Reliability Assessment of Actuator Architectures for Unmanned Aircraft

B. Vanek

Institute for Computer Science and Control
Hungarian Academy of Sciences
H-1111 Budapest, Kende u 13-17, HUNGARY

Abstract – *A reliability assessment framework is developed for small scale Unmanned Aerial Vehicles. The analysis considers several candidate architectures with different numbers of servos and controllable surfaces. It is assumed that servo faults can be detected with some rate of false alarm and missed detection. The flight envelope is analyzed to determine the fault levels for which it remains possible to control the aircraft. For these "flyable" fault levels, it is assumed that the flight control law can be reconfigured to safely land the aircraft. Finally, the estimate of the aircraft catastrophic failure rate is based on the histogram of (pre-fault) control command distributions, mean time between failure of the individual servos, missed detection rates for built-in tests, and false alarms. The analysis results provide clear trade-offs between these various parameters as well as the number and configuration of the servos.*

Keywords: UNMANNED AERIAL VEHICLES, RELIABILITY ASSESSMENT, FLIGHT CONTROL ARCHITECTURE

1. Introduction

The Unmanned Aerial Vehicle (UAV) industry is undergoing a rapid transformation due to the emergence of several commercial applications, projected to surpass military spending in the coming years [5]. The rapid growth period of the past years, mainly driven by research and development (R&D) projects will fuel a second industrial boom, the commercial and civil drone market is expected to develop strongly during the next few years and could reach 2 billion dollars by 2015, driven by new technological capabilities, lower production costs and changes to the regulatory framework.

The main barrier for the widespread use of UAVs is their inability to routinely access the common airspace. This is due to a combination of regulatory and technical challenges. On the regulatory side, significant work is currently undertaken both in the US and in the EU to establish the framework for seamless integration into the national airspace. On the technical side there are a variety of issues including the need for sense & avoid technologies, secure communication and human factors. UAVs lack the operational experience of conventional aircraft, hence they pose a significant risk for air traffic and for the humans on the ground [19]. The U.S. Federal Aviation Administration has yet to propose rules to govern the use of commercial robotic aircraft in U.S. skies, but it predicts that 7,500 unmanned craft weighing 55 pounds (25 kilograms) or less will be operating in the U.S. by 2018. There is strong interest from agriculture, mining, and infrastructure companies in using drones in Europe also [3].

The remainder of this paper focuses on one specific technical issue: the design of a reliable UAV architecture, since reliability of most existing UAS is far below that required of manned commercial and manned military aircraft. The MQ-1 Predator recorded an accident rate of 13.7 for every 100,000 hours for its first 10 years of operation, the MQ-9 Reaper has fared better than the Predator, partially thanks to its triple redundant flight control system and the more rigorous systems engineering approach behind it, incurring 3.17 mishaps per 100,000 hours which is getting close to the mishap rate of the two fighter jets, the F-16 and F-15, which have posted mishap rates of 1.96 and 1.47 respectively [19]. On the other hand, improving the reliability of commercial UAS will be difficult because payload and economic considerations prevent the use of triplex redundancy (the standard design technique used to achieve high reliability in safety critical aerospace systems [15]). In fact, most commercial UAS on the market [14] fly with single string avionics and use only two actuator surfaces. To raise the reliability of small commercial UAS some level of redundancy will be required both on the avionics side by the mean of fault tolerant control, and also on the aerodynamics side, using physically redundant flight control surfaces.

The present article provides an approach on designing and assessing the overall reliability of these small, and affordable UAVs to help understanding the inherent design trade-offs in systems engineering. The main challenge is to combine hardware redundancy with analytical redundancy based fault tolerant control, which provides the required reliability at the lowest cost and system weight/complexity. The control system layout, control design assumptions and the flight control surface architecture influenced by faults are considered within this article. Clear trade-offs are established between possible tolerable faults, the layout of flight control surfaces and the overall reliability of various candidate UAV architectures.

2. Problem Formulation

Based on the motivations in the previous section, a method is proposed to assess the reliability of various UAV actuator architectures without the need for extensive flight testing. The proposed method is of general nature and can be applied to any UAV. However a specific small UAV (BALDR) is used as a concrete example for the reliability calculations. BALDR

is a small UAV, based on the Ultra Stick 120 airframe, that is maintained by the university of Minnesota, [16]. A simulation environment is available for this UAV. The centerpiece of the environment is the high-fidelity nonlinear six degrees-of-freedom model of the Ultra Stick 120 aircraft. The aerodynamic parameters in this model were estimated based on wind tunnel tests conducted at the NASA Langley Research Center [13,7]. The simulation environment and the flight control computer allow for extensive software-in-the-loop and processor-in-the-loop simulations of the aircraft model. The entire simulation environment, details about the aircraft fleet, components, wiring, and data from numerous flight tests have been made open-source and can be freely downloaded from this website: [16].

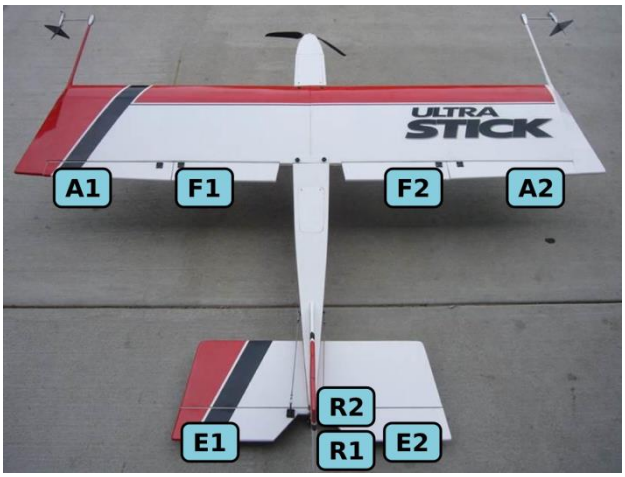

Figure 1: The BALDR UAV with the control surfaces labeled (A – aileron, F – flap, E – elevator, R – rudder).

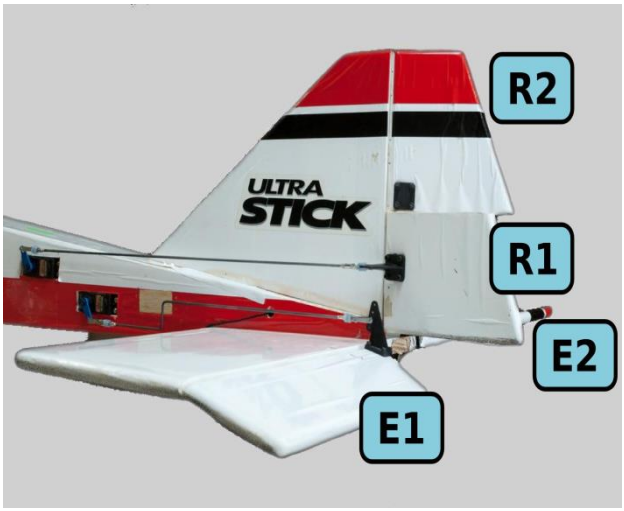

Figure 2: Tail of the BALDR UAV with the control surfaces labeled (E – elevator, R – rudder).

The goal of the current study is to assess the impact of various actuator architectures on the overall system reliability. The overall system reliability can be quantified via the probability of catastrophic failure of the aircraft. In this study, catastrophic failure is defined as the inability of the aircraft to reach a proper landing site. The failure rate of the actuators is much greater than the other units due to the wear of the moving parts. They usually make up more than half of the components in number, so they can be considered the greatest contributor to the overall reliability of a UAV. In case of an actuator failure a path must be generated from any starting point to the landing site, which requires, at the minimum, the ability to fly straight with a constant altitude, turn with a maximum specified turning radius (at constant altitude) and descend with a minimum specified flight path angle. These requirements can be presented as a minimal flight envelope in the flight path angle – heading rate ($\gamma - \dot{\psi}$) plane. This minimal flight envelope is explained in detail in section 4.

This paper only considers faults in the servos of the aircraft. Engine failure is not considered because of the assumption that the aircraft can glide to a safe landing. There are several servo failure modes such as jamming, runaway, loss of efficiency, disconnection and oscillatory [6]. The last three failure modes are more common in large aircrafts where larger loads are present and resonance can occur because of the aeroelastic behaviour of the airframe. Jamming and runaway failures can occur in small aircrafts and can lead to catastrophic failures. Runaway failures are considered an extreme case of jamming at the physical limits. In this paper, only jam faults of the control surface is considered in the reliability assessment.

The BALDR has eight unique aerodynamic control surfaces: split elevators $(E1, E2)$, split rudders $(R1, R2)$, ailerons $(A1, A2)$, and flaps $(F1, F2)$. These control surfaces are shown in figures 1 and 2. Each of the eight aerodynamic control surfaces is actuated by an independent servo motor. Different combinations of the eight surfaces allow for different actuator architectures to be defined. 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 is considered positive. In addition, all the surfaces have a deflection range $[-25°, +25°]$. Increasing the number of servos on an aircraft increases reliability, if the architecture is properly designed, but it also adds to the cost and weight of the system. To analyze this trade-off, five actuator architectures are defined below for the BALDR aircraft for which the probability of catastrophic failure is estimated in section 5.

- coupled ailerons, single elevator, single rudder, coupled flaps (4 servos)
- decoupled ailerons, single elevator, single rudder, no flaps (4 servos)
- coupled ailerons, split elevators, single rudder, no flaps (4 servos)
- coupled ailerons, single elevator, single rudder, no flaps (3 servos)
- decoupled ailerons, single elevator, no rudder, no flaps (3 servos)

These configurations will hereafter be referred to as v0, …,

v4. The configuration v0 is only used for flight envelope assessment in section 4. The eight different control surfaces of the BALDR are coupled differently depending on the actuator configuration. As an example, for the v0 configuration, $A1 = -A2$, $E1 = E2$, $R1 = R2$, and $F1 = F2$.

There are several simplifying assumptions to make the analysis tractable in the early design phase. First, it is assumed that a Fault Detection and Isolation (FDI) algorithm is used to detect actuator faults. Simple bulit-in-tests and model based methods are both considered as parts of the FDI algorithm. However, only statistical properties of the FDI like missed detection and false alarm rates are considered. Dynamic properties like detection time are neglected at this point. It is also assumed that, if the aircraft is trimmable after a fault has occurred, an appropriate reconfigurable control law is available. In other words, transitions between trim points are without loss of control. Only single faults are considered as multiple faults occurring at the same time have negligible probabilities. Another assumption is that the deflection of a control surface is independent of time, which enables us to use independent and identically distributed probability density functions in the calculations. The high fidelity nonlinear simulation of the BALDR allows for the determination of trim points. The failure probability calculation requires the knowledge of the reliability of a single servo (usually expressed by the Mean Time Between Failure – MTBF).

The analysis method has three distinct steps:

- acquiring control surface distributions
- determining flight envelopes and stuck surface ranges
- estimating the probability of catastrophic failure

The probability distributions of control surface deflections are used to compute the probability of a surface being stuck in the range where faults cannot be tolerated. The ranges for each surface are determined by discovering the allowable trim points or actuator jamming faults. The probability of catastrophic failure is then estimated by summing the probabilities of the various surfaces being stuck in the range where faults cannot be tolerated.

3. Distribution of Control Signals

Determining the distribution of the aircraft's control signals is needed for the evaluation of the final probability of failure. These distribution functions are influenced by several factors, including the mission profile, the control algorithm and exogenous disturbances (sensor noise, wind gusts and atmospheric turbulence). Control algorithms play a large part in forming the distributions and therefore in the reliability of a UAV. As an example, using the rudder for coordinated turns or simply yaw rate damping results in different control signal characteristics. Controller dynamics also affect the shape of the distributions. A conservative controller yields small variance around the trim point, while a more agile controller results in the deflections more spread out.

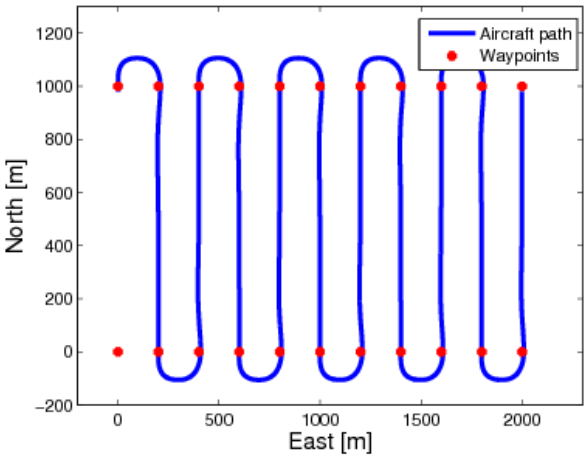

Figure 3: Aircraft path during area scanning mission.

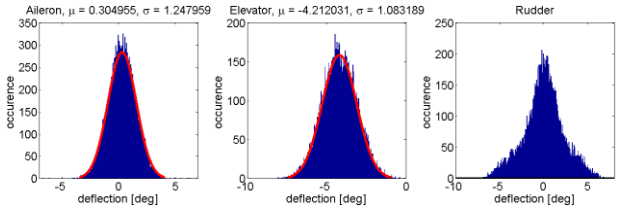

Figure 4: Control surface distributions during line segment following.

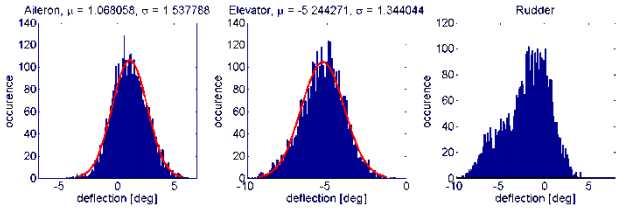

Figure 5: Control surface distributions during circular orbit following (right turns only).

Histograms of control surface deflections can be plotted from flight data or simulations, then probability density functions can be estimated for these histograms. Generating the histograms directly from measurements may not always be practical because it would require flight tests for every mission profile considered. The mission profile, in fact, can be broken down into different elements like straight-level flight, banked turns and steady ascents and descents. If the distributions of the control signals are known for these modes, the overall distributions can be constructed by combining them with weighting that accounts for the probability of being in each mode during the mission:

$$p_i(\delta) = p_i(\delta|mode = 1)p(mode = 1) + \cdots$$

$$+p_i(\delta|mode = n)p(mode = n), \quad (1)$$

where $p_i(\delta|mode = n)$ is the probability distribution function of the ith control surface during mode n and $p(mode = n)$ is the probability of being in mode n. This way histograms obtained from one mission profile can be used to generate histograms for another one and the effect of different profiles on UAV reliability can be evaluated.

Figure 3 shows a typical area scanning path for the BALDR UAV obtained from the Software-in-the-Loop simulation (duration is 588 s). It consists of three modes: straight level flight and left and right banked turns. Figures 4 and 5 show the distributions of the control surfaces for two phases of the mission. Normal distributions are fitted to ailerons and elevators as they are approximately Gaussian while rudder distributions appear to be multi-modal and cannot be characterized easily. Aileron trim values are near zero degrees: the small mean is used to compensate for motor torque. In addition, the mean aileron deflection during a banked turn is also near zero, as shown by figure 5. This is because a large aileron deflection is only required to transition to a banked turn; once the desired roll angle is achieved, the ailerons return to their small trim value. On the other hand, the elevator trim is affected by the turn to produce more lift, as can be seen by a change of 1.03 degrees. The variances of the distributions are somewhat greater in the turns. Rudder distributions are different in the two modes: for the straight flight they are symmetrical but for the turn one of the side lobes is missing. The reason for this is that only right turns were used to generate the histograms while the straight flight contained both positive and negative rudder deflections for disturbance rejection.

The probability of being in each mode is estimated from the mission profile as the fraction of time spent in that mode. For the area scanning mission the probabilities of the modes can be calculated from the geometry of the scanned area and the distance between the scanning lines. For the path shown in figure 3 the waypoints are 1000 m apart in the North and 200 m apart in the East direction. The resulting probabilities are 0.13 for both left and right turns and 0.74 for straight flight.

4. Flight Envelope Assessment

This section gives a cursory introduction to aircraft flight envelopes, since this concept is important for the subsequent section. The aircraft equations of motion [11, 2], 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. 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 components in the body-fixed frame are: roll rate (p), pitch rate (q), and yaw rate (r). The airspeed components in the body-fixed frame 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 v0, there are only four unique aerodynamic inputs. In addition, the throttle for the motor is τ. Consequently, the input vector is $u = [\tau, E, R, A, F]$. As expected, the input vector will change appropriately, 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. 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, as shown in equation (4).

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

A subset of the flight envelope is straight and level flight, i.e. unaccelerated flight at constant altitude. This subset is mathematically described in equation (5). The key property of this subset is the zero flight path angle $(\bar{\gamma} = 0)$.

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

Level flight is, by definition, at constant altitude. When the aircraft descends steadily, at a constant negative flight path angle $(\bar{\gamma} < 0)$, the envelope is described by equation (6).

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

Another subset of the flight envelope is steady banked turns at constant altitude. A steady banked turn is defined by a constant heading rate $(\dot{\psi})$. Left banked turns are described by a negative $\dot{\psi}$ and right banked turns are described by a positive $\dot{\psi}$. These subsets are mathematically defined in equations (7) and (8).

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

$$\mathbb{F}_{banked,right} = \{(\bar{x}, \bar{u}): \dot{\bar{x}}_r = 0, \dot{\psi} > 0, \bar{\gamma} = 0, \dot{\bar{u}} = 0\} \quad (8)$$

These subsets can be computed by applying numerical optimization techniques to the nonlinear aircraft model that was introduced in section 2. The nonlinear aircraft model can be trimmed and linearized, using routines developed in-house, at any operating point within the flight envelope. For straight & level flight, operating points are best expressed as pairs of (V, α). A rectangular grid of such (V, α) pairs is generated for $V \in [10,40] m/s$ and $\alpha \in [0°, 20°]$. The grid resolution is $0.1 m/s$ and $0.1°$ for V and α, respectively. The

nominal flight condition for the BALDR is $(V, \alpha) = (23m/s, 4.72°)$. 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) – (8)). 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 minima that is closest to the initial condition.

Paper [4] conducted a similar trim state discovery for another Ultra Stick 120 version. The work presented in this paper draws on the results and conclusions outlined in [4] and connects them to the probability of catastrophic failure in section 5. A more thorough treatment of aircraft flight envelopes can be found in [9, 20, 17].

A limited flight envelope assessment is presented only for configuration v0. The envelope corresponding to longitudinal straight & level flight can be used to determine the stuck ranges for the elevator and flaps. This envelope is shown in the $V \times \alpha$ plane in figure 6 and in the $F \times E$ plane in figure 7. Trim points are marked by colored crosses in both these figures. In figure 6, the trim points are 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 α. Trim points at high airspeeds have low α and vice-versa. 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 6.

The high speed boundary is a collection of trim points that define the highest achievable airspeeds and lowest achievable angles of attack. Conversely, at the stall boundary, the stall angle of attack (approximately $15°$) is reached at low airspeeds. The high speed and stall boundaries are due to output constraints. The other two boundaries are due to input saturation. The TE up flap boundary defines trim points for which flaps are deflected to $-25°$ (trailing edge up). The TE down flap boundary defines trim points for which flaps are deflected to $+25°$ (trailing edge down). It is interesting to 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, the envelopes for other configurations can be extracted by looking at certain isolines. As an example, consider configuration v3, where no flaps are used. The flight envelope for this configuration would simply be the green isoline for $F = 0$ shown in figure 6.

In figure 7, the trim points are colored based on the value of α. Three important conclusions can be drawn from this figure. Firstly, it is seen that trim points exist for the entire range of flap deflections, as shown by the TE up/down flap boundaries. Secondly, 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 a catastrophic failure of the aircraft. As an example, for configuration v3 ($F = 0$), trim points exist for the elevator range $[-25°, -4°]$. It is seen that, 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.

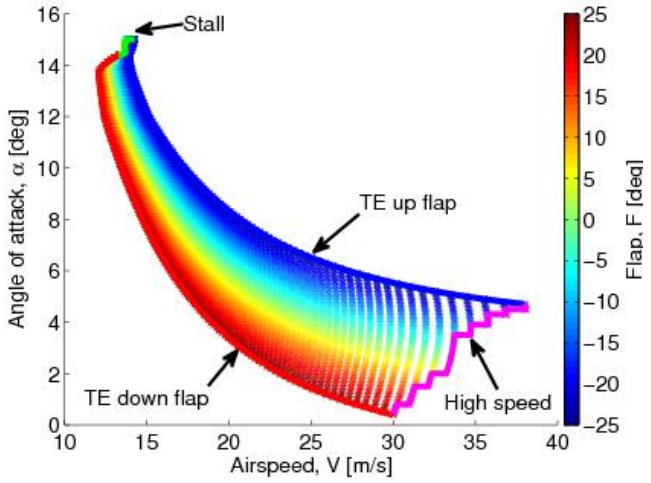

Figure 6: Longitudinal flight envelope in the $V \times \alpha$ plane.

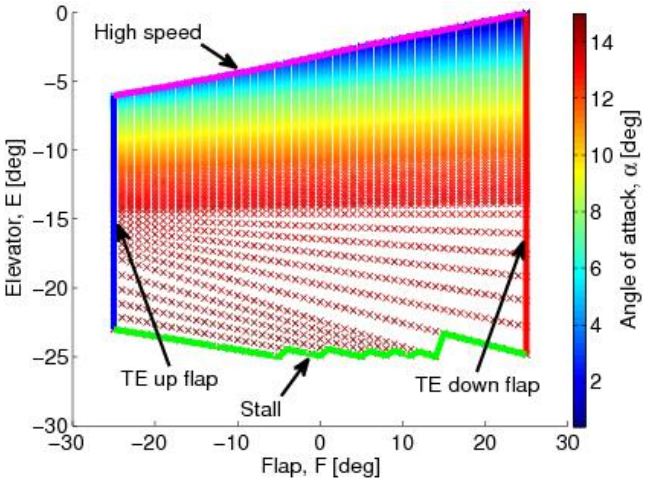

Figure 7: Longitudinal flight envelope in the $F \times E$ plane.

A stuck surface fault is called *allowable* if the aircraft can safely fly home in the presence of this fault. In order to safely fly home, the aircraft should be able to execute some limited maneuvers. The flight envelope subsets, that were defined earlier, can be used to describe these limited maneuvers. The aircraft should be able to fly straight and level, execute either left or right banked turns with some minimum $\dot{\psi}$, and descend steadily at some minimum γ. These limited maneuvers together form the minimal flight envelope. This can be visualized in the $\gamma - \dot{\psi}$ plane, as shown in figure 8. It is reasoned that 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.

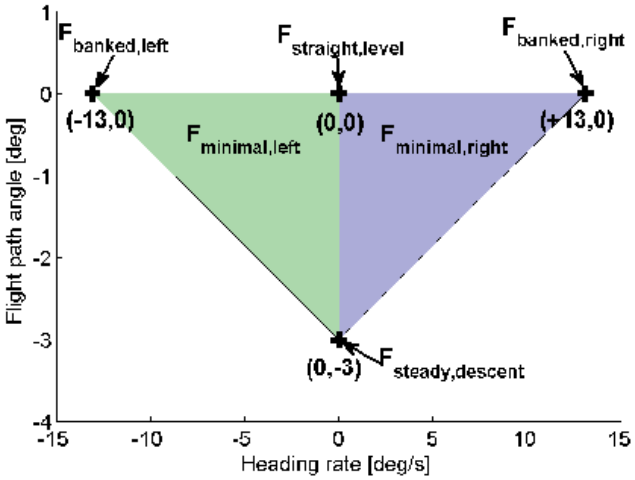

Figure 8: Minimal flight envelope

Config.	Elevator(s)	Rudder(s)	Aileron(s)
v1	[-25,-1]	[-25,+25]	[-25,+25]
v2	[-25,+25]	[-25,+25]	[-11,+12]
v3	[-25,-4]	[-25,+25]	[-7,+10]
v4	[-25,-1]	N/A	[-25,+25]

Table 1: Allowable stuck surface ranges

For this research, the maximum required turning radius is 87 m. This value was selected because it is sufficiently larger than the minimum achievable turning radius of 54 m, while still allowing for reasonably large heading rates. At a nominal airspeed of $V = 20\text{m/s}$, an 87 m turning radius corresponds to a heading rate of $\pm 13^{\circ}/s$. The minimum required flight path angle is chosen as $\gamma = -3^{\circ}$ since this is representative of typical glide slopes. The four points shown in figure 8 define two triangles: $\mathbb{F}_{minimal,left}$ and $\mathbb{F}_{minimal,right}$. 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. Hence, it is sufficient to check for the existence of trim points at the vertices of the two triangles.

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 $\mathbb{F}_{straight,level}$ and $\mathbb{F}_{steady,descent}$, and either of the subsets $\mathbb{F}_{banked,left}$ and $\mathbb{F}_{banked,right}$. In other words, a stuck fault is called allowable if trim points can be found either in $\mathbb{F}_{minimal,left}$ or $\mathbb{F}_{minimal,right}$. 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 figure 8. Then, the intersection of these trimmable ranges is calculated between $\mathbb{F}_{straight,level}$, $\mathbb{F}_{steady,descent}$, and $\mathbb{F}_{banked,left}$. This intersection is called the trimmable range for $\mathbb{F}_{minimal,left}$. In a similar way, the trimmable range for $\mathbb{F}_{minimal,right}$ is calculated. The union of $\mathbb{F}_{minimal,left}$ and $\mathbb{F}_{minimal,right}$ is defined as the allowable stuck surface range.

The allowable stuck surface ranges for v1 through v4 are given in Table 0. For configurations that have a single elevator (v1, v3, v4), it is seen that the range is never positive, i.e. no trim points exist for positively stuck elevator. However, the allowable range is $[-25^{\circ}, +25^{\circ}]$ when split elevators are present (v2). Another interesting observation is that stuck rudder faults can always be tolerated as long as no explicit constraints are placed on β. Lastly, decoupled ailerons (v1 and v4) have the full allowable range as compared to coupled ailerons (v2 and v3). The allowable stuck surface ranges presented here in conjunction with the distribution of control signals, presented in section 3, allow for the computation of the probability of catastrophic failure for each of the four configurations.

5. Probability of Catastrophic Failure

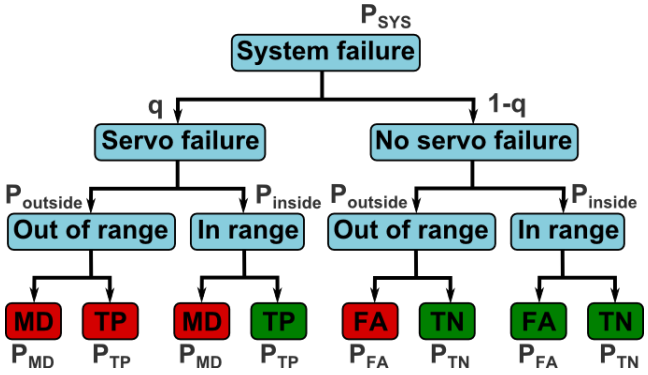

Figure 9: System level failure as a tree of different events (MD – missed detection, TP – true positive, FA – false alarm, TN – true negative).

The final step of the assessment is the calculation of the probability of catastrophic failure. It is computed as the sum of the probabilities of a control surface getting stuck outside its allowable range. In addition to this, the missed detection and false alarm events of the FDI algorithm can be included in the calculation on a probabilistic basis. These events can be illustrated in a fault tree (figure 9), which decomposes system level failure into lower-level events of the failure of the servo and the FDI algorithm's decisions about the servo's state. Events that lead to catastrophic failure are marked as red, ones that do not are marked with green. The events of missed detection and false alarm can be characterized with the conditional probabilities $P_{MD} = P(missed\ det.\ |\ servo\ failure)$ and $P_{FA} = P(false\ alarm\ |\ no\ servo\ failure)$.

From the distribution functions obtained in section 3 the probability of a control surface being in a given range can be

computed. The probability that the ith surface is outside the allowable range $[lu]$ is given by:

$$P_{outside,i} = P(\delta_i > u \vee \delta_i < l) = 1 - \int_l^u p_i(\delta_i) d\delta_i. \quad (9)$$

The probability of the ith surface getting stuck outside the allowable range is obtained by multiplying this with the servo failure rate $q = 1/MTBF$. The total probability of catastrophic failures due to all possible actuator faults outside their allowable range is given by:

$$P_{SYS} = \sum_{i=1}^{N} qP_{outside,i}, \quad (10)$$

where N is the number of control surfaces.

Missed detections lead to catastrophic failure because the control algorithm cannot reconfigure to accommodate the fault, both when the fault is inside and outside the allowable range. The case when the fault is outside the range is already included in equation (10), so only servo faults inside the allowable range have to be considered:

$$P_{SYS,MD} = P_{SYS} + \sum_{i=1}^{N} q(1 - P_{outside,i})P_{MD}. \quad (11)$$

In addition, it is assumed that false alarms lead to catastrophic failure only outside the allowable range, since assumed faults inside the range can be tolerated by the controller. False alarms that occur when the servo is outside the allowable range do not always lead to catastrophic failure. However, this assumption is made as it is more conservative and thus yields an upper bound on the failure rate. Since the false alarm probability has meaning only in case of there is no servo fault, the probability indicating this case must be included in its calculation:

$$P_{SYS,MD,FA} = P_{SYS,MD} + \sum_{i=1}^{N} (1 - q)P_{outside,i}P_{FA}. \quad (12)$$

The probability of catastrophic failure has been evaluated for the four configurations of the BALDR UAV defined in section 2. Figure 10 shows the probabilities as a function of servo MTBF with with the missed detection and false alarm rates held at $P_{MD} = 0.05$ and $P_{FA} = 0.01$, respectively. The servo MTBF values for the evaluation are chosen so that they range from a common R/C-grade servo to high performance ones used on large military UAVs [12]. The MTBF of high performance servos for small UAVs, like the ones from [18], are approximately 1000 hours, and fall between these bounds. The value of 0.05 for the missed detection rate is based on industrial values for built-in tests. Specifically, for bulit-in-tests the missed detection rate is usually estimated by fault coverage obtained from Fault Tree Analysis methods. Typical values are above 95% [1] which corresponds to the 0.05 missed detection rate used in figure 10. It is possible to achieve lower missed detection rates using more advanced methods, e.g. model-based methods, but this would require a more detailed stochastic analysis [8]. The value selected for the false alarm rate, $P_{FA} = 0.01$, is assumed to be achievable with current fault detection methods. Note that there is an inverse relationship between the missed detection and false alarm rates.

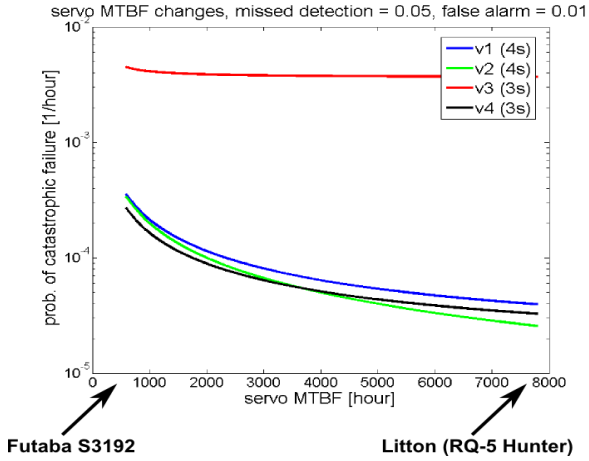

Figure 10: Probability of failure as a function of servo MTBF.

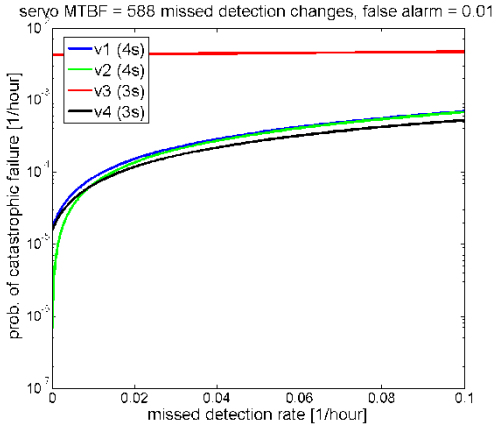

Figure 11: Probability of failure as a function of missed detection rate.

Figure 10 shows that configuration v3 has the lowest level of reliability. The probability of failure for v3 is two orders of magnitude higher than that of the other designs. This configuration has no split surfaces and the ailerons are coupled which leaves few possibilities for reconfiguration, as can be seen from the allowable ranges. The second-worst is v1 despite having 4 servos. Compared to v3, v1 has an extra servo that decouples the ailerons, which extends their allowable range to $[-25°, +25°]$. This greatly increases the reliability of v1 relative to v3. However the elevator range is only slightly improved and hence v1 remains the second-worst design. In fact v1 (with four servos) is less reliable than v3 (with 3 servos). This demonstrates that increasing the number of servos does not necessarily increase the aircraft reliability. Finally, the two most reliable configurations are v2 (with four servos) and v4 (with three servos). These designs have similar reliability numbers. For low servo MTBF v4 is better, but for high MTBF values v2 performs better. While using more servos / control surfaces expands the allowable ranges, it also adds failure modes to the system. When higher quality servos are used, it is beneficial to have more servos. This explains why v2 (with four servos) is more reliable at high MTBF. On the other hand, when low quality servos are used, it is beneficial to have fewer servos. This is

why v4 is more reliable at low MTBF. Thus if higher quality servos can be used for a UAV, it is worth considering an architecture with split surfaces. If only low-cost components are affordable, then a simplified design which minimizes the number of control surfaces achieves the best reliability.

Figure 11 shows the effect of missed detection rate. The results in this figure are shown for fixed MTBF = 588 hours and false alarm $P_{FA} = 0.01$. Configuration v3 has the lowest reliability figure, regardless of missed detection rate. For missed detection rates near zero, v2 is the best, in fact for $P_{MD} = 0$ it has 0 probability of failure. This is based on the assumption that two servo faults are extremely unlikely and thus negligible. For higher missed detection rates, v4 has the highest reliability. A similar trade-off can be observed to the effect of servo MTBF: if the missed detection rate is low, then it is advantageous to have more servos. If missed detection rate is high, using fewer servos results in increased reliability. If no or only limited performance FDI algorithms are available, then an architecture using only a minimal set of servos achieves the best reliability. On the other hand, if high-performance FDI algorithms can be used on a UAV, architectures with more than the minimal number of servos can be considered.

6. Conclusion

A method has been proposed for assessing the reliability of small scale UAVs based on their actuator architecture, mission profile and flight control law. The method was demonstrated for a specific UAV, for which four actuator configurations were assessed. The method can be extended to beyond simply comparing different actuator architectures. Different airfames can also be compared: for example a conventional aircraft with a flying wing. Future work will involve assessing the reliability of flying wing airframes with several different actuator architectures. The results from this research is expected to give valuable insight to small UAV designers, so that they can incorporate reliability requirements right from the drawing board.

The proposed method carries the weight of several simplifying assumptions. These assumptions can be relaxed and the method can be refined. As an example, motor faults can be included in the analysis to make it more realistic. Another key assumption is that the existence of trim points after the onset of a fault is sufficient for reconfiguration. Future work will involve the incorporation of the fault detection, isolation and reconfiguration into the analysis

7. Acknowledgement

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 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" in cooperation with Raghu Venkataraman, Peter Seiler from University of Minnesota and Márk Lukátsi from MTA SZTAKI.

8. References

[1] Boeing Aerospace Company. Built-in-test verification techniques, 1987.

[2] M. V. Cook. *Flight Dynamics Principles*. Elsevier, second edition, 2007.

[3] 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. *COM(2014) 207 final*, 2014.

[4] P. Freeman and G. Balas. Actuation failure modes and effects analysis for a small uav. In *American Control Conference*, Portland, OR, June 2014.

[5] Frost & Sullivan. Study analysing the current activities in the field of uav. *EC Enterprise and Industry Directorate-General*, 2011.

[6] P. Goupil. Oscillatory failure case detection in the A380 electrical flight control system by analytical redundancy. *Control Engineering Practice*, 180 (9):0 1110 – 1119, 2010.

[7] G. Hoe, D. Owens, and C. Denham. Forced oscillation wind tunnel testing for faser flight research aircraft. In *AIAA Atmospheric Flight Mechanics Conference*, Minneapolis, MN, August 2012. AIAA.

[8] B. Hu and P. Seiler. Certification analysis for a model-based UAV fault detection system. In *AIAA Guidance, Navigation, and Control Conference*, National Harbor, MD, USA, 2014. doi: http://dx.doi.org/10.2514/6.2014-0610 .

[9] N. H. McClamroch. *Steady Aircraft Flight and Performance*. Princeton University Press, 2011.

[10] J. F. Murtha. An evidence theoretic approach to design of reliable low-cost uavs. Master's thesis, Virginia Polytechnic Institute and State University, 2009.

[11] R. C. Nelson. *Flight Stability and Automatic Control*. McGraw-Hill, second edition, 1998.

[12] Office of the Secretary of Defense. Unmanned aerial vehicle reliability study, 2003.

[13] D. Owens, D. E. Cox, and E. A. Morelli. Development of a low-cost sub-scale aircraft for flight research: The faser project. In *25th AIAA Aerodynamic Measurement Technology and Ground Testing Conference*, San Francisco, CA, June 2006. AIAA.

[14] M. Rester, P. Spruyt, T. De Groeve, O. Van Damme, and A. Ali. Unmanned aerial systems for rapid mapping. Technical report, JRC Scientific and Policy Reports, 2013.

[15] C. R. Spitzer. *The Avionics Handbook*. CRC Press, 2001.

[16] University of Minnesota. Uav research group. www.uav.aem.umn.edu, 2014.

[17] J. M. Urnes, E. Y. Reichenbach, and T. A. Smith. Dynamic flight envelope assessment and prediction. In *AIAA Guidance, Navigation and Control Conference and Exhibit*, Honolulu, HI, August 2008. AIAA.

[18] Volz Servos GmbH. Endurance test da 22-30-4128, 2009.

[19] C. Whitlock. When drones fall from the sky. *The Washington Post*, 2014.

[20] J. E. Wilborn and J. V. Foster. Defining commercial transport loss-of-control: A quantitative approach. In *AIAA Atmospheric Flight Mechanics Conference and Exhibit*, Providence, RI, August 2004. AIAA.