Managing the Risks Remotely Piloted Aircraft Operations Pose to People and Property on the Ground

Reece A. Clothier, Brendan P. Williams and Kelly J. Hayhurst

July 21, 2016

Abstract

Worldwide there is much effort being directed towards the development of a framework of airworthiness regulations for remotely piloted aircraft systems (RPAS). It is now broadly accepted that regulations should have a strong foundation in, and traceability to, the management of the safety risks. Existing risk models for RPAS operations do not provide a simple means for incorporating the wide range of technical and operational controls into the risk analysis and evaluation processes. This paper describes a new approach for modelling and evaluating the risks associated with RPAS operations near populous areas based on the barrier bow tie (BBT) model. A BBT model is used to structure the underlying risk management problem. The model focuses risk analysis, evaluation, and decision making activities on the devices, people, and processes that can be employed to reduce risk. The BBT model and a comprehensive set of example risk controls are presented. The general model can be applied to any RPAS operation. The foundations for quantitative and qualitative assessments using a BBT model are also presented. The modelling and evaluation framework is illustrated through its application to a case-study rotary wing RPAS for two operational scenarios. The model can be used as a basis for determining airworthiness certification requirements for RPAS.
1 Introduction

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

- A collision between an remotely piloted aircraft (RPA) 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 management of the risks associated with 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 [2, 3]. 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 organisations, people, and processes used in the design, manufacture, and maintenance of the system.

In most countries RPAS are required to be in an airworthy condition in order to conduct flights in the National Airspace System (NAS) (refer to Volume 16, Chapter 2, Section 1, Paragraph 3 [4]). However, airworthiness regulations for the broad spectrum of RPA types have yet to be developed. 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 apply the existing manned airworthiness regulatory framework to RPAS [5]. However, this “off-the-shelf approach” [6] is unlikely to lead to an acceptable regulatory outcome for all RPA types [2]. More recently NAAs have advocated the adoption of a risk-based approach [7]. 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 [8]). Regulations become “the legislative embodiment of the outcomes of the risk management process. Specifically, they are legal requirements describing how various stakeholders (e.g., RPAS operators) should go about treating safety risks; requirements relating to the implementation of controls or measures to modify, mitigate, or otherwise reduce the risk” [9]. A risk-based approach ensures safety regulations have a foundation in, and traceability to, the underlying safety-related hazards that need to be managed. The adoption of 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” [10].

Essential to any risk-based approach are models that can be used to assess (qualitatively or quantitatively) identified risks. Models supporting the analysis of the risks posed by RPA to people and property on the ground include:

- Modelling the failures leading to RPA unintended ground impact [11];
- High-level risk models relating the system-level failures to ground causalities [12–22]. Some of the factors considered within theses 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 [23, 24];
- Modelling 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 [25–29].

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 [1]) and these are not taken into account in existing casualty risk models [12–22]. An additional model is needed to provide a systematic classification of the different technical and operational controls available to manage the risk of RPAS operations; and to characterise how these controls contribute towards a reduction in risk.

¹RPA is the flying component of a remotely piloted aircraft system
In this paper a new qualitative barrier bow tie (BBT) model is proposed, based on the preliminary framework developed in [9, 30]. The primary advantage of the BBT model is that it focuses the analysis and subsequent decision making activities on the risk controls (i.e., the practical devices, policies, or processes) that can be implemented. The BBT model provides an over-arching framework for existing models. Section §2 of this paper describes the components of the BBT model and Section §3 describes the application of BBT models to RPA operations over populous areas. A description of how to make assessments of risk using a BBT model is presented in Section §4. In Section §5 we propose a qualitative framework for the evaluation of the safety cases developed using a BBT model. Finally, a qualitative case-study RPAS operation is assessed using the BBT framework in Section §6.

2 Barrier Bow Tie Models

A BBT model 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 BBT model was in Imperial Chemistry Industry course notes on hazard analysis, delivered in 1979 at the University of Queensland, Australia [31]. The Royal Dutch / Shell Group developed the BBT modelling approach as a company standard to “seek assurance that fit-for-purpose risk controls were consistently in place throughout all operations world-wide” [31]. Since then, BBT models have “achieved widespread popularity” [32] being applied in the risk management of a wide range of industries, including defence, oil and gas, medical, and food production sectors [31, 33].

Within the aviation sector, the United Kingdom Civil Aviation Authority (CAA) has defined a strategy to “to identify how to maximise the use of bow tie risk models as an effective and proactive safety risk management tool, both by the CAA and industry...” [34]. The BBT modelling approach is used for all operational risk assessment by Australian air traffic service provider Airservices Australia [33]. Further, the Australian Defence Force (ADF) recommends the use of BBT models, stating that they are “particularly useful in proactive accident and incident prevention, and the management of safety within a system” [32]. The ADF have also provided an example initial operational risk analysis for RPAS using a BBT model (p.3A12, [35]). BBT models have been previously applied to the risk management of RPAS operations in non-segregated airspace [36–38] and for modelling the risks associated with RPA ground impact [9, 30].

2.1 Advantages and Disadvantages

BBT models have a number of benefits. The models provide a simple means for relating identified risks to the practical activities that can be undertaken to mitigate them. BBT models are specifically designed to illustrate the physical and procedural controls that are in place to manage hazards [32]. They provide a simple means for representing all the applicable events as well as the relationships between them [33]. The simple graphical structure of a BBT model can be easily communicated and comprehended by a wide range of risk stakeholders [9, 31, 33].

A BBT model can bring together elements from domains “traditionally treated separately” [33]. Threats due to human error, procedure error, equipment failure and also external, management and organisational factors that can contribute to a common top event can all be represented in a single model [33]. A BBT model can also be used as the 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 [33]. Further, they can be readily integrated with generally accepted organisational system models, such as James Reason’s model [39] of the organisational accident [9, 32, 33]. Perhaps the most significant advantage of a BBT model is 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 the controls, and the consequences associated with the loss (or breach) of controls across multiple accident scenarios [9].

A disadvantage to the use of BBT models is that a separate BBT model must be created for each identified top event (defined in Section §3.1), and the subsequent models are not necessarily independent. The relationships between the BBT models (e.g., due to secondary hazards or a commonality in controls)
must be identified and maintained using a separate tool (e.g., a detailed risk register or dependency diagram). Finally, the depiction of separate barriers within a BBT model can be misleading; leading to 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 organisational factors, and through the identification of controls contributing to multiple barriers.

2.2 BBT Models and the Risk Management Process

A BBT model 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, BBT models are not a hazard identification tool nor can they be used to identify the initiating threats, controls, or consequence states.

The primary use of BBT models is in the risk analysis, evaluation, and treatment processes. A BBT model can be used to support qualitative or quantitative analysis of the risks; providing the over-arching structure for combining other quantitative analysis techniques (e.g., fault trees, human error analysis, etc.). The BBT model can be used to support judgements of the acceptability of risks, and is particularly useful in those decision frameworks where acceptability of risk requires the implementation of best practice controls, or the proactive consideration of controls independent of the assessed level of risk, for example, those frameworks that require risks to be reduced to a level So Far As Is Reasonably Practicable (SFAIRP) [40]. BBT models can also assist in the implementation, communication and consultation, and integration of the safety risk management process within the broader safety management system of an organisation [33].

3 BBT Model of RPA Ground Impact Hazard

Building from the preliminary modelling work presented in [9, 30], this section describes the general anatomy of BBT models and their application to the hazard of RPA ground impact. The objective is to provide a general BBT framework that can be tailored to the analysis of any RPAS operation.

Each BBT model describes a top event, which is associated with a particular hazard. The top event is linked to its potential initiating events (referred to as threats) and the possible consequential outcomes given its occurrence. A path or trajectory (hereafter referred to as a path) originating at a threat and terminating at a consequence defines a risk scenario that needs to be managed. Placed along these paths are the barriers that aim to prevent, control, or otherwise mitigate risk. A conceptual BBT model is illustrated in Figure 1, the components of which are further described in the following sub-sections. The reader is referred to [31, 32, 41] for a description of the process used to develop BBT models.

Figure 1: Anatomy of a barrier bow tie model

---

2Risk management process as defined in ISO31000:2009 [8].
3.1 Hazards and Top Events

Central to a BBT model is the hazard and its associated top event(s). The International Civil Aviation Organization (ICAO) defines hazard as “a condition or an object with the potential to cause death, injuries to personnel, damage to equipment or structures, loss of material, or reduction of the ability to perform a prescribed function” [42]. Adopting this concept of hazard, we can define the primary hazard of interest as the impact of the RPA, or its components, with the ground. The at-risk entities of value are the people and property on the ground and the RPA itself, as illustrated in Figure 2. People and property can be further classified as:

1. First parties - people and property directly associated with the operation of the RPAS (e.g., the remote pilot, 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 a RPA, etc.);
3. Third parties - people and property not associated with, nor derive direct benefit from, the operation of a RPA.

Distinction between the different types of parties is made to reflect differences in the acceptability of risk. Priority is typically on the management of risks to third parties. From [1], the secondary hazards potentially arising due to the occurrence of a RPA ground impact include:

1. Release of hazardous materials (e.g., chemical payloads, composite fibre, or ordnance) following a ground impact;
2. Progression of fires, release of shrapnel, the collapse of buildings, motor vehicle accidents, etc. arising as a result of the RPA impacting the ground. This can include subsequent hazards arising due to downstream effects like a loss of power, damage to critical infrastructure, or hazards that arise due to a failure to meet mission objectives.

The relationships between the primary and secondary hazards, and the different entities at risk are illustrated in Figure 2. The primary risk scenario of concern is illustrated by the thicker blue arrow.

BBT models, however, have adopted a more relaxed interpretation of hazard. More specifically, the concept of hazard is identified with a condition, object, or an activity often describing a ‘normal’ aspect of an operating environment [41]. Applying this concept of hazard to the problem at hand, the primary hazard can be identified as the operation of a RPA over, or in the vicinity of, a populated area. One or more top events can be associated with this hazard. Within a BBT model, top events describe the undesired system states at which there is a release or loss of control over a hazard [32, 41]. For the hazard of RPA operations near populous areas, the top event of principal concern is an impact between the RPA, or its components, with the ground.

A separate BBT model should be developed for each hazard (primary and secondary) and for each associated top event. A secondary hazard can also be listed as a specific outcome consequence state associated within the high level BBT for a primary hazard (Figure 1). It should be noted that incorporating secondary hazards in this manner does not take into consideration the controls that can be implemented to mitigate the consequences associated with the secondary hazard. It is beyond the scope of this paper to develop BBT models for each secondary hazard, suffice to say that the same general approach can be readily applied to these hazards. It is also worth noting that some of the risks associated with secondary hazards are inherently addressed through management of the risks associated with a primary hazard.

3.2 Threats

Threats are defined as a possible direct cause for the top event [41], or an agent acting to defeat the protection of a hazard, and cause its release, or failure modes through which the hazard can materialise [32].

Clothier et al. [9] identify three high level threat types based on a review of existing classifications proposed in the literature [30, 43, 44]. The threat types align with the “most feared events” defined
in Part 1309 System Safety Standards for RPAS [45], thus a direct connection can be made between the BBT model and system safety analysis. A fourth threat type is proposed here, that of dropped or jettisoned components:

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 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 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.

These threats provide the top-level set of “failure modes” to which all failure identification and analysis methods should trace. As stated in [44] the primary differentiator between the UDS and LOC threats is that the former should allow on-board systems and/or the remote pilot to guide the RPA to a safer landing location, whereas a LOC threat will “probably provide no opportunity for choosing the landing location and can result in an impact at high velocity” [44]. The assignment of a failure mode will depend on the characteristics of the aircraft under failure (e.g., glide ratio), as such any assumptions should be explicitly stated. Fundamentally there are two key attributes to be considered: control over choice of impact location, and impact energy [30].

These high level threats can arise through all manner of technical, operational, and environmental causes. For example, an operator exceeding airframe load limits, encountering adverse weather, or errors made during maintenance are some of the many potential causes for the DOJC threat. The specific causes can be identified through an array of failure identification and analysis techniques (e.g., functional hazard assessment (FHA), fault tree analysis (FTA), hazard and operability (HAZOP) analyses, event tree analysis (ETA), structured brainstorming, etc.). Each identified failure must be associated with one or more of the high level threats (i.e., UDS, LOC, DOJC or CFIT). This defines the first component of a scenario to be managed (refer to Section §4.2). If a particular failure can be associated with more than one threat, then a unique scenario must be defined for each.
3.3 Consequence States

The consequence or loss events describe the set of possible outcome states that need to be avoided. As described in Section §3.1, of principal concern are those scenarios that have the potential to cause the death or serious injury of people, and secondarily, significant damage or loss to property or the RPA.

Aviation risk management frameworks traditionally measure consequence on a categorical or ordinal scale. The discrete scale establishes the set of consequence states depicted in Figure 1. For example, ICAO [42] defines a severity scale with the qualitative descriptors of: negligible, minor, major, hazardous and catastrophic (p.2-29, [42]). In this manner, the output assessments can be directly input to a risk matrix.

Alternatively, existing definitions of aviation accident and reportable incidents can be used to define the set of consequence states. Relevant definitions can be found in Annex 13 to the Chicago Convention [46]. In the U.S., an unmanned aircraft accident means “an occurrence associated with the operation of any public or civil unmanned aircraft system that takes place between the time that the system is activated with the purpose of flight and the time that the system is deactivated at the conclusion of its mission, in which: (1) Any person suffers death or serious injury; or (2) The aircraft has a maximum gross takeoff weight of 300 pounds or greater and sustains substantial damage” [47]. One can question the suitability of the criteria for an accident, given that there is no person on-board the RPA. Provided there are no casualties or significant damage to third party property, one could then argue that the loss of the RPA does not constitute an accident.

It is worth noting that contemporary and proactive safety management systems monitor more than accident events. Lead indicators and reportable events other than accidents (e.g., a RPA fly away, failure to follow procedures, “near misses”, etc.) can be associated with breaches in barriers or failures in controls constituting the barriers.

3.4 Barriers and Controls

A barrier refers to “a collection of controls that contribute towards a reduction in the probability and/or magnitude of consequence associated with a particular event within a chain of events describing a risk scenario” [9]. The ISO31000:2009 [8] definition of a risk control is adopted, specifically: “any process, device, practice, or other action which modifies risk.” A single control can contribute to the provision of more than one barrier, and hence independence between barriers cannot be assumed. A notable feature of our definition is that a barrier is a “system of controls” [9], and subsequently, the barrier function (the risk reduction) is an emergent property arising from the integrated behaviour of its component controls.

As illustrated in Figure 1, barriers (and their constituent controls) can be classified as preventative or mitigative. This classification is based on whether the barriers contribute to a reduction in the probability of occurrence and/or the magnitude of the top event, or whether they contribute to a reduction in the probability of occurrence and/or magnitude of the loss event given the occurrence of the top event, respectively [9].

A preliminary classification of barriers is developed in [9, 30]. The barriers collectively describe the various mechanisms available to a regulator or RPAS operator to reduce or otherwise modify the risks associated with the primary hazard of a RPA ground impact. The existing classification of barriers is extended to include the additional threat of DOJC, and is briefly defined below.

3.4.1 Hazard Elimination Barrier

The first preventative barrier is the Hazard Elimination Barrier, which describes the collection of controls that aim to eliminate the hazard, and hence the occurrence of the top event. Not carrying out the mission is an example of one of the few practical controls that belong to this barrier. When evaluating the barrier, one would need to determine whether there was a reasonable alternative means for performing the mission. When evaluating options for hazard elimination it is important to consider the level of risk associated with an alternate means of performing the mission. Specifically, any risks transferred to other parties or new risks introduced through the use of the alternate means. Whilst difficult to implement, this barrier is included for completeness as hazard elimination is a valid consideration under standard risk management decision making frameworks.
3.4.2 System Reliability Barrier

The System Reliability Barrier describes the collection of controls that contribute towards a reduction in the probability of occurrence of the UDS, LOC, and DOJC threats. The system reliability barrier is typically provided through the implementation of controls that provide assurance in the airworthiness of the system. Example controls include the use of high reliability components and system architectures, software and design assurance, pre-flight checks and planning, a comprehensive system of maintenance, or mission duration limits, which in turn reduces the probability of a threat being realised in a given mission. Examples of controls are provided in Table 3.

3.4.3 Terrain Awareness Barrier

The Terrain Awareness Barrier describes the collection of controls that contribute towards a reduction in the probability of the CFIT threat. Many of the controls could be incorporated under the other preventative barriers, however, a separate barrier is illustrated due to the large number and specificity of the identified controls for CFIT. Controls include crew familiarisation with the operating area, mission planning with automated terrain clearance checking, obstacle collision avoidance systems, online waypoint verification tools, forward looking cameras, and RPA observers. Example controls belonging to the Terrain Awareness Barrier are provided in Table 4.

3.4.4 Failure Recovery Barrier

The final preventative barrier is the Failure Recovery Barrier. The Failure Recovery Barrier describes the collection of controls that combine to reduce the probability of an impact, given the occurrence of a recoverable UDS, LOC, or DOJC event. Example controls are provided in Table 5. These are largely engineering-based controls, which include autonomous capabilities such as position hold or return to base in the advent of a loss of communications, reversion to manually piloted mode of operation on failure of the autopilot, engine restart, or the use of adaptive and fault tolerant control systems capable of maintaining flight under system failure. The successful application of these controls may allow the system to recover normal flight, or continue flight in a degraded mode or elevated risk state.

3.4.5 Impact Location Barrier

The first mitigative barrier is the Impact Location Barrier. This barrier describes the collection of controls that reduce the probability of the impact occurring in a populated region (or region where an entity of value resides). Example controls include operations at remote test sites, use of software geofences, automated flight termination systems, the use of terrain features or obstacles to constrain potential impact locations or limiting the duration of the mission spent over, or in proximity to, populated areas. Example controls belonging to the Impact Location Barrier are provided in Table 6.

3.4.6 Energy Management Barrier

The Energy Management Barrier describes those controls that contribute towards a reduction in the magnitude and/or the probability of occurrence of the conditions for damage/harm at a given impact location. The conditions, or “stresses”, are the harmful phenomenon (e.g., kinetic energy, pressure/blast wave, radiated energy, etc.) that have the potential to cause loss to the identified entities of value. Example controls include parachutes, the use of energy-minimal flight profiles, air bags, inherently low energy RPA, frangible RPA, propeller shrouds, and features that provide assurance in the containment of stored energy. Example controls are provided in Table 7.

3.4.7 Exposure Barrier

The Exposure Barrier encompasses those controls that contribute towards a reduction in the probability that an entity of value is actually present at the impact location. The primary difference between the Exposure Barrier and the Impact Location Barrier is that the latter focuses on minimising the probability of an impact occurring in a potentially populated area, whereas the former aims to reduce
the likelihood that people are actually present at the impact location. Examples include flight planning, flying only over sparsely populated regions, developing public awareness of the operation, and alerting systems on-board the RPA. Example controls belonging to the Exposure Barrier are provided in Table 8.

### 3.4.8 Entity Response Barrier

The *Entity Response Barrier* describes the collection of controls that reduce the magnitude of the consequence and/or the probability of realising the maximum level of consequence, to an entity of value subject to the harmful impact condition. Examples include personal protective equipment (PPE) or ensuring that the affected entities of value are resilient (*e.g.*, the physiological and psychological susceptibility of the person to harm). These controls are generally not practical to implement for a third party population. Some additional example controls are provided in Table 9.

### 3.4.9 Loss Intervention Barrier

The *Loss Intervention Barrier* is the final mitigative barrier that describes those controls that reduce the probability of realising the full magnitude of the potential consequence. Unlike those controls belonging to the *Entity Response Barrier*, these controls are not directly associated with the entity of value, but the response of the RPAS operator and supporting emergency services. Examples include having defined emergency procedures, personnel with first aid training, and emergency equipment (refer to Table 10).

### 3.4.10 Summary of Barriers

The barriers provide one means of classification of the wide range of technical and operational devices, practices, policies, and inherent properties of the system and its operation that can be used to reduce the risk presented to people and property on the ground. Other classifications are possible. The basis for classification used in this paper is the risk function. It is also possible to sub-classify controls under each barrier. For example, the hierarchy of controls (*i.e.*, eliminate, substitute/isolate, engineer, administrate, or PPE) is used in Tables 3-10 to sub-classify controls. Again, other valid classification schemes could be applied. The hierarchy of controls was used here as it can assist in demonstrating “duty of care” [40], for describing the effectiveness and acceptability of controls and evaluating risk within decision making frameworks.

### 3.5 Escalation Factors

Barriers are not infallible. Standard system safety analysis techniques are used to determine how various controls can technically fail. In addition to technical failures, one must also consider how humans contribute to the failure of controls. James Reason’s Swiss Cheese Model [39] provides an accepted framework for describing how humans and organisational environments can contribute to failures in controls. Errors and violations are the product of latent conditions arising from poor working conditions and deficiencies in organisational processes (refer to [39]). Further discussion on the integration of the Swiss Cheese Model and BBT model can be found in Annex F to Section 3, Chapter 9 of [32]. These failures, errors, and conditions are represented within a BBT model as escalation factors. Escalation factors are defined as “threats or operational issues that could compromise/defeat the effectiveness of the control they affect” [32], or conditions that lead “to increased risk by defeating or reducing the effectiveness of controls (a control decay mechanism)” [41]. An example of how escalation factors are represented within a BBT model is provided in Figure 1.

It is beyond the scope of this paper to identify and describe escalation factors associated with all of the controls identified in Tables 3-10. However, to illustrate the concept of an escalation factor, consider the use of human RPA observers. Example escalation factors include:

- Poor visual conditions (*e.g.*, rain, fog, glare, or dust) that prevent the observer from identifying the RPA and/or spotting people within the operational area;
• Fatigue or degraded performance due to the long duration of a mission or a demanding schedule of missions;
• Inadequate viewshed due to poor placement of the observer or obstructions due to terrain or buildings;
• Failure of the radio used to communicate with other members of the remote crew (RC);
• Observer being distracted;
• Poor, misinterpreted, or ignored communication between the RC and the observer.

Most important is ensuring that the activity undertaken to identify escalation factors goes beyond the technical focus of a typical system safety analysis to include consideration of the operational, environmental, human, and organisational contributions to the degradation or failure of a control. In so doing, a BBT model takes into consideration both the technical and operational airworthiness of a system.

3.6 Escalation Barriers

The final components of a BBT model are the escalation barriers. An escalation barrier describes a control or collection of controls that are put in place to reduce or modify the effect an escalation factor has on another control. These can be thought of as “second tier” risk mitigations, describing devices, people, or processes implemented throughout the design, manufacture, maintenance, and operation of the RPAS to provide assurance in the performance/provision of controls. To exemplify the concept in terms of our example escalation factors, escalation controls could include:

• Procedures defining weather and visibility minima, which take into account the visual performance of the observers;
• Procedures for rotation of RPA observers, and the creation of a system for managing the risk of observer fatigue;
• Procedures to survey the operational site and design flight plans taking into account the viewshed of observers;
• The use of high quality radios, having a backup radio, and including radios within the system of maintenance;
• Personnel training in crew resource management and effective team communication.

An example of how escalation barriers are represented within a BBT model is provided in Figure 1.

3.7 Summary

The complete BBT modelling framework is illustrated in Figure 3. The model provides a generic framework for assessing the risk associated with RPAS operations (discussed in the next section). The barriers provide a risk-based classification of the practical devices, people, or processes that can be used by RPAS operators and regulators to reduce risk.

4 Risk Assessment Using a BBT Model

BBT models are most often used to support qualitative risk assessments but can also be used to provide quantitative assessments. A description of how assessments of risk can be determined from a BBT model has not been previously presented in the literature.
Figure 3: High level barrier bow tie model for RPA ground impact risk assessments. Note: individual controls, escalation factors, and escalation barriers are not shown.

4.1 Measuring Risk

There are numerous definitions for risk (refer to Aven et al. [48] for a comprehensive discussion of the various interpretations of risk). Civil aviation safety risk management frameworks adopt a ‘classical’ interpretation of risk, whereby safety risk is defined as the “the predicted probability and severity of the consequences or outcomes of a hazard” [42].

In civil aviation risk management frameworks risk assessments are made through the use of a risk matrix, which separates the measurement of risk into measures of the magnitude of the consequence and the likelihood of its occurrence. The risk matrix provides the means to map these component measures to a level of risk. An example risk matrix and component consequence/severity and likelihood scales widely utilised in aviation risk management are provided on p.2-29 of [42].

4.2 Scenario Assessment

An individual BBT model starts with the definition of a finite set of threats (T), as given in Eq.1. Each element of T is a description of an identified failure state (e.g., “engine loss”). Also specified is a set of outcome consequence states (C) as given in Eq.2, with each element c_r describing one of level of the scale of loss (refer to Section §3.3). Each path beginning at an initiating threat, t_q, and terminating at a particular loss state, c_r, defines a risk scenario, s_m, that needs to be managed. The complete set of M scenarios within a BBT model is contained in the set (S). For each scenario, and beginning at the threat t_q, the analyst determines the controls and in turn the set of barriers that are in place to manage the probability of realising the consequence state c_r. The set B comprises the barriers implemented for the particular scenario s_m. Each element of B corresponds to the label of a implemented barrier (e.g., ‘system reliability’, ‘failure recovery’, ‘impact location’, ... etc.), refer to Eq. 3. It is important to note that the specification of B is unique to the scenario s_m.

\[
T = \{ t_q : q = 1, 2, ..., Q \} \quad (1)
\]
\[
C = \{ c_r : r = 1, 2, ..., R \} \quad (2)
\]
\[
B = \{ b_n : n = 1, 2, ..., N \} \quad (3)
\]
\[
S = \{ s_m : m = 1, 2, ..., M \} \quad (4)
\]

A particular scenario s_m is described through the tuple:

\[
s_m = < t_q, B, c_r > \quad where \quad s_m \in S \quad (5)
\]
The measure of risk associated with a particular scenario \( s_m \) is denoted \( R(s_m) \) and is expressed by the tuple:

\[
R(s_m) = < X(s_m), P(s_m) >
\]  

(6)

Where, \( X(s_m) \) is the magnitude of consequence and \( P(s_m) \) its probability of occurrence for the scenario \( s_m \). The scenario description given in Eq. 9 includes the specification of the loss state of interest (i.e., \( c_r \)) and therefore \( X(s_m) = |c_r| \).

The assessment of \( P(s_m) \) starts with an assessment of the unmitigated probability of the initiating threat occurring, \( P(t_q) \). Existing system safety analysis techniques (FTA, FMECA, etc.), reliability data, or expert judgement can be used to determine the threat probability. A single failure can have multiple failure modes (i.e., can be associated with the realisation of more than one threat), and can influence the probability of occurrence of other failures. Such dependencies need to be accounted for in the assessment of \( P(t_q) \).

The next step is to assign probabilities to each of the implemented barriers along the scenario path. At this juncture we must recognise the somewhat misleading nature of the term ‘barrier’. With the exception of controls belonging to the hazard elimination barrier\(^3\); barriers do not prevent the loss scenario from manifesting but reduce its likelihood of occurrence. Thus, the loss event could occur despite all barriers being implemented and performing as expected. It is also necessary to recognise that barriers are substantiated by real world devices, people, and processes, the performance limitations of which can result in the loss of a barrier. Subsequently, the barrier probability assessment for a given barrier \( P(b_n) \) is given by:

\[
P(b_n) = P(v|f)P(f) \quad \forall b_n \in B
\]  

(7)

where \( P(v|f) \) is the conditional probability characterising the barrier risk function; and \( P(f) \) is the probability that the barrier is functioning (i.e., performs its defined risk function as intended). \( P(v|f) \) is the probability-reduction achieved through consideration of all of the constituent controls belonging to the barrier, given they are working. The effectiveness of each control is assessed in relation to how it contributes to the barrier risk function. Assessments of \( P(f) \) are made through consideration of the escalation factors and escalation barriers for each control. Additional factors relevant in the assessment of \( P(v|f) \) and \( P(f) \) are explored in Section §5.1. It is worth noting that Eq.7 assumes that a barrier has no effectiveness if there is a failure in the controls (a conservative assumption).

The barrier probability assessment is repeated for each of the barriers in the set \( B \). It is important to note that the ‘layered’ depiction of barriers in a BBT model can be misleading, in that it suggests that all barriers are independent from each other and from initiating threats. In performing the assessment of barrier probabilities (Eq. 7) it is important to note that:

- Threats are not necessarily independent or mutually exclusive;
- Controls can be common to more than one barrier;
- There can be common external factors (e.g., weather) that impact on the performance \( P(v|f) \) and reliability \( P(f) \) of multiple barriers; and
- The degradation or failure of one barrier can influence the performance \( P(v|f) \) and reliability \( P(f) \) of other barriers.

As such, independence cannot be immediately assumed in the computation of \( P(v|f) \) and \( P(f) \) for implemented barriers. Subsequently, determining the probability of a given loss scenario \( P(s_m) \) is complex and dependent on the particular barriers implemented, the system, its concept of operation, and operating environment. BBT models are used at a high level, which makes the identification of dependencies particularly complex. Whilst this challenge is not unique to BBT models, it does, in part, explain why

\(^3\) In reality most elimination controls do not truly eliminate risk but transfer the risk to another system. Refer to Section §3.4.1
BBT models are more commonly used to support qualitative risk assessments. If the naive assumption of complete independence between all barriers and threats could be assumed, then \( P(s_m) \) could be determined using Eq. 8.

\[
P(s_m) = P(t_q) \prod_{n=1}^{N} P(b_n)
\]  

Under this formulation, \( P(s_m) \) represents the residual probability of occurrence of the consequence state for the scenario taking into account the performance and functioning of all of the implemented barriers. As discussed previously, the dependencies between the barriers within \( B \) and the initiating threat \( t_q \) are not taken into account in the evaluation of \( P(s_m) \). A risk matrix can then be used to determine \( R(s_m) \) from the component measures \( X(s_m) \) and \( P(s_m) \). This risk represents the residual risk after implementation of the barriers. This process can be repeated to determine measures of risk for each of the \( M \) scenarios defined within the BBT model.

### 4.3 Aggregated Risk Assessments

Aviation safety regulators typically require risks to be reported and managed at various levels of aggregation. The lowest level of management is that of the individual scenario, where the analysis, evaluation, and treatment of risk is explored in relation to each scenario defined within the BBT model. These measures can be aggregated, to provide insight into how risks are managed for a particular top event, then aggregated again for all top events comprising a hazard, and so on, for all hazards in a given operation.

A single BBT model can be used to provide risk assessments at the aggregated level of a top event, where the measure of risk \( R(e) \) for a particular top event, \( e \), is expressed as the tuple:

\[
R(e) = < X(e), P(e) >
\]

Where, \( X(e) \) is the magnitude of consequence associated with the top event \( e \), and \( P(e) \) is the probability of occurrence of \( X(e) \). The two component-measures of \( R(e) \) are found through aggregation of the component measures \( X(s_m) \) and \( P(s_m) \) associated with all of the constituent scenarios in \( S \). Various methods can be used to perform this aggregation.

In aviation safety assessments it is common practice to assign the highest plausible level of consequence when aggregating risks. ICAO [42] interprets this as the scenario with the maximum level of consequence, assuming all non-plausible scenarios have been eliminated. \( X(e) \) would thus be found by finding the maximum level of consequence for all of the scenarios associated with the top event \( e \), as given in Eq. 10. This aggregation approach is conservative. As described in [49], such assumptions can lead to sub-optimal outcomes from decision making. Further, this method of aggregation is not made on the basis of risk. As such, scenarios with lower levels of consequence but higher probability of occurrence (and hence higher potential level of risk) would not be accounted for in the aggregation.

\[
X(e) = \max_{s_m \in S} X(s_m)
\]  

If the conservative approach is adopted, then \( P(e) \) can be determined through aggregating the probability of those scenarios in \( S \) where \( X(s_m) \) is equal to \( X(e) \), Eq.11 and Eq.12.

\[
A = \{ s_m | X(s_m) = X(e), P(s_m) \}
\]

\[
P(e) = \sum_{\forall s_m \in A} P(s_m)
\]  

It is important to note that Eq.12 assumes independence between scenarios. A hazard can comprise multiple top events, with each represented using a separate BBT model. A similar process can be used to aggregate the assessments for each top event \( e \) associated with a given hazard to provide an aggregated assessment of the risk for that hazard. The aggregation would need to take into account the dependencies between the realisation of the top events (i.e., between each BBT model) in addition to the potential dependencies between threats.
4.4 Generating Risk Profiles from BBTs

A risk profile describes the consequence probability distribution for a given top event or hazard. For discrete events, the risk profile is a tabulation of the probability of each consequence state, $P(c_r)$, for all scenarios associated with $e$, as given in Eq.13 and Eq.14. With reference to Eq.13, the set $D$ is a subset of $S$. $D$ comprises the tuples $< X(s_m), P(s_m) >$ of those scenarios in $S$ where the consequence of that scenario $X(s_m)$ is equal to a defined value $X(c_r)$. $P(c_r)$ is then found using Eq.14. The process of determining $D$ and calculating $P(c_r)$ is repeated for all levels of consequence in $C$; providing a tabulation of probability versus level of consequence. The tabulation can then be displayed graphically with $X(c_r)$ on the x-axis and $P(c_r)$ on the y-axis. It is important to note that Eq.14 does not account for dependencies between the scenarios.

$$D = \{ s_m | X(s_m) = X(c_r), P(s_m) \}$$ (13)

$$P(c_r) = \sum_{\forall s_m \in D} P(s_m)$$ (14)

Cumulative risk profiles can also be determined by modifying Eq.13 to include only those scenarios with a magnitude of consequence greater than or equal to the magnitude of each level of consequence, as shown in Eq.15, and then tabulating or graphing the result.

$$D = \{ s_m | X(s_m) \geq X(c_r), P(s_m) \}$$ (15)

5 Qualitative Evaluation of a BBT Model

Risk assessments are used within the risk evaluation and treatment processes to make decisions in relation to the acceptability of residual risks and the need for further mitigative actions, respectively. The As Low As Reasonably Practicable (ALARP) framework is widely used within civil aviation safety risk management frameworks to guide decision making (e.g., [42, 50, 51]). However, a determination that residual risks are acceptable (tolerable) is only one aspect that needs to be considered in decision making. Here, it is proposed that risk evaluation include consideration of assurance in the management of risk. Assurance is the degree of confidence and evidence that the risks are (or will be) managed to acceptable levels. In this section we propose an additional set of criteria that can be used to show assurance in the management of the risks using a BBT model.

A safety argument can exhibit a number of desirable qualities that contribute to assurance in the management of risk. Indeed, existing aviation safety literature [42, 52–54] propose numerous such qualities, which can be assigned and assessed at various levels of abstraction within the BBT model. Assurance in the development of the BBT model itself (i.e., the people and processes used to develop the BBT model) are not considered in this paper. Inspiration for such factors could be found through exploring aviation design process and quality assurance guidelines.

5.1 Evaluation of the Risk Controls

Numerous desirable qualities can be associated with the individual controls identified in a BBT model. These ‘assurance’ qualities are presented in Table 1.

The quality of effectiveness of a control is the degree of risk reduction it provides, and is captured in the assessment of $P(v|f)$. The reliability of a control is taken into account in the assessment of $P(f)$. In determining $P(f)$, assessors should ensure that escalation barriers/controls are in place for all significant escalation factors. $P(f)$ should also be evaluated at different points in the mission and environment to account for potential differences in the availability of the control. For example, RPA operations beyond visual or radio communications range of the RPS can significantly impact the availability of controls. Unless autonomous triggering capabilities exist on-board the RPA, then controls such as flight termination and parachute systems, whilst working properly, cannot be activated. The integrity of the system can also be taken into account in an assessment of $P(f)$. Integrity is typically provided

---

4ICAO adopts a variation on the ALARP framework (refer to Chapter 2 [42])
through the existence of escalation barriers, which include built-in-test, inspection, warning, or alerting functions. **Verifiability** is closely related to the concept of **enforceability** described as “the extent to which compliance with new rules, regulations or operating procedures can be monitored” [42]. In the context of aviation safety, a control should be documented in relevant operational manuals (i.e., flight, operation, or maintenance manuals) and implemented in practice (e.g., a process is followed or a device is implemented).

Other qualities that are important in decision making but not related to assurance include cost, practicality, acceptability of the controls, and introduced risk. **Acceptability** describes the extent to which the control is consistent with stakeholder paradigms [42]. **Introduced Risk** describes the magnitude of additional risk introduced to a system through the use of a control [42]. Neither **acceptability** nor **introduced risk** are taken into account in the assessment of $P(f)$ or $P(v|f)$. For example, the hazards introduced due to the use of an explosive flight termination system need to be identified and assessed in a separate BBT model.

### Table 1: Assurance qualities in risk controls

<table>
<thead>
<tr>
<th>Quality</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effectiveness</td>
<td>The extent to which a control reduces or eliminates the safety risks.*</td>
</tr>
<tr>
<td>Reliability</td>
<td>The probability that a control will perform its required function under specified conditions, without failure, for a specified period of time.†</td>
</tr>
<tr>
<td>Availability</td>
<td>The probability that a control is ready for use or in a functioning state at a given point in time.† This is defined in relation to the context in which the control is implemented (mission and environment).</td>
</tr>
<tr>
<td>Integrity</td>
<td>The probability that a barrier (or control) completes its intended function with no undetected error, or if there is an error, the probability that the error will be detected and a usable integrity flag generated within a specified maximum time.§</td>
</tr>
<tr>
<td>Verifiability</td>
<td>A control is verifiable if it can be checked or audited (by a person, tool, or other means) to determine whether it is effective or correctly implemented. This requires that the control be accessible or observable.‡</td>
</tr>
</tbody>
</table>

* Definition based on that provided in [42].
† Definition based on that provided in [52, 53].
§ Definition based on that provided in [55].
‡ Definition based on that provided in [55].

### 5.2 Barrier-Level Evaluation

The “system of barriers” should, to the maximum extent possible, exhibit the properties of **coverage**, **depth**, and **independence**. Coverage is the proportion of all scenarios mitigated through the implementation of barriers. Ideally, all scenarios should have at least one barrier in place. A system of barriers that provides multiple barriers for each scenario is said to exhibit **depth**. However, it is important to note that the benefit of depth can be offset through the existence of common mode failures in controls, or environmental or organisational factors that can affect the performance of multiple barriers. Two or more barriers exhibit a high degree of **independence** if they have no controls or escalation factors in common. Independence can be assessed through the use of common mode analysis techniques such as those described in [53].

### 5.3 Communication of Evaluation Results

Risk evaluation has been extended beyond judgements of measures of risk to now include consideration of assurance. The next challenge is to provide a means for presenting these additional dimensions to
decision makers. One visual method that could be used in the evaluation of barriers and controls is the Kiviat diagram. Kiviat diagrams, also referred to as radar or spider plots, have previously been used to profile the risks for various aviation sectors, including RPAS [56]. Kiviat diagrams provide a simple means for communicating multivariate assessments and a tool to aid decision making.

An example Kiviat diagram for evaluating risk controls is presented in Figure 4. Shown in Figure 4 are the evaluation of two example controls and the minimum regulatory criterion for each quality. Each quality is defined along a separate axis of the diagram. An ordinal, interval, or ratio scale must be defined for each quality. Relative comparisons can be made along each axis, thus providing a graphical means for ascertaining compliance to regulatory criteria (if available). The visual overlay of multiple assessments on a single diagram also provides a simple means for comparing alternate controls or barriers. For example, and referring to Figure 4, the two controls exhibit similar performance with respect to six of the assurance qualities. However, Control Two has greater availability than Control One. Both controls fail to meet the required level of reliability. Control One also fails to meet the regulatory requirement for verifiability and introduced risk. It is important to note that when using Kiviat diagrams comparisons between axes are misleading and the enclosed region has no meaning.

![Kiviat diagram example](image)

**Figure 4: Example Kiviat diagram for evaluation against regulatory criteria**

6 **BBT Analysis of Case Study RPAS Operations**

The case study is based on a desktop analysis undertaken by researchers at the NASA Langley Research Center [57]. The objective of the desktop analysis was to determine the extent to which existing certification and airworthiness standards could be applied to a rotary wing RPA. The output was a suggested set of design and performance standards, or mock-certification basis. The certification basis was specific to a particular RPAS concept of operation (CONOP). Described within the CONOP are a number of technical and operational mitigations, which were used to offset the risk to people and property on the ground. These mitigations facilitated dispensations in the application of the existing manned airworthiness standards, and in effect, provided the “safety context” for the certification basis proposed in the NASA report.

The BBT model was used to structure the safety context for the certification basis for the different CONOPs described in [57]. Detailed analysis for the particular scenario of engine system failure is presented.
6.1 Case Study Remotely Piloted Aircraft System

The certification basis was developed for a single engine, tandem-rotor RPA. The Dragonfly Pictures DP-14 Hawk™, pictured in Figure 5, was used as a practical example in the report. Some of the attributes and performance characteristics of the DP-14 are presented in Table 2. The DP-14 is powered by a Solar T62 80 horsepower gas-turbine engine. The RPA can be operated beyond visual line of sight (BVLOS) of the remote pilot station (RPS) through the use of an Iridium™ satellite command and control link (CCL). The remote pilot (RP) cannot take direct remote control of the RPA but the RP can monitor its status and, if required, initiate pre-programmed actions via the RPS and CCL. The RPA is capable of automated take-off and landing, and automated flight between defined waypoints. The RPA can detect and avoid (DAA) ground-based obstacles through the use of short-range sensors and avoidance algorithms implemented on-board the RPA. The RPAS has a geofence capability, flight termination system, and has pre-programmed responses to common failure scenarios such as loss of the CCL or navigation failure. More information on the DP-14 can be found in [57, 58].

![Figure 5: Dragonfly Pitctures DP-14 Hawk™ Remotely Piloted Aircraft](image)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Measure [units]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum gross mass</td>
<td>408 [kg]</td>
</tr>
<tr>
<td>Fuselage length and width</td>
<td>4.1, 0.53 [m]</td>
</tr>
<tr>
<td>Rotor diameter and separation</td>
<td>3.96, 2.44 [m]</td>
</tr>
<tr>
<td>Maximum endurance</td>
<td>2.4*, 4.3† [hr]</td>
</tr>
<tr>
<td>Cruise and max true airspeeds</td>
<td>72, 105 [kn]</td>
</tr>
<tr>
<td>Maximum operational altitude</td>
<td>15,000 [ft above mean sea level]</td>
</tr>
</tbody>
</table>

* With 195 kg of payload. † With 45 kg of payload.

6.2 Visual Line of Sight Spraying Operations

The first CONOP described in [57, 58] is targeted aerial spraying within visual line of sight (VLOS) of the RPS. For this CONOP the operational area is limited to 0.25 square mile blocks of farmland. The terrain is relatively flat with all obstacles mapped prior to flight. The regions of crop requiring spraying...
are contained within the operational area and are known prior to the flight. Flight planning is conducted prior to flight.

A containment zone encompassing the operational area along with an additional margin from each boundary is established. All remote crew (RC) are situated outside of the containment zone, and procedures prior to, and during the operation ensure that no people are in the containment zone. The RPA is operated at only a few feet above the height of the crops and only during low wind conditions to minimise dispersal of fertiliser or chemicals. The RPA may climb to higher altitudes in order to avoid obstacles. The maximum permitted height is 400 ft above ground level (AGL), which is implemented as a constraint in the autopilot software. The maximum permitted height reduces as the RPA approaches the containment zone boundary. The RPA typically flies at low speed and standard procedures limit operations to daylight visual meteorological conditions (VMC).

6.3 Broad Area Spraying Operations

The second CONOP for the DP-14 RPAS is broad area weed identification and spot treatment. Broad area aerial spraying is typically undertaken in rural areas or in regions where weeds are difficult to access from the ground.

The region of operation is rural and sparsely populated. In contrast to the VLOS farming CONOPs, the terrain is undulating and not all obstacles are known \textit{a priori} the flight. In addition, there is the possibility third parties are present in the operational area. The operational area is large. This, combined with the complex nature of the terrain means that VLOS between the RPA and RP may not be maintained throughout the mission.

The areas requiring treatment are not entirely known prior to the flight. Thus, a typical broad area spraying mission comprises separate search and treatment phases. During the search phase the RPA operates at a higher altitude (limited to 400ft AGL) and uses on-board multi-spectral cameras to identify regions requiring weed treatment. The treatment phase involves the slow descent of the RPA to a few feet AGL, then low altitude manoeuvring during spray delivery, followed by a slow climb back to the pre-defined search height.

6.4 Threats

The differences between the CONOPs will lead to differences in the unmitigated probability of threats, $P(t_q)$. A detailed failure analysis is required to estimate $P(t_q)$. However, some general examples are presented to illustrate some of the potential differences between $P(t_q)$ determined for the different CONOPs.

Both CONOPs require manoeuvring at relatively low speeds. However, broad area spraying also requires transitions from altitude, with the exact timing and location of these transitions not known \textit{a priori} the flight. As a result, the probability of CFIT and LOC is likely to be higher for broad area spraying missions. The longer duration of broad area spraying missions, and the need for altitude transitions, can also increase the probability of failures leading to UDS, LOC, and DOJC during flight. The probability of human errors potentially leading to UDS, LOC, and CFIT are expected to increase with mission factors such as increasing mission duration (e.g., due to fatigue, boredom, etc.), operations beyond VLOS (e.g., reduced situational awareness, increased workload, attention, dependency on automation, etc.), and increasing complexity of the missions flown (e.g., due to increased workload).

Certain characteristics of the CONOPs will have a tendency to reduce the probability of CFIT. For VLOS spraying missions, flying at constant altitudes over relatively flat and obstacle-free terrain tend to reduce the probability of CFIT. For broad area spraying missions, a significant proportion of the flight is expected to be completed at altitudes above the height of potential obstacles, which also serves to reduce the probability of CFIT. Operational characteristics that can increase the probability of CFIT include the need for manoeuvring at very low altitudes, dynamic flight plans, operations over complex (or less well known) terrain, and operations in the presence of unmapped obstacles. These factors are all present in broad area spraying missions, and hence the unmitigated probability of CFIT is expected to be higher in those missions than for VLOS spraying missions.
6.4.1 Engine System Failure

More detailed analysis is presented for the particular scenario of an engine system failure. There is extensive knowledge of turbine engine systems, the various means of their failure, and their associated failure modes. Common failure identification techniques include FTA and FMECA. Example failures include fuel starvation or contamination, mechanical failures, the ingestion of foreign objects (including birds), or errors in engine control system software, etc. The associated failure modes range from partial loss, through to complete and instantaneous loss, of propulsion. Engine system failure has a direct impact on the generation of lift and the controllability of the rotorcraft. Subsequently, engine failure modes can be classified as belonging to UDS and LOC. Some engine failures can also result in the high speed ejection of components (e.g., turbine disks and fan blades); such failure modes can be classified as DOJC. Analysis presented herein will focus only on those engine failure modes which result in UDS and LOC. It is also worth noting that engine failure can impact electrical power generation on board the RPA, which in turn can result in the occurrence of an UDS or LOC event.

It can be expected that the unmitigated probability of an engine failure \( P(t) \) will differ for the two CONOPs. For example, broad area spraying missions may place higher stresses on the engine (e.g., heavier payload, increased number of transitions from altitude, longer duration of missions, etc.) than for VLOS spraying missions. Detailed FMECA and FTA would need to be undertaken to identify the contributing failures and determine the likelihood of occurrence of engine failure for each CONOP.

6.5 Implementation of Barriers for the Engine Failure Scenario

The BBT models for the engine system failure scenario are depicted in Figure 6 for both CONOPs. The Failure Recovery Barrier may be implemented for broad area spraying missions due to the higher operating altitude of the RPA during search phases of the flight. Operating at a higher altitude often provides the time necessary for systems to detect and respond to failures before ground impact. In this scenario an engine re-start or other failure response is unlikely, so while considered, the barrier provides no additional active controls. If controls under this barrier are required, then a higher operating altitude would be required. This is an example of how the model can prompt additional considerations.

A number of differences in the controls used to implement the barriers can also be observed. Firstly, for VLOS spraying missions, the Impact Location Barrier can be implemented through flight planning controls (i.e., operating at very low speeds and altitudes), which serve to reduce the size of the impact location footprint. For broad area spraying missions, high terrain features and tall trees can also be used to constrain the impact footprint. For broad area spraying missions, high terrain features and tall trees can also be used to constrain the impact footprint.

For the Energy Management Barrier, the height above ground of VLOS spraying missions means that the RPA has an inherently lower geo-potential energy, and hence, aids in reducing the magnitude of kinetic energy at ground impact. Configuration management can also be employed for VLOS spraying missions. Specifically, the minimum amount of chemical payload and fuel required to perform the mission can be calculated and loaded to the RPA. This reduces the magnitude of energy (kinetic and chemical potential) at ground impact. For broad area spraying missions, the higher altitude of operations above ground level enables the use of alternate controls under the Energy Management Barrier. Namely, the RPA has the potential to deploy emergency and forced landing systems. Autorotation\(^6\) can also be used to reduce the potential ground-impact energy. The dynamic and unplanned nature of broad area spraying missions makes the implementation of configuration management controls more difficult.

Both VLOS and broad area spraying missions utilise site selection as a means of implementing the Exposure Barrier. This control is inherent to the rural and remote areas in which these missions take place. For VLOS spraying missions, the selected site is unpopulated and third party access to the site can be controlled through the use of RPA observers. RPA observers reduce the probability of third parties entering the operational area and in turn, reduce the probability that third parties are exposed to a potential impact. RPA observers can be strategically placed at locations where third parties are most likely to enter the operational area (e.g., paths or roads). However, factors such as increased personnel cost and introduced risks associated with the use of RPA observers will need to be weighed

\(^6\)Autorotation describes the state where the action of air moving up through an unpowered rotor causes the rotor to spin. This in-turn generates lift, facilitating a controlled rate of descent.
against the assessed benefits of their use. For broad area spraying missions over large and rugged areas, it is assumed that these costs substantially outweigh any risk reduction gained through the use of RPA observers.
Visual Line of Sight Spraying Operations

Figure 6: BBT models for the engine system failure scenario
6.6 Escalation Factors and Escalation Barriers

Escalation factors need to be determined for each identified control depicted in Figure 6. Presentation of the complete identification and analysis of escalation factors is beyond the scope of this research paper. Three escalation factors described specifically in the context of the engine system threat scenario are presented. Namely, the failure of the RPA observer to prevent a third party from intruding into the operating area, the loss of the command and control link, and a loss of the ability to navigate.

6.6.1 Third Party Intrusion into Operating Area

Potential causes leading to a failure of the RPA observer to detect and prevent people from entering the operational area are largely environmental (e.g., terrain and weather related) or human performance related (e.g., lack of training, fatigue, boredom, distraction, limitations in human visual performance, etc.). As such the escalation barrier is largely substantiated through procedural and administrative controls. Escalation controls include:

- Strategic placement of RPA observers taking into account overlapping observer viewsheds and the ability of the RPA observer to intercept a detected intruder;
- The development and implementation of a fatigue risk management system, which could include specifying duty limits;
- Specifying minimum vision requirements for personnel (e.g., 20/20 vision with corrective aids);
- Procedure to check and monitor visual conditions;
- Providing personnel with training in human factors;
- Providing visual aids such as binoculars;
- Elimination of potential distractions (no cellphones).

The analysis for this escalation factor is depicted graphically in Figure 7.

**Visual Line of Sight Spraying Operations**

![Diagram of RPA observers failing to prevent third party from entering operating area](image)

Figure 7: Third party intrusion into operating area and its impact on controls

6.6.2 Loss of the Command and Control Link

The loss of the Command and Control Link (CCL) was identified as an escalation factor to the provision and effectiveness of multiple barriers for both missions. ICAO [59] defines a loss of CCL as “any situation in which the RPA can no longer be controlled by the RP due to the degradation or failure of
the communications channel between the RPS and RPA. The degradation or failure may be temporary or permanent and can result from a wide range of factors.”

Most RPAS CCLs utilise radios operating in the Very High Frequency (VHF) spectrum. Reliable communications in the VHF band require a direct line of sight between the transmitter and receiver. For RPAS that utilise VHF radios, the probability of a loss of CCL is likely to be higher for broad area spraying missions than for VLOS spraying missions. This is due to the complex nature of the terrain and the inability to survey communications performance across the entire operational area. The DP-14, however, uses satellite communications for its CCL. Subsequently, direct radio frequency line of sight between the RPA and RPS is not required. A loss of the CCL for the DP-14 is likely to occur due to:

- A loss of radio frequency line of sight between the RPA and satellite, or a failure of the satellite system. For example, this may occur as a result of masking due to high terrain or obstacles;
- Insufficient link margin to account fluctuations due to weather or noise floor;
- Interference;
- A technical failure in the radio systems on-board the RPA or on the RPS.

As can be observed in Figure 8, multiple barriers are potentially impacted due to a loss of the CCL. More barriers are impacted for broad area spraying missions than for VLOS spraying missions. Controls belonging to the Failure Recovery and Impact Location Barriers are particularly impacted. For example, a loss of the CCL renders ineffective controls involving input or action by the RC. These include the reversion to RP control, and the remote activation of flight termination and emergency landing systems. Controls that aid RC in the detection and prevention of failures (e.g., engine health monitoring) are also impacted. A loss of CCL can also impact the Loss Intervention Barrier by reducing the ability of the RC to locate the RPA post-impact and thereby hindering an effective emergency response. The relatively large number of barriers impacted by a potential loss of the CCL indicates that it is a significant escalation factor requiring management and assurance.

As depicted in Figure 8, the escalation barrier can be substantiated through a range of technical/engineering and administrative/procedural controls, including:

- Improving the reliability of the radio system through the use of higher quality radio equipment and redundant architectures;
- Minimising the impact of interference through the use of a secondary CCL implemented in a different frequency band; or hybrid time and frequency division multiplexing;
- Developing and implementing procedures for the RC to monitor radio performance;
- Implementing autonomous behaviours on-board the RPA (e.g., the autonomous triggering of flight termination or emergency landing systems) in the advent of a loss of the CCL.

The use of a mix of engineering and administrative controls provides greater assurance in the management of the escalation factor. However, the addition of technical controls (including autonomous software behaviours) increases the scope of airworthiness requirements. For example, assurance in the correct behaviour of autonomous functions implemented in software would be needed.
Visual Line of Sight Spraying Operations


High reliability radio systems. Multiple and frequency diverse CCLs (e.g., time and frequency diversity modulation). CCL performance monitoring. Autonomous implementation of functions on-board the RPA.

System Reliability Barrier

Failure accommodation Failure procedures

Impact Location Barrier

Geofence Remotely-triggered flight termination

Energy Management Barrier

Emergency/forced landing system

Loss Intervention Barrier

Emergency response procedures

Figure 8: Loss of the Command and Control Link (CCL) and its impact on controls

Broad Area Spraying Operations


High reliability radio systems. Multiple and frequency diverse CCLs (e.g., time and frequency diversity modulation). CCL performance monitoring. Autonomous implementation of functions on-board the RPA.

System Reliability Barrier

Health monitoring

Failure Recovery Barrier

Health monitoring Failure accommodation Failure procedures

Impact Location Barrier

Geofence Remotely-triggered flight termination

Energy Management Barrier

Emergency/forced landing system

Loss Intervention Barrier

Emergency response procedures

Figure 8: Loss of the Command and Control Link (CCL) and its impact on controls
6.6.3 Loss of Navigation

Loss of navigation was also identified as a critical escalation factor. A loss of navigation is defined here as the situation where information pertaining to the location of the RPA is lost, compromised, degraded, or lacks sufficient integrity for it to be used. There are many potential causes for a loss of navigation. For the DP-14 some examples include:

- The loss, compromise or degradation of the signal in space from the Global Navigation Satellite System (GNSS). This could be due to masking, multipath interference, poor satellite geometry, spoofing, GNSS system failure, etc.;
- A hardware failure in the navigation computer;
- Flaws or faults in software used to determine the navigation solution;
- Undetected erroneous inputs to the navigation computer (e.g., a partially blocked air pressure sensor);
- Incorrect maps or reference datums;
- Failure to correctly initialise the navigation system prior to flight.

Interesting to note is that the potential causes for a loss of navigation are broad, covering technical, environmental, and human related causes. In the case of the engine system failure scenario, the potential impact of a loss of navigation primarily impacted the mitigative barriers (as depicted in Figure 9).

Given a loss of navigation, safety controls such as a geofence can not be relied upon. Forced landing systems are also compromised, as is the ability of the RC to field an effective emergency response. However, there are a variety of technical and administrative controls that can be used to substantiate an escalation barrier. Some examples include:

- Implementing a navigation system that is capable of operating in situations of GNSS denial (e.g., systems capable of simultaneous localisation and mapping, or the use of high grade inertial navigation systems);
- Improving the reliability of the navigation system through the use of higher quality equipment and redundant architectures;
- Certifying navigation software to a high design assurance level;
- Implementing a navigation system capable of fault detection, exclusion, and accommodation;
- Using certified maps and procedures to check the maps used prior to flight;
- Implementing procedures for the correct initialisation of the navigation system.

For VLOS spraying missions, there is the additional escalation control of the RPA observers, who can provide the RP with backup navigation information through the visual observation of the RPA.
Visual Line of Sight Spraying Operations

Loss of Navigation
- GNSS loss, denied, spoofed, degraded navigation.
- Hardware failures.
- Flaws in software.
- Undetected erroneous inputs to the navigation computer.
- Incorrect maps or reference datum.
- Incorrect initialisation.

Escalation Barrier
- Use of RPA observers.
- A navigation system capable of operating in GNSS denied conditions.
- Improving the reliability of the navigation system.
- High software design assurance level.
- Resilient navigation systems.
- Use of certified maps.
- Initialisation procedures.

Impact Location Barrier
- Geofence

Energy Management Barrier
- Low altitude (low geo-potential energy)

Loss Intervention Barrier
- Emergency response procedures

Engine Failure

Failure Recovery Barrier
- Failure procedures

Figure 9: Loss of navigation and its impact on controls

Broad Area Spraying Operations

Loss of Navigation
- GNSS loss, denied, spoofed, degraded navigation.
- Hardware failures.
- Flaws in software.
- Undetected erroneous inputs to the navigation computer.
- Incorrect maps or reference datum.
- Incorrect initialisation.

Escalation Barrier
- A navigation system capable of operating in GNSS denied conditions.
- Improving the reliability of the navigation system.
- High software design assurance level.
- Resilient navigation systems.
- Use of certified maps.
- Initialisation procedures.

Impact Location Barrier
- Containment Geofence

Energy Management Barrier
- Emergency/forced landing system

Loss Intervention Barrier
- Emergency response procedures

Figure 9: Loss of navigation and its impact on controls
6.7 Evaluation and Summary

As evident in Figure 6, there are limited preventative controls for managing the risks associated with an engine failure. Instead, the risks associated with both spraying missions are primarily managed through the substantiation of mitigative barriers. Of particular interest to the NASA certification study was determining the requirement for a certified propulsion system for the DP-14.

For VLOS spraying missions the casualty risk due to an engine failure is largely managed through the Impact Location and Exposure Barriers. The controls substantiating these barriers have high availability and effectiveness. Through analysis of the associated escalation factors and escalation barriers, it is possible to provide a high degree of assurance in the provision of these barriers. This in turn reduces the need for the implementation of other barriers, specifically, the need for a certified propulsion system (an airworthiness control under the System Reliability Barrier). The focus of airworthiness regulation and oversight can instead be directed towards the mechanisms that provide assurance in the provision of these two barriers.

Conversely, for broad area spraying missions, the Impact Location and Exposure Barriers cannot be substantiated with the same degree of assurance. Few of the identified controls are available for all phases of the mission. The need for the implementation of additional barriers is primarily dependent on the argument that the probability of exposure of third parties is sufficiently low (achieved through the control of site selection under the Exposure Barrier). Thus, the need for a certified engine (or the implementation of additional risk controls) will depend on the particular site where the spraying operation takes place, which will be a primary factor in determining whether third parties are present in the operational area.

6.8 Discussion

Developing a safety case for the operation of RPAS involves the identification, assessment and evaluation of a complex array of technical and operational safety controls. Whilst the BBT model does not help in the identification of hazards nor in the identification of the various means for controlling them, it does provide a simple means for structuring the diverse range of controls into a cohesive “risk picture” for assessment and evaluation. The structure also supports the prompting of questions that may lead to the identification of hazards or controls. In the case of the NASA study [57], the model can provide a means for determining how the complex array of technical and operational risk controls contributed to the overall risk management of the DP-14 operation. The template barriers and graphical nature of the BBT model facilitates a simple comparison of the two complex risk pictures; and in turn, a basis for more rational discussion around the setting of airworthiness certification requirements for the DP-14 RPAS.

The BBT model facilitated a more comprehensive evaluation of controls, whereby each control could be evaluated in isolation and as an integrated part of the system of barriers implemented to manage the risk. This is a particularly important feature of the BBT modelling approach in the context of developing regulations for RPAS. Individual controls identified within a BBT model (including those substantiating escalation barriers) represent the points of regulation available to regulatory authorities. The BBT model allows for the setting of minimum requirements on the performance and reliability of these controls with a clearer understanding of how each control contributes to the overall risk picture. Significant controls can be readily identified as those which are the primary means for implementing a barrier, or those controls that are common to multiple barriers for one or more threats or hazards.

The BBT model facilitates more holistic decision making in relation to the determination of airworthiness requirements for RPAS. Specifically, airworthiness requirements can be explored in the context of the entire “system of controls” and not just the reliability of the RPAS itself. People, processes, and devices critical to the overall safety of the mission are identified within the model. Airworthiness regulations can be targeted towards providing assurance in controls critical to the overall safety of the operation. The model also helps to identify the critical elements in the development of a safety case. For example, key to an acceptable safety case for broad area spraying missions will be the provision of sufficient assurance in the control of third party exposure to the ground impact hazard.
7 Conclusion

There is growing precedence in the use of barrier bow tie (BBT) models as a best practice risk modelling tool across a wide range of industries. This paper has introduced the use of BBT models in the risk analysis of RPAS operations over populous areas.

The airworthiness certification of RPAS operations requires consideration of a much broader range of technical and operational factors than is traditionally considered in the certification of conventionally piloted aircraft. The BBT model facilitates a more comprehensive assessment of all of the technical and operational factors that can be used to control risk. This in turn allows airworthiness requirements to be tailored taking into account all available risk controls.

The case study application served to highlight the general features of the modelling approach but also the benefits of its application in support of the development of regulations for RPAS. Specifically, the model widened the scope of airworthiness certification to potentially include the provision of assurance in the various safety nets used to control risk.

The BBT model can provide the over-arching modelling framework needed to bring together existing risk identification and analysis tools used in aviation risk assessment. Further work is needed to explore how the output from a BBT model can be used within existing aviation risk evaluation and decision making frameworks, including the ALARP and SFAIRP decision making approaches. It is proposed that the control-centric nature of a BBT model would support the more proactive treatment of risks; a key principle for reducing risk SFAIRP.
## Appendix - Tables of Controls

### Table 3: Example Controls Under the System Reliability Barrier

<table>
<thead>
<tr>
<th>Control</th>
<th>Type</th>
<th>Threats</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-flight checklist</td>
<td>Administrative</td>
<td>LOC, UDS, DOJC</td>
<td>Comprehensive pre-flight checklist including system inspection and start up procedure.</td>
</tr>
<tr>
<td>Built-in test</td>
<td>Engineering</td>
<td>LOC, UDS</td>
<td>In-built software and hardware run on initialisation of the system to test critical components (e.g., GPS lock and telemetry link communications check, calibration of air data sensors, battery level, connection of operational radio control gear, etc.).</td>
</tr>
<tr>
<td>Airworthiness</td>
<td>Engineering</td>
<td>LOC, UDS, DOJC</td>
<td>Application of sound design, manufacture, and maintenance practices to provide a degree of assurance in the technical airworthiness of the system (e.g., fail-safe and redundant architectures, use of high quality components, independent unit and system-level testing, etc.). Design of the system to an approved standard.</td>
</tr>
<tr>
<td>Health monitoring</td>
<td>Engineering</td>
<td>LOC, UDS, DOJC</td>
<td>Any system (sensors, algorithms and displays) that can provide a warning or alert to the RP or other on-board systems to the imminent occurrence of a failure. System health monitoring (e.g., low battery, loss of GPS lock, and communications signal strength) with automated visual and aural warnings, health display and alerting within the RPS.</td>
</tr>
<tr>
<td>Flight planning</td>
<td>Administrative,</td>
<td>LOC, UDS, DOJC</td>
<td>Procedures and equipment to plan flights of minimum duration, and to ensure operations are well within the flight envelope (e.g., minimisation of flight loads). Low number and duration of flights. Can include the use of automated flight planning tools that ensure flight plans are within defined performance constraints.</td>
</tr>
<tr>
<td>Communications range check</td>
<td>Administrative</td>
<td>LOC</td>
<td>Telemetry and control receiver range test over the extremities of the mission area.</td>
</tr>
<tr>
<td>Weather check</td>
<td>Administrative</td>
<td>LOC, DOJC</td>
<td>Weather minimums established and the requirement for weather checks pre-flight.</td>
</tr>
<tr>
<td>Shrouds</td>
<td>Engineering</td>
<td>LOC, DOJC</td>
<td>Failsafe locking mechanisms, tethers, shrouds, and shielding to prevent the dropping of stores, or the uncontained release of rotors.</td>
</tr>
<tr>
<td>Control</td>
<td>Type</td>
<td>Threats</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------</td>
<td>---------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Site survey</td>
<td>Administrative</td>
<td>CFIT</td>
<td>Procedure for the inspection of the operational area to identify obstacles and terrain features that pose a hazard and to check the accuracy and completeness of existing maps. Situational awareness of the various terrain and obstacle hazards is necessary for the implementation of all other strategic terrain awareness controls.</td>
</tr>
<tr>
<td>Mission planning</td>
<td>Administrative</td>
<td>CFIT</td>
<td>Procedure to plan missions prior to flight to ensure adequate clearance from known terrain and obstacles. Application of lateral and vertical offsets during mission planning should reflect uncertainty in navigation performance, expected weather and uncertainty in the position of obstacles and height of terrain.</td>
</tr>
<tr>
<td>Mission checking</td>
<td>Engineering</td>
<td>CFIT</td>
<td>Use of automated software-based flight planning and assessment tools that check for adequate clearance of mapped obstacles/terrain.</td>
</tr>
<tr>
<td>No fly zones</td>
<td>Engineering</td>
<td>CFIT</td>
<td>Implementation of no fly zones in software-based mission planning systems. This can be linked to a geofence capability.</td>
</tr>
<tr>
<td>Weather minimums</td>
<td>Administrative</td>
<td>CFIT</td>
<td>Procedure to check weather and visibility conditions are within predefined limits. Limits defined to ensure adequate control and visibility for clearance of terrain and obstacle clearance.</td>
</tr>
<tr>
<td>Detect and avoid</td>
<td>Engineering</td>
<td>CFIT</td>
<td>Engineering devices for detecting and avoiding (DAA) terrain and obstacles. This can include the use of on-board sensors and algorithms (on-board or in the RPS) that alert the RP to closure with terrain or obstacles. In addition to alerting, these systems can also provide automated action (stop, land, manoeuvre, return to base). Positioning systems that automatically maintain a predefined stand-off distance from infrastructure.</td>
</tr>
<tr>
<td>Online mission checking</td>
<td>Engineering</td>
<td>CFIT</td>
<td>Use of automated software-based flight planning and assessment tools that check for adequate clearance of mapped obstacles/terrain. These tools are used during the mission for changes to existing flight paths.</td>
</tr>
<tr>
<td>RPA observers</td>
<td>Administrative</td>
<td>CFIT</td>
<td>The use of trained observers whose documented role includes maintaining visual observation of the RPA to ensure clearance of terrain and obstacles. This function is intended to supplement the RP’s responsibility to maintain safe clearance.</td>
</tr>
<tr>
<td>Environment monitoring</td>
<td>Administrative /  Engineering</td>
<td>CFIT</td>
<td>Equipment and procedures to ensure weather and visibility conditions remain within the predefined limits necessary for clearance of terrain and obstacles. Equipment can include weather stations.</td>
</tr>
<tr>
<td>Control</td>
<td>Type</td>
<td>Threats</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Health monitoring</td>
<td>Engineering</td>
<td>LOC, UDS, DOJC</td>
<td>Systems that detect, diagnose, and alert the RP or on-board systems to the occurrence of a recoverable failure during flight. This includes automated health monitoring systems or the display of system health information to the RP.</td>
</tr>
<tr>
<td>RPA observers</td>
<td>Administrative</td>
<td>LOC, UDS, DOJC</td>
<td>The use of trained observers whose documented role includes maintaining observation of the RPA to detect in-flight failure and alert the RP. This function is intended to supplement the RP’s responsibility to maintain awareness of the RPA health.</td>
</tr>
<tr>
<td>Failure accommodation</td>
<td>Engineering</td>
<td>LOC, UDS, DOJC</td>
<td>Engineering systems that provide an opportunity for recovery from a failure or attempt to accommodate the failure or fault so as to allow the system to continue flight. Examples include an engine restart capability, auto-position hold, automated return to base function, system reboot capability, or fault tolerant control systems.</td>
</tr>
<tr>
<td>Reversion to remote pilot control</td>
<td>Administrative</td>
<td>LOC, CFIT UDS,</td>
<td>The role and supporting systems that allow the RC to take action to recover from a failure state. Requires alerting, an operational command and control link, and RP awareness of the operational state. It is only effective for recoverable failures where there remains some control authority. Highly dependent on the skill of the RP.</td>
</tr>
<tr>
<td>Failure procedures</td>
<td>Administrative</td>
<td>LOC, UDS, DOJC</td>
<td>Documented procedures for diagnosing and addressing recoverable failures (e.g., engine restart procedures).</td>
</tr>
</tbody>
</table>
Table 6: Example Controls Under the Impact Location Barrier

<table>
<thead>
<tr>
<th>Control</th>
<th>Type</th>
<th>Threats</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flight planning</td>
<td>Administrative</td>
<td>LOC, UDS, DOJC, CFIT</td>
<td>Predominantly strategic activity to design the flight path or mission area to maintain a minimum distance from known populations or boundaries. Altitude limits can also be used to minimise the size of the potential impact area and hence its overlap with surrounding populated areas. Minimising the time spent in those regions within the mission area that are close to a populated area.</td>
</tr>
<tr>
<td></td>
<td>Isolation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical containment</td>
<td>Isolation</td>
<td>LOC, UDS, DOJC, CFIT</td>
<td>Using high terrain, trees, or other structures (netting, large buildings) as a physical barrier between the RPA and an exposed populated.</td>
</tr>
<tr>
<td>Geofence</td>
<td>Engineering</td>
<td>LOC, UDS, DOJC, CFIT</td>
<td>A system that predicts or detects the crossing of a containment boundary and executes a pre-defined function (e.g., alert RPS, hold in-situ, or activate flight termination, forced landing or return to base functions).</td>
</tr>
<tr>
<td>Reversion to remote pilot control</td>
<td>Engineering / Administrative</td>
<td>LOC, UDS</td>
<td>Technical and piloting capability that allows the RP to influence the trajectory of the RPA resulting in impact in a non-populated area. Requires adequate alerting, command and control link. Effectiveness is highly dependent on the ability of the RP and the remaining control authority.</td>
</tr>
<tr>
<td>Flight termination system</td>
<td>Engineering</td>
<td>LOC, UDS, DOJC, CFIT</td>
<td>A system that on activation (by geofence, by health monitoring systems, or manual triggering by a member of the RC) immediately brings the RPA to earth. Action can include an automated constant rate descent, or other pre-defined automatic control sequence that causes the RPA to come to earth.</td>
</tr>
<tr>
<td>Forced/Emergency landing systems</td>
<td>Engineering</td>
<td>UDS</td>
<td>Systems for the detection and termination of flight to a suitable / non-populated area. For failures where there is still some degree of control over the aircraft state.</td>
</tr>
<tr>
<td>Shrouds or payload tethers</td>
<td>Engineering</td>
<td>DOJC</td>
<td>Containing or reducing the energy of ejected or dropped stores so as to reduce the probability they impact outside the designated operating area.</td>
</tr>
<tr>
<td>Tethers</td>
<td>Engineering</td>
<td>LOC, UDS, DOJC</td>
<td>Tethering the RPA to the ground.</td>
</tr>
</tbody>
</table>
### Table 7: Example Controls Under the Energy Management Barrier

<table>
<thead>
<tr>
<th>Control</th>
<th>Type</th>
<th>Threats</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parachutes</td>
<td>Engineering</td>
<td>LOC, UDS, DOJC</td>
<td>Reduction of the rate of descent and hence transfer of energy to an impacted person or building through the use of an energy reducing device. Also increases the time potentially impacted individuals have to take avoiding action.</td>
</tr>
<tr>
<td>Air bags</td>
<td>Engineering</td>
<td>LOC, UDS, DOJC</td>
<td>Reduction of the transfer of energy to an impacted person or building through the use of inflatable cushions.</td>
</tr>
<tr>
<td>Frangibility</td>
<td>Engineering</td>
<td>LOC, UDS, DOJC, CFIT</td>
<td>Use of energy-absorbing materials or structural designs that minimise the transfer of energy to an impacted person or building. This includes the use of energy dissipative propeller materials.</td>
</tr>
<tr>
<td>Small RPA</td>
<td>Engineering</td>
<td>LOC, UDS, DOJC, CFIT</td>
<td>RPA that inherently lack the energy or physical properties necessary to cause harm. For example, very small RPA operating at low speeds.</td>
</tr>
<tr>
<td>Emergency / Flight termination</td>
<td>Engineering / Administrative</td>
<td>LOC, UDS, DOJC, CFIT</td>
<td>Flight termination/emergency-landing procedures or automated sequences that establish the aircraft on an energy minimal flight path. This can include auto-rotation, steep stalls, gradual spirals, and constant rate descents.</td>
</tr>
<tr>
<td>Shrouds</td>
<td>Isolation</td>
<td>LOC, UDS, DOJC, CFIT</td>
<td>Devices that protect impacted individuals from laceration or penetration from rotating parts.</td>
</tr>
<tr>
<td>Engine kill</td>
<td>Engineering</td>
<td>LOC, UDS, DOJC, CFIT</td>
<td>Systems that automatically kill the propulsion system on impact or proximity to impact.</td>
</tr>
<tr>
<td>Configuration management</td>
<td>Administrative</td>
<td>LOC, UDS, DOJC, CFIT</td>
<td>Defined procedures to minimise the magnitude of potential harm caused by the RPA in its nominal flight configuration (<em>e.g.</em>, operating only with minimal fuel, batteries, with only necessary stores/payload, <em>etc.</em>).</td>
</tr>
<tr>
<td>Fuel containment</td>
<td>Engineering</td>
<td>LOC, UDS, DOJC, CFIT</td>
<td>Use of battery bags or puncture resistant fuel tanks.</td>
</tr>
<tr>
<td>Control</td>
<td>Type</td>
<td>Threats</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------</td>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Site selection</td>
<td>Administrative</td>
<td>LOC, UDS, DOJC, CFIT</td>
<td>Operating over or near areas of low population density. Flying in remote areas where there is a decreased likelihood that a person will enter the mission area, or be present in the surrounding areas (should the RPA depart the designated operating area).</td>
</tr>
<tr>
<td>Time of operation</td>
<td>Administrative</td>
<td>LOC, UDS, DOJC, CFIT</td>
<td>Operating at times of the day or year when people are less likely to be present in the operational area, surrounding areas, or predefined flight termination / emergency landing areas. For example, flying over the beach in winter, or operating late at night when most people are asleep.</td>
</tr>
<tr>
<td>RPA observers</td>
<td>Administrative</td>
<td>LOC, UDS, DOJC, CFIT</td>
<td>The use of trained observers whose documented role includes maintaining visual observation of the designated operating area or flight termination / emergency landing area for the detection of intrusions by third parties; alerting third parties to the operation of the RPA; or alerting the RP to the presence of a third party within the operating area. This function is intended to supplement the RP’s responsibility to maintain situational awareness of the operating area.</td>
</tr>
<tr>
<td>Public awareness</td>
<td>Administrative</td>
<td>LOC, UDS, DOJC, CFIT</td>
<td>Strategic (pre-flight) communication and engagement activities to build public awareness of RPAS operation, and to discourage approaching/entering designated operational areas.</td>
</tr>
<tr>
<td>Warning signs</td>
<td>Administrative</td>
<td>LOC, UDS, DOJC, CFIT</td>
<td>A form of public awareness, placing signs around operating areas or flight termination / emergency landing areas warning as to the presence of RPAS operations and discouraging entry to the areas.</td>
</tr>
<tr>
<td>Fencing</td>
<td>Isolation</td>
<td>LOC, UDS, DOJC, CFIT</td>
<td>Ensuring the designated operating area or flight termination / emergency landing area remains clear of third parties through the use of pedestrian fencing or barriers.</td>
</tr>
<tr>
<td>Alerting systems</td>
<td>Engineering</td>
<td>LOC, UDS, DOJC, CFIT</td>
<td>Security systems alerting remote crew to the intrusion of a designated operational area.</td>
</tr>
<tr>
<td>Impact alarms</td>
<td>Engineering</td>
<td>LOC, UDS, DOJC</td>
<td>Audible alarms or visual warning systems that alert people on the ground to a pending impact. These systems are reliant on the individuals taking appropriate and timely action to avoid the impact (a weak control).</td>
</tr>
</tbody>
</table>
Table 9: Example Controls Under the Entity Response Barrier

<table>
<thead>
<tr>
<th>Control</th>
<th>Type</th>
<th>Threats</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Helmets and glasses</td>
<td>Personal Protective Equipment</td>
<td>LOC, UDS, DOJC, CFIT</td>
<td>Protective equipment for exposed entities.</td>
</tr>
<tr>
<td>Resilient entities</td>
<td>Engineering Administrative</td>
<td>LOC, UDS, DOJC, CFIT</td>
<td>Ensuring that the entities potentially impacted are resilient to harm. For damage to people, this could include minimising the exposure of small children to the activity (if at all possible). For buildings, engineered features such as concrete construction that make the building more resilient to impact damage.</td>
</tr>
<tr>
<td>Shelters</td>
<td>Isolation</td>
<td>LOC, UDS, DOJC, CFIT</td>
<td>Providing temporary structures or other protective mechanisms for exposed people (e.g., behind vehicles).</td>
</tr>
</tbody>
</table>

Table 10: Example Controls Under the Loss Intervention Barrier

<table>
<thead>
<tr>
<th>Control</th>
<th>Type</th>
<th>Threats</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency services</td>
<td>Administrative</td>
<td>LOC, UDS, DOJC, CFIT</td>
<td>Predominantly strategic activities to maximise the responsiveness of emergency services. This can include advising emergency services as to the activity taking place, joint development of emergency plans, proximity of operation to local services, checking availability of emergency services and access before operations.</td>
</tr>
<tr>
<td>Emergency procedures</td>
<td>Administrative</td>
<td>LOC, UDS, DOJC, CFIT</td>
<td>Strategic activity to develop emergency plans. Tactical activities such as pre-flight briefings of emergency procedures.</td>
</tr>
<tr>
<td>Emergency training</td>
<td>Administrative</td>
<td>LOC, UDS, DOJC, CFIT</td>
<td>Personnel trained in first aid and the use of fire or other emergency equipment.</td>
</tr>
<tr>
<td>Emergency equipment</td>
<td>Engineering</td>
<td>LOC, UDS, DOJC, CFIT</td>
<td>Fire extinguishers and first aid equipment.</td>
</tr>
</tbody>
</table>
Acknowledgments
The authors would like to acknowledge Dr Natasha Neogi from NASA Langely Research Center, and Ms. Sarah Mecklem from Boeing Research & Technology Australia, for valuable contributions made in reviewing early versions of this paper. This research, in part, was sponsored by a 2014 Civil Aviation Safety Authority Research Grant.

References


[29] Radi, A., Human injury model for small unmanned aircraft impacts, Civil Aviation Safety Authority (CASA), Canberra, Australia, 2013.


[34] CAA, “CAA Strategy for Bowtie Risk Models,” Tech. rep., Civil Aviation Authority, United Kingdom, August 2015.


[41] CAA, “Introduction to Bowtie: How this risk assessment tool works,”.


[45] NATO, “NATO Standardization Agreement (STANAG) - Unmanned Aerial Vehicles Systems Air-
worthiness Requirements (USAR),” Tech. Rep. STANG 4671, North Atlantic Treaty Organization

[46] ICAO, “Annex 13 to the Convention on International Civil Aviation - Aircraft Accident And In-
cident Investigation, 10th Edition,” Tech. rep., International Civil Aviation Organization (ICAO),
Montréal, Canada, July 2010.


Group, Civil Aviation Authority (CAA), United Kingdom, July 2010.

[51] CASA, “Risk Management Framework,” Tech. rep., Civil Aviation Safety Authority (CASA), Can-
berra, Australia, December 2014.

SAE International, October 2010.

[53] SAE, “Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne

ington, D.C., December 2000.

[55] Sabatini, R., Moore, T., and Hill, C., “A New Avionics Based GNSS Integrity Augmentation System:

unmanned aircraft systems,” Technical report, Commonwealth Scientific and Industrial Research
Organisation (CSIRO), Canberra, Australia, June 2013.

G. F., “Mock Certification Basis for an Unmanned Rotorcraft for Precision Agricultural Spraying,”
Tech. Rep. NASA/TM-2015-218979, National Aeronautics and Space Administration (NASA), Lan-
gley Research Center, Hampton, VA, November 2015.

[58] DPI, “DP-14 Hawk Specification Sheet,” Tech. rep., Dragonfly Pictures Incorporated (DPI), Ess-
ington, PA, 2014.

Civil Aviation Organization (ICAO), Montréal, Canada, 1st ed., 2015.