AIAA 2013-4761

Guidance, Navigation, and Control and Co-located Conferences
August 19-22, 2013, Boston, MA
AIAA Guidance, Navigation, and Control (GNC) Conference

Qualitative Failure Analysis for a Small Quadrotor Unmanned Aircraft System

Isaac J. Olson[1] and Ella M. Atkins[2]
University of Michigan, Ann Arbor, Michigan, 48109

As Unmanned Aircraft Systems (UAS) become more prevalent, their safety and integration into the National Airspace System has become a topic of much debate. Current regulations are difficult to apply to UAS, particularly small UAS for which development, certification, and production costs must be kept at a minimum to remain competitive. This prohibits the use of triple or even double redundancy in their designs and limits the amount of validation and verification the developers may perform. Proper identification and analysis of the risks these systems pose is important to determine their level of safety and the potential consequences of system failures. This paper presents a failure analysis for the Michigan Autonomous Aerial Vehicles team's quadrotor UAS as a potential first step in understanding risks which in turn can inform any safety certification process for small quadrotors. Failure modes were identified by keeping flight logs and data over all of the team's 1000+ indoor flight tests in 2012. Causes and results of each failure mode were determined and methods to mitigate the failures were considered. This process has increased the safety of the MAAV vehicle suite and is being used in ongoing work to develop a quantitative probabilistic risk assessment capability.

I. Introduction

Unmanned Aircraft Systems (UAS) have become increasingly popular platforms and are essential for our economic competitiveness. A major challenge is to characterize their potential to pose risk to people and property as a precursor to civil UAS certification and deployment on a broad scale. Many of the commercial applications such as structural inspection or law enforcement support would require the UAS to fly over populated areas and interact with other aircraft. However, before UAS may safely be integrated into the National Airspace System (NAS), proper measures must be taken to ensure the UAS are not endangering persons or property in their vicinity, especially because average number of failures per flight hour tend to be much higher with UAS than with manned aircraft.[1] Although not regulated by the Federal Aviation Administration (FAA), indoor flight for surveillance/monitoring applications also has the potential to introduce risk of harm, particularly if the vehicle is not well-maintained or well-constructed and the operator is not vigilant with respect to safety. In the NAS, the ability to "sense and avoid" other air traffic is an important standard to achieve.[2,3] Developing common regulations and operational protocols required for safe operations of these systems can be difficult because of the large variety of UAS types, sizes, and flight profiles.[4,5,6] The paradigm shift from protecting onboard occupants to those on the ground and in other aircraft also introduces regulatory challenges. Large UAS may be regulated similarly to manned aircraft, but Small UAS (SUAS) are typically not able to meet stringent regulatory requirements such as triple redundancy because of their small weight, volume, and the need to minimize costs.[7,8] Therefore identification and analysis of the risks associated with each UAS class is of paramount importance.

This paper identifies and analyzes the risks of the Michigan Autonomous Aerial Vehicles (MAAV) team's quadrotor SUAS. MAAV competes in the International Aerial Robotics Competition (IARC), which presents a unique challenge in all areas of UAS design, fabrication, control, and automation. The ongoing mission is to fly a SUAS into an unknown building, recognize signs to locate a specific room, find and retrieve a flash-drive in the room, drop off a decoy flash drive, and exit the building in under ten minutes while remaining undetected and avoiding all obstacles. In addition, the vehicle is limited to 1.5 kg and must be able to fly through a 1.0 m by 1.0 m window. To overcome this challenge, MAAV has created a custom quadrotor with a robust attitude controller as well as navigation and path planning software.

[1] Undergraduate, Aerospace Engineering, 1010 E. Ann Street, AIAA Student Member.
[2] Associate Professor, Aerospace Engineering, 3056 FXB, 1320 Beal Ave, AIAA Associate Fellow

This paper is organized as follows. An overview of the quadrotor design developed by the MAAV team is given in Section II. Identified failure scenarios are described in Section III, while the risks posed by loss of control are given in Section IV. Conclusions and future work are provided in Section V.

II. MAAV Quadrotor Small UAS

The IARC poses a number of design constraints on the quadrotor, some explicit and others implicit. The competition rules dictate that the vehicle have gross weight not exceeding 1.5 kg and must fit through a 1.0 m by 1.0 m window to autonomously enter and exit the competition course. The vehicle must carry all of the sensors necessary to complete the mission autonomously as well as sufficient stored energy to fly for the duration of the mission (limited to 10 minutes). Thus, the vehicle must have a low unburdened mass with high payload capacity. Minimizing the mass is therefore one of the main design drivers for the airframe. Additionally, because of the space requirements, MAAV integrates custom circuit boards onto the airframe to accommodate the necessary electronic components as compactly as possible.

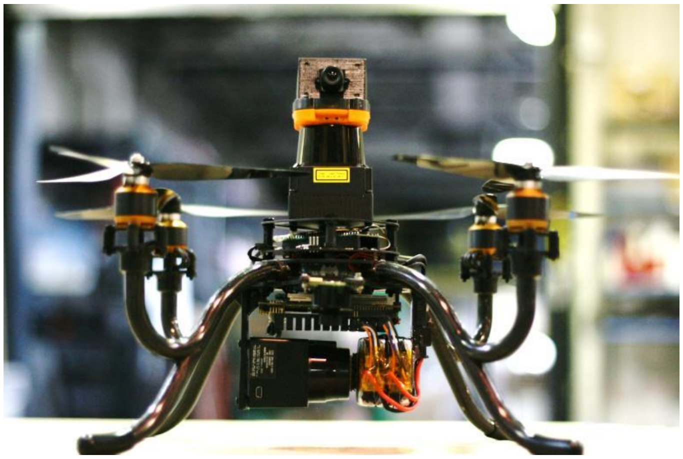

Figure 1: MAAV Quadrotor Small UAS

A. Airframe

The 2012 competition vehicle, as seen in Figure 1, features all the components necessary to complete the mission with a mass of only 1.35 kg, which meets the IARC mass constraint. The airframe is constructed with a center aluminum ring and four shaped carbon tubes that serve as both landing gear and motor supports. These tubes are fastened to the aluminum with a high strength, composite-to-metal epoxy. This airframe is cheap and easy to fabricate, costing only around $20 and producible in about five hours of work spread across three days due to epoxy dry time requirements. The frame is capable of withstanding most impacts that occur during testing, but in the event of a severe crash, the inexpensive carbon arms fracture and absorb most of the impact while saving the more expensive payload. After such a crash, components can easily be swapped to a new airframe and the vehicle can be ready to fly again after only a few minutes.

B. Power Supply and Propulsion

The vehicle is powered by a single three cell, 11.1 V lithium polymer battery pack. This battery has a capacity of 4000 mA hours and can operate the four vehicle motors at typical flight speeds for about 15 minutes. The quadrotor's propulsion system consists of four Axi-Gold 2212/26 Motors with nine inch, three bladed propellers that are capable of providing around 35 N of total thrust, equivalent to lifting about 3.5 kg on Earth. This provides sufficient power to adequately maneuver without going beyond the motor's ideal rpm range. The motors are each controlled by a Castle Creations Phoenix-25 Brushless Motor Controller, which allows for the rapid changes to motor rpm necessary for quadrotor flight.

C. Circuit Boards and Processing

The vehicle has a custom circular printed circuit board located on top of the center aluminum ring. The board handles power distribution to motors and supports the sensors and processors. Onboard processing is performed by a 720 MHz Gumstix Overo Fire Computer-on-Modules and a 1.1 GHz dual core Intel Atom Pico ITX. The Gumstix runs control loops and sends commands to the motor controllers while the Atom is dedicated to running a

Simultaneous Localization And Mapping (SLAM) algorithm to build a map and send laser and camera information back to the ground station.[9] The avionics architecture is illustrated in Figure 2.

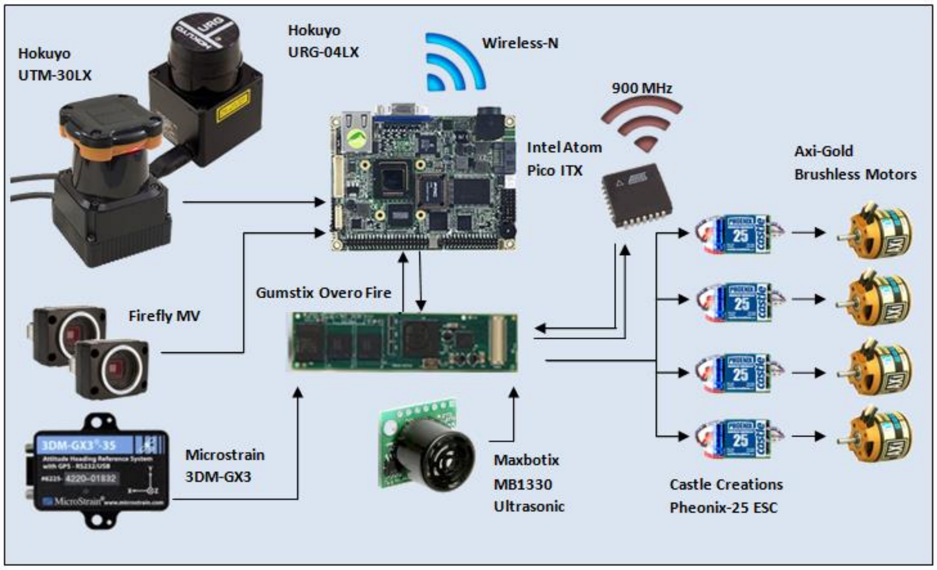

Figure 2: MAAV system architecture

D. Sensors

In order to maintain stability and complete mission tasks, the quadrotor requires real time data about its state and its environment. Onboard sensors were selected for the quality and rate of the data provided. Attitude data including the vehicle's attitude and angular rates is gathered by a Microstrain 3DM-GX3-25 Attitude and Heading Reference System (AHRS). The AHRS provides pre-filtered data at 125 Hz that feeds directly into the control loops to stabilize the vehicle. Data for outer loop position control is gathered by a Maxbotix MB1330 ultrasonic sensor for height data, a Hokuyo UTM-30LX laser range finder for horizontal plane localization and mapping, and a Hokuyo URG-04LX laser range finder for vertical plane obstacle detection. The ultrasonic sensor is managed by an Atmel ATtiny84 which communicates to the Gumstix via I2C. The ultrasonic sensor has a maximum range of about 20 feet with a data rate of 10 Hz. The horizontal laser range finder provides 1080 ranges at 40 Hz over a 270 degree field of view with a maximum range of 30 m, storing these distances as floating point numbers. This data is processed on the Atom and converted to a map with the vehicle's location and obstacles in the area. These scans are also sent to the ground station to construct a global map and correct the position estimate obtained from onboard calculations. The vertical laser range finder functions similarly to the horizontal one, but only returns 520 points at 10 Hz with a maximum range of 4 m, as map-building is emphasized in the lateral (horizontal) plane and data pipelines are constrained. In addition to stability and localization sensors, the quadrotor uses two 752x480 resolution Point Grey Firefly MV Cameras to detect the Arabic signs and flash drive specific to the IARC.

III. Identified Failure Scenarios

An important first step in the risk analysis process is identifying the potential failure modes of each subsystem. This will not only help identify areas of the system that might need extra safety features but also will enable operators of the vehicle to diagnose problems that occur during testing. Ideally, after identifying the failure modes of a given system, the developers will be able to improve the system to bring the probability of those failures below an acceptable threshold. This may not always be possible, especially with a SUAS where adding redundancy may not be an option due to mass/cost restrictions. However, knowing the potential failures of a system will still help developers identify potential methods to mitigate the results of one of these failures and will help in the analysis of risk and safety for vehicle certification purposes.

Some failure modes are fundamentally hardware-related while others are fundamentally software-related; others can emerge as a combination of factors, e.g., when a hardware anomaly uncovers a software problem. Additionally, a possible mitigation for a hardware failure mode may be a software modification and vice versa. Thus it is critical to consider both aspects of the system when identifying both failure modes and the methods to mitigate them.

By analyzing flight logs and data of the MAAV team's tests over 2012, the observed failure modes of its subsystems have been compiled along with their causes, results, and possible risk mitigation methods. This paper presents the results of this analysis. While this work does not represent the exhaustive list of possible failures for the entire system, it does incorporate failure modes that have been observed when testing the system as well as others that have been identified as possible. Primary classes of failures for the small quadrotor UAS operating with the sensors described above are presented below and are organized by subsystem.

A. Height Sensor Failure Modes

Loss of valid return from the height sensor happens under well-known circumstances and can cause the vehicle to become unstable in vertical (z) axis motion which introduces the potential for loss-of-control (LOC). For constrained indoor flight, an LOC event inevitably results in a very near-term impact. If detected, the operator or automation can kill thrust which minimizes risk imposed by rotating blades and kinetic energy build-up due to LOC. The goal therefore in the small quadrotor with single-string sensors and actuators is to first maximize reliability and robustness of hardware and software, and second to ensure that the failure, if detected, introduces acceptable risk. Although relevant for height sensor failure, this discussion of LOC is general to all failures with potential to induce LOC.

Failure modes, their causes, and their effects are summarized below in Table 1. The ultrasonic sensor will return erroneous data if the vehicle flies above the maximum range of the sensor, if the vehicle pitches sufficiently for the sensor's cone to not include the ground directly below it, or if the vehicle flies over an obstacle since the sensor returns the minimum observed distance. Most of these failures or error conditions could result in the vehicle rapidly trying to change its height and potentially colliding with an obstacle.

Table 1: Height sensor failure modes

Failure Mode	Causes	Results	Mitigation Methods
Measurement noise	Vibration from airframe	Reduces controller accuracy and stability	Damping material, Kalman filters
Loss of return from ground	High roll or pitch, flying above sensor range	Possible loss of control	Height measurement from downward facing laser
Return from object other than ground	Improper filtering, obstacles in flight path	Induces sudden motion in z axis, possible loss of control	Height measurement from downward facing laser
Cease to function	Power surges from circuit board	Loss of control	Height measurement from downward facing laser, open loop control with Kalman filter until safe landing

By using vibration damping material, some of the sensor noise can be reduced; however, after analyzing the failure modes of this sensor, it becomes apparent that improved performance can be achieved by using the downward facing laser scanner for height control which provides redundancy thus eliminating many of the Table 1 failure modes. Because the laser scans in a plane, measurement error resulting from pitching or rolling the vehicle can be easily eliminated. Similarly, as long as the sensor receives a return from the ground at some angle, the dangers of flying over obstacles can be eliminated by averaging the longest vertical components in the return set. However, this makes the system susceptible to errors due to uneven floors or depressions in the floor, so robustness can be improved by annotating positions in the global map with their base floor height profile data.

Even when using a downward facing laser scanner the possibility of the sensor ceasing to function still presents a dangerous failure mode. By using an extended Kalman filter, AHRS accelerometer data and predicted applied force from the motors can be used to probabilistically integrate the vehicle's vertical velocity and position. The accuracy of these values is highly sensitive to proper calibration of the sensors and motors, and the values are likely to drift given even small inaccuracies in either calibration. However, MAAV has been able to perform test flights with no height feedback and observe sufficiently slow drift to safely control the vehicle for approximately 60 seconds. This would be enough time for a SUAS operating at low altitudes to make a controlled descent and landing. If during the descent the height sensor becomes active again, the flight can be resumed and directed to either continue its mission or return to base. Additionally, adding more sensor measurements to the Kalman filter can significantly reduce the drift and noise of the filtered data. One possibility would be to use a velocity estimate from a camera running visual odometry algorithms to correct the filtered velocity value. By this method, the vehicle could stay airborne for much longer, potentially having enough time to select a safe landing site before initiating its descent.

B. AHRS Failure Modes

The possible loss of the AHRS is an important failure mode to consider because without proper precautions and safety features, this would almost certainly cause a LOC event. This scenario has not yet been observed on the MAAV vehicle, but AHRS failure has been documented in manned and unmanned aircraft with failures often linked to electrical problems or previous damage. Besides complete failure, other errors in AHRS data such as noise, incorrect individual readings, or misaligned mounting of the unit can induce varying levels of instability in the controller. The relevant failure modes and their effects are given below in Table 2. Figure 3 provides a directed (causal) graph illustrating the causes, failures, and induced risks. This graph demonstrates the connectivity of some of the failure modes as well as providing a structure that can be represented as a Bayesian Network for quantitative aviation safety risk modeling[10] once sufficient flights were recorded with a stable (unchanging) platform to accurately calculate the probabilities for each edge.

Table 2: AHRS failure modes

Failure Mode	Causes	Results	Mitigation Methods
Measurement noise	Vibration from airframe	Reduces controller accuracy and stability	Damping material, Kalman filters
Failure to connect to Gumstix	Loss of USB connection (usually only on boot up)	Reset vehicle before takeoff	Switch to UART communications
Magnetometer reading offset	High current near AHRS	Unreliable yaw from AHRS, offset based on current	Use laser range finders for yaw measurements
Uneven mounting	Cramped mounting area, uneven damping material placement	Angular biases in AHRS measurements	Calibration cycle to remove biases
Cease to Function	Unobserved behavior, possibly damage from previous impact or power surge	Loss of control	Sensor redundancy (mass restrictive)

AHRS placement and mounting can be modified to reduce the effects of vibration-induced noise and high current (electromagnetic) interference introduced by the motors. Using rubber washers or other damping material can greatly reduce the vibrations experienced by the AHRS. Additionally, mounting the unit away from the section of the circuit board that supplies the high motor currents greatly reduces the magnetometer bias. Neither of these methods is perfect, so it is also beneficial to take additional measures to prevent these failure modes. AHRS noise can be further reduced by feeding data through a Kalman filter or an AHRS that has internal filters, or both. If the magnetometer bias is still present, despite the new AHRS placement, true yaw value can be obtained through the laser scanner when operating in an environment with distinct features. If operating outdoors, heading could be obtained from GPS; however, because GPS heading is velocity based, the heading would have to be correlated with the attitude of the vehicle at that time. This would most likely not provide a reliable heading measurement, but could be used as an input to a filter to determine improved estimates.

Examining reliability of the AHRS connection for USB versus UART connection, and using the most reliable connection, can also reduce failure probability. For the MAAV system, the UART was observed to provide significant improvement because the USB plug on the Gumstix board is not tolerant to induced vibrations or misalignment; many recorded connection failures were caused by this plug. Alternatively, soldering the USB lines to the USB breakout pins on the Gumstix interface board may reduce this risk.

The final failure management mechanism is to avoid LOC or at least minimize risk to the environment when losing the AHRS mid-flight. It is possible to design a filtering algorithm to use the outer loop (e.g., laser scanner) sensor data to infer the inner loop state (namely roll and pitch). As long as this data is determined at a sufficient rate, it should be possible to still land the quadrotor safely if this failure occurs. Using the bottom laser scanner, it is possible to determine the pitch of the vehicle if the ground under it is level or if the inclination of the ground is known because the laser receives returns in a line along the ground out the front and back of the vehicle. Using simple trigonometry, it is possible to compute pitch from this data at a rate of about 10 Hz (laser update frequency). This is only about a tenth of the normal frequency of the control loop, so it would not be sufficient for a precise, stable flight, but it will be sufficient for a controlled but likely imperfect landing. Similarly, if the environment is mapped, it is possible to determine roll from comparing a scan to the known environment data; however, this will be quite slow. Additionally, changes in position can be added to the filtering algorithm to estimate the roll and pitch. Using these data sources, a good Kalman filter or particle filter may be able to stabilize the vehicle sufficiently to guide it to a safe landing.

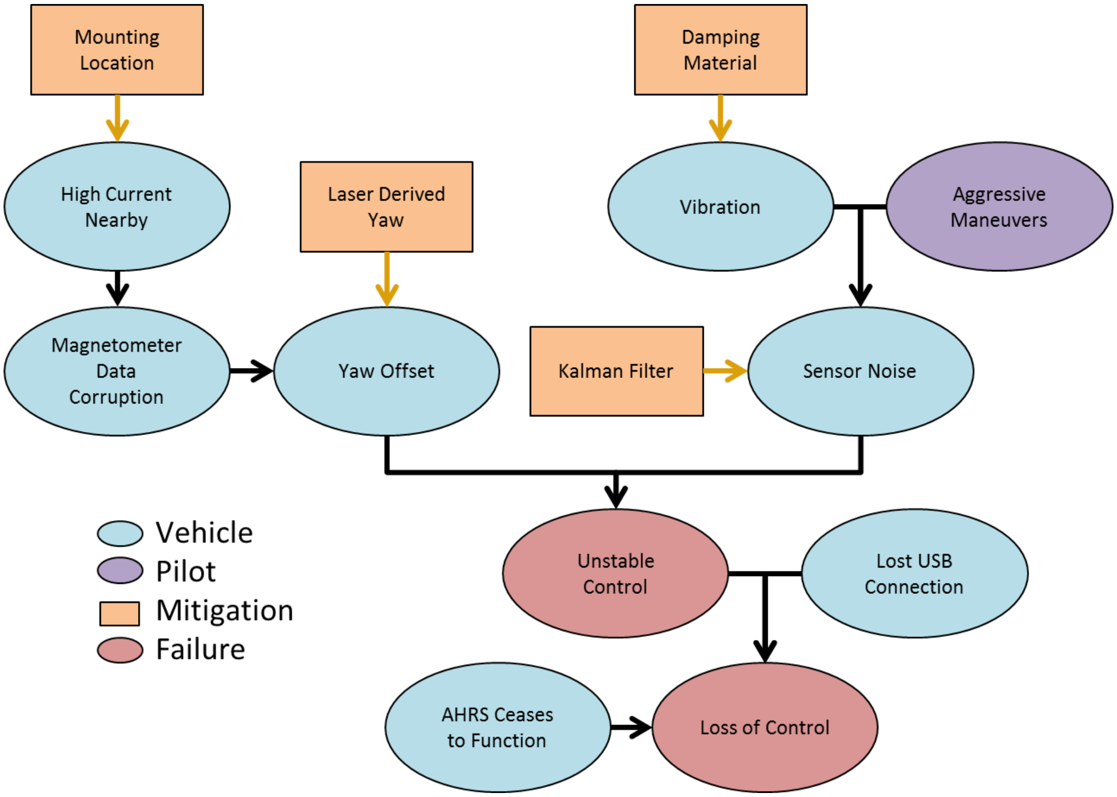

Figure 3: AHRS failure mode graph

C. Motor Failure Modes

Motor seizing is a particularly catastrophic, albeit rare failure mode. In most motor failure cases with a quadrotor, loss of control is unavoidable. Fortunately, this has not been observed during flight; however, occasionally on startup, one motor will seize momentarily causing the craft to flip over while still on the ground. In flight seizing could potentially occur after of progressive degradation of the motor, possibly accelerated by getting particles such as sand in the motor housing. This could also be caused by an Electronic Speed Controller (ESC) failure or an environmental hazard. The relevant failure modes are show in Table 3.

Because the loss of a motor mid-flight would almost certainly cause loss of control of the vehicle, prevention methods are the primary means of minimizing risk due to loss of motor on a quadrotor. Proper care, logging of use, and inspection/repair of the motors and electronic speed controllers (ESCs) are essential. Although MAAV's quadrotor is flown by young students indoors, the team has established protocols that help ensure motors and ESCs in particular are not misused and not inadvertently damaged. Preventing degradation due to contaminant ingestion in the motor housing is a constant consideration, e.g. debris from safety ropes used during testing as they can easily get pulled into the housing, melt, and bind the mechanism. Care should also be taken while flying to avoid overheating the ESCs. This is usually not difficult due to battery life constraints, but when testing with a power supply, the ESC temperature must be taken into account.

Table 3: Motor failure modes

Failure Mode	Causes	Results	Mitigation Methods
Seizing	Improper ESC startup sequence, catching in environment hazard, full degradation, burnt out ESC	Loss of control, overheating if current is maintained	RPM sensing
Degradation	Prolonged use, particles in motor housing	Reduced thrust, affects control of vehicle, eventually seize	Proper upkeep
ESC Overheating	Prolonged use, seized motors, overdraw on current, poor air circulation, hot environment	burnt out speed controller	Proper testing lengths
Burnt out ESC	Prolonged overheating	Poor control near end of life, motor seizing, loss of control	RPM sensing

Besides these prevention methods, it is also beneficial to have methods to detect when a motor is beginning to seize or had seized. Much of this can be accomplished by having RPM feedback to identify the drop in RPM. Worst-case, if motor seized but was sensed the vehicle would be instructed to preemptively turn off the other propellers to avoid hurting any onlookers. If the change in RPM was gradual, the vehicle might still be able to land safely if the event was detected sufficiently early or the degradation was sufficiently slow. Note that it might be possible to regain a certain amount of control of the vehicle if one of the motors seized, but its flight path would, by necessity, be a tumbling and very dangerous one. This would have to be its own research topic, but if the control problem it presents is solved, it could provide an emergency landing method if this failure were to occur.

D. Ground Station Communications Failure Modes

Communication loss otherwise known as lost link is an extremely important failure mode to consider as it affects virtually all types of UAS and is a potentially dangerous situation. For a vehicle like the MAAV small quadrotor operating in an enclosed environment, the most likely outcome introducing risk is collision with some obstacle, which can damage the vehicle or the obstacle which could include people or valuable property. Because the quadrotor's range is fairly small, it is unlikely that the vehicle could exit the signal range of an alternative communication method such as a kill switch. It is also extremely unlikely that the vehicle could either be lost or crash in a place that was unrecoverable. Thus, the lost link problem is simplified, and redundancy through a simple kill switch device has been determined by IARC organizers as a sufficient mitigation for lost link.

For the quadrotor, which uses 2.4 GHz WiFi, loss of communications can be due to signal interference, router problems, or going out of range. High network traffic on the WiFi channel can also delay data transmission sufficiently to significantly disrupt communication. If the vehicle is under manual control, these losses of communication will cause a loss of control if the vehicle is not first disabled using the kill switch, which operates using a different frequency and has a safe landing command if an immediate kill is not required. If the vehicle is flying in autonomous mode, losing communications to the ground station prohibits the vehicle from being able to navigate with the global map. In this instance, the vehicle could maintain hovering until communications are regained, or perform a safe landing after a certain amount of time elapses. The relevant failure modes are shown in Table 4.

One method to prevent a runaway vehicle scenario due to lost link is maintaining a separate communications link that can be used in event of primary link failure. In the case of the MAAV quadrotor, this secondary channel is the 900 MHz kill switch that can command either a safe landing or a hard kill of all vehicle thrusters. In the event of communications loss, either kill signal can be used depending on the severity of the situation. Because the obstacle avoidance and local positioning software are run on the vehicle and do not require communication with the ground station to run, in the event of a link failure with no other anomalies, the MAAV quadrotor would be capable of executing either a safe hover until communications are regained or a safe landing procedure if the vehicle is unable to reestablish the link.

Table 4: Ground station communications failure modes

Failure Mode	Causes	Results	Mitigation Methods
Loss of WiFi	Router problems, loss of signal due to interference	Navigation disabled, runaway vehicle	Disable with kill switch, return to base
Data latency and loss	Router problems, high network traffic	Data processing on ground is not real time, navigation delayed	Safe hover
Delay receiving commands	Router problems, high network traffic	Unresponsive to pilot input	Safe hover

E. Navigation Algorithm Failure Modes

Due to the complexity of the navigation algorithms used to maintain stability, achieve SLAM, and autonomously maneuver through the environment, there are many potential points of failure in the navigation capability. Careful testing of the software eliminates many potential failures that would be realized without such testing and greatly reduce the probability of others, however software remains difficult to fully validate due to its complexity, motivating the numerous flight tests that are currently only feasible to conduct indoors given FAA policies. When navigating in an indoor enclosed environment, collision with obstacles is much more likely. In confined areas, even small disturbances or instabilities can result in catching a propeller and losing control. The same outcome could also result from an error in navigation that causes controlled flight into an obstacle. This may result from the vehicle failing to detect an obstacle due to sensor failure or limitations such as restrictions to 2D obstacle detection. It could also result from the algorithm detecting the obstacle but failing to avoid it. Some areas may also create significant recirculation currents that can cause disturbances that could lead to a crash.

Besides those listed above, there may be other failure modes related to vehicle navigation that do not result in loss of control but that do hinder completion of the vehicle’s mission. Errors in global mapping can cause the vehicle to create a bad data association and become lost within the building. For the MAAV vehicle, this is also influenced by the building layout because long, featureless hallways will confuse the laser scanner and make it difficult to determine the amount the vehicle has translated. Another minor failure mode is inefficient exploration which results from poor decision making by the navigation algorithms when choosing how to explore the building and which turns to take. This can be further exacerbated by a waypoint following algorithm that is jittery or causes the vehicle to move in an overly aggressive or overly passive manner. These types of failures will not necessarily result in the vehicle losing control, but could result in the vehicle being unable to complete its mission or completing the mission inefficiently. The relevant failure modes are summarized below in Table 5 and illustrated in the directed graph (Figure 4). Because the observed navigation failures are primarily software-related, some of the probabilities corresponding to links in the graph could be found through extensive testing of the code in a simulator as well as characterizing environments in terms of parameters which affect the performance of the algorithms. Certainly, if the primary laser scanner itself fails, the vehicle could remain safe by landing in place but would not be able to continue its mission.

Table 5: Navigation algorithm failure modes

Failure Mode	Causes	Results	Mitigation Methods
Controlled Flight into Obstacle	Failed to detect obstacle, noisy control, recirculation currents	Loss of control	Maintain greater distance from obstacles, use a full 3D detection system, prop guards
Bad map association	Featureless rooms or hallways	Incorrect global map, incorrect position estimates	Integrate visual markers into navigation
Inefficient navigation	Poorly tuned exploration algorithms	Excess time spent, jittery waypoint following	Test and tune navigation algorithms

Robustness in navigation algorithms will go a long way to avoiding many of these failures. Having sufficiently accurate vehicle control to precisely follow paths generated by the navigation code also reduces the likelihood of a crash. Using prop guards prevents light collisions with some obstacles from causing a major crash. To increase the chance that the vehicle will detect all obstacles as it traverses its environment, extra sensors or different sensor configurations can be used. With its two laser scanners mounted such that their scanning planes are perpendicular to each other, the vehicle can obtain a full 3D scan of the environment by rotating while moving. Use of computer vision with multiple cameras around the vehicle could accomplish a similar result. To reduce the risk of recirculating airflow (indoors) causing collisions, the vehicle is tested and tuned for a windy environment, a task MAAV has undertaken by blowing large fans on the platform and in the future by testing the quadrotor in the University of Michigan's 5' x 7' wind tunnel.

Mitigating the potential for navigation algorithm failure is primarily accomplished by making more robust algorithms. The frontier classification and selection algorithm currently in use[9] can continue to be tuned and improved to allow for more efficient exploration. The waypoint following algorithm can also be better validated particularly with respect to how it commands maneuvers that keep the vehicle from straying aggressively from the central path. Potential issues associated with improper map construction will also need to be identified and mitigated in future work.

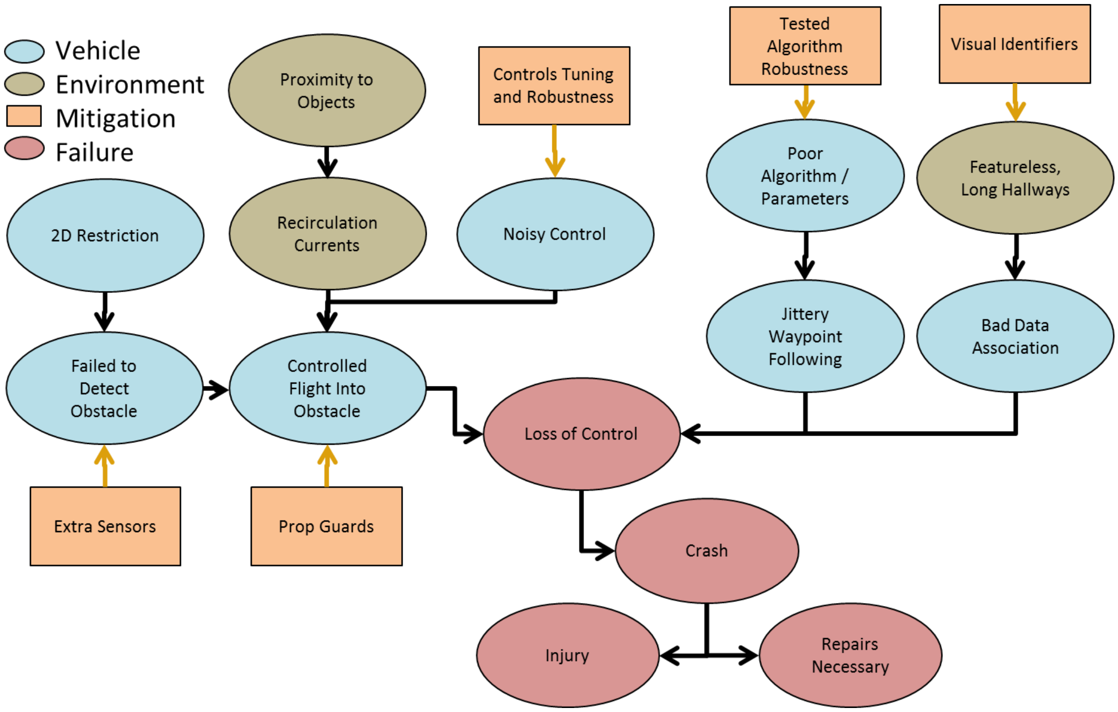

Figure 4: Navigation failure mode graph

IV. Risks Associated with Loss of Control (LOC)

Because the quadrotor flies at low altitude and in enclosed indoor environments, loss of control almost always results in the vehicle crashing. In these cases, the vehicle may sustain heavy damage to its airframe and sometimes may break a sensor, but the impact of the crash does not usually pose a risk to its environment because of its low mass and velocity. In fact, if the motors are still spinning as the vehicle losses control, the propellers are the biggest hazard to people near the vehicle. In rare circumstances, it may be possible to ignite the battery pack, which could present a large risk to the vehicle's surroundings if not extinguished, but the battery pack is comparable to that carried in a laptop thus poses limited risk so long as it is properly packaged.

The primary risk from a crash given a controlled environment is damage to the vehicle itself. If only the carbon airframe was damaged, the vehicle can usually be repaired using less than $10 of materials; however, if the vehicle has been repaired like this multiple times, the airframe may need to be replaced, costing around $20 and at least a day of manufacturing. In the case of a hard impact, one or both of the lasers may be damaged requiring much more expensive repairs. The lasers can be sent to the manufacturer to be repaired in the case of minor damage for approximately $300, but if they need to be replaced, replacements cost around $5000.

Throughout all of MAAV's flight tests in 2012, statistics were recorded on frequency of various failure modes. The most relevant failures include unstable control, height data failure, motor seizing, and low battery voltage, statistics for which are shown below in Table 6. Due to the rapidly changing nature of a developing project, the frequencies of these failures cannot be assumed to be representative of the probabilities that similar events will happen in future flights. Instead, they demonstrate the likely frequency of failures during the development of such systems. By analyzing the causes of each failure, the team has continued to refine their system, reducing the failure rates of subsequent flights.

Table 6: Frequency of Failure Modes in 2012 MAAV Test Flights

Failure Mode	Crash	Unstable Control	Height data failure	Motor Seizing	Low Battery Voltage
Frequency (Failures/Flights)	0.7%	2.4%	6.9%	1.2%	4.5%

The frequency of failures during the development phase of the MAAV quadrotor is well above the required limit for FAA certification of light aviation. Because the vehicle is small and meant for indoor flight, the team is able to continue developing the system to reduce the frequency of these failures; however, if tests required outdoor flights in designated testing locations, it would be much more difficult to fully develop while complying with regulations.

V. Conclusion and Future Work

This paper has summarized potential failure modes associated with a small autonomous quadrotor UAS deployed for indoor flight operations, and has proposed mitigation strategies to ensure the vehicle operates safely despite the potential for failures in the single-string avionics necessary given weight, volume, and cost constraints. Risk identification and analysis are important steps in the development and eventual certification of UAS because this process will inform all users of procedures and protocols to enable safe operations, and will assist those crafting regulations and applicable safety standards for unmanned vehicles to be integrated into NAS. This analysis is especially important for SUAS because their size and cost usually prohibit extensive redundancy in their design. The major risks of the MAAV quadrotor were resolved with mitigation methods and other improvements that increase the safety of the system. Such improvements in turn have enabled the team to be more successful in their operations due to less "down-time" for repairs or redesign.

In the future, this analysis could be improved by gathering a larger sample set of test flight data to identify the statistical probability of the identified failure modes. Because the MAAV system is still being improved and is constantly evolving, it can be difficult to gather a sufficiently large sample set in a stable, long-term configuration, although trends and stable subsystem statistics can certainly be computed. By determining the actual probabilities of specific failure modes as well as the extending the analysis of the risks associated with loss of control, more definitive metrics regarding the system's safety will be determined.

Acknowledgments

This research was made possible through the cooperation and assistance of the Michigan Autonomous Aerial Vehicles team with support from NASA's UAS in the NAS program under contract NNX11AO78A.

References

[1] R. Loh, Y. Bian, and T. Roe, "UAVs in civil airspace: Safety requirements," *IEEE Aerospace and Electronic Systems Magazine*, Vol. 24, No. 1, 2009, pp. 5-17.

[2] M. Correa, J. B. Camargo Jr., M. A. Rossi, and J.r R. Almeida Jr., "Improving the Resilience of UAV in Non-Segregated Airspace Using Multiagent Paradigm," *Second Brazilian Conference on Critical Embedded Systems*, Sao Paulo, Brazil, 2012, pp. 88-93.

[3] R. N. Weber and E. Euteneuer, "Avionics to Enable UAS Integration into the NextGen ATS," *Guidance, Navigation, and Control Conference*, AIAA, Toronto, Ontario, Canada, 2010.

[4] N. Cameron, M. Webster, M. Jump, and M. Fisher, "Certification of a Civil UAS: A Virtual Engineering Approach," *Modeling and Simulation Technologies Conference*, AIAA, Portland, Oregon, 2011.

[5] D. M. Marshall, “UAS Standards, Regulations, and Developmental Strategies: A Global Effort,” *Infotech@Aerospace*, AIAA, Garden Grove, California 2012.

[6] V. G. Ambrosia, B. Cobleigh, C. Jennison, and S. Wegener, “Recent Experiences with Operating UAS in the NAS,” *Infotech@Aerospace*, AIAA, Rohnert Park, California, 2007.

[7] C. Casarosa,, R. Galatolo, G. Mengali, and A. Quarta, “Impact of safety requirements on the weight of civil unmanned aerial vehicles,” *Aircraft Engineering and Aerospace Technology*, Vol. 76, No. 6, 2004, pp. 600.

[8] E. M. Atkins, A. D. Khalsa, and M. D. Groden, “Commercial Low-Altitude UAS Operations in Population Centers,” *9th AIAA Technology, Integration, and Operations Conference*, Hilton Head, South Carolina, 2009.

[9] D. C. Moore, A. S. Huang, M. Walter, E. Olson, L. Fletcher, J. Leonard, and S. Teller, “Simultaneous Local and Global State Estimation for Robotic Navigation,” *Proceedings of the IEEE International Conference on Robotics and Automation*, 2009.

[10] J. T. Luxhøj, and D. W. Coit, “Modeling low probability/high consequence events: an aviation safety risk model,” In *Reliability and Maintainability Symposium,RAMS, Annual* (pp. 215-221), IEEE, 2006.