AIAA AVIATION Forum
5-9 June 2017, Denver, Colorado
17th AIAA Aviation Technology, Integration, and Operations Conference

Failure Mode Effects Analysis and Flight Testing for Small Unmanned Aerial Systems

Louis J. Glaab[1] and Michael J. Logan[2]
NASA Langley Research Center, Hampton, VA

The Unmanned Aerial Systems (UAS) Traffic Management (UTM) project is working to provide a structure for small UAS (sUAS) operations and provide air traffic management and information services in support of future envisioned sUAS operations. One primary aspect of the UTM project is the development of the UTM server that sUAS operators would interface with to perform their missions. Another aspect of the UTM project is to perform research and analysis towards the development of sUAS vehicles that could safely operate in the UTM system. These vehicles would be required to operate beyond visual line of sight (BVLOS) of the operator, be capable of allowing one operator to operate multiple vehicles, perform missions in low- and high-density populated areas and operate in areas with significant manned aircraft activity. The risk of these sUAS operations needs to be acceptable to the general public.

In order to help focus sUAS research efforts (both for the UTM project and potentially others), a Failure Mode Effects analysis (FMEA) of representative sUAS vehicles was performed. FMEAs are performed by gathering together subject matter experts (SMEs) regarding the vehicle systems and proposed operations to determine a list of credible failures, their effects, and mitigation strategies. One objective was to comprehensively define, to a preliminary design level, commercially viable sUAS. Another objective was to define the failure modes for these vehicles. A third objective was to categorize those failure modes to determine areas where further testing and analysis could effectively mitigate the risk from sUAS/UTM operations. Flight tests of representative platforms are also discussed.

Nomenclature

BVLOS	=	Beyond Visual Line of Sight
EFC	=	*Effects of Failure Categorization*
FMEA	=	Failure Modes and Effects Analysis
GCS	=	Ground Control Station
sUAS	=	Small UAS, generally considered as under 55lbs.
UAS	=	Unmanned Aircraft System
IMU	=	Inertial Measurement Unit
UTM	=	UAS Traffic Management
WOT	=	Wide Open Throttle
V/TOL	=	Vertical Take Off and Landing

I. Introduction

The integration of sUAS into the National Airspace System is desirable for a variety of reasons including economics, public safety, and others. To facilitate this valuable integration, NASA's UTM program seeks to

[1] Assisstant Branch Head, Aeronautics Systems Analysis Branch, Member.
[2] UTM Off-Nominal Flight Test Principal Investigator, Aeronautics Systems Analysis Branch, Senior Member.

develop enabling technologies, primarily air traffic management concepts and services for low-altitude BVLOS flight[1]. Concurrent with these developments, risk-based safety analysis is being conducted to ensure that the level of risk, and subsequent requirements, is commensurate with the intended flight operations. For example, there may be a higher level of requirements imposed on the sUAS system for operations in dense, urban areas over people than those which would be expected for a rural agriculture operation.

An FMEA was undertaken to begin to identify, and to the extent possible, quantify the level of risk associated with various types of system, subsystem, and component failures. Results from the FMEA were then used to identify areas which necessitated further analysis and/or actual flight testing. This report describes the initial FMEA results and then describes the novel test method employed to evaluate an array of failure scenarios that are significant for sUAS operations.

II. Failure Modes and Effects Analysis

Failure Mode Effects Analysis (FMEA) is a highly-structured, systematic technique for performing failure analyses. It is nominally one of the first steps performed in a system reliability assessment as discussed in Reference 2. One of the first steps in an FMEA is to break the system down into a manageable number of subsystems. Each subsystem is then evaluated to determine both its likely failure modes, and probabilities of failure, and how they propagate into the system under evaluation. For this effort, an initial FMEA was performed to analyze sUAS vehicles envisioned for UTM applications. One objective of the FMEA effort was to define areas where more analysis and/or testing were required.

Vehicles considered for UTM operations were assumed to have the following characteristics: 1) In general vehicles were assumed to be well under 55 lbs (more like 25 lbs), 2) Be able to transport some significant amount of payload (such as 5lbs), 3) Be relatively low cost per unit, such as $20k to $40k, 4) Operate beyond visual line of sight, 5) Have a range of up to 10 miles, but can vary, 6) Have an endurance of up to approximately 60 minutes, 7) Be able to operate autonomously for short periods of time (on the order of several minutes) and 8) Perform self-separation from cooperative targets. These vehicle characteristics were assumed in order to satisfy envisioned safety and societal acceptance of sUAS vehicles operating in close proximity to the general public while still performing economically-viable functions.

Table 1 provides a listing of the vehicle sub-systems considered for the FMEA effort. A group of subject matter experts were assembled in the areas of navigation, sensors, automation, operations, structures, propulsion, aerodynamics, communications and stability and control. For each sub-system the team was asked to: 1) Identify failure modes and probabilities of the failure modes for each of the sub-systems listed, 2) Define the effect of the failures that were considered to be greater than Extremely Unlikely as defined in Table 2, and 3) Categorize those effects into one of several categories.

Table 1. Subsystem Definitions for generic sUAS.

#	Name	Function
1	Structure	Hold everything together
2	Battery	Power everything
3	Motors	Provide lift, control effectors
4	Autopilot	Provides control inputs, integrate sensor input, manages flight path
5	GPS	Provides primary position information
6	Gyros	Provides attitude rate info
7	Accelerometers	Provides attitude info
8	Wires	Connect avionics

9	Connectors	Connect avionics
10	Camera	Surveillance, S2D
11	ADS-B	Airtraffic SA
12	Payload	Provide business case
13	Telemetry	Provides communication to/from vehicle
14	ESCs	Control motors
15	Servos	Articulate aerodynamic control surfaces

The failure categories were defined as: 1) having only small effects (Ratings 1 through 3 in Table 3) with low uncertainty, 2) same as 1 but with high uncertainty, 3) significant effects (Ratings 4 and 5 in Table 3) with low uncertainty, and 4) same as 3 with high uncertainty. Failure categories with low uncertainty and low-impact were not considered for further analysis or testing. Failure categories with significant effects and low uncertainties were considered to be potential enginnering and design challenges for future research and development. Failure categories with significant effects and high uncertainties were used to define high-priority test conditions for the current effort.

Table 2. Likelihood of failure occurence definitions.

Rating	Meaning
A	Extremely Unlikely (Virtually impossible or No known occurrences on similar products or processes, with many running hours)
B	Remote (relatively few failures)
C	Occasional (occasional failures)
D	Reasonably Possible (repeated failures)
E	Frequent (failure is almost inevitable)

Table 3. Effects of failure categorization.

Rating	Meaning
I	No relevant effect on reliability or safety
II	Very minor, no damage, no injuries, only results in a maintenance action (only noticed by discriminating customers)
III	Minor, low damage, light injuries (affects very little of the system, noticed by average customer)
IV	Critical (causes a loss of primary function; Loss of all safety Margins, 1 failure away from a catastrophe, severe damage, severe injuries, max 1 possible death)
V	Catastrophic (product becomes inoperative; the failure may result in complete unsafe operation and possible multiple deaths)

During the analysis, there were several types of failures for which the resulting effects were not known, or were not known to any degree of certainty quantitatively. For example, the effects of motor failures for multi-rotors was one failure area with both significant potential effects and a high degree of uncertainty. Control surface failures for fixed-wing aircraft with redundant control surfaces (i.e. dual elevators) were categorized similarly. As such, a series

of flight experiments were conducted to obtain quantitative data on specifc types of failures and other types of off-nominal conditions over a broad range of potential sUAS types.

III. Off-Nominal Flight Test Experiments

The UTM Off-Nominal Flight Exeriments were envisioned as a way to quantify the actual effects of failures on the ability of sUAS to operate under off-nominal conditions, primarily component or subsystem failures. The expectation is that if a broad enough range of representative platforms and component/subsystem types are studied, more broad conclusions can be drawn which would influence future system designs to make for more robust, and ultimately, more safe sUAS for BVLOS operations. Further, having these effects carefully implemented and comphrehensively documented for representative mission task elements allows for a more "real-world" determination of failure hazards.

A. Description of representative test platforms

Three representative platforms were chosen for the first round of flight test experiments. These sUAS platforms were modified to allow for simulating a failure under controlled circumstances. For multi-rotor type sUAS, provisions were made to be able to switch the throttle signal going to one of the rotor motor controllers to a value selectable by the radio-control transmitter. This allowed for the test to simulate both a complete failure of a rotor simulating loss of motor controller, motor failure, power wires/connectors, or prop failure, and a "partial" failure simulating a control signal issue where the control signal pulse width modulation to the motor controller is frozen via a "hold last valid setting" by the motor controller. In the case of fixed-wing sUAS, provisions were made to be able to fail control surfaces (e.g., right aileron, right side elevator, and rudder) at selectable positions to simulate a servo failure or a mechanically jammed control surface. In addition, the fixed-wing vehicle was outfitted to incorporate the ability to selectively disable the on-board GPS.

All three platforms used the Pixhawk autopilot as being representative of the types of autopilots currently being used by industry. For these tests, the current stable releases of the flight software were used, Arducopter V3.5 for the multirotors, Arduplane 3.7 for the fixed-wing.

1. Flight Test Approach

A series of flight test scenarios were developed to assess failure responses for the three different platforms. For the multi-rotors, two likely failure scenarios were developed, one where the vehicle is in a stable hover and the other where the vehicle was navigating a constant altitude waypoint pattern. In these tests, the throttle settings used included nominal hover, +/-25%, +/-50%, -75%, and -100% (i.e., full off). Note that during testing, it was determined for both types of multi-rotors that a +50% throttle setting or above was unrecoverable in hover.

For the fixed-wing platform, scenarios were developed that required the vehicle to fly a constant altitude rectangular box patter. Control surface failures included neutral, positive and negative deflections. Additionally, the on-board GPS would be selectively disabled during a waypoint following function. For both the multi-rotor and fixed-wing aircraft testing was conducted in a deliberate build-up approach. The magnitude and severity of the failures were incrementally increased until the vehicle could no longer perform its mission (i.e. hover or waypoint flight for the multi-rotors, waypoint flight for the fixed wing, respectively) or a loss of control.

Figure 1 shows one of the multi-rotors referred to as "Y-6-2". This vehicle weighs approximately 4.6lbs. and is approximately 18" in diameter. It is a 3 arm configuration with motors on both the top and bottom of each arm. The motor selected for "failure" was the top right motor. The standard open-source Arducopter airborne software was used "out of the box" with no tuning specific to the platform.

Figure 1. Y-6-2 sUAS Configuration.

Figure 2 shows the second multi-rotor, a Tarot X6, used in the experiments. This vehicle weighs approximately 10.5lbs. and is roughly 40" in diameter. The motor selected for the "failure" was the right center motor. The vehicle also had a video camera and transmitter which was downlinked to the ground control station (GCS). Again, the Pixhawk installed used the standard open-source software for the autopilot functions.

Figure 2. Tarot X6 sUAS configuration.

The fixed-wing sUAS is shown in Figure 3. It is a former U.S. Army target drone converted to have an autopilot, landing gear, and back-pointing camera to obtain visual control surface deflections. Flight weight for the vehicle was approximately 19lb. A multiplexer was installed which allowed for selection of the control surface failure setting via the radio control transmitter. In addition, a GPS power relay was installed to enable the ability to cut power to the GPS module, observe the response, and restore power to the GPS. The Pixhawk open-source airborne software suite was used and only "tuned" well enough to follow a waypoint pattern reasonably accurately.

Figure 3. Modified FWM-117B sUAS named MigLH.

B. Descriptions of tests conducted

Tests were conducted on both the multi-rotors and the fixed-wing sUAS. For the multi-rotors, throttle changes ranging from -100% (full off) to +100 (WOT) were planned. During the testing, it was found that neither multi-rotor could recover from a +50% or higher off-nominal condition so testing was limited to a range of -100% to +25% throttle setting. For the fixed-wing aircraft, tests were planned for each type of control surface (aileron, elevator, rudder) of stuck neutral, stuck full up and full down, and +/- 25% and +/-50%. In addition, a test to assess the robustness of the navigation algorithms were conducted via selective failure of the GPS unit. Table 4 shows the initial starting plan for the flight tests. The progression of failures was designed to start at the most benign case (neutral trim value) and progressively increase the failure to define an envelope of tolerable failures.

Table 4. Flight Experiments Conducted.

Flight Experiment Schedule					
Flt #	Vehicle	Total Time	Mode	Fail setting	Failure PWM
1	Y-6-2	9	Loiter	Mid	1525
				Mid-25%	1401
				Mid+25%	1687
				Mid-50%	1292
				Mid+50%	1710
				Mid-75%	1202
				Mid+75%*	Not Flown
				Mid-100%	1130
				Mid+100%*	Not Flown
2	Y-6-2	10	Auto	Mid	1525
				Mid-25%	1401
				Mid-50%	1292
3	Y-6-2	10	Auto	Mid-75%	1202
				Mid-100%	1130
				Mid+25%	1687
4	Tarot X6	9	Loiter	Mid	1468
				Mid-25%	1320
				Mid+25%	1565
				Mid-50%	1275
				Mid+50%	1664
				Mid-75%	1250
				Mid+75%*	Not Flown
				Mid-100%	1131
				Mid+100%*	Not Flown
5	Tarot X6	10	Auto	Mid	1468
				Mid-25%	1320
				Mid-50%	1275
6	Tarot X6	10	Auto	Mid-75%	1250
				Mid-100%	1131
				Mid+25%	Not flown
7	MigLH	12	Auto	Check Flight	Check Flight
8	MigLH	12	Auto	Aileron fail - neutral	1503
				Aileron fail +25%	1621
				Aileron fail -25%	1389
				Aileron fail -75%	1259
				Aileron fail -100%	1130
10	MigLH	12	Auto	Rud fail - neutral	1502
				Rud fail +25%	1629
				Rud fail +50%	1743
				Rud fail +100%	1878
11	MigLH	12	Auto	Elev fail - neutral	1505
				Elev fail -25%	1330
				Elev fail +25%	1658
				Elev fail -50%	Not flown
				Elev fail +50%	1752
12	MigLH	10	Auto	GPS power fail	n/a

C. Preliminary Results and discussion

The two multi-rotors tested had very similar response characteristics even though they are physically different. Both multi-rotors had little difficulty maintaining a stable hover when the failed motor was at the nominal hover setting and didn't respond to autopilot commanded throttle changes. As can be seen in Figure 4, the response to a nominal hover throttle "failure" had little impact on the ability to station keep a stable hover. However, as the throttle setting decreased, the resulting pitch and roll response became much more dynamic. The upper plot in Figure 4 represents the step failure trigger (red) and the failure throttle setting (green). The lower plot shows the vehicle's response to the step changes in throttle setting resulting from the failures. Failures in the positive direction (throttle setting above nominal hover) were more dramatic with the +50% and higher resulting in the inability of the autopilot to recover a stable hover.

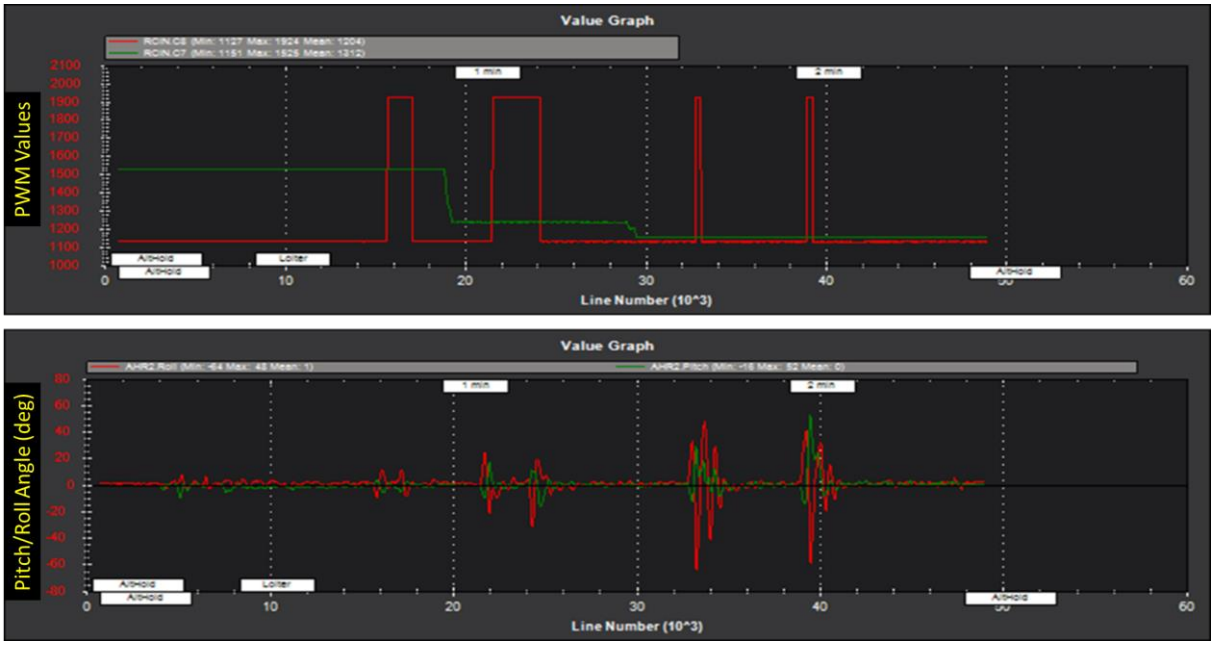

Figure 4. Pitch and roll response to step motor throttle setting changes for Y-6-2.

The Tarot X6 sUAS exhibited similar responses to failures. As can be seen in Figure 5, a total shutdown of one of the rotors is quite rapid with the opposing rotor throttle setting being decreased (but not turned off) by the autopilot to compensate. As was seen with the Y-6-2, the vehicle was able to regain a stable hover but was unable to navigate to any significant degree. Figure 6 shows the waypoint path of the Tarot X6 with the rotor failure occurring on the left straight leg. Notice that while the vehicle was able to progress in a more-or-less straight line, the vehicle could not navigate the corner and was unable to continue the mission.

Figure 5. Tarot X6 in Hover with Right Center Motor Shut Down.

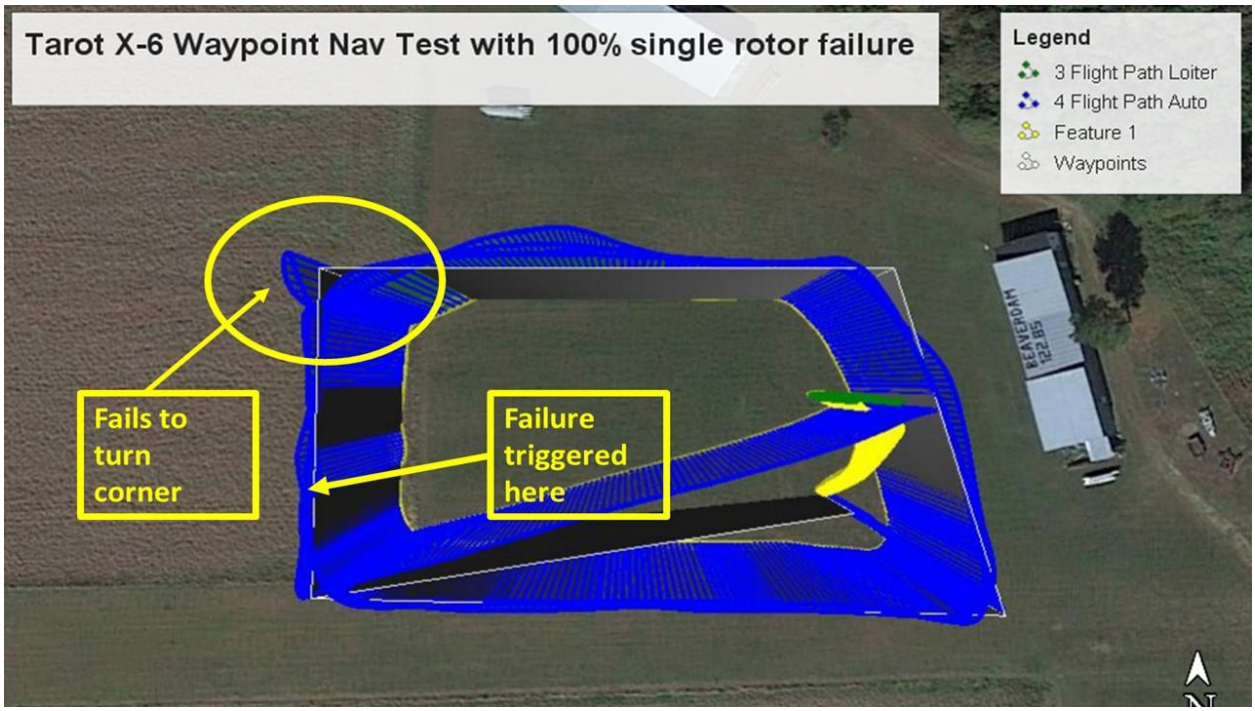

Figure 6. Tarot X6 Waypoint Navigation with Rotor Failure.

In the case of the fixed-wing sUAS, the vehicle had less difficulty with an aileron failure than with elevator failure. As can be seen in Figure 7, a neutral failure is indistinguishable from nominal operation. Navigation with +/- 25% shows some deviation from the intended path but the vehicle recovers. Note that the aileron failure is actually only applied to the right aileron.

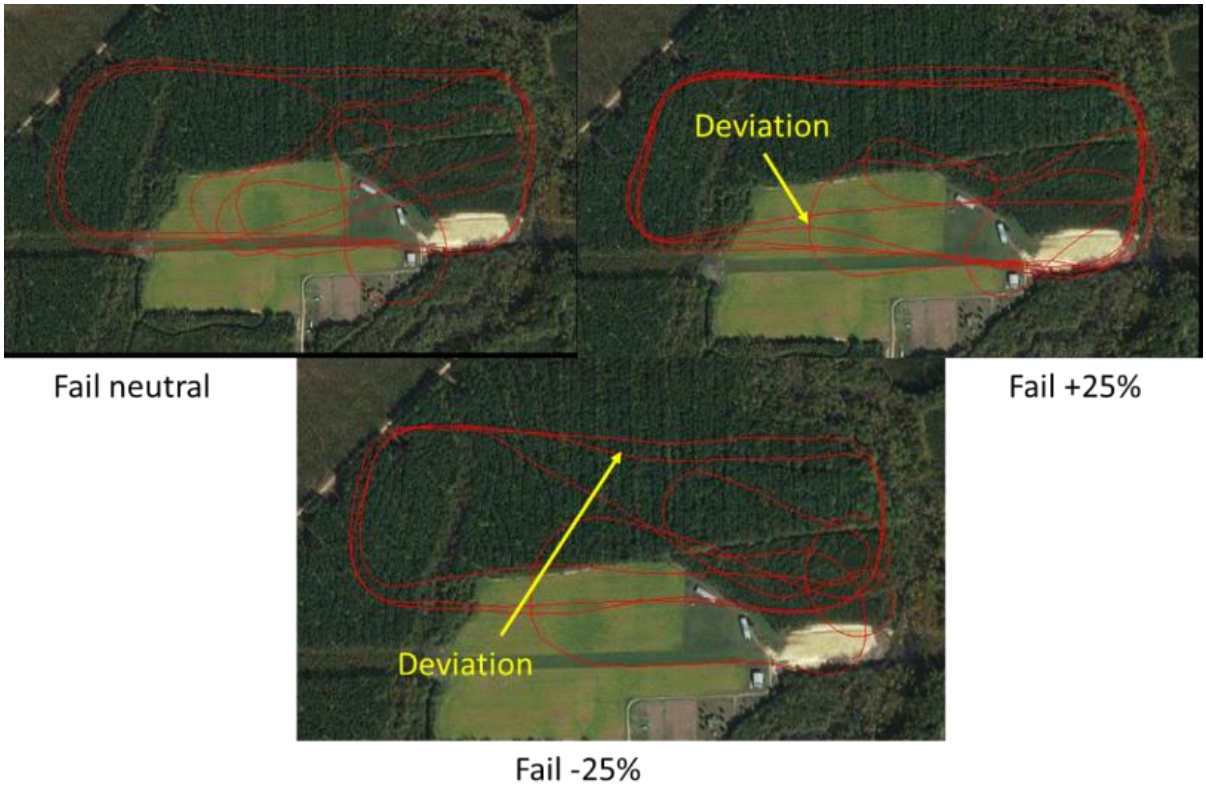

Figure 7. Waypoint Navigation with Neutral, +25%, and -25% right aileron deflection.

Based on the testing done, as the deflection of the failed aileron approaches full, either +100% or -100%, the vehicle can more or less hold a straight line but slowly loses the ability to negotiate a turn. To determine what happens in the event of one of two ailerons failing, we can look at how the autopilot responds. Figure 8 shows when the right aileron is failed (red line going from bottom to top), the autopilot shifts to a bias in the aileron command (blue line). The larger the off-nominal deflection of the failed aileron, the greater this bias becomes. Clearly, at the limit, the non-failed aileron will become saturated and the vehicle will only be able to make proverse turns or the rudder will have to be sized to provide directional control in the event of a full-deflection aileron failure.

Figure 8. Autopilot Aileron Response to Varying Aileron Failure Settings.

Elevator failures exhibit similar, if not more pronounced, effects. Figure 9 indicates that when half the elevator is failed in the neutral position (blue line), the remaining elevator is able to maintain flight path. As the failed elevator deflection is raised or lowered from nominal, the autopilot applies a bias to the commanded elevator output (red line). The green line on the plot shows the failure "trigger" when the value goes from low to high. Comparison of the blue line (failure command) with the red line (autopilot elevator command) indicates the level of commanded failure. Similarly, in subsequent tests were conducted, half the elevator was set to full up elevator, the remaining elevator was set by the autopilot to full down, the airspeed declined precipitously, the throttle was essentially shut off, and the vehicle eventually recovered level flight just above stall speed. Full down elevator failure resulted in the inability to recover. Maximum down aileron failure resulted in the vehicle still being able to navigate, albeit at a degraded capability, around the waypoint pattern. Maximum rudder failures resulted in a significant sideslip however, the vehicle was able to navigate, but to a very degraded level. Of all the failures, down elevator was the most severe with the vehicle unable to tolerate anything greater than 25% down.

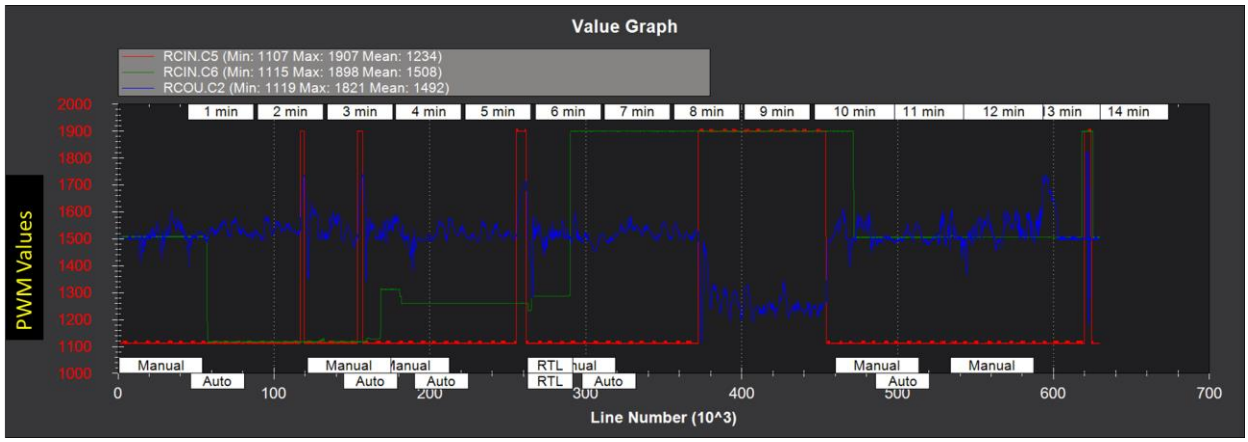

Figure 9. Autopilot Elevator Response to Varying Elevator Failure Deflections.

Investigating the effects of GPS failure produced some interesting results, some expected, some unexpected. When the GPS failure is initiated, power to the GPS unit is turned off which results in an immediate loss of the GPS solution. Figure 10 shows that when the GPS unit fails (upper plot), the vehicle became distressed almost immediately. As a result, the vehicle pitches over and begins to descend (lower plot). Since the thinking a-priori was that the autopilot would continue normally for some period of time using its IMU solution in a "dead reckoning" mode, this was an unexpected result.

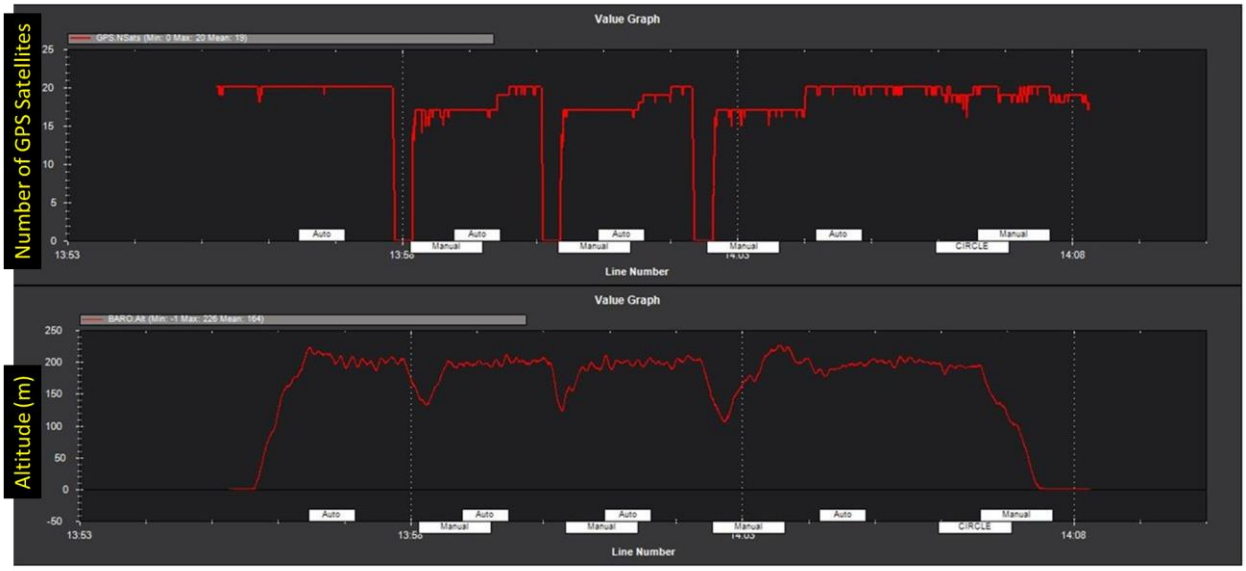

Figure 9. GPS Failure Effect on Altitude.

One additional result that was determined during the testing was that the power to the external magnetometer comes from the power the GPS is using. So, when the GPS power was cut, the external compass also failed. There was little difference between the internal compass being "primary" vs. the external compass being "primary" since the end result was virtually identical – loss of GPS means nearly immediate vehicle distress. In future tests, it may be possible to isolate power to the external compass such that a GPS failure can be induced without losing one of the two compasses. Robust power distribution should also be a design consideration for future system developers.

While power loss to the GPS unit is an unlikely failure mode, the loss of a GPS solution is not and can be caused by a number of factors, such as solar flares, electromagnectic interference in the aircraft, multi-path GPS signals, etc. Having redundant GPS units on-board and a more robust "dead reckoning" ability in the event of total GPS loss should be considered mandatory for sUAS planning BVLOS operations.

Future flight tests would be focused on improving the understanding of the internal details of these and other failures and their effects, some of which are currently ill-understood. These tests could also include testing the ability of vehicles, both fixed and multirotor, to make a safe descent and landing in the presence of various failures as would be required in an emergency. Similarly, determining a method that could be used to navigate in the presence of failures, especially for the multi-rotors, will be key in making a safe return in the event of a major failure. In addition, more vehicle types such as octocopters, helicopters, lower drag fixed-wing vehicles, and hybrid V/TOL vehicles should be studied to see if there are generic trends common to all different types of sUAS and which failures cause issues which might be unique to a given type of platform. Finally, additional work is being planned to provide recommended "best practices" for improving the safety, reliability, and robustness of sUAS

IV. Conclusions

The testing of a an array of sUAS platforms provided insight into possible failure modes and their effects. Results from an intial FMEA performed on envisioned sUAS vehicles performing UTM-defined missions provided insight into a range of potential vehicle responses to potential failiure modes. Selected failure modes with significant consequences and uncertainties were selected for an intial off-nominal flight test. Preliminary results from recent flight test experiments indicate that for multi-rotors with six rotors:

- Failure of a rotor on a hexacopter does not automatically cause a complete loss of control in hover and straight-line flight unlike quadcopters where previous flight experience has indicated departure from controlled flight in the event of a rotor failure.
- Failure of a single rotor in hover may allow for a descent and landing in place and confirms this failure to be have a failure effect categorization (EFC, from Table 3) of 2.
- However, failure of a single rotor drastically diminishes the ability of the multi-rotor to turn and navigate in general with a EFC of 5, much higher than originally anticipated.
- More robust resilience to single rotor failures will be needed to allow multi-rotor sUAS to operate BVLOS over people (or an increase in the number of rotors required with the consequent reduction in endurance).

For fixed-wing platforms, the following can be observed:

- Failure of individual control surface servos (assuming redundant servos) in a neutral position are generally not noticeable and are recoverable without significant impact on maneuverability confirming an anticipated EFC of 2.
- Failures around a small band of neutral/trim can be tolerated by the basic autopilot design tested for pitch, roll, and yaw control surfaces that remain within the EFC of 2.
- Failure of one of two control surfaces to its maximum extent can create an inability to navigate and possibly to maintain control of the vehicle resulting in a EFC of 5.
- The most severe failures were down elevator commands.
- Preventing the failure of a control surface to lock at its maximum extent should be considered mandatory for a robust sUAS.

In the case of GPS, preliminary findings are that:

- Failure or loss of GPS for more than brief periods will cause the IMU solution to degrade very rapidly with today's autopilots, EFC of 5.
- Redundant GPS units should be considered mandatory for sUAS operating BVLOS.
- More robust intermittent GPS methods of navigation should be considered a requirement for BVLOS operation of both fixed-wing and multi-rotor platforms.

In addition, autopilot sensor systems should be designed such that a failure of one sensor will not impact the remaining sensors. More failure tolerant power distribution approaches should be considered.

The demand for the ability of sUAS to operate beyond visual line-of-sight will continue to grow exponentially. However, consideration must be given to the likely failure modes, mitigations for those failures, and overall safety improvement of sUAS before routine BVLOS operations will be enabled.

References

[1]Kopardekar, Parimal, etal, "Unmanned Aircraft System Traffic Management (UTM) Concept of Operations", AIAA 2016-3292, 16th AIAA Aviation Technology, Integration, and Operations Conference, 13-17 June 2016, Washington, D.C.

[2]Hayhurst, Kelly J etal, "Preliminary Considerations for Classifying Hazards of Unmanned Aircraft Systems", NASA/TM-2007-214539, February 2007.