Reliability Assessment of Actuator Architectures for Unmanned Aircraft *

Márk Lukátsi, *,‡ Raghu Venkataraman, † Bálint Vanek * and Peter Seiler †

* Institute for Computer Science and Control, Hungarian Academy of Sciences (MTA SZTAKI)
† Department of Aerospace Engineering and Mechanics, University of Minnesota (UMN AEM)
‡ corresponding author, (e-mail: lukatsi@sztaki.hu)

Abstract: A framework is developed for small scale Unmanned Aerial Vehicle reliability assessment. The possibility of flight control system reconfiguration is analysed in-depth related to optimising control system layout and aerodynamic control surface actuation.....

---

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 [Frost & Sullivan, 2011]. 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, which is a combination of legal and technical challenges. They lack the hundred years of operational experience of conventional aircraft, hence they pose a significant risk for air traffic and for the humans on the ground. More than 400 large U.S. military drones crashed in major accidents worldwide between Sept. 11, 2001, and December 2013 Whitlock [2014].

During its first dozen years of existence, the MQ-1 Predator crashed at an extraordinarily high rate for every 100,000 hours flown, it was involved in 13.7 Class A accidents. Since 2009, as the Air Force has become more experienced at flying drones, the mishap rate for Predators has fallen to 4.79 Class A accidents for every 100,000 flight hours. 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 Class A mishaps per 100,000 hours over the five years of 2009-2013. Air Force officials pointed out that the crash rate for Reapers now approaches the standard set by two fighter jets, the F-16 and F-15, which over the past five years have posted Class A mishap rates of 1.96 and 1.47 respectively, according to statistics from the Air Force Safety Center at Kirtland Air Force Base in New Mexico.

The civil sector is seeing improved capability at a lower price also, largely due to the availability of commercial off-the-shelf (COTS) equipment. But the wast majority of the civil applications do not require, and unable to afford, large platforms where redundancy similar to commercial aircraft fly-by-wire systems can be realised.

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 for tasks like inspecting crops or gathering geospatial data.

The European Union also called for action to enable the progressive integration of UAVs into civil airspace from 2016 onwards. The report European Commission [2014] focuses on UAVs for civil use and responds to the call of the European manufacturing and service industry to remove barriers to the introduction of UAVs in the European single market.

Some of the key technologies are not yet available to allow for the safe integration of RPAS. R&D efforts are focused on the validation of these technologies. R&D is carried out by different research programmes managed by various organisations around the world including FAA, EASA, NASA, Eurocontrol and others. The technologies which need further development and validation according to the consensus of these stakeholders are:

- Command and control, including spectrum allocation and management;
- Detect and avoid technologies;
- Security protection against physical, electronic or cyber-attacks;
- Transparent and harmonized contingency procedures;
- Decision capabilities to ensure standardized and predictable behaviour in all phases of flight; and
- Human factor issues such as piloting.

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 tradeoffs in systems engineering. The main challenge is to combine hardware redundancy with analytical redundancy based fault tolerant control, which provides
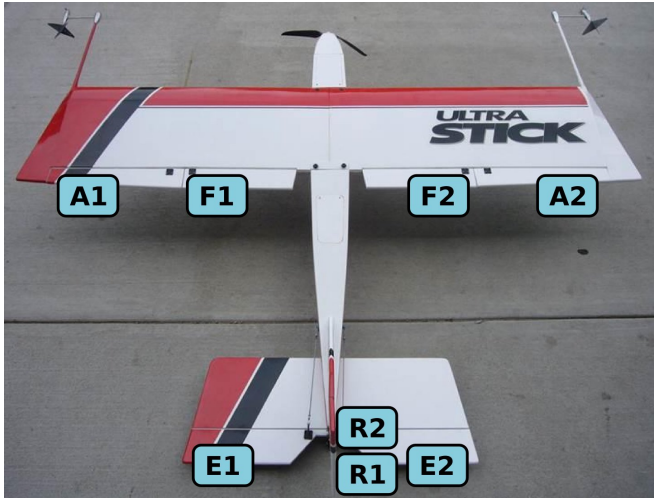
Fig. 1. The FASER UAV with the control surfaces labeled (A – aileron, F – flap, E – elevator, R – rudder).

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 observations in the previous section a method is proposed to assess the reliability of various UAV design architectures without the need of extensive flight testing. The proposed method is of general nature but a case study of a small-scale low-cost UAV is used as an example for the concepts and calculations. This is the FASER UAV of the UMN AEM which is based on an Ultra Stick 120 airframe and for which a simulation environment is available. The centerpiece of the environment is the high-fidelity nonlinear six degrees-of-freedom model of the UltraStick 120 aircraft. The aerodynamic parameters in this model were estimated based on wind tunnel tests conducted at the NASA Langley Research Center [Owens et al. [2006], Hoe et al. [2012]]. 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 University of Minnesota [2014].

The goal of the current study is to assess the impact of various actuator architectures on the overall system reliability. This is achieved by estimating the probability of catastrophic failure of the aircraft which is defined by the inability to fly the aircraft to 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, and usually they 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 by a specified turning radius (at constant altitude) and descend with a specified flight path angle. These requirements can be formulated together by specifying a minimal flight

Fig. 2. Tail of the FASER UAV with the control surfaces labeled (E – elevator, R – rudder).

envelope in the γ – $\dot{\psi}$ plane which contains the points corresponding to the above conditions.

In case of engine failure the aircraft can glide to a safe landing spot if it is in the glide slope, so only servo faults are considered in this context. The failure cases of a servo are mainly the jamming or runaway of a control surface, limitations due to excessive loads, degradation of deflection rates and oscillatory failure [Goupil [2010]]. 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 maximum or minimum deflection, so the assessment is based on the jamming fault mode.

The UltraStick 120 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. 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 FASER aircraft for which the probability of catastrophic failure is estimated in Section 5.

v0. coupled ailerons, single elevator, single rudder, coupled flaps (4 servos)
v1. decoupled ailerons, single elevator, single rudder, no flaps (4 servos)
v2. coupled ailerons, split elevators, single rudder, no flaps (4 servos)
v3. coupled ailerons, single elevator, single rudder, no flaps (3 servos)
v4. 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 UltraStick are coupled differently depending on the actuator configuration. As an example,
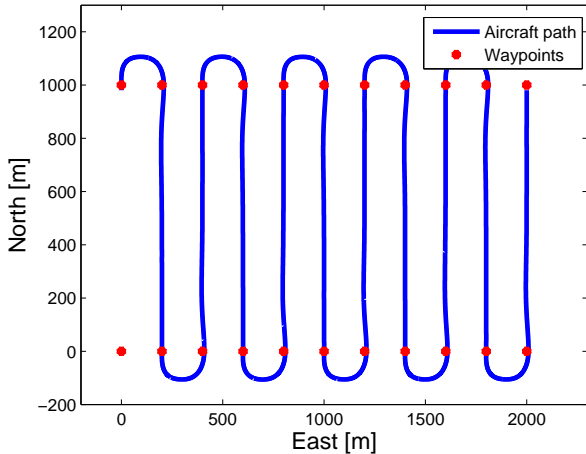
Fig. 3. Aircraft path during area scanning mission.

for the v0 configuration, $A1 = -A2$, $E1 = E2$, $R1 = R2$, and $F1 = F2$.

Our analysis makes several simplifying assumptions to make the analysis tractable in the early design phase. First, it is assumed that an FDI algorithm is used to detect actuator faults, but only statistical properties like missed detection and false alarm ratios are considered, dynamic properties like detection time are neglected at this point. It is also assumed that a reconfigurable control law is used that can stabilize the aircraft after a fault if the aircraft remains trimmable. Hence, if a trim point can be found after a fault has occurred, it is assumed that that trim point can be reached without loss of control. Only single faults are considered as multiple faults occurring at the same time have negligible probabilities compared to them. Another assumption is that the deflection of a control surface (therefore the probability of failure for a control surface) is independent of time, which enables us to use time-independent distributions in the calculations. The determination of trim points requires an aerodynamic model of the aircraft and 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 flight envelopes for actuator jamming faults and relating them with the minimal flight envelope. The probability of catastrophic failure is then estimated by summing the probabilities of the 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. Using the rudder for coordinated turns or simply yaw rate damping results in different control signal characteristics, just like using symmetrically coupled or decoupled ailerons. 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.

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:

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

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 FASER UAV obtained from the SIL 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 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 so easily. Aileron trim values are expected to be near zero degrees (transitioning to a turn needs aileron deflections but once the roll demand is achieved the aileron returns to zero degrees), the small differences are caused by the correcting action due to the motor torque. 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 initial errors for which the autopilot used the rudder in both directions. The same histograms were generated with a control law that does not use the rudder which are not shown here (they are required by one of the configurations analysed in Section 5).

The probabilities of being in each mode can be estimated from the mission profile. For the area scanning mission the ratio of the time spent in straight flight and in turns 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.
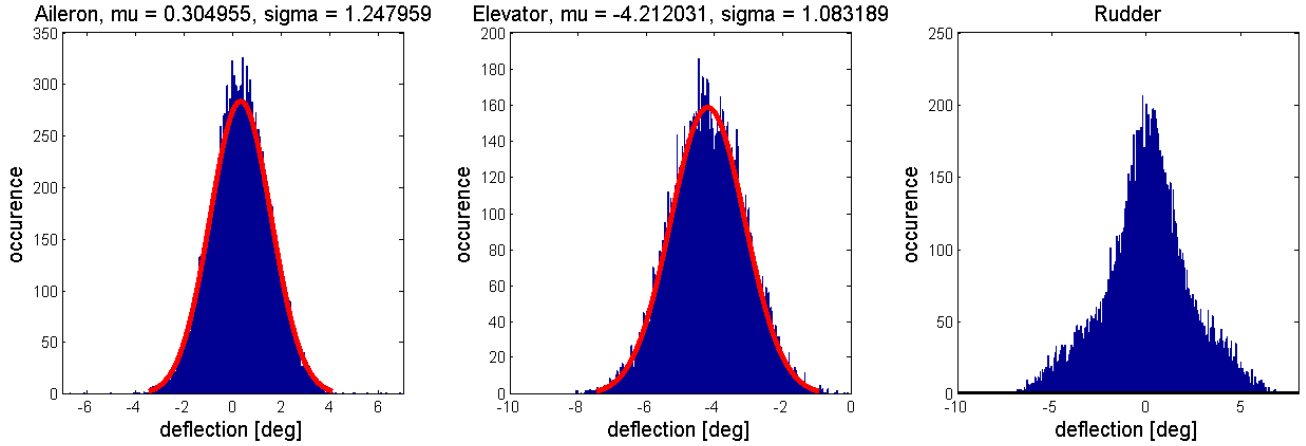
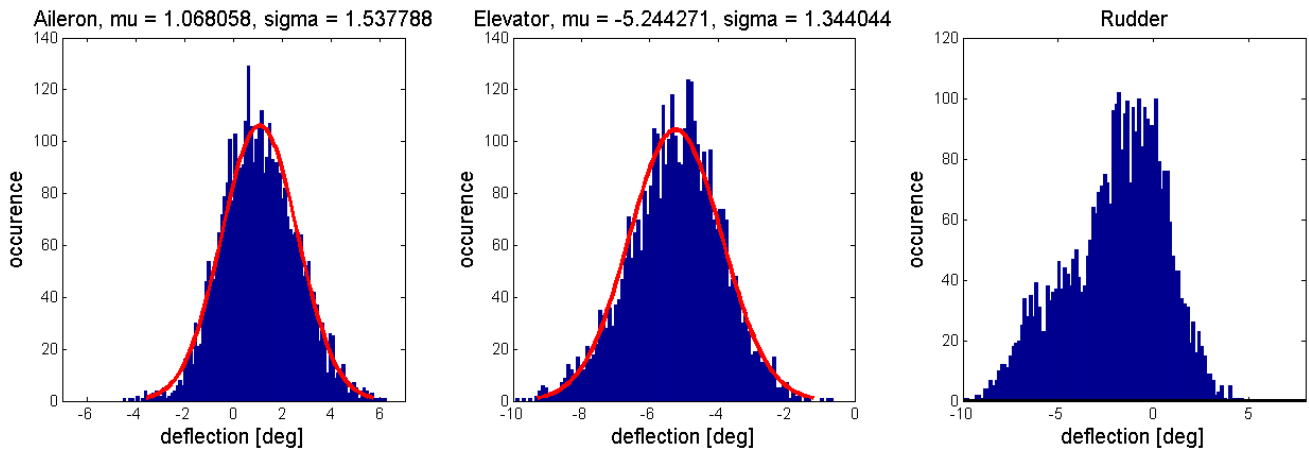Fig. 4. Control surface distributions during line segment following.

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

4. FLIGHT ENVELOPE ASSESSMENT

4.1 Introduction

This section gives a cursory introduction to aircraft flight envelopes, since this concept is important for the subsequent section. The aircraft equations of motion [Nelson [1998], Cook [2007]] can be described in the nonlinear state-space form as shown in equations 2 and 3.

$$\dot{x} = f(x, u) \qquad (2)$$
$$y = h(x, u) \qquad (3)$$

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.

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

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 $(\bar{\gamma} = 0)$.

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

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.

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

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 $0.1m/s$ and $0.1°$ for V and α, respectively. The nominal flight condition for the UltraStick 120 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.

A limited longitudinal flight envelope assessment of the UltraStick 120 is presented next. This is followed by analyses to determine the range of allowable stuck surface faults for the UltraStick 120 versions introduced in Section 2. While a flight envelope assessment is not required per say to determine the allowable stuck surface faults, it gives valuable insight into the distribution of trim points across different flight conditions. This insight will be useful for future work involving reconfigurable control design.

Freeman and Balas [2014] conducted a similar trim state discovery for the UltraStick 120. The work presented in this paper draws on the results and conclusions outlined in Freeman and Balas [2014] and connects them to the probability of catastrophic failure in section 5. A more thorough treatment of aircraft flight envelopes can be found in McClamroch [2011], Wilborn and Foster [2004], Urnes et al. [2008].

4.2 Longitudinal flight envelope for configuration v0

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.

Lastly, it is seen that there are more trim points, that are more spread out, for $E \in [-10°, 0°]$. This also happens to be the low α region ($\alpha \in [0, 9°]$). Although nothing formal is derived in this paper, it can be reasoned that reconfigurable control laws will have a better chance of recovering the aircraft with an elevator failure in this range. On the other hand, the availability of trim points is sparse in the high alpha region ($E \in [-15°, -25°]$). This will likely have an adverse impact on reconfigurable control. While flight envelopes are insightful and help visualize the distribution of trim points, they are not necessary to simply determine the allowable stuck surface ranges. In the next section, a more direct approach is taken in order to determine the allowable stuck surface ranges for each actuator configuration.

4.3 Allowable stuck surface ranges

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 in section 4.1, 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.
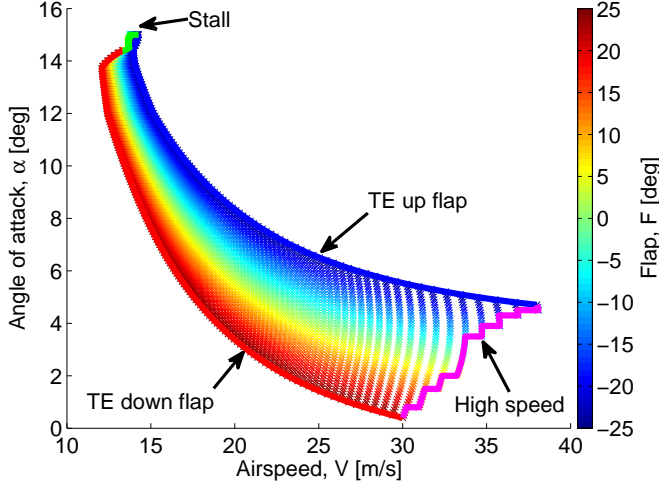
Fig. 6. Longitudinal flight envelope in the $V \times \alpha$ plane.
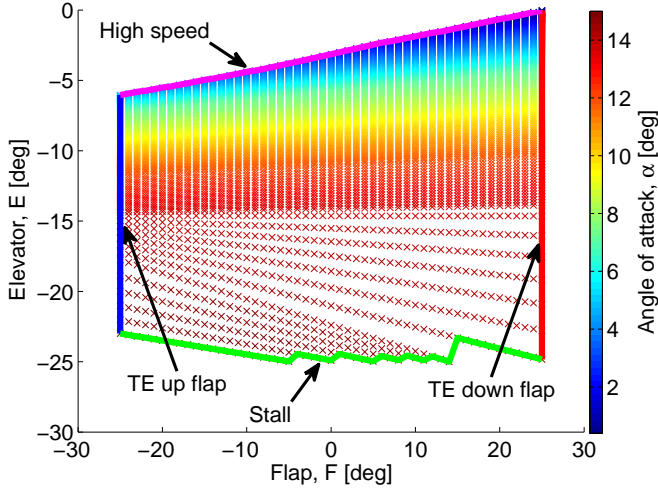

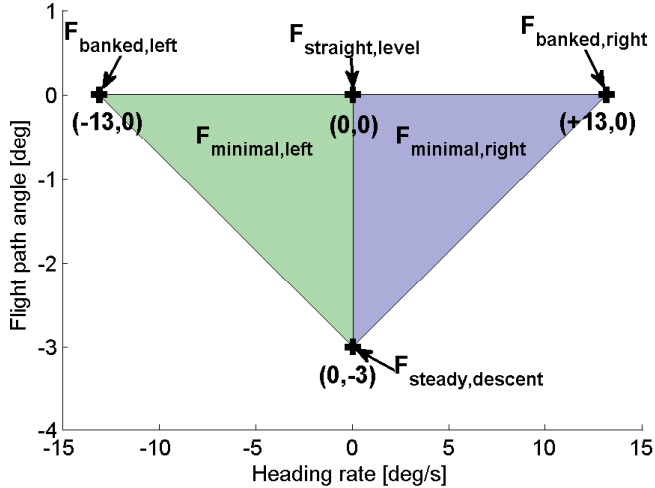Fig. 7. Longitudinal flight envelope in the $F \times E$ plane.

Fig. 8. Minimal flight envelope

For this research, the minimum required turning radius was selected as 87m. This corresponds to a heading rate of $\pm 13°/s$ at a nominal airspeed of $V = 20$m/s. The minimum required flight path angle is chosen as $\gamma = -3°$ since this is representative of typical glide slopes. The four points shown in figure 8 define two triangles: $\mathbb{F}_{minimal,left}$

Table 1. Allowable stuck surface ranges

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]

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 1. 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 $[-25°, +25°]$ 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

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, other events 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 $[l \; u]$ 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 failure is given by summing the contributions for all control surfaces:

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

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:

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

Contrary, false alarms lead to catastrophic failure only outside the allowable range, since the faults inside the range can be tolerated by the controller, even if they come from false alarms. 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:

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

However, dynamic properties of the FDI algorithm like detection time cannot be included in the analysis this way.

The probability of catastrophic failure has been evaluated for the four configurations of the FASER UAV defined in Section 2. Figure 10 shows the probabilities in function of servo MTBF with fixed missed detection and false alarm rates. Figures 11 and 12 show them in function of missed detection and false alarm rate with fixed servo MTBF and fixed false alarm and missed detection rate, respectively. The servo MTBF values for the evaluation are chosen so that they range from a common R/C-grade servo Murtha [2009] to a high-fidelity unit used on large military UAVs of the Secretary of Defense [2003]. The MTBF of high-fidelity servos for small UAVs, like the ones from Volz, are somewhere between these values GmbH [2009]. The missed detection and false alarm rates are chosen to be $P_{MD} = 0.05$ and $P_{FA} = 0.01$ [reference needed]. There is a trade-off between these two properties, i.e. choosing one of them to be smaller increases the value of the other for a given FDI algorithm.

Configuration v3 has the lowest level of reliability, its probability of failure is two magnitudes 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, thus it is an example of an improperly designed architecture. Compared to v3, one servo is used to decouple the ailerons, which extends their allowable range to $[-25°, +25°]$, but the elevator range is only slightly improved which still contributes to system failure. The other two configurations (v2 with 4 servos and v4 with 3 servos) have similar
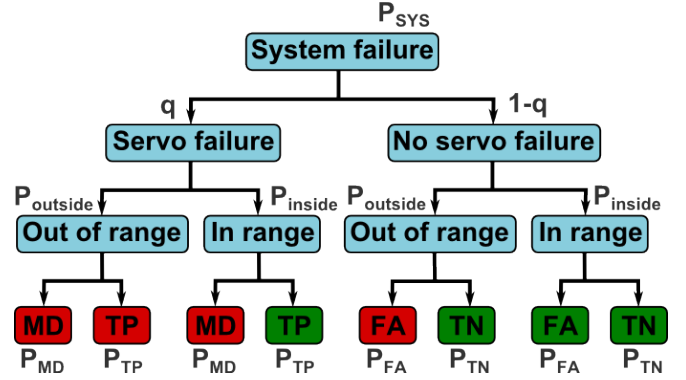

Fig. 9. System level failure as a tree of different events (MD – missed detection, TP – true positive, FA – false alarm, TN – true negative).
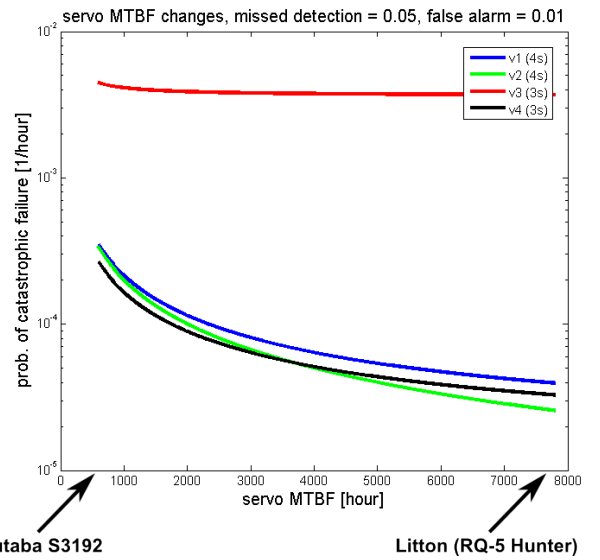

Fig. 10. Probability of failure in fuction of servo MTBF.

reliability, for low servo MTBF v2 is better, but for high MTBF values v4 performs better. This can be explained by the fact that using more servos adds more failure modes to the system, but also have the advantage of adding more options for the reconfigurable controller. This advantage overcomes the effect from increased failure modes as servo quality increases. 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 more servos a configuration has the more its reliability is affected by missed detection rate, as can be seen from the slope of the curves. The effect of false alarm rate can be seen in figure 12. Because the term is proportional to $P_{outside}$, it is most visible on the configurations having the smallest allowable fault ranges (e.g. v3).

6. CONCLUSION

A method has been proposed for the reliability assessment of small scale UAVs based on their actuator architecture, mission profile and on-board control system. The method is introduced using the case study of the FASER UAV, for which four actuator configurations have been analysed.
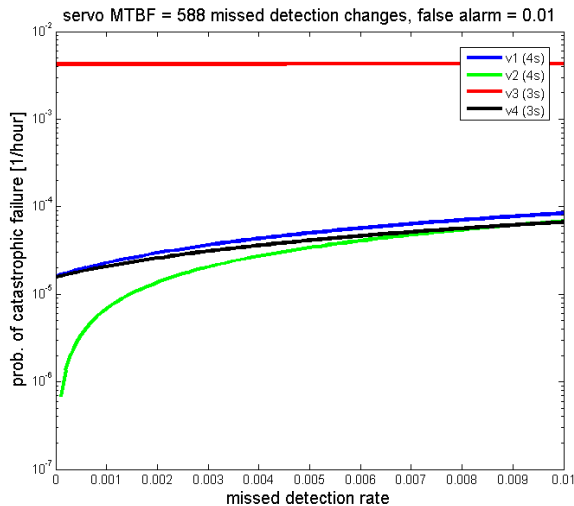
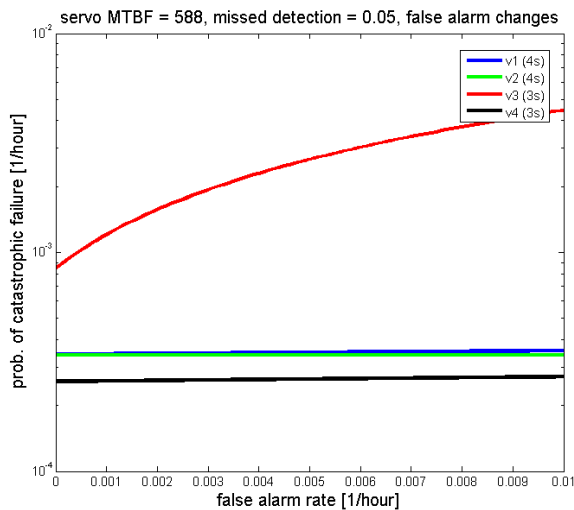Fig. 11. Probability of failure in fuction of missed detection rate.

Fig. 12. Probability of failure in fuction of false alarm rate.

Our goal is to compare not just different actuator architectures of the same aircraft but also designs with different airframes (e.g. a flying wing and a conventional airframe). The wind tunnel tests of a flying wing UAV at UMN (the miniMUTT) is in progress, so its high-fidelity aerodynamic model will soon be available for our studies.

The method can be extended and refined at several points, largely due to the simplifying assumptions made for the initial approach. One obvious extension is the incorporation of motor faults into the analysis. The key assumption that the trimmable region in a flight envelope is the same region where the controller can stabilize the system is a very simplistic one, so our aim is to use a more sophisticated approach for the discovery of flight envelopes in the future. The assumption that the deflection of control surfaces is time-independent also has to be revised and a more rigorous stochastic analysis of the system has to be carried out. Our plans also include the study of control system design in respect to overall system reliability.

REFERENCES

Michael V. Cook. *Flight Dynamics Principles*. Elsevier, second edition, 2007.

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.

Paul Freeman and Gary Balas. Actuation failure modes and effects analysis for a small uav. In *American Control Conference*, Portland, OR, June 2014.

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

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

P. Goupil. Oscillatory failure case detection in the A380 electrical flight control system by analytical redundancy. *Control Engineering Practice*, 18(9):1110 – 1119, 2010.

Garrison Hoe, D Bruce Owens, and Casey Denham. Forced oscillation wind tunnel testing for faser flight research aircraft. In *AIAA Atmospheric Flight Mechanics Conference*, Minneapolis, MN, August 2012. AIAA.

N. Harris McClamroch. *Steady Aircraft Flight and Performance*. Princeton University Press, 2011.

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

Robert C. Nelson. *Flight Stability and Automatic Control*. McGraw-Hill, second edition, 1998.

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

D Bruce Owens, David E Cox, and Eugene 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.

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

James M Urnes, Eric Y Reichenbach, and Timothy A Smith. Dynamic flight envelope assessment and prediction. In *AIAA Guidance, Navigation and Control Conference and Exhibit*, Honolulu, HI, August 2008. AIAA.

Craig Whitlock. When drones fall from the sky. *The Washington Post*, 2014.

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