

# Reliability Assessment of Actuator Architectures for Unmanned Aircraft

Raghu Venkataraman\* and Peter Seiler†  
*University of Minnesota, Minneapolis, MN 55455, USA*

Márk Lukátsi‡ and Bálint Vanek§  
*Hungarian Academy of Sciences, Budapest, H-1111, Hungary*

Standards are currently being developed for civil unmanned aircraft to operate safely in the national airspace. A key requirement for aircraft certification is reliability assessment. Traditional reliability assessment methods make assumptions that are overly restrictive when applied to unmanned aircraft. This article presents a step-by-step reliability assessment method that is tailored for unmanned aircraft. In particular, this article investigates the effects of stuck actuator faults on the overall reliability. Several candidate actuator architectures, with different numbers of controllable surfaces, are compared to gain insight into the effect of actuator placement on reliability. It is assumed that a fault detection algorithm is available and affected by known rates of false alarms and missed detections. The overall reliability is shown to be dependent on several parameters, including hardware quality, fault detection performance, mission profile, flight envelope, and operating point.

## I. Introduction

The small Unmanned Aerial Vehicle/System (UAV/UAS) industry is undergoing a rapid transformation due to the emergence of several commercial applications, such as law enforcement, search and rescue, and precision agriculture [1]. The commercial UAV market is projected to surpass the military market in the coming years [2]. Despite these economic indicators, widespread commercial use of UAVs is still several years

---

\* Graduate Student, Department of Aerospace Engineering & Mechanics; venka085@umn.edu

† Assistant Professor, Department of Aerospace Engineering & Mechanics; seile017@umn.edu

‡ Researcher, Systems and Control Laboratory, Computer and Automation Research Institute; lukatsi@sztaki.hu

§ Senior Research Fellow, Systems and Control Laboratory, Computer and Automation Research Institute; vanek@sztaki.mta.hu



Fig. 1: Sentera Vireo [7] - an example small UAV.

away. A barrier for UAV commercialization is their (current) inability to safely and reliably access common airspace. This is due to a combination of regulatory and technical challenges. On the regulatory side, significant work is currently underway, both in the United States (US) and in the European Union (EU), to establish a long-term framework for the seamless integration of UAVs into their respective national airspaces [3–5]. Some researchers have proposed basing the certification requirements on the type and ownership of the property being overflown [6]. On the technical side, challenges such as sense and avoid capabilities, secure communication, human factors, and reliability need to be addressed.

To understand the challenges of integrating UAVs into the national airspace, consider the current safety standards set by the FAA for manned commercial aircraft. In order for a manned commercial aircraft to be certified, there should be no more than one catastrophic failure per billion hours of flight operation. Airframe manufacturers, such as Boeing, meet the  $10^{-9}$  failures-per-flight-hour standard by utilizing hardware redundancy in their designs [8, 9]. On the other hand, most civil UAVs have reliabilities that are orders of magnitude below the  $10^{-9}$  level [10]. As an example, consider the Sentera Vireo [7] pictured in figure 1. Most components on the Vireo are low-cost and low-reliability. Moreover, small UAVs, such as the Vireo, are single-string designs, implying that there are single points of failure that lead to catastrophic failure. Installing multiple copies of analogous components is not economical for small UAVs, since they have limited payload and stringent design constraints [11].

Alternatively, cross-functional hardware redundancy (components that perform two or more functions) offer a better approach for increasing UAV reliability. When dealing with small UAVs, any type of hardware redundancy must be used judiciously due to size, weight, and power constraints. This article demon-

strates that, given a limited design space, it is beneficial in some cases to replace traditional control surfaces with cross-functional ones. As an example, consider ailerons that are no longer constrained to deflect anti-symmetrically. Removing this constraint effectively turns ailerons into elevons. Elevons are cross-functional because they can provide both pitch and roll control authorities. In this article, the design space is limited by the maximum number of actuators installed on the aircraft.

Increasing the reliability of UAVs is just one side of the story: These increases need to be quantified in order to prove compliance with certification standards. The aerospace industry has traditionally relied on methods such as fault tree analysis and failure modes and effects analysis for reliability quantification [12, 13]. These traditional reliability analysis methods are used to prove compliance with the Federal Aviation Regulations (FAR). In particular, they model the effect of the fault as a binary process: a fault, if present, will lead to a catastrophic failure. As a consequence, they yield conservative results since there may be fault modes that degrade performance, but do not necessarily lead to catastrophic failure. This article proposes a reliability analysis method for unmanned aircraft, wherein faults are treated probabilistically. In doing so, credit is given to the fact that some fault modes can be tolerated with degraded performance, but do not necessarily lead to catastrophic failure.

Reliability quantification methods provide a critical feedback loop to the aircraft designer. The system-level reliability of a UAV can be decomposed into those of the individual subsystems using a fault tree. Information about the reliability contributions of individual subsystems can help aircraft designers make more intelligent design trade-offs. This article specifically considers the reliability contribution of the actuator subsystem. The actuator subsystem consists of the aerodynamic control surfaces and the servo motors that drive them. The phrase *actuator architecture* is used to describe the placement of control surfaces and how they are connected to the servo motors. The actuator architecture of an aircraft affects its flight envelope which, in turn, affects its system-level reliability. This article provides a reliability assessment framework, using which different UAV actuator architectures are compared in a case study. The candidate actuator architectures are different in the extent to which they exploit cross-functionality in the aerodynamic control surfaces. In addition to being an analysis tool, the framework can help understand aircraft design trade-offs.

The reliability assessment framework and the case-study were originally reported in [14], wherein the effects of two parameters (servo reliability and missed detection rate) were investigated. This article advances

the results of [14] in three main areas: (1) model fidelity, (2) mission profile, and (3) trim point of the aircraft. First, while a high fidelity aircraft model was used in [14], this article demonstrates that a lower fidelity model can equivalently be used in the analysis without significant differences in the reliability estimates. Second, in addition to the lawnmower mission profile presented in [14], this article demonstrates how the system-level reliability is related to the mission being flown. Third, this article demonstrates the effect of the operating/trim point on the system-level reliability. The second and third points effectively demonstrate that the reliability of a UAV is dependent on its operating conditions.

## II. Problem Formulation

### A. Overview

The reliability of an aircraft is typically quantified by the probability of catastrophic failure. For the work presented in this article, catastrophic failure is defined as loss of aircraft (LOA). Loss of aircraft results when the UAV is unable to safely reach a proper landing site due to irrecoverable loss of control (LOC). Catastrophic failures have several causes, such as actuator failure, sensor failure, structural damage, weather-related phenomena, etc. Since this article specifically considers the reliability of the actuator subsystem, actuator faults are the primary failure modes of interest. Actuators contain many moving parts and are amongst the least reliable components on a UAV. Since actuators are connected to aerodynamic control surfaces, actuator faults directly affect the flight dynamics of the UAV. Many small UAVs use hobby-grade servo motors, which have failure times on the order of thousands of hours. Actuator failures can lead to significant loss in controllability of the aircraft and, eventually, catastrophic failure. It is possible, in some cases, to adequately compensate for actuator failures by utilizing other actuators present on the aircraft.

Actuators found on UAVs can fail in several different modes, such as bias, stuck-at, hardover, floating surface, oscillatory, and increased deadband or stiction [15]. This article will only consider stuck actuator faults and analyze the impact on the system-level reliability. Servo reliability will be quantified by the *mean time between failures* (MTBF). The motor-propeller pair on a UAV can also be called an actuator, but is not considered in this article. It is assumed that, under a motor failure, the aircraft can glide to a safe landing site. The analysis method is presented as a generic step-by-step procedure in section III. This article also presents a case-study, wherein the proposed analysis method is applied on an example small UAV.

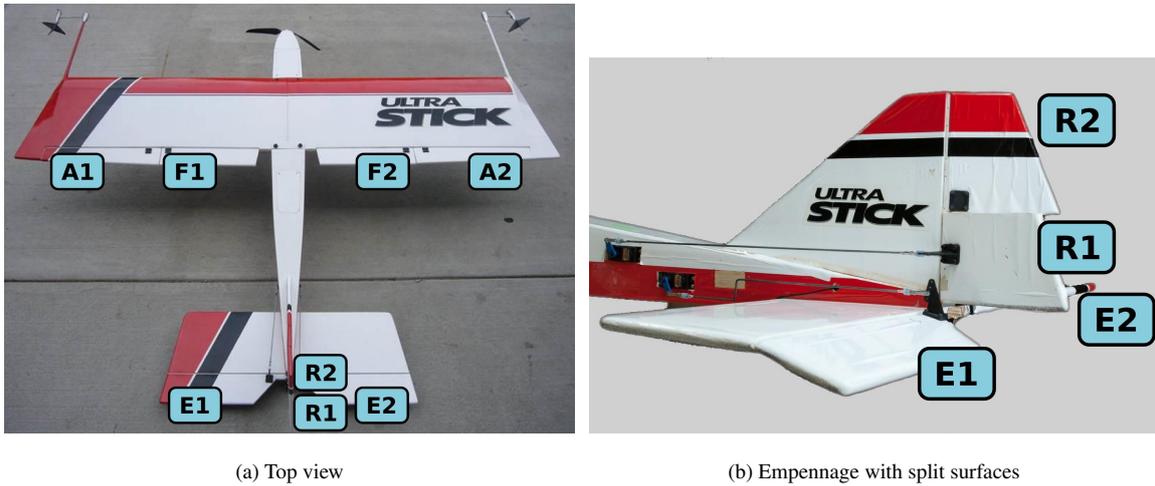


Fig. 2: Baldr with labeled control surfaces (A – aileron, F – flap, E – elevator, R – rudder).

### B. Airframe and Actuator Architecture

The case-study involves a small UAV, named Baldr, that is maintained and operated by UMN’s UAV Research Group. Baldr is based on the Ultra Stick 120 airframe, and is pictured in figures 2a and 2b. The Ultra Stick 120 [16] is a commercial, off-the-shelf, radio-controlled aircraft with a wingspan of 1.92m and a mass of about 8kg. The UMN UAV Research Group has retrofitted the airframe with custom avionics for enabling research in the areas of real-time control, guidance, navigation, and fault detection. The avionics include a sensor suite, a flight control computer, and a telemetry radio [17–19].

A high-fidelity simulation environment for the Ultra Stick 120 is publicly available [17]. This simulation environment was built using Matlab/Simulink and contains models for the aircraft subsystems. The rigid body dynamics are implemented using the standard six degrees-of-freedom, nonlinear aircraft equations of motion [20]. The aerodynamic stability and control derivatives were identified from wind tunnel experiments [21, 22]. The simulation models the forces and moments and the propwash generated by the electric motor and propeller pair. The simulation also includes actuator and sensor models. Environmental effects, such as wind gusts, atmospheric turbulence, and the Earth’s gravitational and magnetic fields are modeled using subsystems. The nonlinear aircraft model can be trimmed and linearized at any flight condition within the flight envelope of the aircraft. The simulation environment and the flight control computer allow for extensive software-in-the-loop and hardware-in-the-loop simulations. The entire simulation environment, details about the aircraft fleet, components, wiring, and data from numerous flight tests have been made open-access [17].

Additional details about the actuator subsystem are provided here. Baldr has a total of eight aerodynamic control surfaces, consisting of a pair each of flaps, ailerons, elevators, and rudders. Each of the eight surfaces is actuated by a dedicated servo motor. These surfaces are labeled in figures 2a and 2b as flaps ( $F_{1,2}$ ), ailerons ( $A_{1,2}$ ), elevators ( $E_{1,2}$ ), and rudders ( $R_{1,2}$ ). The sign convention of the control surfaces is as follows. A trailing edge down deflection of the elevators, ailerons, and flaps is considered positive. A trailing edge left deflection of the rudders, when viewed top-down with the aircraft nose pointing forward, is considered positive. In addition, all the surfaces have a deflection range of  $[-25^\circ, +25^\circ]$ .

The presence of eight aerodynamic control surfaces makes Baldr a highly over-actuated UAV. Such high levels of over-actuation make Baldr an effective test platform for reconfigurable flight control. On the other hand, most commercial fixed-wing small UAVs are equipped with either three or four control surfaces. In order to draw conclusions on the reliabilities of typical small UAVs, comparable actuator architectures need to be defined. This can be achieved by artificially constraining the actuators and control surfaces of Baldr, as desired. For example, Baldr has two elevators ( $E_{1,2}$ ) that are independently actuated. By constraining them to deflect together symmetrically, a configuration that more closely represents typical small UAVs can be obtained. In order to setup the case-study, five actuator architectures are defined in table 1. The first column lists the name of the configuration along with the minimum number of servos required to realize the same (given in parenthesis). For example, v1 (4) indicates that a minimum of four servos is required to realize configuration v1. The next four columns list the constraints placed on Baldr's ailerons, elevators, rudders, and flaps, respectively. For example, v1 has decoupled ailerons that can each deflect independently of the other, coupled elevators and coupled rudders that are constrained to deflect together symmetrically, and no flaps. The last column lists an acronym for each configuration denoting the constraints placed on the ailerons, elevators, rudder, and flaps, respectively. The symbols are: C=Coupled, D=Decoupled, and N=None.

It should be noted that configuration v0 is listed in table 1, but is not part of the case study. It is used exclusively for the flight envelope assessment, as explained in section III of the article. The case-study specifically compares configurations v1 to v4. In selecting these four configurations, the design space was restricted by limiting the total number of actuators to four. In terms of weight, four is a reasonable number of actuators on a small UAV. These four configurations were chosen because they are representative of the most common actuator architectures found in small UAVs. As an example, flaps are not very common

Table 1: Actuator architectures of Baldr: v0 (flight envelope assessment) and v1–v4 (case-study).

Config.	Ailerons	Elevators	Rudders	Flaps	Acronym
v0 (4)	Coupled	Coupled	Coupled	Coupled	CCCC
v1 (4)	Decoupled	Coupled	Coupled	None	DCCN
v2 (4)	Coupled	Decoupled	Coupled	None	CDCN
v3 (3)	Coupled	Coupled	Coupled	None	CCCN
v4 (3)	Decoupled	Coupled	None	None	DCNN

in small UAVs since they perform a very specific function and are not used for the majority of the flight duration. Consequently, configurations v1 to v4 do not have flaps. On the other hand, different combinations of pitch and roll control authorities are covered using elevators and ailerons. Table 1 indicates that the five configurations vary in the extent to which Baldr’s control surfaces are constrained. For example, v3 is the most constrained configuration since its ailerons, elevators, and rudders are each coupled. Although the configurations are representative of small UAV architectures, not all permutations and combinations of control surfaces are considered. The primary objective is to provide a methodology that may easily be repeated for other actuator architectures that are not considered in this article.

When all the actuators are healthy, a typical, nominal flight control law is used to actuate all the aerodynamic control surfaces. As will be shown in the subsequent sections, the nominal flight control law plays an important role in the analysis. Many commercial UAVs operate with a *classical* flight control law, wherein the throttle and the elevators are used purely for longitudinal control (pitch and airspeed), and the ailerons and the rudders are used purely for lateral-directional control (roll and yaw). These classical flight control laws are typically implemented on commercial, off-the-shelf autopilot systems such as the Procerus Kestrel or the 3DR Pixhawk. To maintain compliance with the state-of-practice and to simplify the analysis, it is assumed that the same classical nominal flight control law is used uniformly across configurations v1 to v4 listed in table 1. This nominal flight control law is implemented even if the ailerons and/or elevators are decoupled. In other words, the controller is designed to operate the ailerons anti-symmetrically, the elevators and rudders symmetrically, and hold the flaps at their zero positions. Comparing this description with table 1, it is seen that the nominal flight control law is designed specifically for configuration v3. However, all other

configurations can be reduced to  $v_3$  by placing restrictions on the control law. In essence, when there are no actuator faults, there is effectively only one closed-loop configuration. However, after the occurrence of an actuator fault, the flight control law is reconfigured to take advantage of any decoupled surfaces. An alternative approach would be to design individual flight control laws for each configuration, but this has a disadvantage. Specifically, since flight control laws can be designed in several different ways, it would be difficult to compare the four different configurations unless a common baseline was set.

### III. Reliability Analysis Method

The reliability analysis method is a generic step-by-step procedure that yields the probability of catastrophic failure of a given airframe and actuator architecture. Several assumptions are made to make the analysis tractable. First, it is assumed that a fault detection and isolation (FDI) algorithm is available to detect actuator faults. The FDI algorithm could either be built-in tests (self-diagnostics within actuators) or centralized monitoring systems. There is prior literature documenting the application of such FDI algorithms to UAVs [23, 24]. For simplicity, only statistical properties, such as missed detection and false alarm rates, are considered. In this article, these statistical properties are borrowed from [25]. Second, it is assumed that if the aircraft is trimmable after a fault has occurred then an appropriate reconfigurable control law is available. In other words, transitions between trim points are without loss of control. It may be argued that the existence of a trim point after a fault has occurred is not sufficient in order to fly to a safe landing spot. However, this assumption is a good starting point for the analysis presented. Third, it is assumed that multiple faults occur with negligible probabilities. Hence, the reliability assessment conducted in this article only considers single actuator faults. Multiple actuator faults can be considered, at the expense of a more complicated analysis [26]. Finally, this article only considers the undesirable consequences of LOA and not those of loss of mission (LOM), wherein the mission is aborted, but the aircraft is able to land safely. LOM would need to be penalized in order to ensure that false alarms are not frequently declared by the FDI algorithm. This is not investigated in this article since it is assumed that the FDI algorithm has been properly designed.

First, it is useful to consider a bird's-eye view of the entire analysis method. The fault tree pictured in figure 3 provides such a top-down perspective. The head of the fault tree is the final quantity of interest, i.e. the probability of catastrophic failure  $P_{SYS}$ . There are three levels below the head of the tree, each of

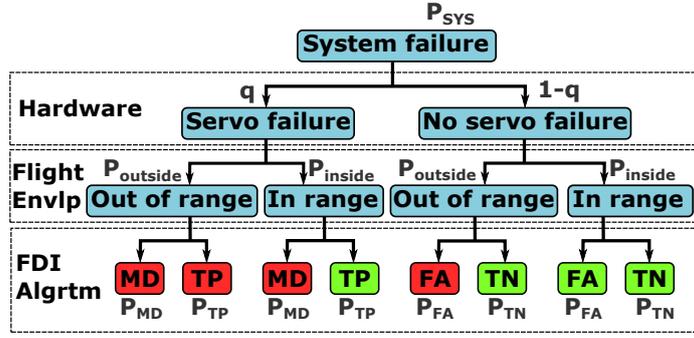


Fig. 3: Fault tree based on a multi-state reliability model (MD – missed detection, TP – true positive, FA – false alarm, TN – true negative).

which essentially describes a different type of contribution to the probability of catastrophic failure. Each of these three levels is enclosed by a dashed box and is labeled by the type of contribution made: hardware faults, flight envelope constraints, and FDI algorithm performance. The first contributor is hardware faults, of which servo failures are considered in this article. This level describes two servo failure events, in terms of the servo failure rate ( $q$ ) and its complement ( $1 - q$ ). The component-level reliability of many aircraft servos are reported by the manufacturers using the metric of mean time between failures (MTBF). Consequently,  $q$  is set equal to  $1/\text{MTBF}$ . Moreover, it is assumed that all the servos on the aircraft have the same MTBF level. Traditional aircraft reliability analyses stop at this level and conclude that any servo failure leads to catastrophic failure, in the absence of traditional hardware redundancy. In other words, the fault tree is described by only two states:  $q$  and  $(1 - q)$  and yields conservative results.

The next level of the tree removes this conservatism by including the contributions made by the flight envelope of the aircraft. This level gives credit to the fact that some servo failures are tolerable as long as they are within the flight envelope of the aircraft.  $P_{outside}$  is the probability of a servo failing outside the flight envelope.  $P_{inside}$  is the probability of a servo failing inside the flight envelope. Finally, the bottommost level of the tree further reduces conservatism by including the contributions made by the FDI algorithm. Any FDI algorithm has four events: missed detection, true positive, false alarm, and true negative. In total, there are eight different events at the bottommost level of the tree. The two main differentiators between the traditional and the proposed reliability analysis method are the contributions made by the flight envelope and the FDI algorithm. Owing to the two extra levels, the fault tree pictured in figure 3 is a *multi-state reliability model*. The hardware, flight envelope, and FDI algorithm levels each have two states, totaling to

eight states. The remainder of this section gives the details of the analysis method, decomposed into three steps: (1) determining the distribution of control surfaces, (2) flight envelope assessment, and (3) estimating the probability of catastrophic failure.

#### A. Distribution of Control Surfaces

The first step in the analysis is determining the probability distributions (histograms) of the control surfaces. These are influenced by several factors, such as mission profile, flight control law, and exogenous disturbances (sensor noise, wind gusts, and turbulence). In this section, particular attention will be given to the effect of the mission profile on the probability distributions. There are two methods to compute these histograms. The first is a direct numerical method wherein the histograms are computed from flight data or model-in-the-loop simulations. This method requires the entire mission profile to be simulated or actually flown by the UAV. This may not always be feasible since flying or simulating entire mission profiles can be resource-intensive. In addition, in the early design stages, a flight-ready UAV may be unavailable.

The second method is an indirect analytical method wherein the mission profile is decomposed into  $M$  modes. If the control surface distributions are known for these modes, the overall distributions can be constructed by combining them with appropriate weights, as shown in equation (1).

$$p_{\Delta_i}(\delta_i) = \sum_{j=1}^M p_{\Delta_i}(\delta_i | mode = j) P(mode = j) \quad (1)$$

Here,  $p_{\Delta_i}(\delta_i)$  is the probability density function (PDF) of the deflection of the  $i$ th control surface, denoted by the random variable  $\Delta_i$ , evaluated at a value of  $\delta_i$ . Further,  $p_{\Delta_i}(\delta_i | mode = j)$  is the conditional PDF of the  $i$ th control surface, conditioned on the event that the aircraft is flying in mode  $j$ . The weight  $P(mode = j)$  associated with each conditional PDF is the probability of occurrence of each mode for  $j = 1, 2, \dots, M$ . These probabilities are estimated from the mission profile by computing the fraction of time spent in each mode. Hence,  $p_{\Delta_i}(\delta_i)$  can be computed for each  $i = 1, 2, \dots, N$ , where  $N$  denotes the total number of control surfaces. In this analytical approach, only a small library of PDFs need to be stored in order to be able to generate PDFs for arbitrary missions.

A typical lawnmower pattern that is used for the aerial photography of farmland is shown in figure 4. When the entire mission is executed at constant altitude, it can be decomposed into three modes: straight and level flight, and left and right banked turns. Altitude changes can be captured by the additional modes

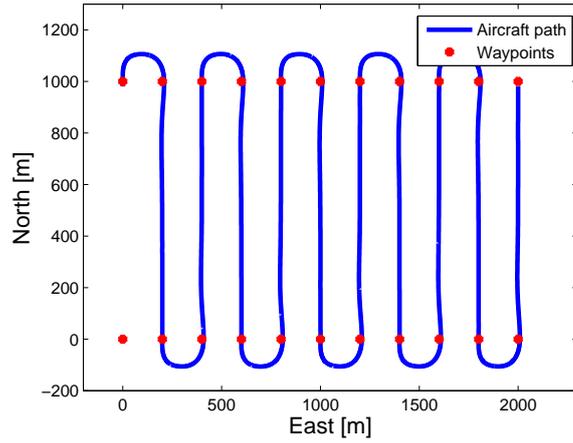


Fig. 4: Aircraft path during area scanning mission.

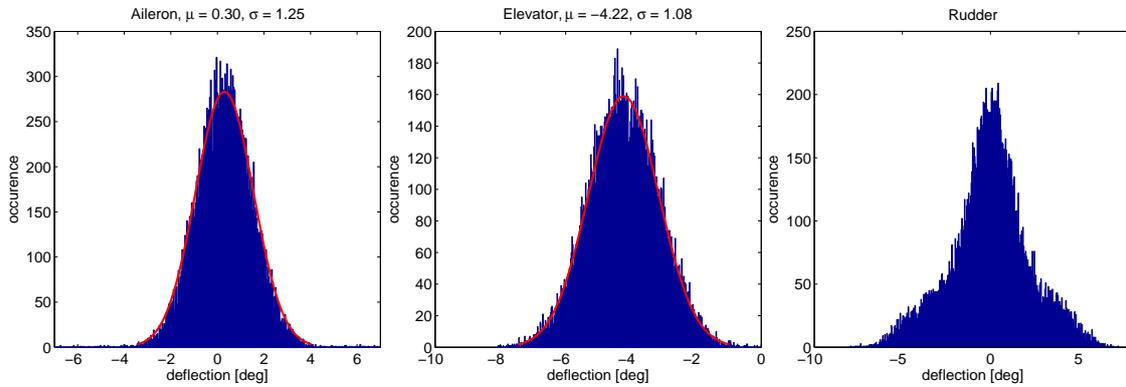


Fig. 5: Control surface distributions for straight and level flight. Number of bins is 400. Normal distributions are fitted to the aileron and elevator histograms.

of ascending and descending flight. In the direct method, the entire mission is simulated using the model of Baldr, with the baseline flight control law. In the indirect method, the three modes can be independently simulated for a short duration. Then, equation (1) can be applied to compute the PDF for the entire mission. The probabilities of the modes can be calculated from the geometry of the flight path shown in figure 4. The waypoints are 1000m and 200m apart in the North and East directions, respectively. Consequently, the probability of being in a banked turn is 0.26, and the probability of being in straight and level flight is 0.74. There is a nonzero difference between the direct and indirect methods: this is presented in the results section.

As an example, figure 5 shows the histograms of the deflections of the ailerons, elevator, and rudder, for the straight and level flight mode. The horizontal axis shows the deflection in degrees and the vertical

axis shows the occurrence. Similar distributions can be obtained for the left and right banked turns, but are not shown here. The analysis is capable of handling arbitrary histograms. However, for illustrative purposes, normal distributions are fitted to the histograms of the aileron and elevator deflections. As mentioned previously, before a fault occurs, the same nominal flight control law is used uniformly across all five configurations listed in table 1. Consequently, the histograms only depend on the mission being executed and not on the specific configuration. This assumption allows the reliabilities of the different configurations to be compared. Although only one mission profile is presented in this section, distributions for other mission profiles can be easily obtained using either the direct or the indirect method.

Other parameters affecting these distributions include sensor noise, atmospheric turbulence, and wind gusts. This highlights the fact that reliability should not be treated as a static quantity that depends only on aircraft parameters. The latter two parameters imply that aircraft reliability is a dynamic quantity that is dependent on and changes with the prevailing environmental conditions. While this article investigates the impact of mission profile on the overall reliability, similar studies can be conducted to investigate the impact of sensor noise and turbulence. Another major parameter affecting these distributions is the flight control law. As an example, the rudder will have different distributions depending on whether the control law is tuned for coordinated turns or yaw rate damping. More generally, the gains of the control law affect the probability distributions which, in turn, affect the overall reliability. By properly tuning the control law, the distributions can be tailored to meet performance and reliability requirements. This will be investigated in the future.

## B. Flight Envelope Assessment

The second step in the analysis is assessing the flight envelope of the aircraft. The aircraft equations of motion [27, 28] can be described in the nonlinear state-space form as shown in equations (2) and (3).

$$\dot{x} = f(x, u) \quad (2)$$

$$y = h(x, u) \quad (3)$$

In these equations,  $x \in \mathbb{R}^n$  is the state vector,  $u \in \mathbb{R}^m$  is the input vector, and  $y \in \mathbb{R}^p$  is the output vector.  $n$ ,  $m$ , and  $p$  are the number of states, inputs, and outputs, respectively. In addition,  $f : \mathbb{R}^n \times \mathbb{R}^m \rightarrow \mathbb{R}^n$  is the state function and  $h : \mathbb{R}^n \times \mathbb{R}^m \rightarrow \mathbb{R}^p$  is the output function. The state vector is:  $x = [\phi, \theta, \psi, p, q, r, u, v, w]^T$ . Here,  $\phi$ ,  $\theta$ , and  $\psi$  are the Euler angles of the aircraft. The aircraft's angular

velocity in the body-fixed frame are: roll rate ( $p$ ), pitch rate ( $q$ ), and yaw rate ( $r$ ). The airspeed components in the body-fixed axes are  $u$ ,  $v$ , and  $w$ . We also define a reduced order state vector that does not contain  $\psi$ :  $x_r = [\phi, \theta, p, q, r, u, v, w]^T$ .  $x_r$  is used in the definitions of the flight envelopes.

For configuration v0 (CCCC), there are only four unique aerodynamic control inputs. In addition, the throttle is  $\tau$ . Consequently, the control input vector is  $u = [\tau, E, R, A, F]$ . The input vector will change depending on the actuator configuration. The studies conducted in this article make use of certain elements in the output vector  $y$ . The airspeed, angle of attack, and angle of sideslip are denoted by  $V, \alpha$ , and  $\beta$ , respectively. The flight path climb angle and heading rate are denoted by  $\gamma$  and  $\dot{\psi}$ , respectively.

Aircraft typically fly around equilibrium or trim points. These are operating points at which some state derivatives are zero, and others have constant values. The collection of all such trim points defines the steady flight envelope  $\mathbb{F}$  of the aircraft. In this article, zero rate of change of  $x_r$  is the basis for defining the steady flight envelope, as shown in equation (4).

$$\mathbb{F} = \{(\bar{x}, \bar{u}) : \dot{\bar{x}}_r = 0, \dot{\bar{u}} = 0\}, \quad (4)$$

where  $(\bar{x}, \bar{u})$  denotes an equilibrium point. A subset of the flight envelope is straight and level flight, wherein the flight path angle is zero. This subset is mathematically described in equation (5).

$$\mathbb{F}_{straight,level} = \{(\bar{x}, \bar{u}) : f(\bar{x}, \bar{u}) = 0, \bar{p} = \bar{q} = \bar{r} = 0, \bar{\gamma} = 0, \dot{\bar{u}} = 0\} \quad (5)$$

When the aircraft descends steadily, at a constant flight path angle, the envelope is described by (6).

$$\mathbb{F}_{steady,descent} = \{(\bar{x}, \bar{u}) : f(\bar{x}, \bar{u}) = 0, \bar{p} = \bar{q} = \bar{r} = 0, \bar{\gamma} < 0, \dot{\bar{u}} = 0\} \quad (6)$$

Steady banked turns at constant altitude are defined by constant heading rate. For example,  $\dot{\psi} < 0$  describes left banked turns, as shown in equation (7).

$$\mathbb{F}_{banked,left} = \{(\bar{x}, \bar{u}) : \dot{\bar{x}}_r = 0, \dot{\psi} < 0, \bar{\gamma} = 0, \dot{\bar{u}} = 0\} \quad (7)$$

Similarly, right banked turns are defined using  $\dot{\psi} > 0$ . These subsets can be computed by applying numerical optimization techniques to the nonlinear aircraft model that was introduced in section II. The model can be trimmed using routines developed in-house, at any operating point within the flight envelope [17]. For straight and level flight at constant altitude, operating points are best expressed as pairs of  $(V, \alpha)$ .

A rectangular grid of such  $(V, \alpha)$  pairs is generated for  $V \in [10, 40] \text{m s}^{-1}$  and  $\alpha \in [0^\circ, 20^\circ]$ . The grid resolution is  $0.1 \text{m s}^{-1}$  and  $0.1^\circ$ . The nominal flight condition for Baldr is  $(V, \alpha) = (23 \text{m s}^{-1}, 4.72^\circ)$  and an altitude of 100m. The trim routine is called at each grid point after being initialized with the nominal flight condition. For a specific subset, the trim routine finds the minimum of a nonlinear, multi-variable cost function subject to the appropriate constraint (equations (5)–(7)). Matlab’s Optimization Toolbox contains the *fmincon* function that is well suited for this purpose. This optimization problem is non-convex and, in general, has multiple local minima. The *fmincon* function returns the minimum that is closest to the initial condition. A similar trim state discovery for another Ultra Stick 120 version was reported in [29]. The work presented in this article draws on the results therein and connects them to the probability of catastrophic failure in section III C. A more thorough treatment of aircraft flight envelopes can be found in [30–32].

The fidelity of the model plays an important role in the flight envelope assessment. High-fidelity estimates of the aerodynamic parameters of Baldr are available from extensive wind tunnel tests [21, 22]. Such wind tunnel tests are generally possible only for aircraft that have reached an advanced stage of design and build. However, small UAV designers may be interested in knowing the reliability of their aircraft in the early design stage, in order to make the right decisions. In the early design stage, it is common to have estimates of the linear aerodynamic stability and control derivatives. Hence, it is imperative that the proposed reliability assessment method work even when only low-fidelity aerodynamics are available. In order to demonstrate this, the high-fidelity aerodynamics of Baldr are downgraded to linear derivatives. Baldr’s nonlinear aerodynamics are implemented as lookup tables that are parameterized on the flight condition. A Taylor series expansion of these nonlinear functions result in stability and control derivatives. As an example, a Taylor series expansion of the coefficient of lift is shown in equation (8), where the trim values are denoted with an overline,  $\epsilon$  denotes the linearization error, and  $\delta_i$  denotes the deflection of the  $i$ th control surface.

$$C_L(\alpha, \beta, q, \delta_1, \dots, \delta_N) = C_L(\bar{\alpha}, \bar{\beta}, \bar{q}, \bar{\delta}_1, \dots, \bar{\delta}_N) + \left. \frac{\partial C_L}{\partial \alpha} \right|_{(\bar{x}, \bar{u})} (\alpha - \bar{\alpha}) + \left. \frac{\partial C_L}{\partial \beta} \right|_{(\bar{x}, \bar{u})} (\beta - \bar{\beta}) + \left. \frac{\partial C_L}{\partial q} \right|_{(\bar{x}, \bar{u})} (q - \bar{q}) + \sum_{i=1}^N \left. \frac{\partial C_L}{\partial \delta_i} \right|_{(\bar{x}, \bar{u})} (\delta_i - \bar{\delta}_i) + \epsilon \quad (8)$$

In order to match the high-fidelity flight envelopes, all aerodynamic parameters cannot be uniformly downgraded. The longitudinal dynamics of aircraft are strongly affected by the angle of attack. In particular, figure 6 shows the dependence of the coefficients of drag ( $C_D$ ), lift ( $C_L$ ), and pitching moment ( $C_m$ ) on

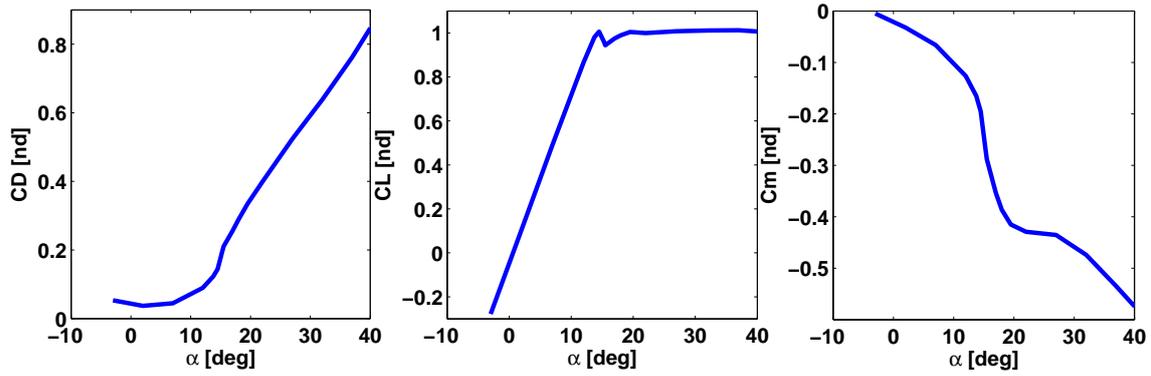


Fig. 6: Nonlinear dependence of  $C_D$ ,  $C_L$ , and  $C_m$  on  $\alpha$ .

$\alpha$ , for Baldr. In this figure, all other parameters are held constant at their respective trim values. All three coefficients are reported with respect to the reference point used during the wind tunnel tests. In the early design stage, potential flow-based computational tools are often used to estimate linear stability and control derivatives. Potential flow, by its very definition, does not account for viscous effects. However, it is the viscosity in the flow that leads to the separation of the boundary layer at high angles of attack. This boundary layer separation is the reason behind the nonlinear behavior that is seen at high angles of attack in the plots of  $C_L$  vs  $\alpha$  and  $C_m$  vs  $\alpha$ . The nonlinear behavior that is seen at low angles of attack in  $C_D$  vs  $\alpha$  is due to the addition of profile drag and induced drag [33].

However, it is possible to characterize the nonlinearities shown in figure 6 even without wind tunnel test data. The nonlinearity seen in the  $C_D$  vs  $\alpha$  plot can be replicated using the drag polar, which is typically a quadratic dependence of  $C_D$  on  $C_L$ . The nonlinearity seen in the  $C_L$  vs  $\alpha$  plot can be replicated with knowledge of the stall angle of attack and peak  $C_L$  of the aircraft. It is harder to estimate the nonlinearity in the  $C_m$  vs  $\alpha$  plot. However, a conceptual aircraft design typically includes the initial aerodynamic profile of the aircraft. Given an aerodynamic profile, there is prior work demonstrating the application of the principle of superposition to combine the results from potential and viscous flow theories for this very purpose [34, 35]. Based on the premise that the nonlinearities shown in figure 6 can be estimated in the early design stage, a *medium fidelity* aerodynamic model of Baldr is created. In this medium fidelity model, all aerodynamic dependencies are linear, except for  $C_D$ ,  $C_L$ ,  $C_m$  vs  $\alpha$ . The wind tunnel-based nonlinear dependencies are retained for these three coefficients in the medium fidelity model. Next, this medium fidelity model is validated against the high fidelity model by comparing the equilibrium/trim points of the two models.

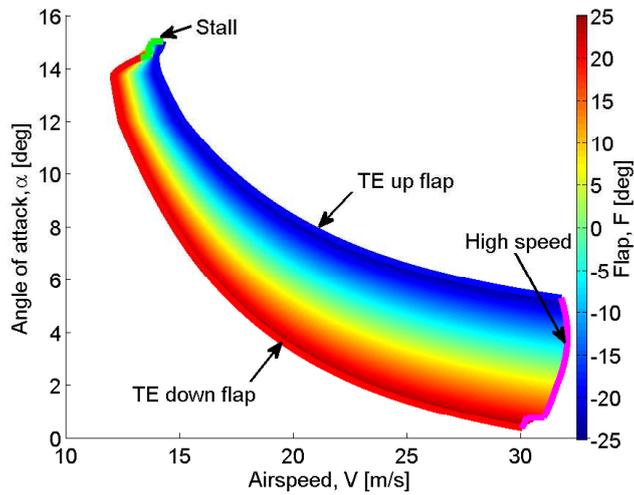


Fig. 7: Longitudinal flight envelope in the  $V - \alpha$  plane.

For illustrative purposes, a limited flight envelope assessment is presented for configuration v0 (CCCC). Note that similar assessments can be performed for the other configurations listed in table 1 as well, but are not shown in this article. The flight envelope of v0 is presented mainly to develop intuition for the problem. The envelope corresponding to longitudinal straight and level flight can be used to determine the stuck ranges for the elevator and flaps. This envelope is shown in the  $V - \alpha$  plane in figure 7. Every point inside this envelope is a trim point that is colored based on the value of the flap deflection. There are several interesting observations. First, as expected, there is an inverse relationship between  $V$  and  $\alpha$ . Second, since a nonlinear aircraft model is being trimmed, the inputs and outputs are implicitly constrained. As a result, the flight envelope has well-defined boundaries, as seen in figure 7.

The high speed boundary is a collection of trim points that are characterized by high airspeeds and low angles of attack. The high speed boundary is due to an upper limit on the thrust available. The trim point corresponding to the highest achievable airspeed occurs at a flap deflection of zero, since neutral flaps correspond to the minimum drag configuration. A trailing-edge down flap deflection, while further decreasing the angle of attack, will increase the total drag and, therefore, decrease the airspeed. At the stall boundary, the stall angle of attack ( $15^\circ$ ) is reached at low airspeeds. The stall boundary is due to a constraint on the output variable  $\alpha$ . The TE down/up flap boundary defines trim points for which flaps are deflected to  $\pm 25^\circ$  (trailing edge down/up). Note that within these boundaries, fixed flap deflections define isolines that follow the general shape of the envelope. Although this envelope is plotted for configuration v0, certain isolines

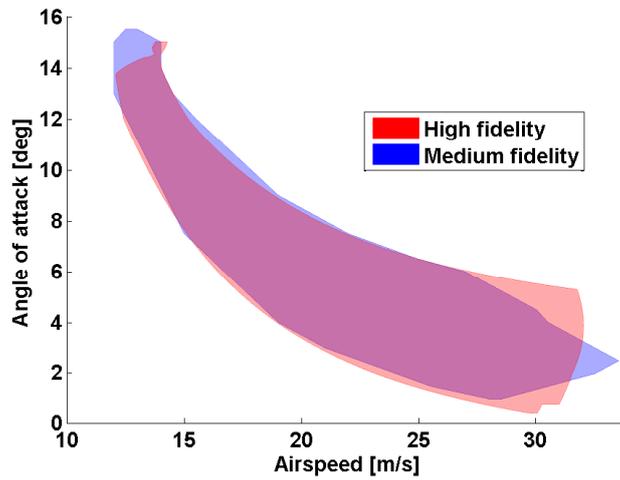


Fig. 8: Model validation using flight envelopes.

define the envelopes for other configurations. As an example, consider configuration v3 (CCCN), where no flaps are used. The flight envelope for this configuration would simply be the isoline for  $F = 0$  in figure 7.

Figure 8 shows the longitudinal flight envelope in the  $V - \alpha$  plane generated using the high and medium fidelity models, colored as red and blue patches, respectively. There is large overlap between the two models in the middle of the flight envelope. On the contrary, there is reduced overlap near the stall and high speed boundaries of the envelope. This reduced overlap is a natural consequence of model fidelity reduction. Specifically, the medium fidelity model does not capture certain regions near the high speed boundary. This is due to the inaccuracies of modeling drag at low angles of attack using the linear control derivative  $\frac{\partial C_D}{\partial \delta_i}$ . In addition, the medium fidelity model predicts the existence of trim points above the stall boundary predicted by the high fidelity model. This is due to the inaccuracies of modeling lift and pitching moment at high angles of attack using the linear control derivatives  $\frac{\partial C_L}{\partial \delta_i}$  and  $\frac{\partial C_m}{\partial \delta_i}$ . The match obtained between the two models in figure 8 is sufficient for the remainder of the analysis.

Figure 9 shows the flight envelope in the  $F - E$  plane with the trim points colored based on the value of  $\alpha$ . Three important conclusions can be drawn from this figure. First, it is seen that trim points exist for the entire range of flap deflections, as shown by the TE up/down flap boundaries. Second, there are no trim points for a positively deflected elevator. This implies that if the elevator was to get stuck positively, the result would be catastrophic. As an example, for configuration v3 (CCCN) ( $F = 0$ ), trim points exist for the elevator range  $[-25^\circ, -4^\circ]$ . Finally, for any given flap deflection, the high speed boundary is reached

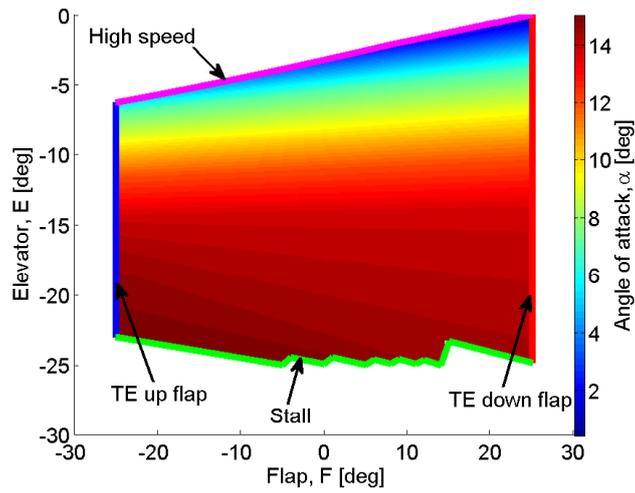


Fig. 9: Longitudinal flight envelope in the  $F - E$  plane.

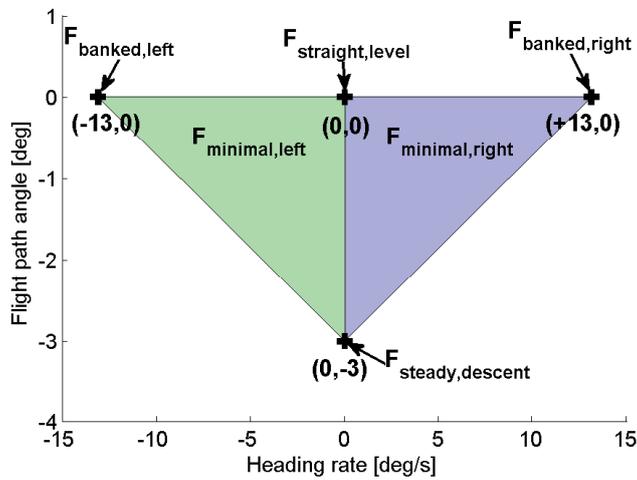


Fig. 10: Minimal flight envelope

when the elevator is deflected to its highest trimmable value. Conversely, the stall boundary is reached for the lowest trimmable value of the elevator.

Next, the flight envelope assessment is used to compute the allowable limits on the stuck control surface deflections. A stuck surface fault is called *allowable* if the aircraft can safely fly to a landing site in the presence of this fault. In order to safely fly to a landing site, the aircraft should be able to execute some limited maneuvers. The aircraft should be able to fly straight and level, execute either left or right banked turns with some minimum required turn rate  $\dot{\psi}$ , and descend steadily at some minimum required flight path angle  $\gamma$ . The minimum turn rate constraint corresponds to a maximum turn radius. These limited maneuvers form the minimal flight envelope in the  $\gamma - \dot{\psi}$  plane (figure 10). As long as the actual flight envelope, in the

presence of a stuck fault, is larger than this minimal flight envelope, the aircraft can safely fly home.

This research considers small UAVs that execute typical aerial photography missions. Referring back to the lawnmower pattern introduced in figure 4, it is seen that the turn radii encountered during such missions is on the order of 100m. In addition, in many practical applications, UAVs are required to stay within a geofence in order to ensure that they do not breach terrestrial property limits. The virtual boundaries defined by the geofence drive the performance requirements for the UAV. For this case-study, the maximum required turning radius is set as 87m. This is sufficiently larger than the minimum achievable turning radius of 54m, while still being under the typical mission radius of 100m. (Note that the specific value of 87m is not significant and is chosen purely for illustrative purposes.) At a nominal airspeed of  $V = 20\text{m s}^{-1}$ , an 87m turning radius corresponds to a heading rate of  $\pm 13^\circ/s$  and a bank angle of  $28^\circ$ . The minimum required flight path angle is assumed to be  $\gamma = -3^\circ$ , since this is representative of typical glide slopes. (Again, a different value of the glide slope may be used without any loss in generality.) The four points shown in figure 10 define two triangles:  $\mathbb{F}_{\text{minimal, left}}$  and  $\mathbb{F}_{\text{minimal, right}}$ . Furthermore, it is assumed that if trim points exist at the vertices of either of these two triangles, trim points exist in all of the corresponding triangle.

For any given stuck fault, in order to safely fly home, at least one trim point needs to be found in each of the subsets  $\mathbb{F}_{\text{straight, level}}$  and  $\mathbb{F}_{\text{steady, descent}}$ , and either of the subsets  $\mathbb{F}_{\text{banked, left}}$  and  $\mathbb{F}_{\text{banked, right}}$ . In other words, a stuck fault is called allowable if trim points can be found either in  $\mathbb{F}_{\text{minimal, left}}$  or  $\mathbb{F}_{\text{minimal, right}}$ . In checking for the existence of trim points, no explicit constraints (such as a zero sideslip angle requirement) are placed on  $V$ ,  $\alpha$ , and  $\beta$ . The following steps describe the calculation of the allowable stuck surface ranges. First, the trimmable range for each surface is calculated at each of the four points shown in figure 10. Then, the intersection of these trimmable ranges is calculated between  $\mathbb{F}_{\text{straight, level}}$ ,  $\mathbb{F}_{\text{steady, descent}}$ , and  $\mathbb{F}_{\text{banked, left}}$ . This intersection is called the trimmable range for  $\mathbb{F}_{\text{minimal, left}}$ . In a similar way,  $\mathbb{F}_{\text{minimal, right}}$  is calculated. The union of  $\mathbb{F}_{\text{minimal, left}}$  and  $\mathbb{F}_{\text{minimal, right}}$  is defined as the allowable stuck surface range.

The allowable stuck surface ranges for v1 to v4, generated using the medium fidelity model, are given in table 2. The coupling constraints imposed on each configuration are reflected in table 2. For example, v1 and v4 have decoupled ailerons that have a stuck surface range of  $\pm 25^\circ$ . This is because, the port and starboard ailerons can each deflect independently of the other and a failure in either aileron can be compensated by the

Table 2: Allowable stuck surface ranges in degrees (medium fidelity)

Config.	Aileron(s)	Elevator(s)	Rudder(s)
v1 (DCCN)	[-25,+25]	[-25,-1.5]	[-25,+25]
v2 (CDCN)	[-11,+11]	[-25,+16]	[-25,+25]
v3 (CCCN)	[-8,+8]	[-25,-4.1]	[-25,+25]
v4 (DCNN)	[-25,+25]	[-25,-1.5]	N/A

other. On the other hand, v2 and v3 have ailerons that are constrained to deflect anti-symmetrically, and have a much narrower stuck aileron range. v2 is the only configuration to have decoupled elevators. Since faults in either elevator can be compensated by the other, v2 has a broad stuck elevator range of  $[-25^\circ, +16^\circ]$ . On the other hand, v1, v3, and v4 have narrower stuck elevator ranges since all three of them have coupled elevators. Note that for all configurations that have a rudder, stuck faults in the full deflection range of  $\pm 25^\circ$  are allowable. This is because, rudder faults simply induce a non-zero sideslip velocity that is always within the allowable flight envelope.

There are small differences between the results listed in table 2 and those generated using the high fidelity model, reported in [14]. Specifically, the elevator ranges for v1 (DCCN) and v4 (DCNN) differ by  $0.5^\circ$ , v3 (CCCN) differs by  $0.1^\circ$ , and v2 (CDCN) differs by  $9^\circ$ . While the difference in v2 might appear excessive, it does not matter in the computation of the probability of catastrophic failure. This is because  $+16^\circ$  is sufficiently removed from the  $\pm 6\sigma$  bounds straddling the mean of the elevator deflection ( $-4.2^\circ$  in figure 5). Values outside the  $\pm 6\sigma$  bounds contribute negligibly to the overall reliability. The only other differences in the allowable stuck surface ranges are for the aileron deflections of v2 and v3, both of which have coupled ailerons. Specifically, the aileron ranges for v2 differs by  $1^\circ$  and v3 differs by  $2^\circ$ . Once again, since these limits are outside the  $\pm 6\sigma$  bounds, these differences do not contribute significantly to the overall reliability. This will be investigated in more detail in section IV.

### C. Probability of Catastrophic Failure

The third (and final) step in the analysis is the computation of the probability of catastrophic failure ( $P_{SYS}$ ). As explained previously, this step combines the results of sections III A and III B. It is useful to

once again refer to the fault tree pictured in figure 3. Considering the bottommost level of the fault tree, it is seen that there are eight different events. The false alarm and missed detection probabilities are given by  $P_{FA}$  and  $P_{MD}$ , respectively. The events that lead to catastrophic failure are colored red and those that do not are colored green. Consider, a servo that fails when the control surface is positioned outside its allowable range. In this scenario, there is at least one point in the minimal flight envelope (figure 10) where the aircraft cannot be trimmed. Consequently, this analysis predicts catastrophic failure, irrespective of the fault classification made by the FDI system (MD and TP are both colored red).

On the other hand, a servo that fails when the control surface is positioned inside its allowable range will lead to catastrophic failure only if the FDI algorithm has failed to detect this fault. Consequently, only the MD block is colored red, while the TP block is colored green. If no servos have failed, the FDI algorithm can have two outcomes: false alarm or true negative. If the control surface is positioned outside its allowable range and the FDI algorithm declares a false alarm, this event is assumed to lead to catastrophic failure (FA is colored red and TN is colored green). On the other hand, if the control surface is positioned inside its allowable range and no servo failures have occurred, neither FA nor TN have any negative consequences.

The probability of the  $i$ th surface being outside its allowable range is  $P_{out,i} = 1 - \int_l^u p_{\Delta_i}(\delta_i) d\delta_i$ , where  $l$  is the minimum value and  $u$  is the maximum value of the corresponding allowable range. The complement is  $P_{in,i} = 1 - P_{out,i}$ . The probability of the  $i$ th surface getting stuck outside the allowable range is  $qP_{out,i}$ .  $N$  denotes the total number of control surfaces. The total probability of catastrophic failure is given in (9).

$$P_{SYS} = \sum_{i=1}^N [qP_{out,i} + qP_{in,i}P_{MD} + (1 - q)P_{out,i}P_{FA}] \quad (9)$$

The first term in equation (9) results from the fact that both MD and TP result in catastrophic failure when a control surface gets stuck outside its allowable range. On the other hand, the second term in equation (9) shows that only MD results in catastrophic failure when a control surface gets stuck inside its allowable range. This is because the controller can be reconfigured if the fault is detected properly. The third term in equation (9) shows that false alarms lead to catastrophic failure, but only outside the allowable range. It is reasoned that upon declaring a false alarm, the power supply to the servo may be shutoff. If this causes the servo to get stuck, a catastrophic failure may result if the control surface is outside its allowable range.

The introduction to section III listed the assumptions made to make the reliability analysis tractable. One of the key assumptions was that multiple actuator faults occur with negligible probabilities. In order to

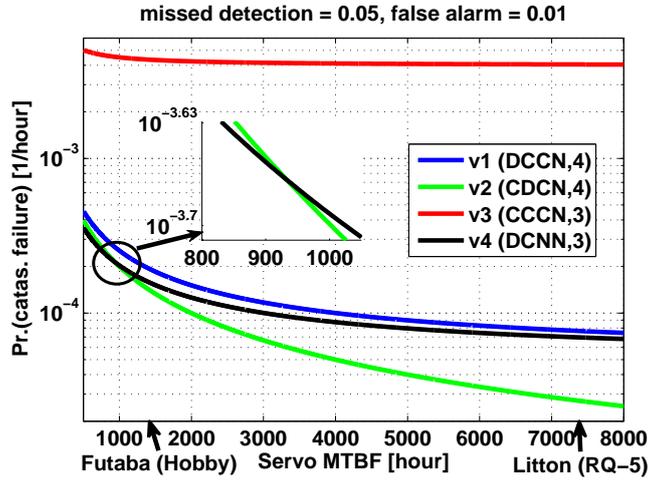


Fig. 11: Reliability vs. MTBF for lawnmower pattern.

motivate this assumption, consider the analysis method presented in [26]. The expression for the probability of catastrophic failure given in equation (9) is similar, in form, to equation (21) in [26]. The effect of all dual actuator failure modes is captured by the first term of equation (21) in [26]. This term can be ignored in the current article as long as  $q^2$  is several orders of magnitude smaller than  $P_{SYS}$ . The reliability analysis results presented in section IV demonstrate that this is indeed the case. The reliability analysis presented in [26] is more rigorous and considers the interactions between different failure modes. However, unlike this article, [26] does not consider the contributions made by the flight envelope.

#### IV. Reliability Analysis Results

##### A. Effects of MTBF and $P_{MD}$

The analysis method described in section III is applied to estimate the overall reliabilities of the actuator architectures listed in table 1. The overall reliability depends on several different parameters: MTBF,  $P_{FA}$ ,  $P_{MD}$ , mission profile, trim point, model fidelity, etc. In this section, the first set of results are presented by treating servo MTBF and  $P_{MD}$  as parameters. The entire lawnmower mission profile is simulated with the medium fidelity model at the nominal trim point.

Figure 11 shows the reliabilities as functions of the servo MTBF with fixed values of  $P_{MD}$  and  $P_{FA}$ . The servo MTBF axis spans the range from 500 hours to 8000 hours. A typical example on the low-reliability end is a Futaba hobby-grade servo [36]. A typical example on the high-reliability end is a Litton military-grade servo that is used on the RQ-5 Hunter UAV [37]. The values for the missed detection and false alarm

probabilities are taken from [25] and are set as  $P_{MD} = 0.05\text{h}^{-1}$  and  $P_{FA} = 0.01\text{h}^{-1}$ . Note that although reference [25] pertains to commercial passenger aircraft, it is a good starting point for this analysis. The analysis can be repeated for other parameter values, if needed. The probability of catastrophic failure for v3 is two orders of magnitude greater than that of the other architectures. This is because configuration v3 has no decoupled surfaces and has the least cross-functionality in reconfiguration among all the configurations. v1 is the second-to-worst architecture, despite having 4 servos. Compared to v3, v1 has an extra servo that decouples the ailerons and extends their allowable range to  $[-25^\circ, +25^\circ]$ . This greatly increases the reliability of v1 relative to v3.

However, v1 is uniformly less reliable than v2 and v4 over the displayed range of servo MTBF. Note that the only way in which v1 is different from v4 is the presence of a rudder. Despite the rudder, v1 (4 servos) is less reliable than v4 (3 servos). This demonstrates that increasing the number of servos does not necessarily increase the reliability. Whether the addition of a servo increases or decreases the overall reliability depends on the trade-off between the two main contributions to the terms in equation (9). First, in general, adding a control surface expands the allowable flight envelope of the aircraft. This expansion in the allowable flight envelope is reflected by an overall decrease in the terms containing  $P_{out,i}$ . Second, adding a control surface increases the overall probability of missed detections and false alarms, since additional fault modes are introduced. The addition of the rudder in v1 does not contribute to the flight envelope since the rudder is not cross-functional with any of the other control surfaces. However, the addition of the rudder in v1 is detrimental to its overall reliability because of the contribution of missed detections and false alarms in equation (9). The main takeaway from this observation is that although adding a control surface might be beneficial to the performance, it is not necessarily beneficial to the overall reliability. Specifically, the overall reliability will improve only if the benefits of cross-functionality are greater than the penalties of missed detections and false alarms, quantified as explained above.

Finally, the two most reliable configurations are v2 and v4. Excluding the rudder, both v2 and v4 use a three-servo architecture. While v2 has coupled ailerons and decoupled elevators, v4 has decoupled ailerons and coupled elevators. The presence/absence of the rudder in v2 and v4 is the reason for the total number of servos being different. However, table 2 indicates that rudder faults of any magnitude can be tolerated. Thus, the difference between v2 and v4 is primarily driven by the architecture of the elevators and ailerons. Figure

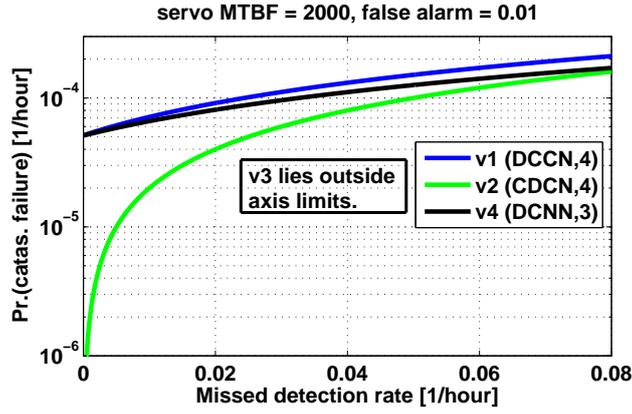


Fig. 12: Reliability vs. missed detection rate.

11 shows these two curves intersecting at  $MTBF \approx 930$  hours. For  $MTBF < 930$  hours, the probability of catastrophic failure is lower for v4. This indicates that for low quality servos, a configuration that decouples ailerons and couples elevators is more reliable. On the other hand, for  $MTBF > 930$  hours, the probability of catastrophic failure is lower for v2. This indicates that for high quality servos, a configuration that couples ailerons and decouples elevators is more reliable.

As mentioned previously, the effect of dual actuator failures can be ignored as long as  $q^2$  is several orders of magnitude smaller than  $P_{SYS}$ . Note that the maximum value of  $q$  is  $10^{-3}h^{-1}$  and corresponds to the minimum MTBF of 1000h. Hence, the maximum value of  $q^2$  is  $10^{-6}/h^2$ . Comparing  $10^{-6}/h^2$  to the range of values for  $P_{SYS}$  plotted in figure 11, it is seen the maximum value of  $q^2$  is two orders of magnitude smaller than the smallest value of  $P_{SYS}$ . Hence, it is justifiable to neglect the contributions of dual actuator failures in the current analysis.

Figure 12 shows the variation of  $P_{SYS}$  with  $P_{MD}$  for fixed values of MTBF and  $P_{FA}$ . As before, v3 is the least reliable, lies outside the axis limits, and is not shown in the figure. Also note that the only difference between v1 and v4 is the presence/absence of the rudder. Hence, in the limit  $P_{MD} \rightarrow 0$ , the penalty of missed detections generated by the rudder in v1 also tends to zero. Given that rudder faults of any magnitude can be tolerated (see table 2), the reliabilities of v1 and v4 converge as the missed detection rate approaches zero. From this observation, one can conclude that if a high performance FDI algorithm is available, a rudder can be added for better performance, without significantly impacting the overall reliability. However, as  $P_{MD}$  increases, the reliabilities of v1 and v4 start to diverge and the addition of the rudder introduces a greater

cost on the overall reliability. Over the entire range of  $P_{MD}$ , v2 uniformly does better than v1 and v4. The relative difference between the reliabilities of v2 and (v1,v4) increases as  $P_{MD}$  decreases, i.e. v2 is an order of magnitude more reliable than v1 and v4 for  $P_{MD} < 0.005\text{h}^{-1}$ . From this observation, one can conclude that if high performance FDI algorithms are available, configurations with coupled ailerons and decoupled elevators are more reliable than the other configurations considered in this article. As  $P_{MD} \rightarrow 0.08\text{h}^{-1}$ , the reliability curves of v2 and v4 intersect. This implies that for FDI algorithms that have high rates of missed detections, a configuration that has decoupled ailerons and coupled elevators (v4) eventually becomes more reliable than v2.

The general conclusions on the different configurations, drawn from figures 11 and 12, can be reasoned and validated using insights from flight dynamics. First, from both figures, it is seen that configuration v2 is the best performing except near the low end of servo MTBF and the high end of  $P_{MD}$ . These observations highlight the importance of decoupled elevators, since v2 is the only configuration featuring two independently actuated elevators. This makes sense from a flight dynamics perspective since the elevators have the most control authority, owing to their large moment arm relative to the center of gravity. While the high control authority of the elevators is useful when a different control surface gets stuck, it is disadvantageous when the elevator itself gets stuck. In particular, large deflections of other control surfaces are required to compensate for small stuck faults in the elevators. Therefore, by decoupling the elevators, two surfaces of comparable control authorities are introduced. Consequently, stuck elevator faults of larger magnitudes can be compensated for by the other elevator. This also shows up as a larger range of  $[-25^\circ, +16^\circ]$  for configuration v2 in table 2. In contrast, all the other configurations have coupled elevators and have smaller allowable stuck surface ranges. In general, elevators are important not only for performance, but also for reliability.

In addition, as servo MTBF decreases, the failure rate  $q$  increases (see equation (9)). For  $\text{MTBF} < 930$  hours, the terms contributed by the elevators to the probability of catastrophic failure exceed the terms contributed by the ailerons. Consequently, a configuration that has decoupled elevators (such as v2) becomes less reliable than a configuration that has decoupled ailerons (such as v4). A similar conclusion can be made as  $P_{MD}$  increases beyond  $0.08\text{h}^{-1}$ . For  $P_{MD} > 0.08\text{h}^{-1}$ , the terms contributed by the elevators to the probability of catastrophic failure exceed the terms contributed by the ailerons. Once again, v2 becomes less reliable than v4. The plots shown in figure 11 are functions of several variables such as: servo reliability,

actuator placement, surface coupling, mission, etc. In general, there is a complex interplay between these different variables [38]. All the candidate architectures considered in this case study are single-string designs. Thus, the cross-functionality of the surfaces is a major contributor to the overall reliability of the UAVs. Increasing the cross-functionality between surfaces can help increase the overall reliability with minimal increases in size and weight. In contrast to the analysis method presented in section III, traditional reliability analyses do not take credit for the cross-functionality between components.

While figures 11 and 12 correspond to the medium fidelity model, similar figures can be created for the high-fidelity model. For configurations v1, v3, and v4, the medium fidelity model results in a higher probability of catastrophic failure than the high fidelity model. This observation can be meaningfully related to the allowable stuck surface ranges listed in table 2 and their high-fidelity counterparts reported in [14]. From table 2, the upper limits of the allowable elevator deflection range for v1, v3, and v4, are  $-1.5^\circ$ ,  $-4.1^\circ$ , and  $-1.5^\circ$ , respectively. These limits are within the  $\pm 3\sigma$  bounds straddling the elevator mean of  $-4.2^\circ$ . Consequently, even a  $0.1^\circ$  difference has a noticeable effect on the overall reliabilities. For v2, the only configuration with split elevators, the reduction in fidelity has an insignificant effect. Despite the differences between the high and medium fidelity models, the qualitative trends are similar.

## **B. Effects of Aircraft Operations**

In section III A, the direct and indirect methods were discussed for computing the PDF of the control surface deflections. The differences between the two methods increase with servo MTBF and are seen only in configurations v1 (DCCN), v3 (CCCN), and v4 (DCNN). For an MTBF of 7800 hours, the differences for v1, v3, and v4 are 12.8%, 1.73%, and 12.6%, respectively. For v2 (CDCN), the only configuration with split elevators, the direct and indirect methods yield the same results. The indirect method results in lower probabilities of catastrophic failure than the direct method. This is because the indirect method does not account for the transients that arise when the aircraft transitions from one mode to another. Specifically, the ailerons are active during the transients that arise when the aircraft switches between straight and level and turning flight. The extra aileron deflections during mode transitions are not captured by the indirect method. Despite these differences, the indirect method can be used in lieu of the direct method without adversely affecting the overall trends. The effects of the transients will be investigated in the future.

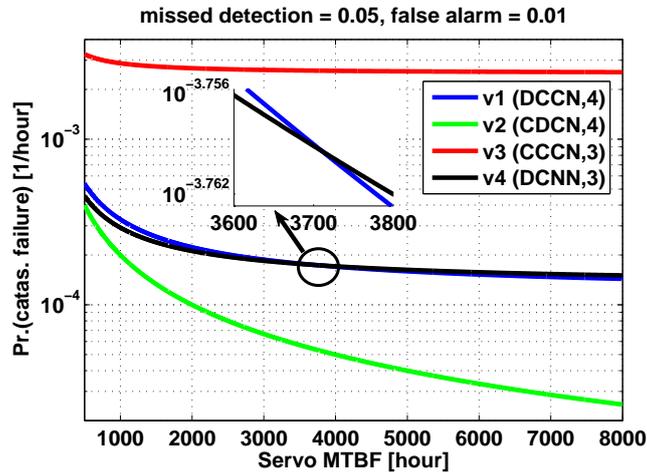


Fig. 13: Reliability vs. MTBF for spiral ascent/descent mission.

In this section, the effects of two aircraft operation parameters on the overall reliability are investigated. The first parameter of investigation is the mission profile. As an example, a spiral ascent/descent mission is considered as an alternative to the lawnmower pattern. Spiral ascents/descents, wherein the aircraft is in a climbing/descending turn, can be useful when altitude needs to be gained/lost while staying within specified property limits. For the first 175s of this example, the aircraft is made to climb at a mean airspeed of  $23\text{m s}^{-1}$ , a mean climb angle of  $3.33^\circ$ , and a mean turn rate of  $12.5^\circ\text{s}^{-1}$ . For the next 175s of this example, the aircraft is made to descend, at the same mean airspeed and turn rate as before, but with a mean climb angle of  $-3.33^\circ$ . Figure 13 shows the resulting overall reliabilities. As before, v3 is the least reliable configuration for all MTBF values. This is because, it is the most constrained configuration wherein all surfaces are coupled. Interestingly, it is seen that v1 and v4 are considerably less reliable as compared to the lawnmower pattern of figure 11. This is not surprising since v1 and v4 have coupled elevators and the spiral mission excites more of the elevator as compared to the lawnmower pattern.

The most reliable configuration, across all MTBF, is v2 since it is the only configuration with decoupled elevators. With the spiral ascent/descent commanding more of the elevator, configuration v2 has the best overall reliability. No intersection between v2 and v4 is seen, unlike figure 11. However, an intersection between v1 and v4 is seen at an  $\text{MTBF} \approx 3700\text{h}$ . As mentioned previously, the only way in which v1 is different than v4 is the presence of the rudder. While the rudder was detrimental to the overall reliability in figure 11, figure 13 suggests that the rudder may be beneficial if high reliability servos are available. Indeed,

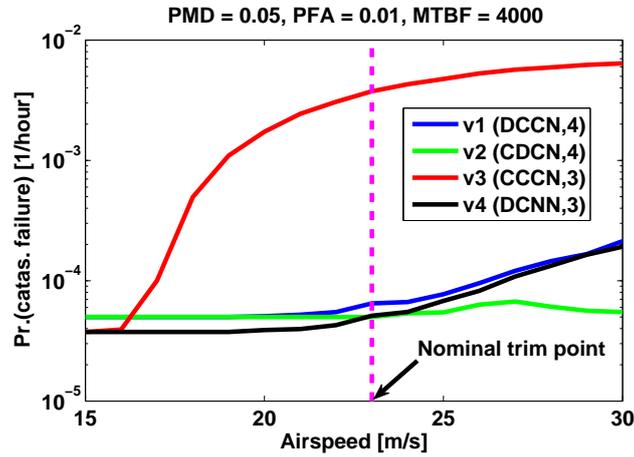


Fig. 14: Reliability vs trim point.

for servo MTBF  $> 3700\text{h}$ , v1 is more reliable than v4 since the rudder can help compensate for aileron faults by providing some rolling moment. This is another example of cross-functionality among the aerodynamic control surfaces. On the other hand, when low reliability servos are present, the additional rudder is more of a liability rather than an asset. Hence, for servo MTBF  $< 3700\text{h}$ , v4 is more reliable than v1. Figure 13 highlights the fact that different mission profiles can result in different trends in the overall reliabilities. In choosing an actuator configuration that results in the highest overall reliability, the aircraft designer must consider the specific mission for which the UAV is intended.

The second parameter that is investigated in this section is the trim point of the aircraft for straight and level flight. Section III B described how trim points for straight and level flight could be expressed as  $(V, \alpha)$  pairs. Moreover, figure 7 showed that when  $F = 0$ , the flight envelope reduced to the green isoline. Given that no configuration among v1 to v4 has flaps, the trim point is uniquely defined by specifying either  $V$  or  $\alpha$ . Figure 14 shows the variation of the overall reliability (on the vertical axis) against the trim airspeed (on the horizontal axis). The trim airspeed is sampled at  $1\text{m s}^{-1}$  increments. The airspeed  $V = 23\text{m s}^{-1}$  is marked with a dashed maroon line, and corresponds to the nominal trim point of Baldr. All the figures preceding figure 14 were plotted for this nominal trim airspeed.

Figure 14 leads to several interesting observations. First, the reliabilities of all four configurations increase with a decrease in the trim airspeed. For this to make sense, consider the allowable stuck elevator range column in table 2. The lower elevator limit corresponds to the highest achievable angle of attack and lowest achievable airspeed. Conversely, the upper elevator limit corresponds to the lowest achievable angle

of attack and highest achievable airspeed. For configurations v1 (DCCN), v3 (CCCN), and v4 (DCNN), the upper limit is much closer to the elevator mean of  $-4.2^\circ$  as compared to the lower limit. This asymmetry is the primary reason behind the first observation. As an example, consider v3, for which the upper elevator limit is  $-4.1^\circ$ . By operating at the nominal trim point  $(V, E) = (23\text{m s}^{-1}, -4.2^\circ)$ , nearly half of the elevator histogram lies outside the allowable range. This results in a high probability of catastrophic failure. However, a decrease in the trim airspeed results in a decrease in the trim elevator deflection. This “pulls” the mean of the histogram more into the center of the allowable stuck elevator range. This results in a smaller portion of the histogram to lie outside the allowable range, and results in a lower probability of catastrophic failure.

The second observation is that the reliabilities of some configurations are more sensitive to the trim airspeed than others. Configuration v3 is the most sensitive to the trim airspeed because v3 has the smallest stuck elevator range of  $[-25^\circ, -4.1^\circ]$ . Hence, the trim airspeed, and trim elevator deflection, have a large impact on the overall reliability. On the other hand, v2 (CDCN) is the least sensitive because v2 has the largest stuck elevator range of  $[-25^\circ, +16^\circ]$ . The sensitivities of v1 and v4 to trim airspeed are of the same order and are between those of v2 and v3. Moreover, the values of  $P_{SYS}$  for v1 and v4 start to converge with an increase in the trim airspeed. This is because, both v1 and v4 share exactly the same allowable stuck elevator range, as given in table 2. On the other hand, at low trim airspeeds,  $P_{SYS}$  for v1 and v2 converge. This once again shows that when the elevator is deflected sufficiently negatively, the reliability of v1 improves to the level of v2. The same nominal flight control law was used at all the trim airspeeds shown in figure 14. This is not optimal since this flight control law was designed specifically for the nominal trim airspeed. Future work will involve constructing a parameter-varying model of the aircraft and synthesizing gain-scheduled or parameter-varying flight control laws across the trim airspeeds.

## V. Conclusion

This article introduces a model-based framework for the reliability assessment of actuator architectures for unmanned aircraft. The proposed analysis method is described as a step-by-step process and is illustrated through a case-study involving several candidate actuator architectures. The actuator architectures differ in the number of actuators and aerodynamic control surfaces present. Traditional reliability analyses consider

servo reliability as the primary parameter affecting aircraft reliability. Moreover, this dependence is usually modeled by a binary fault tree. This article presents a fault tree that not only includes actuator fault modes, but also the constraints imposed by the aircraft's flight envelope and the performance of the fault detection algorithm. In addition, this article demonstrates the important parametric effects of aircraft operations. Specifically, it is seen that different mission profiles and trim points lead to different trends in the overall reliabilities of the various configurations. Hence, the most reliable actuator architecture is dependent not only on the reliabilities of the on-board components, but also on aircraft operations. In all of these parametric studies, the degree of cross-functionality present among the aircraft's aerodynamic control surfaces plays a crucial role in improving reliability. Cross-functional hardware redundancy provides a judicious way to improve UAV reliability. In order to apply the analysis method, it is sufficient to have a low-fidelity aircraft model. This makes the proposed analysis method particularly attractive for unmanned aircraft designers that want a reliability estimate in the early stages of design. Interesting avenues for future research include investigating the effects of the flight control law and weather conditions, such as atmospheric turbulence, on the probability of catastrophic failure.

#### **Acknowledgments**

The authors thank Gary Balas for inspiration in combining the distinct research topics of reliability and flight dynamics and control analysis. The authors also thank Bin Hu, Aditya Kotikalpudi, and Daniel Ossmann for feedback on the manuscript. The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007- 2013) under grant agreement no. FP7-AAT-2012-314544. This work was also supported by the National Science Foundation under Grant No. NSF/CNS-1329390 entitled "CPS: Breakthrough: Collaborative Research: Managing Uncertainty in the Design of Safety-Critical Aviation Systems".

#### **References**

- [1] Rester, M., Spruyt, P., Groeve, T. D., Damme, O. V., and Ali, A., "Unmanned Aerial Systems for Rapid Mapping," Tech. rep., JRC Scientific & Policy Reports, 2013.
- [2] Frost & Sullivan, "Study Analysing the Current Activities in the Field of UAV," *EC Enterprise and Industry*, 2011.

- [3] United States Congress, “House Resolution 658: FAA Modernization and Reform Act of 2012,” Section 332: Integration of Civil Unmanned Aircraft Systems into National Airspace System.
- [4] Federal Aviation Administration, “Notice of Proposed Rulemaking,” 2015.
- [5] European Commission, “A new era for aviation: Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner,” 2014.
- [6] Atkins, E. M., “Autonomy as an Enabler of Economically-Viable, Beyond-Line-of-Sight, Low-Altitude UAS Applications with Acceptable Risk,” *AUVSI North America Conference*, 2014.
- [7] Sentera, [www.sentera.com](http://www.sentera.com).
- [8] Yeh, Y. C., “Triple-triple redundant 777 primary flight computer,” *IEEE Aerospace Applications Conference*, 1996, pp. 293–307.
- [9] Yeh, Y. C., “Design Considerations in Boeing 777 fly-by-wire computers,” *3rd IEEE International High Assurance Systems Engineering Symposium*, 1998, pp. 64–72.
- [10] Amos, J., Bergquist, E., Cole, J., Phillips, J., Reimann, S., and Shuster, S., “UAV for Reliability,” [www.aem.umn.edu/~SeilerControl/SafetyCritical.shtml](http://www.aem.umn.edu/~SeilerControl/SafetyCritical.shtml), December 2013.
- [11] Spitzer, C. R., *The Avionics Handbook*, CRC Press, 2001.
- [12] Wu, B., *Reliability Analysis of Dynamic Systems: Efficient Probabilistic Methods and Aerospace Applications*, Elsevier, 2013.
- [13] Hamada, M., *Bayesian Reliability*, Springer New York, 2008.
- [14] Venkataraman, R., Lukátsi, M., Vanek, B., and Seiler, P., “Reliability Assessment of Actuator Architectures for Unmanned Aircraft,” *9th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes, SafeProcess*, 2015, pp. 398–403.
- [15] Freeman, P., *Reliability Assessment for Low-cost Unmanned Aerial Vehicles*, Ph.D. thesis, University of Minnesota, Twin Cities, 2014.
- [16] Murch, A. M., Paw, Y. C., Pandita, R., Li, Z., and Balas, G., “A Low Cost Small UAV Flight Research Facility,” *Advances in Aerospace Guidance, Navigation and Control*, edited by F. Holzapfel and S. Theil, Springer-Verlag Berlin Heidelberg, 2011, pp. 29–40.
- [17] University of Minnesota: UAV Research Group, [www.uav.aem.umn.edu](http://www.uav.aem.umn.edu).
- [18] Dorobantu, A., Johnson, W., Lie, F. A., Taylor, B., Murch, A., Paw, Y. C., Gebre-Egziabher, D., and Balas, G., “An Airborne Experimental Test Platform: From Theory to Flight,” *American Control Conference*, 2013, pp. 659–673.
- [19] Lie, F. A., Dorobantu, A., Taylor, B., Gebre-Egziabher, D., Seiler, P., and Balas, G., “An Airborne Experimental Test Platform: From Theory to Flight (Part 1),” *InsideGNSS*, 2014, pp. 44–58.
- [20] Stevens, B. L. and Lewis, F. L., *Aircraft Control and Simulation*, John Wiley & Sons, 1992.

- [21] Hoe, G., Owens, D., and Denham, C., "Forced Oscillation Wind Tunnel Testing for FASER Flight Research Aircraft," *AIAA Atmospheric Flight Mechanics Conference*, 2012.
- [22] Owens, D., Cox, D. E., and Morelli, E. A., "Development of a Low-Cost Sub-Scale Aircraft for Flight Research: The FASER Project," *25th AIAA Aerodynamic Measurement Technology and Ground Testing Conference*, 2006.
- [23] Freeman, P., Pandita, R., Srivastava, N., and Balas, G., "Model-Based and Data-Driven Fault Detection Performance for a Small UAV," *IEEE Transactions on Mechatronics*, Vol. 18, No. 4, 2013, pp. 1300–1309.
- [24] Pandita, R., Bokor, J., and Balas, G., "Closed-loop performance metrics for fault detection and isolation filter and controller interaction," *International Journal of Robust and Nonlinear Control*, Vol. 23, 2013, pp. 419–438.
- [25] Boeing Aerospace Company, "Built-in-test Verification Techniques," Tech. rep., 1987.
- [26] Hu, B. and Seiler, P., "Pivotal decomposition for reliability analysis of fault tolerant control systems on unmanned aerial vehicles," *Reliability Engineering & System Safety*, Vol. 140, 2015, pp. 130–141.
- [27] Nelson, R. C., *Flight Stability and Automatic Control*, McGraw-Hill, 1998.
- [28] Cook, M. V., *Flight Dynamics Principles*, Elsevier, 2nd ed., 2007.
- [29] Freeman, P. and Balas, G., "Actuation Failure Modes and Effects Analysis for a Small UAV," *American Control Conference*, 2014, pp. 1292 – 1297.
- [30] Urnes, J. M., Reichenbach, E. Y., and Smith, T. A., "Dynamic Flight Envelope Assessment and Prediction," *AIAA Guidance, Navigation, and Control Conference*, 2008.
- [31] Keller, J. D., McKillip, R. M., and Kim, S., "Aircraft Flight Envelope Determination using Upset Detection and Physical Modeling Methods," *AIAA Guidance, Navigation, and Control Conference*, 2009.
- [32] Wilborn, J. E. and Foster, J. V., "Defining Commercial Transport Loss-of-Control: A Quantitative Approach," *AIAA Atmospheric Flight Mechanics Conference*, 2004.
- [33] Anderson, J. D., *Introduction to Flight*, McGraw-Hill, 8th ed., 2015.
- [34] Kelly, H. R., "The Estimation of Normal Force and Pitching Moment Coefficients for Blunt-Based Bodies of Revolution at Large Angles of Attack," Tech. rep., U.S. Naval Ordnance Test Station, 1953.
- [35] Kelly, H. R., "The Estimation of Normal-Force, Drag, and Pitching-Moment Coefficients for Blunt-Based Bodies of Revolution at Large Angles of Attack," *Journal of the Aeronautical Sciences*, Vol. 21, No. 8, 1954, pp. 549–555.
- [36] Murtha, J. F., *An Evidence Theoretic Approach to Design of Reliable Low-Cost UAVs*, Master's thesis, Virginia Polytechnic Institute and State University, 2009.
- [37] Office of the Secretary of Defense, "Unmanned Aerial Vehicle Reliability Study," 2003.
- [38] Rice, J. W. and McCorkle, R. D., "Digital Flight Control Reliability - Effects of Redundancy Level, Architecture, and Redundancy Management Technique," *AIAA Guidance, Navigation, and Control Conference*, 1979.