Statistical Inference - Likelihood and Bayes*. Springer, 2013.

[154] D. Kelly and C. Smith, *Bayesian Inference for Probabilistic Risk Assessment: A Practitioners Guidebook*. London: Springer, 2011.

[155] P. M. Lee, *Bayesian Statistics an Introduction*, 4th ed. Chichester, West Sussex: Hoboken, N.J., 2012.

[156] L. Broemeling, *Bayesian Methods for Measures of Agreement*. Boca Raton: CRC Press, 2009.

[157] C. G. Kevorkian, "UAS Risk Analysis using Bayesian Belief Networks : An Application to the Virginia Tech ESPAARO," Virginia Polytechnic Institute and State University, 2016.

[158] F. V. Jensen and T. D. Nielsen, *Bayesian Networks and Decision Graphs*, 2nd ed. Springer Science & Business Media, 2007.

[159] R. R. Rhinehart, "Propagation of Uncertainty," in *Nonlinear Regression Modeling for Engineering Applications: Modeling, Model Validation, and Enabling Design of Experiments*, 1st ed., Chichester, UK: John Wiley & Sons Ltd, 2016, pp. 41–66.

[160] S. V. Gupta, "Propagation of Uncertainty," in *Measurement Uncertainties: Physical Parameters and Calibration of Instruments*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 109–129.

[161] C. Servin and V. Kreinovich, *Propagation of Interval and Probabilistic Uncertainty in Cyberinfrastructure-Related Data Processing and Data Fusion*, 1st ed. Springer International Publishing, 2015.