SAFETY CONSIDERATIONS IN EMERGING ELECTRIC AIRCRAFT ARCHITECTURES

Christopher Courtin and R. John Hansman

This report presents research originally published under the same title at the 18th AIAA Aviation Technology, Integration, and Operations Conference in Atlanta, GA. Citations should be made to the original work with DOI: 10.2514/6.2018-4149.

Report No. ICAT-2018-07
June 2018

MIT International Center for Air Transportation (ICAT)
Department of Aeronautics & Astronautics
Massachusetts Institute of Technology
Cambridge, MA 02139 USA
Safety Considerations in Emerging Electric Aircraft Architectures

Christopher Courtin* John Hansman†
Massachusetts Institute of Technology, Cambridge, 02139, USA

Safety and certification considerations which impact the design of an emerging new class of small, electric aircraft were investigated. Based on an assessment of the different emerging aircraft designs, vehicles were grouped based on lifting and propulsive architecture. Likely certification pathways and the associated airworthiness requirements were investigated. Key hazards were identified, and were classified by severity for each architecture group. The key hazards identified were lithium-polymer battery thermal runaway and energy uncertainty, common mode power system failure, and vehicle automation failure. Mitigation strategies for each identified hazard were identified based on current technology and regulatory requirements. These mitigation strategies were assessed for different vehicle architectures. Aircraft with the ability to controllably glide or autorotate are shown to have lower certification risk.

Nomenclature

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BRS</td>
<td>Ballistic Recovery System</td>
</tr>
<tr>
<td>CTOL</td>
<td>Conventional Takeoff and Landing</td>
</tr>
<tr>
<td>DEP</td>
<td>Distributed Electric Propulsion</td>
</tr>
<tr>
<td>FADEC</td>
<td>Fully Authority Digital Engine Control</td>
</tr>
<tr>
<td>IAS</td>
<td>Indicated Airspeed</td>
</tr>
<tr>
<td>NAS</td>
<td>National Airspace System</td>
</tr>
<tr>
<td>UAM</td>
<td>Urban Air Mobility</td>
</tr>
<tr>
<td>VTOL</td>
<td>Vertical Takeoff and Landing</td>
</tr>
</tbody>
</table>

I. Introduction

There is currently a growing interest in the development and operation of new classes of small, fully electric aircraft targeted specifically at missions in and around major urban metropolitan areas; this is commonly referred to as Urban Air Mobility (UAM). This concept represents a significant departure from the current paradigm of commercial aircraft design, certification, and operations. Proponents of this system argue that it will dramatically increase the regional or intraurban mobility of people living in major metro areas by decreasing travel times, avoiding surface gridlock and leveraging the smartphone-enabled ride-sharing transportation model that has proven effective with ground-based transportation [1]. There are several key challenges that need to be overcome to realize this vision. They are associated with economic and operational feasibility, community acceptance, and vehicle safety. The first three are discussed in more detail by [2], [3] and [4]. This paper will focus specifically on vehicle safety, and in particular the challenges associated with certifying electric aircraft for operations within the existing or near-future National Airspace System (NAS). Certifying vehicles is particularly critical for developing a UAM system because it is a prerequisite for commercial operations at any scale. Historically, the certification process for new types of aircraft is complicated and time-consuming. This is most recently exemplified by the 15+ year flight testing and certification program of the AW609 tiltrotor, now expected to continue at least through 2019 [5].

The goal of this paper is to examine the current and proposed regulatory environment for electric aircraft as well as the design space of emerging architectures, and identify key challenges that must be overcome to achieve certification. These challenges may arise from a lack of applicable regulation, or tension between accepted methods of meeting applicable regulatory requirements and other high-level vehicle drivers such as

*Graduate Student, Aeronautics and Astronautics Engineering, MIT, 77 Mass Ave, Cambridge MA, 02139, AIAA Student.
†T. Wilson Professor, Aeronautics and Astronautics Engineering, MIT, 77 Mass Ave, Cambridge MA, 02139, AIAA Fellow.
weight and cost. It should be emphasized that these challenges are not insurmountable barriers to certification but rather areas where existing technology or vehicle design and certification methods are insufficient. As such, they should be areas of focus for both industry and regulators.

In this paper a brief overview of the expected regulatory environment is given. The emerging design space of all-electric aircraft is then surveyed, and the vehicles are grouped into distinct architecture classes. A preliminary hazard assessment is conducted to identify hazards associated with each vehicle class, and to assess the severity of each. This assessment is focused primarily on hazards associated with novel electric aircraft configurations and technologies. For the most critical hazards identified, potential mitigation strategies and certification challenges are discussed, looking at how they are impacted by vehicle architecture.

As part of this work, previous literature on electric aircraft [6], [7], [8], the risks associated with electric aircraft [9], lithium-ion batteries [10], [11], and proposed electric aircraft operations [12] is considered.

II. Certification Pathways

The expected certification pathway for small electric aircraft is through FAR Part 23, which certifies aircraft for commercial use up to a maximum size of 19,000 lbs or 19 passengers. This standard was recently rewritten to become an industry-based standard, which allows certification under any set of standards acceptable to the administrator [13]. One such set of standards is ASTM 3264, which has been accepted by the FAA as a means of compliance with the Part 23 standards [14]. ASTM 3264 is currently being updated by Committee F44 to allow the certification of electric aircraft [15], but is one clear path by which the necessary regulations could be enacted. This set of standards will be used as a reference for this paper. Certification under other standards may be possible but it is expected that the challenges identified will be broadly similar. The current guidance states that vehicles capable of wing-borne flight during any phase of the mission will be certifiable under the new Part 23 [16], even if they have Vertical Takeoff and Land (VTOL) capability. For simplicity, it will be assumed that vehicles such as multirotors which have VTOL capability but lack wings can also be certified under a similar standard and not the current Part 27, which has no provisions for the certification of electric vehicles. The actual certification pathway for these vehicles is still uncertain. As these regulations are still under development there is uncertainty around some details of the regulations; this will be noted where significant.

ASTM 3264 incorporates a risk-based approach to certification; for a given aircraft, all hazards to which it is exposed must be identified, assessed based on severity, and then mitigated to an acceptable level. The severity of a hazard is a function of both likelihood of occurrence and significance of consequences - high consequence and/or likelihood hazards have high severity. Hazards are classified as high, medium, or low severity according to the risk matrix shown in Figure 1. The horizontal axis shows the likelihood a hazard occurs, and the vertical axis shows the consequence of that occurrence. High severity hazards are shown in red, medium in yellow, and low in green. This matrix will be used in subsequent sections to assess the severity of different hazards for various vehicle architectures.

![Risk matrix showing high-(red), medium-(yellow), and low-(green) severity risk areas.](image)

Consequence is ranked based on a given hazard’s expected effects on the airframe, flight crew, and passengers. The definitions of the various consequence levels according to the relevant risk assessment standard [17] are shown in Table 1.

For the purposes of vehicle certification, a given hazard is considered acceptable if it can be shown to be a
Table 1: Hazard consequence is ranked based on the impact to passengers, crew, and aircraft [17].

<table>
<thead>
<tr>
<th>Hazard Classification</th>
<th>Effect on Aircraft</th>
<th>Effect on Occupants</th>
<th>Effect on Flight Crew</th>
</tr>
</thead>
<tbody>
<tr>
<td>Negligible</td>
<td>No effect</td>
<td>inconvenience</td>
<td>No effect</td>
</tr>
<tr>
<td>Minor</td>
<td>Slight reduction in capability or safety margin</td>
<td>Physical discomfort</td>
<td>Slight increase in workload or use of emergency procedures</td>
</tr>
<tr>
<td>Major</td>
<td>Significant reduction in capability or safety margin</td>
<td>Physical distress or injury</td>
<td>Significant increase in workload or physical discomfort</td>
</tr>
<tr>
<td>Hazardous</td>
<td>Large reduction in capability or safety margin</td>
<td>Serious or fatal injury</td>
<td>Physical distress or excessive workload impairs performance</td>
</tr>
<tr>
<td>Catastrophic</td>
<td>Normally with hull loss</td>
<td>Multiple fatalities</td>
<td>Fatal injury or incapacitation</td>
</tr>
</tbody>
</table>

medium or low severity. The difference between a medium and low severity hazard is based on the NASA Risk Management Handbook [18]; it is useful for hazard assessment but is not meaningful for certification. The ASTM 3230 safety assessment standard defines an acceptable probability of failure as a function of hazard consequence; this boundary is shown as the thick black line in Figure 1 [17]. Qualitatively, occurrence of a catastrophic failure mode must be shown to be extremely improbable, occurrence of a hazardous failure mode must be extremely remote and so on.

Quantitatively, the different probability levels are expressed as the expected number of failures per flight hour. Those quantitative targets differ mainly with the number of passengers. For aircraft with fewer than seven passengers, there is a lower airworthiness level if they are powered by a single reciprocating engine. These are shown in Table 2. There are currently no explicit targets for electric engine, but since most UAM aircraft are expected to be multi-engined with 2-4 passengers, Level II gives the most relevant current safety targets. It should be noted that the Part 25 standard which governs large commercial aircraft requires a $< 10^{-9}$ probability of catastrophic failure per flight hour; this is in line with the Level IV airworthiness standard [19] and is more stringent than the current requirements for small vehicles. When choosing the design level of safety for these vehicles, passenger perception and the need to build confidence in the system will also be considerations; for those reasons a higher level of safety than is mandated may be desirable.

Table 2: Quantitative definitions of differing likelihood levels based on the number of passengers and engine number and type. [17]. Level II is expected to be most relevant for small UAM vehicles

<table>
<thead>
<tr>
<th>Certification Airworthiness Level</th>
<th>Probable</th>
<th>Remote</th>
<th>Extremely Remote</th>
<th>Extremely Improbable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level IV: 10-19 pax</td>
<td>$&lt; 10^{-3}$</td>
<td>$&lt; 10^{-5}$</td>
<td>$&lt; 10^{-7}$</td>
<td>$&lt; 10^{-9}$</td>
</tr>
<tr>
<td>Level III: 7-9 pax</td>
<td>$&lt; 10^{-3}$</td>
<td>$&lt; 10^{-5}$</td>
<td>$&lt; 10^{-7}$</td>
<td>$&lt; 10^{-8}$</td>
</tr>
<tr>
<td>Level II: 0-6 pax, STE, ME</td>
<td>$&lt; 10^{-3}$</td>
<td>$&lt; 10^{-5}$</td>
<td>$&lt; 10^{-6}$</td>
<td>$&lt; 10^{-7}$</td>
</tr>
<tr>
<td>Level I: 0-6 pax, SRE</td>
<td>$&lt; 10^{-3}$</td>
<td>$&lt; 10^{-4}$</td>
<td>$&lt; 10^{-5}$</td>
<td>$&lt; 10^{-6}$</td>
</tr>
</tbody>
</table>

III. Emerging Electric Aircraft Architectures

There are many established and emerging companies developing small, electric aircraft. These vehicles span a broad architecture space, from conventional fixed-wing aircraft that use an electric powertrain in place of a conventional combustion engine to Distributed Electric Propulsion (DEP) tilt-rotors capable of vertical and high speed horizontal flight. For the purposes of this study, it’s useful to categorize these vehicles into the eight architectural classes shown in Figure 2. These are based on how the vehicle generates lift (wings, rotors, or some combination of the two) and whether or not the vehicle utilizes some form of distributed propulsion, which is here defined as having more than three propulsors. Hybrid lift vehicles, which utilizes lift from wings and rotors at different phases of the flight, are further broken down into “Actuating Hybrid Lift” and “Static Hybrid Lift”, depending on whether or not the vertical lift propulsors also tilt to provide thrust in wing-borne flight. The majority of vehicles being developed for UAM applications fall into the Multitrotor, DEP Tilt-Lift, and Stopped Rotor categories.

These eight classes can be further classified into four main meta-groups for the purposes of evaluating the certification challenges, shown as the colored boxes in Figure 2. All vehicle architectures within a group have similar certification challenges. Where significant, the differences between the sub-categories in each group will be discussed (i.e. the difference between Stopped Rotor and DEP Tilt-Lift configurations). What follows is a brief description of the common elements of each group, along with some key assumptions.

**Multirotor**  Multirotor vehicles are supported by rotor lift only through all phases of flight and have a distributed electric propulsion system. Attitude control of multirotors is accomplished using differential thrust between the motors; this is usually done by changing motor speed but can also be done via a variable pitch mechanism on each rotor. These vehicles require an electronic stabilization system to be controllable by a pilot. Due to the likely use of fixed pitch propellers, low rotor inertia, and the lack of mechanical control linkages these vehicles are not capable of autorotation. The primary benefits of multirotor configurations are low cost due to mechanical simplicity and possible noise benefits relative to helicopters due to additional design freedom to vary disk loading, blade frequency, and tip speed [20].

**Distributed Electric Propulsion Powered Lift**  DEP Powered Lift aircraft combine the vertical takeoff and land (VTOL) architecture of a multirotor with wings for increased efficiency and speed during the cruise phase of flight. During the takeoff and landing phases of flight, they have the same behavior as multirotors, including the lack of autorotation capability and the need for a active stabilization system. During cruise, they can be flown as a conventional fixed-wing aircraft. The advantages of this configuration are improved cruise speed and range relative to a multirotor, while maintaining the vertical takeoff and land capability and noise-related design freedom.
Fixed Wing  Fixed Wing vehicles are supported by wing lift through all phases of flight. It is assumed that these vehicles have an electric drive system but use mechanically actuated aerodynamic control surfaces, as is common on most aircraft of this size class. It is also assumed that the wings are sized to provide a survivable unpowered landing speed in the event of an loss of power. This is likely to be equivalent to the current 61 kts maximum stall speed mandated by the historical Part 23. The current standard does not explicitly enforce this limit [13], so an increased stall speed could be traded for improved crashworthiness to maintain equivalent power-out survivability. This is a detailed vehicle design trade not explored here. The benefits of the fixed wing configuration are range, speed, and payload capability as well as much smaller required propulsion systems, which also may have noise benefits.

Rotorcraft  Rotorcraft in this context refers to vehicles that use rotors at least for the takeoff and landing portion of the flight, and possibly for the entire mission, but do not utilize distributed electric propulsion. This category would include all current helicopters, as well as tilt-rotors like the AW609 and proposed slowed-rotor configurations. A defining features of these vehicles is the ability to autorotate in the event of a power loss. All Part 27 rotorcraft must be safely controllable during autorotation [21]; this includes tilt-rotors like the AW609 [22]. Additionally, except for Tilt-lift vehicles these aircraft are controllable without the need for an active stabilization system. The advantages of vehicles in the Rotorcraft group are VTOL capability; Tilt-lift and Static Hybrid vehicles have improved cruise range and speed relative to helicopters.

Autorotation and Gliding  The ability of a vehicle to autorotate or glide in a controllable manner without power is an important safety feature of all current Part 23 or Part 27 vehicles. The ability to autorotate to a controlled, pinpoint landing is one of the reasons helicopters are permitted to operate at low altitudes over dense urban environments [23]. Good power-out controllability may also contribute to the fact that fatal injury rates for engine failures are lower than for other leading causes of small aircraft accidents; 16% compared to 44% for in-flight loss of control or 46% for controlled flight into terrain, based on aggregate general aviation and Part 135 accident statistics from 2013-2015 [24]. Fatal injury is most likely when control of the aircraft is lost. Of the four architecture groups considered, Rotorcraft can autorotate, while Fixed Wing and DEP Powered Lift vehicles can glide.

IV. Preliminary Emerging Hazard Assessment

A preliminary emerging hazard assessment was undertaken to qualitatively identify and assess the key hazard categories for each electric aircraft architecture. Key hazards are considered to be those that arise from the novel electric powertrain or vehicle configuration, and for which risk severity, potential mitigations, or applicable regulations different significantly from current vehicles certified under Part 23. The goal is to highlights key areas where the current regulations may need to be updated or areas where there is tension between current regulatory requirements and vehicle design requirements with current or near-future technology levels.

For each architecture, a list of hazards was developed and each hazard assigned baseline risk severity using the risk matrix shown in Figure 1. This list of hazards and probability/consequence estimates was made based on safety analysis of current electric aircraft [9], proposed capabilities of small electric aircraft [1], the capabilities of similar systems and features of the underlying technology. Published sources (cited throughout) were used as well as conversations with subject matter experts in academia and industry. These estimates are for a generic representative vehicle of each group and not reflective of the details of any specific aircraft; their purpose is to illustrate general trends and high-level considerations. The actual level of risk exposure for any vehicle is highly dependent on the details of the vehicle design and the incorporated safety systems. This baseline does not assume any risk mitigation beyond the vehicle capabilities described in the previous section. Additional safety systems can be designed into the vehicles to reduce these baseline hazards to acceptable levels; these potential mitigation strategies were also identified for each key hazard.

This is not intended to be a comprehensive overview of all possible hazards for these vehicles. The majority of the hazards to which electric aircraft are exposed are similar to conventional aircraft, and there are straightforward ways to mitigate them under the current regulatory paradigm. For example, the hazard posed by a single motor component failure is effectively mitigated by redundant motors, a control system sized for sufficient control in that engine-out case, and design and production standards on the motor component itself. In terms of this hazard, electric aircraft are the same or potentially better than conventional gas-powered vehicles. Component failure and other well-understood hazards such as structural failure do not
constitute key hazard categories and thus are not discussed further. The identified key emerging hazards for electric aircraft are presented in Figure 3 and discussed in detail in the following section.

<table>
<thead>
<tr>
<th>Hazard Description</th>
<th>Multirotor</th>
<th>DEP Powered Lift</th>
<th>Powered Lift</th>
<th>Fixed Wing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Battery Thermal Runaway</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Battery Energy Uncertainty</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Common Mode Power Failure (Low-/High-Altitude)</td>
<td>High/High</td>
<td>High/Medium</td>
<td>Medium/Medium</td>
<td>Medium/Medium</td>
</tr>
<tr>
<td>Fly-By-Wire System Failure</td>
<td>High</td>
<td>High*</td>
<td>Low**</td>
<td>Low</td>
</tr>
<tr>
<td>High-Level Autonomy Failure</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Bird Strike</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
</tr>
</tbody>
</table>

*Including Tilt-Lift vehicles  **Except Tilt-Lift vehicles

**Figure 3:** Key hazards for each electric aircraft configuration group, with a baseline risk severity assessment for each.

A. Common Mode Power System Failure

While redundancy in the powertrain is often cited as a reason that DEP vehicles will be safer than most aircraft, they are still susceptible to common mode power system failures. A common mode failure is when multiple systems fail in the same way for the same reason [25]. There are a number of possible causes of common mode failures, including maintenance errors, manufacturing defects, environmental factors, unforeseen operating conditions, or unexpected software states. Figure 4 shows the baseline (unmitigated) risk for each of the four configuration groups with the position of the P, M, D, or F on the risk matrix. The altitude at which the hazard is considered is shown by the subscript below each letter; altitude can effect both the probability and consequence of a given hazard occurrence. Probability is calculated based on average exposure time of a representative flight profile [26]; if a vehicle spends a relatively small amount of time at low altitude then the probability associated with hazards there is reduced. However, they may be more consequential as discussed below.

For current Part 23 aircraft and Part 27 rotorcraft, a common mode power system failure is not necessarily catastrophic; even with total engine failure those vehicles still have functional primary flight controls and gliding or autorotative performance that makes a survivable landing likely. For this reason, a total power failure is classified as hazardous if it occurs at a point where a vehicle could successfully enter a survivable glide or autorotation. Where this point is depends on a number of factors, including the surrounding terrain, vehicle weight, and altitude at which the power failure occurs. For the purposes of this paper, high altitude is considered any altitude above which the vehicle could enter a survivable glide or autorotation, and low altitude is anything below this point. For vehicles without the ability to glide or autorotate, the minimum effective deployment altitude of an airframe parachute system can be considered a dividing line between low and high altitude.

For a Rotorcraft, autorotation can be entered at any altitude as long as the vehicle has sufficient forward speed. General takeoff and landing procedures for Rotorcraft are design so that entry into autorotation is always possible; this safe flight envelope is generally shown on a height-velocity diagram for these vehicles. For this architecture group the risk of common mode power failure has the same severity at both low and high altitude.

For a Fixed Wing aircraft, there is a small window on takeoff where a total power failure could be
Figure 4: Baseline risk severity associated with common mode power system failure for each vehicle architecture group.

considered catastrophic. This is when the vehicle is too high to return to the runway but too low to have any significant room to maneuver for a safe landing. The duration of that window is very small compared to the total length of the flight; this is generally considered an acceptable risk.

For Multirotor configurations without the ability to autorotate, a common mode power system failure would be catastrophic at any altitude. For DEP Powered Lift vehicle, wings are assumed to provide glide capability similar to a Fixed Wing vehicle; total power failure at high altitudes has a correspondingly lower consequence. This assumes that the wings are sized to a survivable landing speed and there are mechanical control linkages or an isolated electrical actuation system for aerodynamic control surfaces that give sufficient pitch, roll, and yaw control without differential thrust.

At low altitude, the expected takeoff and landing profile is similar to a Multirotor since DEP Powered Lift aircraft also cannot autorotate. However, different takeoff and landing profiles could be used. For example, a takeoff profile similar to a Fixed Wing vehicle would give similar lowered risk exposure, although it could potentially increase the size of the takeoff area required. In general, the DEP vehicles have the ability to quickly transition to wing-borne flight at lower altitudes (a lower risk flight profile) or conducted extended vertical takeoffs (a higher-risk flight profile). A low-altitude transition could be beneficial for efficiency, while a high-altitude transition would be desirable to reduce noise exposure of the surrounding population.

For the purposes of meeting certification standards, representative flight profiles are being developed which could be used to calculate risk exposure [27]. These are based on a low-altitude (50ft) transition maneuver. This raises the an interesting question of whether higher-risk flight profiles would be allowable for commercial operations, where they might be desirable to reduce noise exposure [12]. This requires a much more detailed understanding at a vehicle level of the actual effects of flight profile are on risk, but represents an interesting area of future research.

Table 3: Mitigation strategies for common mode power system failures

<table>
<thead>
<tr>
<th>Mitigation Description</th>
<th>Mitigation Reduces</th>
</tr>
</thead>
<tbody>
<tr>
<td>System redundancy and design practice</td>
<td>Probability</td>
</tr>
<tr>
<td>BRS (Aircraft Parachute)</td>
<td>Consequence</td>
</tr>
<tr>
<td>Autorotation</td>
<td>Consequence</td>
</tr>
</tbody>
</table>

For Multirotor and DEP Powered Lift configurations there are several ways to mitigate this hazard to acceptable levels, either by reducing the consequence or probability of occurrence. These are shown in Table 3 and discussed briefly below.
1. **System Redundancy and Design Practice**

The aerospace industry has demonstrated the capability to develop safe vehicles where total loss of power is unacceptable, Part 25 commercial aircraft being the most notable example. This is done via good systems engineering and safety assessment practices, including detailed assessments of failure probability down to individual component levels [26]. These processes enable the reliable development of the highly redundant systems necessary to mitigate any foreseen common mode failures to safe levels. The challenge in the context of UAM will be developing systems that meet the required levels of safety while staying within the tight cost and weight targets of those vehicles. Additionally, the need to certify a complex, highly flight-critical system may add to the time needed to get regulatory approval for the vehicle. A key issue here is what the required level of safety should be. The level mandated by the regulations is significantly lower than for a Part 25 commercial jet transport. This could reduce the difficulty of developing such a system, since it would not have to be as reliable. If the regulation was precisely met, at the scale of proposed UAM operations this would still lead to a significant number of catastrophic failures every year. To build passenger confidence and trust in the system, a higher level of safety closer to current commercial air travel may be desirable.

2. **Ballistic Recovery Systems**

Ballistic recovery systems (BRS), or airframe parachute systems, are increasingly popular on small GA aircraft and are widely proposed as a mitigation for total electrical system failure in electric aircraft, especially for Multirotor or DEP Powered lift configurations in vertical flight modes where autorotation or gliding is not possible. Current BRS technology has been shown to be effective, but only above a certain combination of airspeeds and altitudes. Figure 5 shows the officially demonstrated (dark blue) and likely (light blue) effective deployment envelope of the ballistic recovery systems for a Cirrus SR20 based on the published handbook. This system is the SR20’s means of compliance with the spin recovery requirements. The deployment time and corresponding altitude loss (from time of system deployment until full inflation of the canopy) of a BRS system is a function of both altitude and airspeed. In the case of the Cirrus system that altitude loss increases from no more than 400 ft if the BRS is deployed while the aircraft is in straight and level flight to more than 900 ft if the aircraft is in a spin [28]. While successful lower-altitude deployments have been reported [29] this requires higher speed and is not guaranteed. Vehicle weight and the details of the parachute design can significantly change the effective deployment envelope.

![Figure 5: The demonstrated (dark blue) and likely successful (light blue) parachute deployment envelopes for a Cirrus SR20.](image)

Multirotor and DEP Powered Lift configurations spend a significant amount of time outside the blue envelope during takeoff, landing, and low-altitude flight. During this time, a BRS would not be an effective mitigation against total power loss. The full-airframe equivalent of a zero-zero ejection seat would be required.
If most flights take place over congested urban areas, it also raises the question of how the impact of ground population should be considered. In dense urban environments, a UAM vehicle descending uncontrolled under a parachute is still a hazard (albeit less of one than without such a system). A full-airframe zero-zero-like ejection system based on the same rocket technology as current military systems would also have significant safety concerns for any bystanders in the deployment area. While BRS systems are certainly beneficial safety systems and should be equipped on all UAM aircraft, they are not a panacea for all hazards and should not replace a highly reliable vehicle design.

3. Autorotation

Incorporation of an autorotation capability into a Multirotor or DEP Powered Lift configuration could give the same power-out capability as a Rotorcraft, with the associated safety benefits. This requires variable-pitch rotors with sufficient inertia and an isolated control system. This will add to vehicle weight and complexity when compared to fixed-pitch rotors.

In summary, the hazard of common mode power system failure is challenging to mitigate outside current BRS operating envelopes for Multirotor or DEP Powered Lift configurations without autorotation capability. This challenge arises from the need to develop a complex, highly redundant system, which could add significant weight and cost, in a vehicle that is very cost- and weight-sensitive. Since this hazard is of higher consequence than for current Part 23 aircraft, the demonstrated probability of failure will need to be correspondingly lower, possibly more in line with Part 25 requirements.

B. Battery Thermal Runaway

The high specific energy of lithium-polymer (LiPo) batteries is the key enabling technology for commercially feasible all-electric aircraft. However, all-electric aircraft typically have very large battery fractions, especially at longer ranges. They are also more weight-sensitive than a conventional gas-powered vehicle [8]. Use of this technology for large-scale energy storage introduces two key hazards - thermal runaway and stored energy uncertainty - that are discussed below.

Thermal runaway is where an internal short circuit cases a rapid and uncontrolled increase in battery temperature, which often results in off-gassing, fire, and/or a battery explosion. This effect can spread rapidly to adjacent cells if they are not physically isolated from each other, and can be caused by a number of factors; over-charging, over-heating, mechanical damage, and manufacturing defects are the most common [30]. While good design practice and operational controls have proven effective in mitigating the first three causes during normal operation, thermal runaways due to manufacturing defects have proven very difficult to reliably prevent. Manufacturing defects in the batteries were the caused of highly publicized thermal runaway events in the lithium batteries on the Boeing 787 [31]. This lead to the development and installation of battery containment systems on all aircraft of this type; these are solid structures than can contain the effects of a thermal runaway, but which add considerable weight to the batery system. While thermal runaway events continue to be reported, these containment systems work as designed so it is no longer considered a reportable safety incident [32]. While there are lithium batteries that have less susceptibility to thermal runaway they have lower specific energy [10]. Current regulations also require a demonstration of the effects of thermal runaway [33].

Figure 6 shows that this hazard applies equally to all vehicle groups, at all altitudes. In-flight fire or explosion is catastrophic whether or not the vehicle has the ability to glide or autorotate after the fact.

Table 4 enumerates the potential mitigations. The most effective current mitigation strategy for battery thermal runaway is the physical containment employed on the Boeing 787 [32]. This containment strategy adds significantly to the weight of the batteries. This reduces the effective specific energy, which is a critical metric for the feasibility of UAM vehicles. For some configuration, it may reduce performance to levels which are not commercially viable. This is especially true for any vertical lift configuration, which requires very high power for takeoff and landings.

For vehicles with wings, the possibility of storing batteries in the wings and combining containment structure with wing primary structure offers one method of more weight-efficiently isolating batteries from the passengers and the rest of the vehicle. More detailed design work is required to determine the benefits of this approach.

Advanced lightweight fire suppression technologies, improved electrical protection and monitoring, and/or improvements in manufacturing and inspection technology are all ways that this issue could be mitigated in
Figure 6: Battery thermal runaway presents a significant source of risk for any all-electric aircraft architecture utilizing lithium-polymer batteries.

Table 4: Mitigation strategies for battery thermal runaway

<table>
<thead>
<tr>
<th>Mitigation Description</th>
<th>Mitigation Reduces</th>
</tr>
</thead>
<tbody>
<tr>
<td>Battery containment and physical separation</td>
<td>Consequence</td>
</tr>
<tr>
<td>Advanced fire suppression</td>
<td>Consequence</td>
</tr>
<tr>
<td>Improved manufacturing, testing, and inspection</td>
<td>Probability</td>
</tr>
<tr>
<td>Improved electrical protection and monitoring</td>
<td>Probability</td>
</tr>
</tbody>
</table>

The certification challenge associated with the risk of battery thermal runaway is the tension between currently acceptable ways of meeting the requirements and the need to reduce battery weight as much as possible to make the vehicles practically viable. Technology beyond what has been certified to date may be required to overcome this challenge.

C. Battery Energy Uncertainty

The amount of useful energy in a LiPo battery depends not only on it’s state of charge (usually measured by cell voltage) but also strongly on it’s age, past charge/discharge cycles and handling, as well as the ambient temperature [34]. This means accurate state estimation of the battery energy cannot be done from a single measurement as it requires knowledge of the battery’s past history. This in turn makes it difficult to verify that reserve mission requirements requirements will be met [35]; there is no battery equivalent of dipping the tank to verify there is sufficient fuel on board. The hazard assessment associated with running out of energy is shown in Figure 7. The reason this is a lower probability hazard for fixed-wing aircraft is due to the fact that inadvertently exceeding reserve requirements is very unlikely occur on takeoff, where it would be most consequential. For Multirotor, DEP Powered Lift, and Rotorcraft configurations this hazard is more likely since some of the highest-power conditions come at the end of the mission during approach and landing. The ability of Rotorcraft to autorotate throughout the landing profile reduces the consequences for that configuration, and the ability to of the DEP Powered Lift vehicle to glide reduces the consequence at high altitude.

There are several ways this hazard can be mitigated, shown in Table 5. The most efficient way to do this would be improved battery monitoring or state estimation technologies. This may need to include entire life cycle monitoring of the batteries used, which would then require the development of the regulatory framework to certify those processes. Redundant or dedicated backup systems could be used, possibly with
more stringent requirements on battery replacement. For example, a single-use emergency battery could be installed as a reserve system, which is replaced after every use. This would increase vehicle cost and potentially weight.

Table 5: Mitigation strategies for battery energy uncertainty

<table>
<thead>
<tr>
<th>Mitigation Description</th>
<th>Mitigation Reduces</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improved battery monitoring and state estimation</td>
<td>Probability</td>
</tr>
<tr>
<td>Redundant Systems</td>
<td>Consequence</td>
</tr>
<tr>
<td>Overdesigned batteries</td>
<td>Probability</td>
</tr>
<tr>
<td>BRS (Aircraft Parachute)</td>
<td>Consequence</td>
</tr>
</tbody>
</table>

The vehicles could be designed for the worst-case allowable battery state, operating at the worst allowable temperature. Since capacity degrades significantly with temperature and age in LiPos, this could result in assured ranges as low as 30-50% of the best-case scenario for a given battery weight [34]. This would in effect reduce battery specific energy, which again reduces vehicle performance. A ballistic recovery system could also mitigate this hazard at high altitudes.

The operational challenge thus arises from the difficulty, with current technology, of definitively knowing how much energy is available at the time of launch. Meeting current reserve mission assurance requirements may require either full life-cycle monitoring of batteries and the development of associated regulations, new state estimation technology, or over-designed battery systems, which negatively impacts vehicle performance.

Hybrid Electric Architectures  The use of lithium-polymer batteries (or batteries in general) is not a requirement for an electric aircraft. Hybrid-electric configurations enable the development of vehicles which take advantage of some of the benefits of distributed electric propulsion while eliminating some of the issues associated with the use of batteries. Although less attractive from a cost, noise, or emissions perspective hybrid power systems are attractive options for near-term development of DEP Fixed Wing, DEP Powered Lift, or Multirotor configurations because they fit within the current regulatory environment and significantly improve vehicle range or payload performance. This reduces the performance impact of the highly redundant systems required to prevent the common mode power system failures. Hybrid architectures reduce the certification risk of an electric aircraft since the acceptable safety targets and design criteria for reciprocating or turbine engines are currently very well established.
D. Fly-By-Wire System Failure

Any all-electric aircraft will require an electronic system for some type of primary flight control. These fall into two broad categories. The first are FADEC-like systems which translate pilot inputs to motor speeds. This could be a simple motor controller or a more complex system that balances thrust between multiple motors, enforces RPM limits at different altitudes, or adjusts maximum power based on motor temperature. The complexity of such a system depends on the specific vehicle power architecture; a DEP Fixed Wing would require a more complex power management system than a twin-engine Fixed Wing. For any configuration, failure of this system would be equivalent to a power system failure, with the same severity for different classes discussed in Section A.

The second category of electronic primary flight control systems is what is conventionally termed a fly-by-wire (FBW) or fly-by-light system. In this case, the system is used to translate pilot inputs into attitude control inputs around all three vehicle axes, as well as controlling the power level. These systems typically incorporate some sort of envelope protection or active stability augmentation. Active stabilization systems are required for any Multirotor or DEP Powered Lift configuration to convert pilot stick inputs into the correct motor differential thrust, and to stabilize the vehicles in vertical flight and in transitional phases. They are also required for Tilt-rotor vehicles, which are grouped into the Rotorcraft architecture class [36]. For Multirotor, DEP Powered Lift, or Tilt-rotor vehicles, failure of this system would result in a loss of vehicle attitude control, which would be catastrophic at any altitude. The severity assessment is shown in Figure 8. Fixed-Wing or Powered-Lift configurations are generally inherently stable and don’t require a fly-by-wire system. Therefore, this is not a hazard to which they must be exposed if they are controlled by conventional means. Some form of autopilot is common on aircraft of this type, but certified systems are available off-the-shelf, which can be overridden by a pilot at any point, and are not generally considered fly-by-wire systems. However, such a system could be installed in vehicles of this type, which could be desirable for envelope protection or improved stability and handling characteristics. In that case, the risk severity increases to the same level as any other FBW-equipped vehicle, and must be mitigated appropriately.

![Figure 8: Unmitigated risk associated with fly-by-wire system failure.](image)

The mitigations for this hazard are shown in Table 6. They are broadly similar to the mitigations for common mode power system failure, with the same limitations on the use of a BRS and coupling between flight profile and risk for a DEP Powered Lift configuration. It is likely that these vehicles would be controllable by a conventional, if complex, deterministic flight control system. The certification and design standards for flight-critical fly-by-wire systems are well developed for commercial jet transports or other Part 25 aircraft. While these systems are currently not common on Part 23 aircraft, they have been certified on business jets [37] and are approaching certification on the AW609 tilt-rotor.

The certification challenge for these vehicles associated with a fly-by-wire system arises from the cost, complexity, and possibly weight requirements of developing a highly redundant and reliable fly-by-wire system for very cost- and weight-sensitive aircraft. Due to the high consequence of the failure of the system, safety levels more in line with current Part 25 aircraft may be needed.
Table 6: Mitigation strategies for flight control system failures

<table>
<thead>
<tr>
<th>Mitigation Description</th>
<th>Mitigation Reduces</th>
</tr>
</thead>
<tbody>
<tr>
<td>System redundancy and design practice</td>
<td>Probability</td>
</tr>
<tr>
<td>BRS (Aircraft Parachute)</td>
<td>Consequence</td>
</tr>
</tbody>
</table>

E. High Level Autonomy Failure

Most proposals for UAM systems identify the need for pilotless operations as critical to the long-term viability and scalability of the concept [1]. The necessary level of autonomy to replace a pilot is not required to certify any configuration electric aircraft; its inclusion would likely complicate the certification process significantly. It is discussed here since it is a common consideration in the development of UAM vehicles.

To replace the pilot within the aircraft, sophisticated systems are required that must, among other things, be capable of sensing the surrounding environment, adapting to any degraded vehicle modes, and replanning the vehicle path. Most proposals for how to develop these systems depend on multiple difference sensor modalities feeding data into advanced machine learning algorithms [38]. There is an incredible amount of work being done in this field, but to date no complete pilot replacement system has been developed. While a detailed assessment of the hazards of this type of system or ways to mitigate them is not possible, it is clear that the failure of such a system would be equivalent to the loss of the pilot; thus, this is a high-severity risk regardless of vehicle configuration.

There are significant certification challenges associated with certifying this type of autonomous system. These challenges arise from the fact that the current development process for certifiable software, described in the DO-178C standard, mandates a verifiable path from high-level requirements to low-level code execution, testable for all expected states of the system. Applicability of this process to advanced automation is challenging due to the large number of possible system states and expected outcomes, the inherently stochastic nature of some of the algorithms, and complexity of and lack of transparency into the underlying processes. A comprehensive overview of the certification challenges associated with advanced autonomous systems is given in [39]. Developing the regulatory framework under which these algorithms will be certified is an area of significant ongoing work.

F. Bird Strike

This is currently an acceptable risk for most aircraft since, while it can be hazardous or in some cases catastrophic, it happens very infrequently. However, it may uniquely impact electric aircraft in two ways. The first is that the probability of occurrence may increase. According to the FAA, 95% of bird strikes take place below about 4500ft AGL, and more bird strikes happen at lower altitudes [40]. Most proposed UAM mission profiles operate in this region of high bird activity, which may lead to higher strike rates than for current aircraft.

The second is that since propulsors for DEP Powered Lift and Multirotor configurations are generally smaller, impacts could cause more damage. In some configuration, debris from one failed propulsor could impact adjacent ones. This could potentially lead to cascading failures, vibratory issues, and degraded flight control. The probability of this type of failure is highly dependent on the details of the vehicle configuration and propeller design; for the risk assessment here is is assumed that the strike on a single bird destroys one propeller. The risk of fratricidal propeller failure should be accounted for during the vehicle development process.

The severity of the bird strike hazard depends strongly on the number of birds impacted, flight speed, vehicle design, and a host of other factors. Bird strikes on flocks, while relatively rare [40], could be much more consequential than strikes on a single bird. The case of bird strike on the fuselage or cockpit, especially during high-speed flight at low altitude, should also be considered. Current standards mandate that cockpit windshields must survive bird strike up to the maximum flap deployment speed [41]; vehicles which cruise at high speed at low altitude may require additional strengthening. The severity rankings in Figure 9 show results for the impact of a single bird on both the propulsor and the cockpit. These rankings assume a bird
strike on a DEP vehicle destroys a single propulsor, while Fixed Wing and Rotorcraft vehicles meet part Part 35[42] and Part 27[43] bird strike survivability requirements, respectively.

![Diagram showing survivability requirements for different vehicle types.]

<table>
<thead>
<tr>
<th>Catastrophic</th>
<th>Hazardous</th>
<th>Major</th>
<th>Minor</th>
<th>Negligible</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>AllCockpit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AllProp</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M - Multirotor</td>
<td>D - DEP</td>
<td>R - Rotorcraft</td>
<td>F - Fixed Wing</td>
<td></td>
</tr>
<tr>
<td>Powered Lift</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Subscripts indicate bird strike on the Cockpit or on a Propulsor.

**Figure 9:** There is uncertainty around the likelihood of bird strikes on low-altitude, high-speed UAM vehicles that could increase the severity of this hazard.

Potential mitigations for the hazard of bird strikes are listed in Table 7. Suitable design standards on the windscreen, as well as on the rotors, has proven effective in current vehicles. Those or similar design standards could be applied to UAM aircraft. The issue of fratricidal rotor failure (whether caused by a bird strike or other debris) can also be mitigated by careful placement of rotors. Redundant motor systems reduce the consequence of a single bird strike. BRS systems would also be effective at high enough altitudes. It is not clear that there is a current certification challenge around bird strikes but there is uncertainty around how frequently they will occur. Frequent occurrence of bird strikes, especially when multiple birds are impacted simultaneously, would make this a more significant challenge. Frequent strikes with multiple bird impacts could be a difficult-to-mitigate cause of common mode power/flight control system failure.

**Table 7:** Mitigation strategies for bird strike

<table>
<thead>
<tr>
<th>Mitigation Description</th>
<th>Mitigation Reduces</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windscreen/Rotor Design Criteria</td>
<td>Consequence</td>
</tr>
<tr>
<td>Redundancy</td>
<td>Consequence</td>
</tr>
<tr>
<td>BRS (Aircraft Parachute)</td>
<td>Consequence</td>
</tr>
</tbody>
</table>

**V. Conclusion**

This analysis identified several key hazard areas for electric aircraft that represent challenging areas where vehicle certification may be a challenge. For all-electric aircraft using lithium-polymer batteries, the risk of thermal runaway due to manufacturing defects is difficult to mitigate without heavy battery containment systems. These are acceptable to regulators but add an unacceptable amount of weight to the vehicle. All-electric aircraft are highly weight sensitive due to the poor specific energy of batteries compared to conventional fuel. New technology is likely required to overcome this challenge, and is an area of substantial research and development. This hazard is significant across all vehicle configurations.

Another battery-related challenge is due to the uncertainty in the amount of useful energy contained in the battery at a given state of charge. For lithium-polymer batteries, this varies considerably with battery age, past discharge history, and ambient temperature. This makes it difficult to meet mandated reserve mission requirements without significantly over-designing the battery, which may add an unacceptable amount of weight.
The hazard of a common mode power system failure is challenging to mitigate outside current Ballistic Recovery System (BRS) operating envelopes for Multirotor or DEP Powered Lift configurations. Since this hazard is of higher consequence than for current Part 23 aircraft, the demonstrated probability of failure will need to be correspondingly lower, possibly more in line with Part 25 requirements. The challenge arises from the impact the development of highly reliable and redundant system will have on the vehicle weight, complexity, and cost.

The challenge of certifying the Fly-By-Wire (FBW) systems on any vehicle equipped with one is similar to that associated with common mode power system failure. The associated risks and required levels of safety are the same, and effects on vehicle weight and cost could be similar. The need to demonstrate this type of system for unique aircraft that may have a large number of different failure modes may also add significant risk and time to the certification process. While they are a requirement only for Multirotor, DEP Powered Lift, and Tilt-rotor vehicles the same challenges would arise if installed on a Fixed Wing, Helicopter, or Static Hybrid.

The hazard of bird strikes, whether to the propulsors or cockpit, may be different for electric aircraft and UAM vehicles in particular because much more of the flight is expected to take place at low altitudes where birds are prevalent and because rotors may be significantly smaller. This, combined with flight at relatively high speeds, may cause the probability or consequence of bird strikes to increase.

While not a requirement for any one type of vehicle, the certification of advanced autonomy also presents a very significant set of challenges. The significance of this is tied to the need for these systems to create a viable UAM network. In assessing how these challenges impact the different vehicle configurations, it can be seen that autorotate or glide capability provides an additional level of safety, especially for operations at low altitude where current BRS systems are not effective. The extent to which low-altitude flight profile is coupled to risk, and how that might effect commercial operations, is an area requiring further research. Hybrid-electric configurations offer significant certification and performance advantages by removing the batteries. However, they have drawbacks in terms of complexity, noise, and vehicle emissions.

Acknowledgments

The authors would like to thank the FAA Joint University Program for Air Transportation Research, which funded this work under Grant # 16-G-011.

References


43 Federal Aviation Administration, “Advisory Circular AC 27-1B - Certification of Normal Category Rotorcraft,” 2014.