Safety Science 101 (2018) 33–47

Contents lists available at ScienceDirect

Safety Science

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

Modelling the risks remotely piloted aircraft pose to people on the ground

Reece A. Clothier[a,b,*], Brendan P. Williams[a], Kelly J. Hayhurst[c]

[a] Boeing Research & Technology, Australia
[b] School of Engineering, RMIT University, Melbourne, VIC, Australia
[c] NASA Langley Research Center, 1 South Wright St, MS 130, Hampton, VA 23681-2199, USA

A R T I C L E I N F O

Keywords:
Unmanned Aircraft System
Remotely piloted aircraft systems
Airworthiness
Barrier Bow Tie Model
Safety case
Risk

A B S T R A C T

Regulations for remotely piloted aircraft systems (RPAS) should have a strong foundation in, and traceability to, the management of the safety risks. This paper describes a new approach for modelling the risks associated with RPAS operations near populous areas to support the development of regulations and safety cases. A review found that existing models do not provide a simple means for incorporating the wide range of technical and operational controls into the risk analysis process. A Barrier Bow Tie Model (BBTM) is proposed as it focuses risk analysis, evaluation, and decision-making activities on the practical devices, people, and processes that can be used to reduce risk. Existing literature and practical controls were reviewed and used to define the components of the model and a case study is used to exemplify its application. More than 50 practical controls were incorporated into the model. The template barriers, controls, and graphical nature of the BBTM facilitated a simple comparison of the two case study RPAS operations and a more structured approach to the setting of airworthiness requirements taking into consideration the wide range of technical and operational factors that can be used to manage risk. The model provides the linkage between a regulation, associated controls, and how the controls contribute to a reduction in risk, which is necessary for the adoption of a risk-based approach to the regulation of RPAS. The BBTM provides a generic framework that can be used to structure the development of safety cases for any RPA operation.

1. Introduction

Remotely piloted aircraft systems (RPAS)[1] are one of the fastest growing aviation sectors. Like all technologies there are risks associated with their use, which arise due to the two primary hazards of Clothier and Walker (2014):

- A collision between a remotely piloted aircraft (RPA)[2] and another aircraft (whether the other aircraft is in the air or on the ground);
- The impact of the RPA, or its components, with people or structures situated on the ground.

The scope of this paper is limited to the latter of these two hazards. The risk to people and property on the ground are primarily addressed through the development and promulgation of airworthiness regulations (Clothier et al., 2011, 2015a). Airworthiness can be broadly defined as a measure of the suitability for flight of an aircraft system. In civil aviation regulations an "airworthy aircraft" is generally considered as the state where an aircraft is compliant to relevant technical requirements governing its design and manufacture, and is in a condition for safe flight. The regulations not only relate to technical standards but also the organizations, people, and processes used in the design, manufacture, and maintenance of the system.

Consensus between National Airworthiness Authorities (NAAs) on a framework of airworthiness regulations for RPAS has yet to be reached. The initial approach adopted by NAAs was to adopt and adapt the existing manned airworthiness regulatory framework (Dalamagkidis et al., 2008). However, this "off-the-shelf approach" (Clothier et al., 2008) is unlikely to lead to an acceptable regulatory outcome for all RPA types (Clothier et al., 2011). More recently NAAs have advocated the adoption of a risk-based approach (Concept of Operations for Drones – A Risk Based Approach to Regulation of Unmanned Aircraft, 2015). Under a risk-based approach, regulation development is guided by a risk management process, which comprises activities to identify, assess, evaluate and treat risks (refer to ISO 31000:2009, AS/NZS ISO 31000, 2009). Regulations essentially become legal requirements for the implementation of controls or measures to modify, mitigate, or otherwise reduce the risk (Clothier et al., 2015b).

* Corresponding author at: Boeing Research & Technology - Australia, Boeing Defence Australia GPO Box 767, Brisbane, QLD, Australia.
E-mail addresses: reece.a.clothier@boeing.com (R.A. Clothier), brendan.p.williams@boeing.com (B.P. Williams), kelly.j.hayhurst@nasa.gov (K.J. Hayhurst).

[1] Also referred to as unmanned aircraft systems or drones.
[2] RPA is the flying component of a remotely piloted aircraft system.

http://dx.doi.org/10.1016/j.ssci.2017.08.008
Received 8 December 2016; Received in revised form 30 June 2017; Accepted 7 August 2017
0925-7535/

Essential to any risk-based approach are models that can be used to assess (qualitatively or quantitatively) identified risks. A comprehensive literature review was undertaken to identify relevant models. The review identified:

- Models of failures leading to RPA unintended ground impact (Ozuncer et al., 2011);
- High-level risk models relating the system-level failures to ground causalities (Weibel and John Hansman, 2004; King et al., 2005; Clothier et al., 2007; Dalamagkidis et al., 2008; Ford and McEntee, 2010; Lum et al., 2011; Wolf, 2012; Knott et al., 2012; Melnyk et al., 2014; Guglieri et al., 2014; Aalmoes et al., 2015). Some of the factors considered within these models include the trajectory under failure, energy on impact, the distribution and density of population on the ground, and population sheltering;
- Models for predicting the location of impact given the occurrence of a failure (Wu and Clothier, 2012; Bradley and Burke, 2012);
- Modeling and analysis to explore the relationship between the impact conditions of the RPA (e.g., energy, composition, dimensions, and frangibility) and the level of harm caused to the people and property impacted (Clothier et al., 2010; Magister, 2010; Fraser and Donnithorne-Tait, 2011; Ball et al., 2013; Radi, 2013).

There is a wide range of technical and operational controls that could be used to reduce the risk associated with RPAS operations in the vicinity of populated areas (see Clothier and Walker, 2014) and these are not taken into account in existing models (Weibel and John Hansman, 2004; King et al., 2005; Clothier et al., 2007; Dalamagkidis et al., 2008; Ford and McEntee, 2010; Lum et al., 2011; Wolf, 2012; Knott et al., 2012; Melnyk et al., 2014; Guglieri et al., 2014; Aalmoes et al., 2015). An additional model is needed to provide a systematic classification of the different controls available to manage the risk of RPAS operations, and to characterize how these controls contribute towards a reduction in risk.

In this paper a new qualitative barrier bow tie model (BBTM) is proposed based on the preliminary framework developed in Clothier et al. (2015b), Williams et al. (2014). The BBTM focuses the analysis and subsequent decision-making activities on the risk controls (i.e., the practical devices, policies, or processes) that can be implemented and can provide an over-arching framework for existing models. Section 2 of this paper describes the components of the BBT model and Section 2 describes the application of a BBTM to RPA operations over populous areas. Finally a case study RPAS operation is described using the BBT modeling in Section 4.

2. Barrier bow tie models

A BBTM is a graphical tool for representing risk scenarios associated with a particular hazard, combining the bow tie analysis methodology and recent barrier models. The first known record of a BBTM was in Imperial Chemistry Industry course notes on hazard analysis, delivered in 1979 at the University of Queensland, Australia (Lewis and Smith, 2010). The Royal Dutch/Shell Group developed the BBTM as a company standard to "seek assurance that fit-for-purpose risk controls were consistently in place throughout all operations world-wide" (Lewis and Smith, 2010). Since then, BBTMs have "achieved widespread popularity" (Australian Air Publication 6734.001, 2012) being applied in the risk management of a wide range of industries, including defense, oil and gas, medical, and food production sectors (Lewis and Smith, 2010; Acfield and Weaver, 2012).

Within the aviation sector, the United Kingdom Civil Aviation Authority has defined a strategy to "identify how to maximize the use of bow tie risk models as an effective and proactive safety risk management tool, both by the CAA and industry…" (CAA Strategy for Bowtie Risk Models, 2015). A BBTM is used for all operational risk assessment by Australian air traffic service provider Airservices Australia (Acfield and Weaver, 2012). Further, the Australian Defence Force (ADF) recommends the use of BBTMs, stating that they are "particularly useful in proactive accident and incident prevention, and the management of safety within a system" (Australian Air Publication 6734.001, 2012) and have provided an example operational analysis for RPAS using a BBTM (p.3A1-AS2, Australian Air Publication 7001.048, 2012). BBTMs have been previously applied to the risk management of RPAS operations in non-segregated airspace (Air Traffic Management Guidelines for Global Hawk in European Airspace, 2010; Unmanned Aircraft Systems – ATM Collision Avoidance Requirements, 2010; Clothier et al., 2015c).

2.1. Advantages and disadvantages

BBTMs provide a simple means for relating identified risks to the practical activities that can be undertaken to mitigate them. They are specifically designed to "illustrate the physical and procedural controls that are in place to manage hazards" (Australian Air Publication 6734.001, 2012) and provide a simple means for representing all the applicable events as well as the relationships between them (Acfield and Weaver, 2012) and their graphical nature can be easily communicated and comprehended by a wide range of stakeholders (Ozuncer et al., 2011; Lewis and Smith, 2010; Acfield and Weaver, 2012).

A BBTM can bring together elements from domains "traditionally treated separately" (Acfield and Weaver, 2012). Threats due to human error, procedure error, equipment failure and also external, management and organizational factors that can contribute to a common top event can all be represented in a single model (Acfield and Weaver, 2012). A BBTM can also be used as an over-arching risk framework; bringing together other analysis techniques such as fault tree analyses (FTA), event tree analyses (ETA), failure mode, effects and criticality analysis (FMECA), software assurance techniques, and human factor analyses (Acfield and Weaver, 2012). Further, they can be readily integrated with generally accepted organizational system models, such as James Reason's Swiss Cheese Model (Reason, 1997) of the organizational accident (Clothier et al., 2015b; Lewis and Smith, 2010; Acfield and Weaver, 2012). Perhaps the most significant advantage of a BBTM is that it focuses analysis and decision making on the mechanisms for controlling risk and can help to establish the relationships between implemented risk controls, the mechanisms for assurance in the provision of those controls, and the consequences associated with the loss (or breach) of controls across multiple accident scenarios (Clothier et al., 2015b).

A disadvantage is that a separate BBTM must be created for each identified top event, and the subsequent models are not necessarily independent. The depiction of barriers within a BBTM can also be misleading; giving the impression that barriers are independent. Independence between barriers cannot be assumed. The dependencies between barriers need to be established through analysis of the environmental and organizational factors, and through the identification of controls contributing to multiple barriers. The relationships between controls, barriers and the different BBTMs must be identified and maintained using separate tools (e.g., a detailed risk register or dependency diagram).

2.2. BBTMs and the risk management process

A BBTM can be used in the risk identification process to assist in the identification and structuring of risk scenarios for an identified hazard and associated top event. However, BBTMs are not a hazard identification tool nor can they be used to identify the threats, controls, or consequence states.

The primary use of BBTMs is in the risk analysis, evaluation, and treatment processes. BBTMs can be used to support qualitative or quantitative analysis of the risks. A BBTM can be used to support judgments of the acceptability of risks, and is particularly useful in