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

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).

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

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