Reliability Assessment of Actuator Architectures for Unmanned Aircraft

Raghu Venkataraman* and Peter Seiler†
University of Minnesota, Minneapolis, Minnesota 55455
and
Márk Lukátsi‡ and Bálint Vanek§
Hungarian Academy of Sciences, 1111 Budapest, Hungary

DOI: 10.2514/1.C033832

Governmental organizations are currently developing standards 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 paper presents a step-by-step, model-based, reliability assessment method that is tailored for unmanned aircraft. In particular, this paper investigates the effects of stuck actuator faults (a common failure mode in electromechanical actuators) 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. In addition to being an analysis tool, the method can help understand aircraft design tradeoffs.

I. Introduction

THE small unmanned aerial vehicle (UAV) 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 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 and in the European Union, 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 [7].

To understand the challenges of integrating UAVs into the national airspace, consider the current safety standards set by the Federal Aviation Administration 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 using traditional hardware redundancy (multiple analogous components) in their designs [8,9]. On the other hand, most civil UAVs have reliabilities that are orders of magnitude worse than the 10^{-9} level [10]. As an example, consider the Sentera Vireo ¶ pictured in Fig. 1. Most components on the Vireo are low-cost and low-reliability.

Traditional hardware redundancy is not economical for small UAVs because they have stringent size, weight, and power (SWAP) constraints [11]. Alternatively, cross-functional hardware redundancy (components that perform two or more functions) is a judicious solution. As an example, consider ailerons that are no longer constrained to deflect antisymmetrically. Removing this constraint effectively turns ailerons into elevons. Elevons are cross-functional because they can provide both pitch and roll control authorities. Thus, given a limited design space, it is beneficial in some cases to replace traditional control surfaces with cross-functional ones.

Increasing the reliability of UAVs is just one side of the story; these increases need to be quantified to prove compliance with certification standards. The aerospace industry has traditionally relied on methods such as fault tree analysis as well as 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, European Aviation Safety Agency Regulations, etc. 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 because there may be fault modes that degrade performance but do not necessarily lead to catastrophic failure. This paper proposes a model-based reliability analysis method for unmanned aircraft, wherein actuator 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 tradeoffs. This research specifically considers the reliability contribution of the actuator subsystem, consisting of the aerodynamic control surfaces and the servomotors that drive them. Of the plethora of fault modes that affect servomotors, the stuck fault (one of the most common failure modes) is considered for

Received 15 December 2015; revision received 15 July 2016; accepted for publication 28 August 2016; published online 3 November 2016.

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

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

‡Researcher, Systems and Control Laboratory, Computer and Automation Research Institute; lukatsi88@gmail.com.

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

¶More information available online at www.sentera.com [retrieved 14 October 2016].

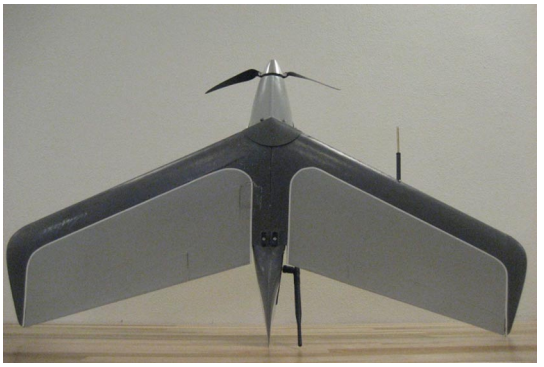


Fig. 1 The Sentera Vireo is an example small UAV.

illustrative purposes. The phrase actuator architecture is used to describe the placement of control surfaces and how they are connected to the servomotors. The actuator architecture of an aircraft affects its flight envelope, which, in turn, affects its system-level reliability. Using the proposed reliability analysis method, different UAV actuator architectures are compared in a case study. The candidate architectures are different in the extent to which they exploit cross-functionality in the aerodynamic control surfaces. To comply with the aforementioned SWAP constraints, this paper places an upper limit on the number of actuators.

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 paper advances the results of [14] in three main areas: 1) model fidelity, 2) mission profile, and 3) trim point of the aircraft. First, although a high-fidelity aircraft model was used in [14], this paper 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 (for geographical surveying) presented in [14], this paper demonstrates how the system-level reliability is related to the mission being flown. Third, this paper demonstrates the effect of the operating/trim point on the system-level reliability. The second and third points demonstrate that the reliability of a UAV is dependent not only on its hardware quality but also on its operating conditions. The new ideas presented in this paper, although demonstrated using the actuator subsystem, have broader applicability to aircraft reliability assessment.

II. Problem Formulation

A. Overview

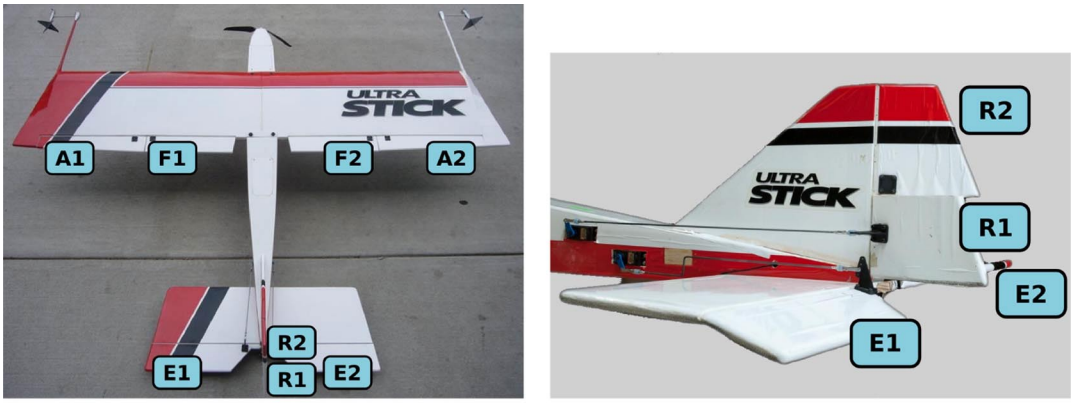
The reliability of an aircraft is typically quantified by the probability of catastrophic failure. For the work presented in this paper, catastrophic failure is defined as loss of aircraft (LOA). LOA results when the UAV is unable to reach a safe landing site due to irrecoverable loss of control. In this paper, a safe landing site is any site designated before takeoff where conditions allow for an aircraft to land without additional damage. Catastrophic failures have several causes, such as actuator failure, sensor failure, structural damage, weather-related phenomena, etc. Because this paper specifically considers the reliability of the actuator subsystem, actuator faults are the primary failure modes of interest. Actuators contain many moving parts and are among the least reliable components on a UAV. Because actuators are connected to aerodynamic control surfaces, actuator faults directly affect the flight dynamics of the UAV. 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 using other actuators present on the aircraft.

Many small UAVs use hobby-grade servomotors, which have failure times on the order of thousands of hours [15]. These servos can fail in several different modes, such as bias, stuck, hard-over, floating surface, oscillatory, and increased deadband or stiction [16,17]. This paper will only focus on stuck actuator faults (including stuck at the physical actuator limit) and analyze their impact on the system-level reliability. In a stuck fault, the actuator gets jammed at the value it was commanded before the failure. That said, the goal of the paper is not to provide a comprehensive reliability assessment of all possible failure modes of the actuator subsystem. Rather, it is to provide a generic step-by-step procedure to conduct such a reliability assessment and demonstrate the same using the stuck actuator fault mode. The motor–propeller pair on a UAV can also be called an actuator but is not considered in this paper. It is assumed that, under a motor failure, the aircraft can glide to a safe landing site.

B. Airframe and Actuator Architecture

To complement the proposed reliability assessment method, this paper applies the same to a case study involving a small UAV, named Baldr, that is maintained and operated by the University of Minnesota's UAV Laboratories [18,19]. Baldr is based on the Ultra Stick 120 airframe and is pictured in Figs. 2a and 2b. A high-fidelity simulation environment was built for the Ultra Stick 120 using Matlab/Simulink, with models for the various subsystems, such as the aircraft dynamics, actuators, sensors, environmental effects, etc. The rigid-body dynamics are implemented using the standard six-degree-of-freedom, nonlinear aircraft equations of motion [20]. The aerodynamic stability and control derivatives are identified from wind-tunnel experiments conducted by NASA [21]. The nonlinear aircraft model can be trimmed and linearized at any flight condition within the flight envelope.

Baldr has a total of eight aerodynamic control surfaces, labeled in Figs. 2a and 2b as flaps ($F_{1,2}$), ailerons ($A_{1,2}$), elevators ($E_{1,2}$), and rudders ($R_{1,2}$). Each surface is independently actuated with the following sign convention: 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 $[-25, +25$ deg].



a) Top view **b) Empennage with split surfaces**

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

Table 1 Actuator architectures of Baldr: number of servos and control surface coupling

Configuration (minimum number of servos)	Ailerons	Elevators	Rudders	Flaps	Acronym
0 (4)	Coupled	Coupled	Coupled	Coupled	CCCC
1 (4)	Decoupled	Coupled	Coupled	None	DCCN
2 (4)	Coupled	Decoupled	Coupled	None	CDCN
3 (3)	Coupled	Coupled	Coupled	None	CCCN
4 (3)	Decoupled	Coupled	None	None	DCNN

The presence of eight aerodynamic control surfaces makes Baldr a highly overactuated UAV. On the other hand, most commercial fixed-wing small UAVs are equipped with four or less control surfaces. To draw conclusions on the reliabilities of typical small UAVs, comparable actuator architectures need to be defined. This is achieved by artificially constraining the actuators and control surfaces of Baldr, as desired. To set up 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 (given in parentheses). The next four columns list the constraints placed on Baldr's ailerons, elevators, rudders, and flaps, respectively. The last column lists an acronym, where "C" is coupled, "D" is decoupled, and "N" is none.

Configuration 0 is used exclusively for flight envelope assessment and is not part of the case study, which compares configurations 1–4. In selecting these four configurations, the design space is 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 are chosen because they are representative of the most common actuator architectures. As an example, flaps are not very common because they perform a very specific function and are not used for the majority of the flight duration. Consequently, configurations 1–4 do not have flaps. On the other hand, different combinations of pitch and roll authorities are covered by elevators and ailerons.

When all the actuators are healthy, a typical, nominal flight control law is employed. 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) [19]. 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 1–4. This nominal flight control law is designed to operate the ailerons antisymmetrically, to operate the elevators and rudders symmetrically, and to hold the flaps at their zero positions. In essence, when there are no actuator faults, there is effectively only one closed-loop configuration. An alternative approach would be to design individual flight control laws for each configuration. However, because flight control laws can be designed in several different ways, it would be difficult to compare the reliabilities without a common baseline.

III. Reliability Analysis Method

The reliability analysis method presented here 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) [22] or centralized monitoring systems [23]. For simplicity, only statistical properties, such as missed detection and false alarm rates, are considered. Second, it is assumed that if the aircraft is trimmable after a fault has occurred then an appropriate reconfigurable control law is available [24]. In other words, transitions between trim points are without loss of control. (A rigorous analysis of this problem requires reachability analysis [24] but is not the focus of this paper.)

Third, it is assumed that multiple faults occur with negligible probabilities. Hence, the reliability assessment conducted in this paper only considers single actuator faults. Fourth, it is assumed that the probability of an actuator getting stuck within a certain deflection range is proportional to the probability of the actuator being positioned within that range. Finally, this paper 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 to ensure that false alarms are not frequently declared by the FDI algorithm. However, this is not investigated in this paper because 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 depicted in Fig. 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 main levels below the head of the tree, each of which describes a different type of contribution to the probability of catastrophic failure. Each of these three levels is enclosed by a 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 stuck servo failures are considered in this paper. This level has two states: stuck servo failure with probability 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/MTBF. Moreover, it is assumed that all the servos on the aircraft have the same MTBF, which is time-invariant and independent of the servomotor usage and position.

The structure of the fault tree depicted in Fig. 3 is affected by the assumptions. For example, in the hardware level, the entire probability of servo failure q is attributed to the stuck mode. This excludes other failure modes, such as the hard-over, wherein an electronic failure causes the actuators to stick at their extreme values. Such hard-over failures can be included in the proposed analysis method by adding additional branches within the hardware level of the fault tree. Although the tree can be made as exhaustive as desired, the focus of this paper is on two new types of levels.

The next level considers the contributions made by the flight envelope of the aircraft. This gives credit to the fact that some servo failures are tolerable as long as the aircraft remains within its flight envelope after the fault. $P_{outside}$ is the probability of a servo being positioned outside the flight envelope. P_{inside} is the probability of a servo being positioned inside the flight envelope. The subsequent level of the tree considers the contributions made by the FDI algorithm. Any FDI algorithm has two pairs of states: missed detection and true positive for q, and false alarm and true negative for $1 - q$. The missed detection (MD) block under an in-range servo failure can be further resolved depending on the robustness of the nominal flight control law. These blocks are elaborated upon in Sec. III.C. The hardware, flight envelope, and FDI algorithm levels each have two states. Considering the further resolution of the MD

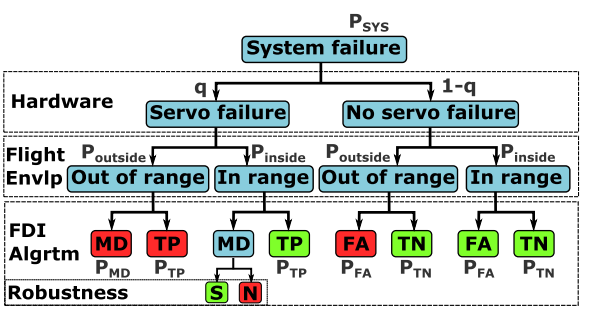


Fig. 3 Fault tree (MD: missed detection, TP: true positive, FA: false alarm, TN: true negative).

**More information available online at http://www.lockheedmartin.com/us/products/procerus/kestrel-autopilot.html [retrieved 14 October 2016].

block, there are a total of nine states, making the fault tree pictured in Fig. 3 a multistate reliability model.

The main distinction between traditional fault trees and the one depicted in Fig. 3 is the type of levels considered. Although traditional fault trees can also run several levels deep, they typically capture only hardware failures, human errors, and software errors [25]. Traditional fault trees, such as those that are applied to large aircraft, are nevertheless complex because of the exhaustiveness of the number and type of fault modes considered. Although this paper does not exhaustively consider all possible fault modes, it does introduce two new types of levels. In particular, the flight envelope and FDI algorithm levels are different because they are not quantified by the failure rate of any hardware component. Rather, the flight envelope layer is governed by the aircraft flight dynamics, and the FDI algorithm layer is governed by a tradeoff between false alarm and missed detection rates. Hence, the proposed fault tree is, in principle, less conservative than its traditional counterpart. 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 because 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 Eq. (1):

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

Here, $p_{\Delta_i}(\delta_i)$ is the probability density function (PDF) of the deflection of the ith control surface, denoted by the random variable Δ_i, evaluated at a value of δ_i. Further, $p_{\Delta_i}(\delta_i|\text{mode} = j)$ is the conditional PDF of the ith control surface, conditioned on the event that the aircraft is flying in mode j. The weight $P(\text{mode} = j)$ associated with each conditional PDF is the probability of occurrence of each mode for $j = 1, 2, \ldots, M$. 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 $i = 1, 2, \ldots, N$, where N denotes the total number of control surfaces. In this analytical approach, only a small library of PDFs need to be predetermined to be able to generate PDFs for arbitrary missions.

Small fixed-wing UAVs typically find application in aerial photography and geographical surveying. An efficient mission profile for aerial photography is the lawnmower pattern, an instance of which is shown in Fig. 4. (This pattern is only used to aid the exposition of the analysis method; the method itself is general enough to be used with any profile.) 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 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.

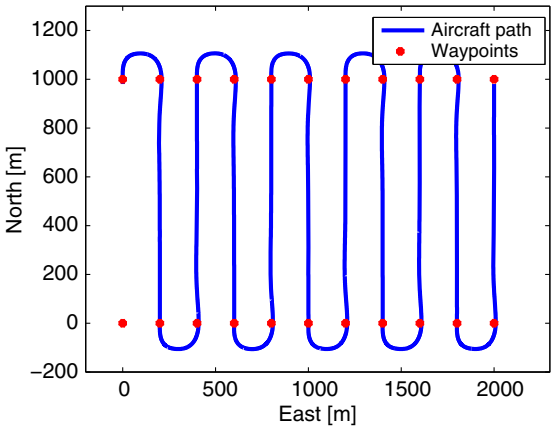


Fig. 4 Aircraft path during area scanning mission.

Then, Eq. (1) can be applied to compute the PDF for the entire mission. The probabilities of the modes can be calculated using the knowledge of the airspeed of the aircraft and the geometry of the flight path. In Fig. 4, the waypoints are 1000 and 200 m apart in the north and east directions, respectively. Consequently, assuming that the entire mission is flown at a constant trim airspeed, the probability of being in a banked turn is 0.26 and of being in straight and level flight is 0.74. There is a nonzero difference between the direct and indirect methods because the indirect method does not account for the transients that occur between two different modes.

As an example, Fig. 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 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. Although this paper 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 [20] can be described in the nonlinear state-space form as shown in Eqs. (2) and (3):

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

$$y = h(x, u) \tag{3}$$

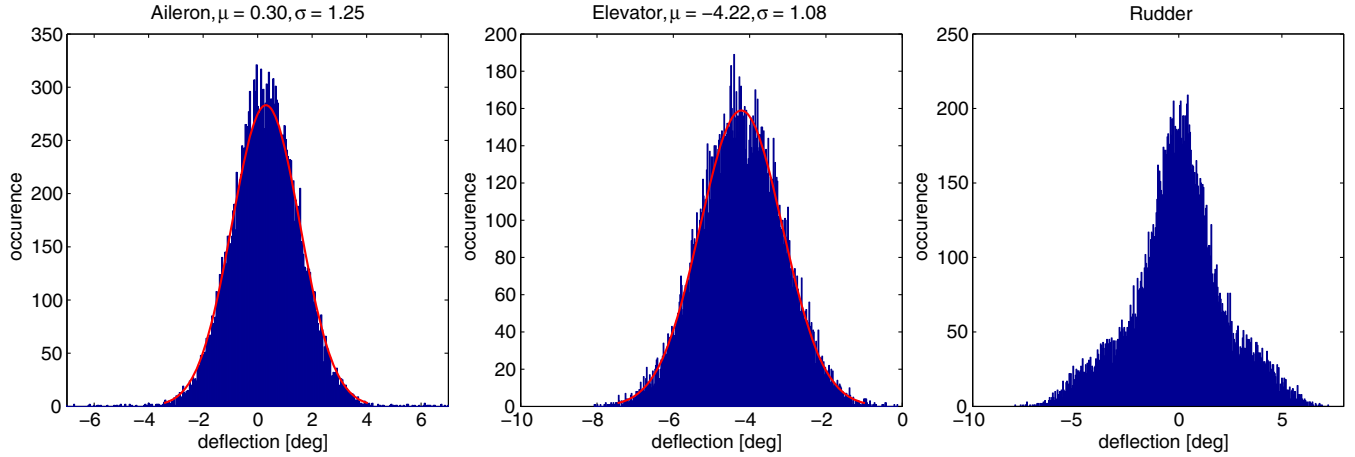


Fig. 5 Control surface distributions for straight and level flight with 400 bins.

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: $\mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^n$ is the state function, and h: $\mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^p$ is the output function. The state vector is $x = [\phi, \theta, \psi, p, q, r, u, v, w]^T$. Here, ϕ, θ, and ψ 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 ψ: $x_r = [\phi, \theta, p, q, r, u, v, w]^T$. x_r is used in the definitions of the flight envelopes.

For configuration 0 (CCCC), there are only four unique aerodynamic control inputs. In addition, the throttle is τ. 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 paper make use of certain elements in the output vector y. The airspeed, angle of attack, and angle of sideslip are denoted by V, α, and β, respectively. The flight-path climb angle and heading rate are denoted by γ and $\dot{\psi}$, respectively.

Aircraft typically fly around equilibrium or trim points. The collection of all such trim points defines the steady flight envelope $\mathbb{F}$ of the aircraft. In this paper, zero rate of change of x_r is the basis for defining the steady flight envelope, as shown in Eq. (4):

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

where $(\bar{x}, \bar{u})$ denotes an equilibrium point. A subset of the flight envelope is steady, wings-level flight at constant altitude, described mathematically as

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

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

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

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

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

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 [14].

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 [21,26]. 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 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. 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 results in stability and control derivatives. As an example, a Taylor series expansion of the coefficient of lift is shown in Eq. (8), where the trim values are denoted with an overline, ϵ denotes the linearization error, and δ_i denotes the deflection of the ith control surface:

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

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, Fig. 6 shows the dependence of the coefficients of drag (C_D), lift (C_L), and pitching moment (C_m) on α 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 α and C_m vs α. The nonlinear behavior that is seen at low angles of attack in C_D vs α is due to the addition of profile drag and induced drag [27].

However, it is possible to characterize the nonlinearities shown in Fig. 6 even without wind-tunnel test data. The nonlinearity seen in the C_D vs α 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 α 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

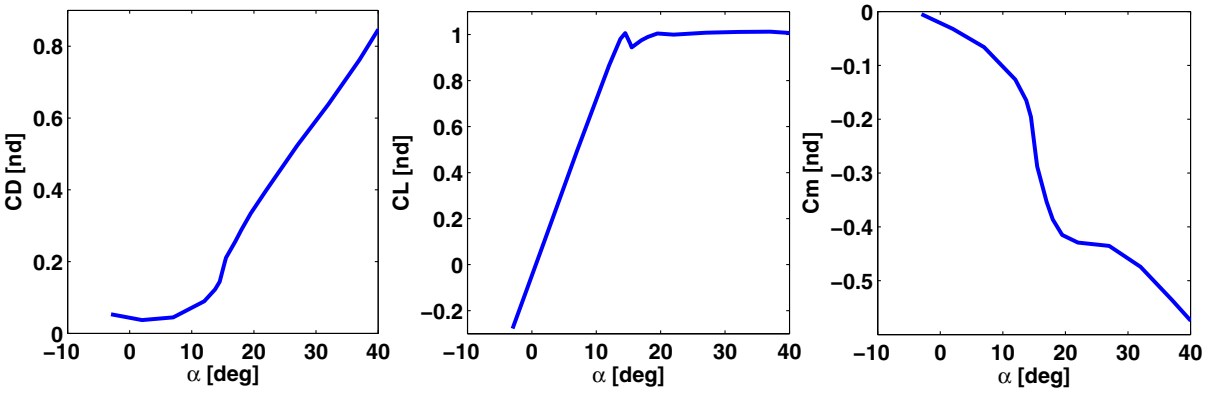


Fig. 6 Nonlinear dependence of C_D, C_L, and C_m on α.

the C_m vs α 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 [28]. Based on the premise that the nonlinearities shown in Fig. 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 α. 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.

For illustrative purposes, a limited flight envelope assessment is presented for configuration 0 (CCCC). Note that similar assessments can be performed for the other configurations listed in Table 1 as well but are not shown in this paper. The flight envelope of configuration 0 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 Fig. 7. Every point inside this envelope is a trim point that has a different value of flap deflection. There are several interesting observations. First, as expected, there is an inverse relationship between V and α. Second, because a nonlinear aircraft model is being trimmed, the flight envelope has well-defined boundaries, as seen in Fig. 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 because 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 deg) is reached at low airspeeds. The stall boundary is due to a constraint on the output variable α. The trailing-edge (TE) down/up flap boundary defines trim points for which flaps are deflected to ± 25 deg (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 0, certain isolines define the envelopes for other configurations. As an example, consider configuration 3 (CCCN), where no flaps are used. The flight envelope for this configuration would simply be the isoline for $F = 0$ in Fig. 7.

Figure 8 shows the longitudinal flight envelope in the $V - \alpha$ plane generated using the high- and medium-fidelity models, shown by two different patches. 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 $(\partial C_D/\partial \delta_i)$. 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 $(\partial C_L/\partial \delta_i)$ and $(\partial C_m/\partial \delta_i)$. The match obtained between the two models in Fig. 8 is sufficient for the remainder of the analysis, as will be shown in Sec. IV.

Figure 9 shows the flight envelope in the $F - E$ plane along with the variation of the angle of attack across trim points. 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 3 (CCCN) ($F = 0$), trim points

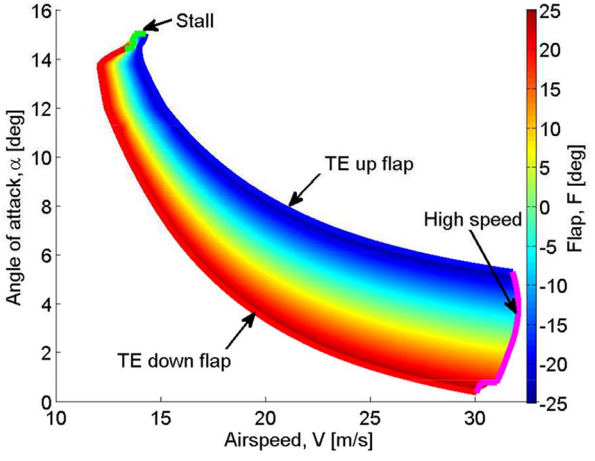


Fig. 7 Longitudinal flight envelope in the $V - \alpha$ plane.

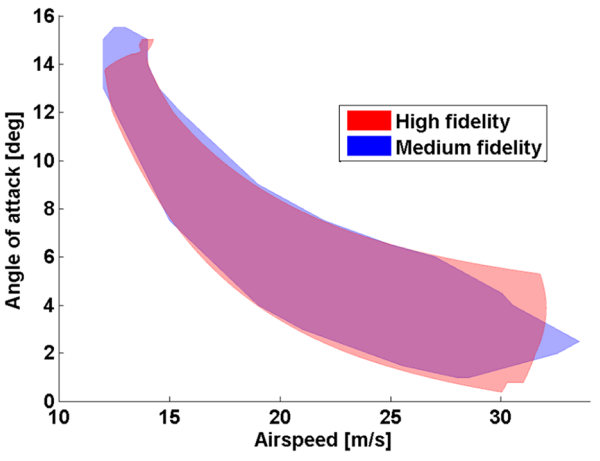


Fig. 8 Model validation using flight envelopes.

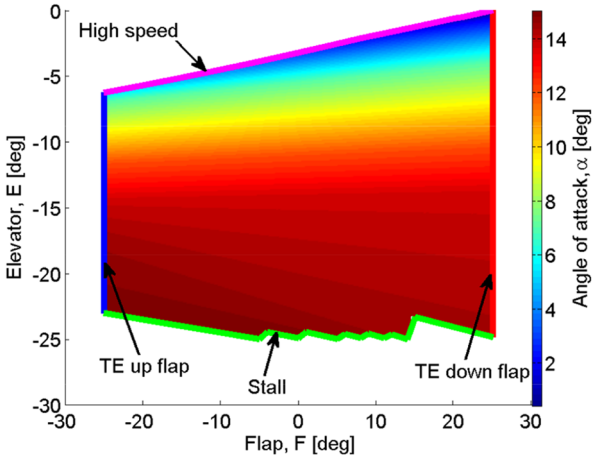


Fig. 9 Longitudinal flight envelope in the $F - E$ plane.

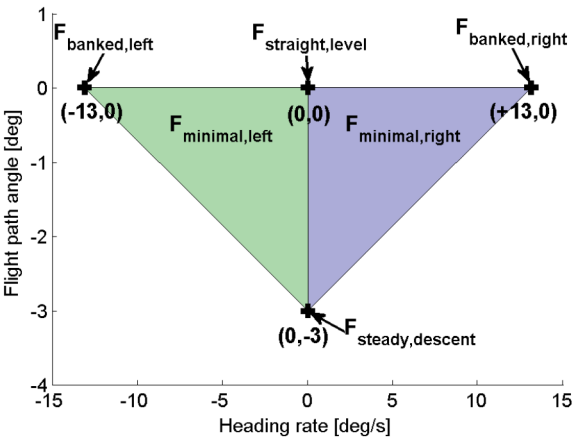


Fig. 10 Minimal flight envelope.

exist for the elevator range [−25, −4 deg]. Finally, for any given flap deflection, the high-speed boundary is reached 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. 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 γ, irrespective of the airspeed. 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 (Fig. 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.

Referring back to the lawnmower pattern introduced in Fig. 4, it is seen that the turn radius encountered during such missions is on the order of 100 m. In addition, in many practical applications, UAVs are required to stay within a geofence to ensure that they do not breach terrestrial property limits. The virtual boundaries defined by the geofence drive the performance and landing requirements for the UAV. For this case study, the maximum required turning radius is set as 87 m. This is sufficiently larger than the minimum achievable turning radius of 54 m, while still being under the typical mission radius of 100 m. At a nominal airspeed of $V = 20$ m $\cdot$ s^{-1}, an 87 m turning radius corresponds to a heading rate of ± 13 deg /s and a bank angle of 28 deg. The minimum required flight-path angle is assumed to be $\gamma = -3$ deg because this is representative of typical glide slopes. The four points shown in Fig. 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, 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 in 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, α, and β. 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 Fig. 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 configurations 1–4, 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, configurations 1 and 4 have decoupled ailerons that have a stuck surface range of ± 25 deg. 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 other. On the other hand, configurations 2 and 3 have ailerons that are constrained to deflect antisymmetrically and have a much narrower stuck aileron range. Configuration 2 is the only configuration to have decoupled elevators. Because faults in either elevator can be compensated by the other, configuration 2 has a broad stuck elevator range of [−25, +16 deg]. On the other hand, configurations 1, 3, and 4 have narrower stuck elevator ranges because all three of them have coupled elevators. Note that, for all configurations that have a rudder, stuck faults in the full deflection range are allowable because rudder faults simply induce a nonzero sideslip velocity.

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 configuration 1 (DCCN) and configuration 4 (DCNN) differ by 0.5 deg, configuration 3 (CCCN) differs by 0.1 deg, and configuration 2 (CDCN) differs by 9 deg. Although the difference in configuration 2 might appear excessive, it does not matter in the computation of the probability of catastrophic failure. This is because +16 deg is sufficiently far out from the $\pm 6\sigma$ bounds straddling the mean of the elevator deflection (−4.2 deg in Fig. 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 configurations 2 and 3, both of which have coupled ailerons. Specifically, the aileron range for configuration 2 differs by 1 deg and configuration 3 differs by 2 deg. Once again, because 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 Sec. 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 Secs. III.A, and III.B. It is useful to once again refer to the fault tree pictured in Fig. 3. Considering the bottommost level of the fault tree, it is seen that there are nine different events. The false alarm and missed detection probabilities of the actuator FDI algorithm are given by P_{FA} and P_{MD}, respectively. Consider a servo that fails when the control surface is positioned outside its allowable range. In this scenario, there is at least one point

Table 2 Allowable stuck surface ranges (medium fidelity)

Configuration	Aileron(s), deg	Elevator(s), deg	Rudder(s), deg
1 (DCCN)	[−25, +25]	[−25, −1.5]	[−25, +25]
2 (CDCN)	[−11, +11]	[−25, +16]	[−25, +25]
3 (CCCN)	[−8, +8]	[−25, −4.1]	[−25, +25]
4 (DCNN)	[−25, +25]	[−25, −1.5]	N/A

in the minimal flight envelope (Fig. 10) where the aircraft cannot be trimmed. Consequently, this analysis predicts catastrophic failure, irrespective of the fault classification made by the FDI system i.e. MD and true positive, or TP, both result in a catastrophic failure.

On the other hand, the FDI classification matters for a servo that fails inside its allowable range. In particular, a true positive will lead to a successful control law reconfiguration. On the other hand, missed detections are acceptable only if the nominal flight control law is robust to the servo fault (depicted by the S block). However, for simplicity, this paper will assume that missed detections under an in range servo failure will always lead to catastrophic failure (i.e., the N block has probability equal to 1). Although this shortcoming affects the accuracy of the results, it increases the conservativeness of the approach. If no servos have failed, the FDI algorithm can have two outcomes: false alarm (FA) or true negative (TN). 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. On the other hand, if the control surface is positioned inside its allowable range and no servo failures have occurred, neither FA nor TN has any negative consequences.

One of the key assumptions made earlier was that the probability of an actuator getting stuck within a certain deflection range is proportional to the probability of the actuator being positioned within that range. The probability of the ith surface being positioned outside its allowable range is

$$P_{\text{out},i} = 1 - \int_l^u p_{\Delta_i}(\delta_i)\,\mathrm{d}\delta_i$$

where l is the minimum value and u is the maximum value of the corresponding allowable range. The complement is $P_{\text{in},i} = 1 - P_{\text{out},i}$. The probability of the ith surface getting stuck outside the allowable range is $qP_{\text{out},i}$. The total probability of catastrophic failure is

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

The first term in Eq. (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 Eq. (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 Eq. (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 shut off. If this causes the servo to get stuck, a catastrophic failure may result if the control surface is outside its allowable range.

Another key assumption made in Sec. III was that multiple actuator faults occur with negligible probabilities. This is a valid assumption because q^2 is several orders of magnitude smaller than P_{SYS}, as shown in Sec. IV. A more rigorous reliability analysis that considers the interactions between multiple failure modes, but not the flight envelope contributions, is given in [29].

IV. Reliability Analysis Results

A. Effects of Mean Time Between Failures and P_{MD}

The analysis method described in Sec. III is applied to estimate the overall reliabilities of the actuator architectures listed in Table 1. The overall reliability depends on several different parameters: servo MTBF, P_{MD}, P_{MD}, mission profile, trim point, model fidelity, etc. In this section, the first set of results is 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 to 8000 h. A typical example on the low-reliability end is a Futaba hobby-grade servo [30]. A typical example on the high-reliability end is a Litton military-grade servo that is used on the RQ-5 Hunter UAV [31]. In addition, there are examples that fall

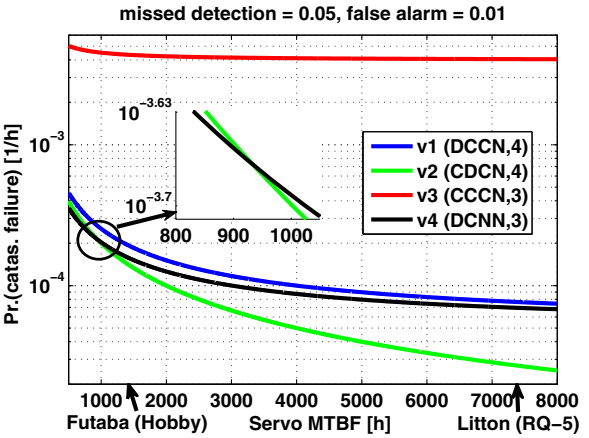


Fig. 11 Reliability vs MTBF for lawnmower pattern for configurations 1–4.

within this range [15]. The values for the missed detection and false alarm probabilities are taken from [22] and are set as $P_{\text{MD}} = 0.05\ \text{h}^{-1}$ and $P_{\text{FA}} = 0.01\ \text{h}^{-1}$. Note that, although [22] pertains to commercial passenger aircraft, it is a good starting point for this analysis. In addition, P_{MD} and P_{FA} values are typically related through a receiver operating characteristic. The probability of catastrophic failure for configuration 3 is two orders of magnitude greater than that of the other architectures. This is because configuration 3 has no decoupled surfaces and has the least cross-functionality in reconfiguration among all the configurations. Configuration 1 is the second-worst architecture, despite having four servos. Compared to configuration 3, configuration 1 has an extra servo that decouples the ailerons and extends their allowable range to [−25, +25 deg]. This greatly increases the reliability of configuration 1 relative to configuration 3.

However, configuration 1 is uniformly less reliable than configurations 2 and 4 over the displayed range of servo MTBF. Note that the only way in which configuration 1 is different from configuration 4 is the presence of a rudder. Despite the rudder, configuration 1 (four servos) is less reliable than configuration 4 (three 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 tradeoff between the two main contributions to the terms in Eq. (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 $P_{\text{out},i}$. Second, adding a control surface increases the overall probability of missed detections and false alarms because additional fault modes are introduced. The addition of the rudder in configuration 1 does not contribute to the flight envelope because the rudder is not cross-functional with any of the other control surfaces. However, the addition of the rudder in configuration 1 is detrimental to its overall reliability because of the contribution of missed detections and false alarms in Eq. (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 previously.

Finally, the two most reliable configurations are configurations 2 and 4. Excluding the rudder, both configurations 2 and 4 use a three-servo architecture. Although configuration 2 has coupled ailerons and decoupled elevators, configuration 4 has decoupled ailerons and coupled elevators. The presence/absence of the rudder in configurations 2 and 4 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 configurations 2 and 4 is primarily driven by the architecture of the

elevators and ailerons. Figure 11 shows these two curves intersecting at MTBF ≈930 h. For MTBF <930 h, the probability of catastrophic failure is lower for configuration 4. 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 h, the probability of catastrophic failure is lower for configuration 2. 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 1000 h. Hence, the maximum value of q^2 is $10^{-6}/\text{h}^2$. Comparing $10^{-6}/\text{h}^2$ to the range of values for P_{SYS} plotted in Fig. 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, configuration 3 is the least reliable, lies outside the axis limits, and is not shown in the figure. Also note that the only difference between configurations 1 and 4 is the presence/absence of the rudder. Hence, in the limit $P_{MD} \to 0$, the penalty of missed detections generated by the rudder in configuration 1 also tends to zero. Given that rudder faults of any magnitude can be tolerated (see Table 2), the reliabilities of configurations 1 and 4 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 configurations 1 and 4 start to diverge, and the addition of the rudder introduces a greater cost on the overall reliability. Over the entire range of P_{MD}, configuration 2 uniformly does better than configurations 1 and 4. The relative difference between the reliabilities of configuration 2 and configurations 1 and 4 increases as P_{MD} decreases (i.e., configuration 2 is an order of magnitude more reliable than configurations 1 and 4 for $P_{MD} < 0.005$ 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 paper. As $P_{MD} \to 0.08$ h^{-1}, the reliability curves of configurations 2 and 4 intersect. This implies that, for FDI algorithms that have high rates of missed detections, a configuration that has decoupled ailerons and coupled elevators (configuration 4) eventually becomes more reliable than configuration 2.

The general conclusions on the different configurations, drawn from Figs. 11 and 12, can be reasoned and validated using insights from flight dynamics. First, from both figures, it is seen that configuration 2 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 because configuration 2 is the only configuration featuring two independently actuated elevators. This makes sense from a flight dynamics perspective because the elevators have the most control authority, owing to their large moment arm relative to the center of gravity. Although 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, +16 deg] for configuration 2 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.

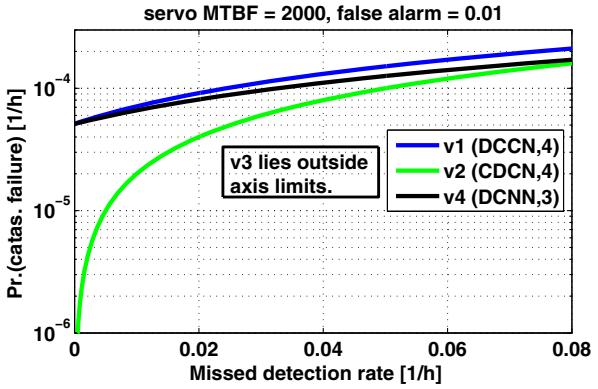


Fig. 12 Reliability vs missed detection rate.

For MTBF <930 h, 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 configuration 2) becomes less reliable than a configuration that has decoupled ailerons (such as configuration 4). A similar conclusion can be made as P_{MD} increases beyond 0.08 h^{-1}. For $P_{MD} > 0.08$ h^{-1}, the terms contributed by the elevators to the probability of catastrophic failure exceed the terms contributed by the ailerons. Once again, configuration 2 becomes less reliable than configuration 4. The plots shown in Fig. 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 [32]. 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.

Although Figs. 11 and 12 correspond to the medium-fidelity model, similar figures can be created for the high-fidelity model. For configurations 1, 3, and 4, 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 configurations 1, 3, and 4, are −1.5, −4.1, and −1.5 deg, respectively. These limits are within the $\pm 3\sigma$ bounds straddling the elevator mean of −4.2 deg. Consequently, even a 0.1 deg difference has a noticeable effect on the overall reliabilities. For configuration 2, 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 in the overall reliabilities are similar. This is observed by comparing Figs. 11 and 12 with their high-fidelity counterparts [14].

B. Effects of Aircraft Operations

In Sec. 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 1 (DCCN), 3 (CCCN), and 4 (DCNN). For an MTBF of 7800 h, the differences for configurations 1, 3, and 4 are 12.8, 1.73, and 12.6%, respectively. For configuration 2 (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.

In this section, the effects of two aircraft operation parameters on the overall reliability are investigated. The first parameter of

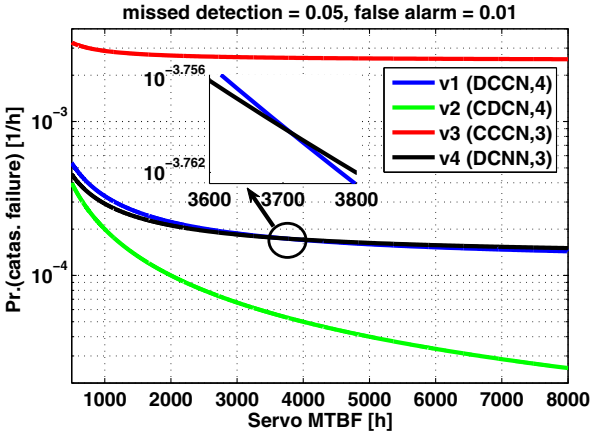


Fig. 13 Reliability vs MTBF for spiral ascent/descent mission.

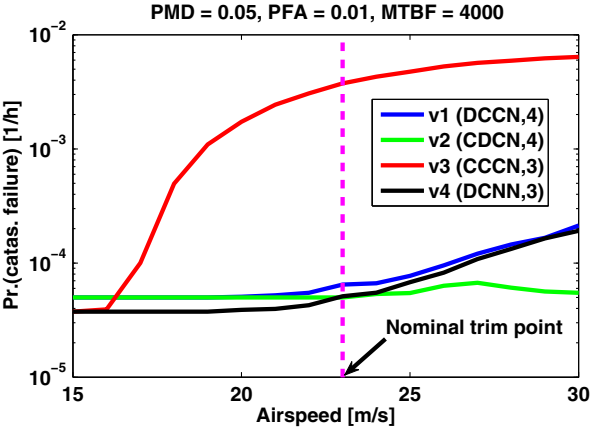


Fig. 14 Reliability vs trim point.

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 175 s of this example, the aircraft is made to climb at a mean airspeed of 23 $\text{m} \cdot \text{s}^{-1}$, a mean climb angle of 3.33 deg, and a mean turn rate of 12.5 deg/s. For the next 175 s 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 deg. Figure 13 shows the resulting overall reliabilities. As before, configuration 3 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 configurations 1 and 4 are considerably less reliable as compared to the lawnmower pattern of Fig. 11. This is not surprising because configurations 1 and 4 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 configuration 2 because it is the only configuration with decoupled elevators. With the spiral ascent/descent commanding more of the elevator, configuration 2 has the best overall reliability. No intersection between configurations 2 and 4 is seen, unlike Fig. 11. However, an intersection between configurations 1 and 4 is seen at an MTBF ≈3700 h. As mentioned previously, the only way in which configuration 1 is different from configuration 4 is the presence of the rudder. Although the rudder was detrimental to the overall reliability in Fig. 11, Fig. 13 suggests that the rudder may be beneficial if high reliability servos are available. Indeed, for servo MTBF >3700 h, configuration 1 is more reliable than configuration 4 because 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 h, configuration 4 is more reliable than configuration 1. 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, α) pairs. Moreover, Fig. 7 showed that, when $F = 0$, the flight envelope reduced to an isoline. Given that no configuration among configurations 1–4 has flaps, the trim point is uniquely defined by specifying either V or α. 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 $\text{m} \cdot \text{s}^{-1}$ increments. The airspeed $V = 23$ $\text{m} \cdot \text{s}^{-1}$ is marked with a vertical dashed line and corresponds to the nominal trim point of Baldr. All of the figures preceding Fig. 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 1 (DCCN), 3 (CCCN), and 4 (DCNN), the upper limit is much closer to the elevator mean of −4.2 deg as compared to the lower limit. This asymmetry is the primary reason behind the first observation. As an example, consider configuration 3, for which the upper elevator limit is −4.1 deg. By operating at the nominal trim point, 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 3 is the most sensitive to the trim airspeed because configuration 3 has the smallest stuck elevator range of [−25, −4.1 deg]. Hence, the trim airspeed and trim elevator deflection have a large impact on the overall reliability. On the other hand, configuration 2 (CDCN) is the least sensitive because configuration 2 has the largest stuck elevator range of [−25, +16 deg]. The sensitivities of configurations 1 and 4 to trim airspeed are of the same order and are between those of configurations 2 and 3. Moreover, the values of P_{SYS} for configurations 1 and 4 start to converge with an increase in the trim airspeed. This is because both configurations 1 and 4 share exactly the same allowable stuck elevator range, as given in Table 2. On the other hand, at low trim airspeeds, P_{SYS} for configurations 1 and 2 converge. This once again shows that, when the elevator is deflected sufficiently negatively, the reliability of configuration 1 improves to the level of configuration 2. The same nominal flight control law was used at all the trim airspeeds shown in Fig. 14. This is not optimal because this flight control law was designed specifically for the nominal trim airspeed. Nevertheless, closed-loop stability was preserved at all trim airspeeds, with some performance degradation at off-nominal trim airspeeds. 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. Conclusions

This paper 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, typically modeled as a binary decision. This paper 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 paper 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 configurations. Hence, the most reliable actuator architecture is dependent not only on the reliabilities of the onboard 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 affects the overall reliability. Cross-functional hardware redundancy provides a judicious way to improve unmanned aerial vehicle (UAV) reliability. 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.

There are several interesting avenues for future research, including relaxing the assumptions made in this paper. One avenue involves relaxing the assumption that the servo failure rate is time-invariant and independent of the servomotor usage and position. In addition, the servo failure rates are borrowed from the manufacturer-issued product specification sheets. Bench-top experiments to validate the numbers and figures of the servos will be investigated in the future. Another avenue involves applying the key concepts introduced in this paper for the reliability assessment of other aircraft subsystems. Future work will also investigate how the design of the flight control law and weather conditions, such as atmospheric turbulence, affect the probability of catastrophic failure. This paper was limited in scope to a specific fixed-wing airframe. A parametric study can be constructed to investigate the effects of aircraft design parameters on the overall reliability. Finally, a similar reliability assessment framework may be constructed for multirotor UAVs.

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 FP7-AAT-2012-314544. This work was also supported by the National Science Foundation under grant 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," Joint Research Centre, TR, Rept. LB-NA-26451-EN-N, Geneva, Switzerland, 2013; also *4th JRC ECML Crisis Management Technology Workshop*.

[2] "Study Analysing the Current Activities in the Field of UAV," Frost and Sullivan, EC Enterprise and Industry, Rept. ENTR/2007/065, Brussels, Belgium, 2011.

[3] "House Resolution 658: FAA Modernization and Reform Act of 2012," Section 332: Integration of Civil Unmanned Aircraft Systems into National Airspace System, 112th U.S. Congress, 2012.

[4] "Notice of Proposed Rulemaking for 14 CFR Part 107," Federal Aviation Administration Rept. FAA-2015-0150, Washington D.C., 2015.

[5] "A New Era for Aviation: Opening the Aviation Market to the Civil use of Remotely Piloted Aircraft Systems in a Safe and Sustainable Manner," European Commission Rept. COM/2014/0207, Brussels, Belgium, 2014.

[6] Atkins, E. M., "Autonomy as an Enabler of Economically-Viable, Beyond-Line-of-Sight, Low-Altitude UAS Applications with Acceptable Risk," *Proceedings of the AUVSI North America Conference*, Vol. 1, Association for Unmanned Vehicle Systems International, Arlington, VA, 2014, pp. 200–211.

[7] Zsedrovits, T., Bauer, P., Pencz, B. J. M., Hiba, A., Gözse, I., Kisantal, M., Németh, M., Nagy, Z., Vanek, B., Zarándy, A., and Bokor, J., "Onboard Visual Sense and Avoid System for Small Aircraft," *IEEE Aerospace and Electronic Systems Magazine*, Vol. 31, No. 9, Sept. 2016, pp. 18–29.

[8] Yeh, Y. C., "Triple-Triple Redundant 777 Primary Flight Computer," *Proceedings of the IEEE Aerospace Applications Conference*, IEEE, New York, 1996, pp. 293–307.

[9] Traverse, P., Lacaze, I., and Souyris, J., "Airbus Fly-by-Wire: A Total Approach to Dependability," *Building the Information Society*, Springer, New York, 2004, pp. 191–212.

[10] Amos, J., Bergquist, E., Cole, J., Phillips, J., Reimann, S., and Shuster, S., "UAV for Reliability Senior Design Project," Univ. of Minnesota Digital Conservancy, Minneapolis, MN, July 2014, hdl.handle.net/11299/16413 [retrieved 14 Oct. 2016].

[11] Spitzer, C. R., *The Avionics Handbook*, CRC Press, Boca Raton, FL, 2001, pp. 11-1–13-1.

[12] Wu, B., *Reliability Analysis of Dynamic Systems: Efficient Probabilistic Methods and Aerospace Applications*, Elsevier, Cambridge, MA, 2013, pp. 1–13.

[13] Hamada, M., *Bayesian Reliability*, Springer, New York, 2008, pp. 125–160.

[14] Venkataraman, R., Lukátsi, M., Vanek, B., and Seiler, P., "Reliability Assessment of Actuator Architectures for Unmanned Aircraft," *Proceedings of the 9th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes, SafeProcess*, Elsevier Ltd., Amsterdam, The Netherlands, 2015, pp. 398–403.

[15] "Endurance Test DA 22-30-4128," Volz Servos GmbH, Rept. DA 22-30-4128, Offenbach am Main, Germany, 2009.

[16] Freeman, P., "Reliability Assessment for Low-Cost Unmanned Aerial Vehicles," Ph.D. Dissertation, Univ. of Minnesota, Minneapolis, MN, 2014.

[17] Goupil, P., "AIRBUS State of the Art and Practices on FDI and FTC in Flight Control System," *Control Engineering Practice*, Vol. 19, No. 6, June 2011, pp. 524–539. doi:10.1016/j.conengprac.2010.12.009

[18] "UAV Laboratories,"Univ. of Minnesota, Minneapolis, MN, Aug. 2010, www.uav.aem.umn.edu [retrieved 14 Oct. 2016].

[19] Lie, F. A., Dorbantu, A., Taylor, B., Gebre-Egziabher, D., Seiler, P., and Balas, G., "An Airborne Experimental Test Platform: From Theory to Flight (Part 1)," *Inside GNSS Magazine*, Vol. 9, No. 2, March–April 2014, pp. 44–58.

[20] Cook, M. V., *Flight Dynamics Principles*, 2nd ed., Elsevier, Amsterdam, The Netherlands, 2007, pp. 66–95.

[21] 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*, AIAA Paper 2006-3306, June 2006.

[22] "Built-in-Test Verification Techniques," Boeing Aerospace Company TR Rept. RADC-TR-86-241, Seattle, WA, 1987.

[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. doi:10.1109/TMECH.2013.2258678

[24] Lombaerts, T., Schuet, S., Wheeler, K., Acosta, D., and Kaneshige, J., "Robust Maneuvering Envelope Estimation Based on Reachability Analysis in an Optimal Control Formulation," *Proceedings of the Conference on Control and Fault-Tolerant Systems (SysTol)*, IEEE, New York, 2013, pp. 318–323.

[25] Stamatelatos, M., Vesely, W., Dugan, J., Fragola, J., Minarick, J., and Railsback, J., "Fault Tree Handbook with Aerospace Applications," NASA TR, Washington, D.C., Aug. 2002, https://www.hq.nasa.gov/office/codeq/doctree/fthb.pdf [retrieved 14 Oct. 2016].

[26] Hoe, G., Owens, D., and Denham, C., "Forced Oscillation Wind Tunnel Testing for FASER Flight Research Aircraft," *AIAA Atmospheric Flight Mechanics Conference*, AIAA Paper 2012-4645, Aug. 2012.

[27] Anderson, J. D., *Introduction to Flight*, 8th ed., McGraw–Hill, New York, 2015, pp. 441–448.

[28] 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. doi:10.2514/8.3121

[29] 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, Aug. 2015, pp. 130–141. doi:10.1016/j.ress.2015.04.005

[30] Murtha, J. F., "An Evidence Theoretic Approach to Design of Reliable Low-Cost UAVs," M.S. Thesis, Virginia Polytechnic Inst. and State Univ., Blacksburg, VA, 2009.

[31] "Unmanned Aerial Vehicle Reliability Study," Office of the Secretary of Defense Washington, D.C., 2003.

[32] Rice, J. W., and McCorkle, R. D., "Digital Flight Control Reliability—Effects of Redundancy Level, Architecture, and Redundancy Management Technique," *Guidance and Control Conference*, AIAA Paper 1979-1893, 1979.