AIAA SciTech Forum
7-11 January 2019, San Diego, California
AIAA Scitech 2019 Forum

10.2514/6.2019-0961

Dynamic Ground Risk Mitigating Flight Control for Autonomous Small UAS in Urban Environments

Corey A. Ippolito[1]
NASA Ames Research Center, Moffett Field, CA, 94035

A significant barrier to entry for unmanned aircraft operation at low-altitude in densely-populated dynamic urban areas is the need to manage risks associated with overflight of people and property. Urban environments are currently inaccessible to autonomous UAS operations supporting a majority of predicted urban use-case scenarios due to unacceptable levels of risk to ground assets. Traditional approaches and strategies for risk-mitigation and safety-assurance focus on separating flight operations away from densely-populated areas, but these strategies cannot be directly applied to operations contained entirely within these densely-populated regions. For large sparsely-populated regions with a stationary population at coarse-granularity, population-density databases can be referenced during the flight planning phase to adjust flight paths to avoid populated regions. Unfortunately, this approach is difficult to apply to densely-populated urban regions. Urban areas lack population sparsity, and at the fine-granularity needed for highly-constrained spaces characteristic of urban environments, population movement is non-stationary, time-varying, and difficult to predict. In this paper, we present a conceptual framework utilizing real-time sensing and active flight control that manages and mitigates ground risk, providing assurance of acceptable levels of safety in this challenging urban scenario. This approach shows promise towards enabling UAS access to inaccessible urban environments, allowing vehicles to identify and exploit the presence of temporarily-safe corridors. In this paper we present the general concept, present a probabilistic risk model framework for estimation, and develop a flight control system architecture for active ground-risk mitigation towards these objectives.

I. Introduction

A significant barrier to entry to the approval of routine unmanned aircraft operation at low-altitudes above densely-populated urban areas is the need to control risks associated with overflight of people and property. Studies anticipate millions of small UAS operating in the U.S. airspace within the next decade, with access to urban operations anticipated to be in high-demand, and with significant economic growth potential identified for this market [1]. NASA's Unmanned Aircraft System (UAS) Traffic Management (UTM) project is seeking to develop a system of services that will allow safe and routine access to low-altitude airspace for small UAS [2][3]. The UTM project will be expanding the scope of the UTM system as it advances from Technical Capability Level (TCL) 3 to TCL 4, as illustrated in Figure 1. The capability targets for NASA's UTM project in TCL 4 include the following [4]:

- Dense Population
- High Traffic Density
- Urban Applications
- Dense Beyond Visual Line-Of-Sight (BVLOS) Operations

[1] Aerospace Scientist, NASA Ames Research Center, Moffett Field, CA 94035, AIAA Senior Member.

Figure 1. Notional UTM Scenarios and Advancement to TCL-4.

Enabling routine high-density BVLOS UAS operations over a densely-populated urban area is a non-trivial goal. One of the most significant barriers to entry for UAS operations over urban environments is the need to manage risk associated with the overflight of people and property [5][6]. Currently, urban environments are inaccessible to most UAS operations except for the simplest use-cases and operations – such as line-of-sight flight operations in a small localized area around operators that can be cleared of ground assets during flight. The outstanding challenges faced in these environments for broader use-case scenarios – such as doorstep-to-doorstep, emergency response, and package delivery – are substantial. For instance, general use-case scenarios require autonomous operations beyond both visual and radio-frequency (RF) communication line-of-sight of the operator. Due to the challenges faced in low-altitude urban environments, UAS operations will face unreliable or severaly degraded air-ground communication linkage, as well as facing degraded or denied satellite-derived navigation performance. The complex atmospheric conditions above urban environments add further hazards and challenges, for instance, degrading the accuracy of motion prediction, degrading stability and control performance, and the loss of assurance and conformance to planned flight trajectories. Another challenging characteristic of urban environments is the high density of highly-valued ground assets. UAS operations will be occurring over static assets, such as property and infrastructure. Dynamic ground objects (DGO), such as people/pedestrians, are free to move around all areas of the urban environment. The location of DGOs and their movement within the urban environment is complex and unpredictable. The consequences of damage or fatality to ground assets are high in relative comparison to the consequences of losing the UAS. As a result, the low-consequence conservative mitigation strategies that enabled UAS operations in less-populated environments, such as instigating controlled or uncontrolled flight termination as a safe failure contingency, are no longer viable over dense urban environments; Flight termination in these environments poses one of the highest risks to ground assets and is one of the least-desirable outcomes. If DGO position is utilized in the risk mitigation approach, high-confidence knowledge of individual DGO locations – perhaps on order of meter-level accuracy for each person – is required, as the consequence is high for even a single civilian casualty.

The shift from sparsely-populated regions to densely-populated urban environments results in an accompanied loss of the key underlying assumption of segregation that many of the frameworks rely on to assure safety and provide acceptable levels of managed risk (Figure 2). Some of the segregation-based approaches utilized or proposed in the literature include geofencing, safe ditch contingency maneuvers, and flight planning to avoid overflight of people through population density databases. Unfortunately, these approaches are difficult to apply to urban environments and do not provide a sufficient framework to address urban ground-asset risk.

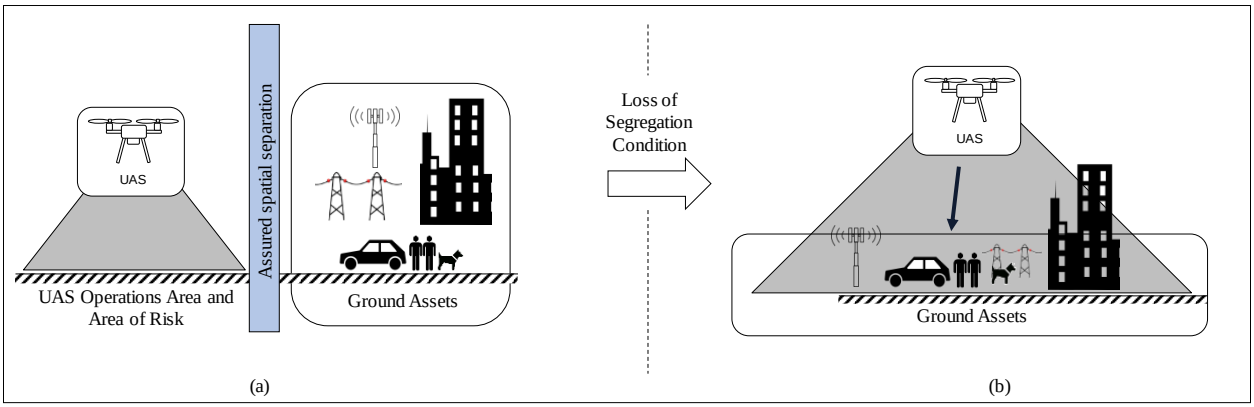

Figure 2. Risk Management Challenge in Urban Environments and Loss of Separation/Segregation.

The NASA Safe Autonomous Flight Environment for the Last 50 Feet (SAFE50) project is conducting an advanced conceptual design study to enable access to low-altitude high-density urban environments through advanced onboard UAS autonomy [5][7]. The conceptual design study focuses on delivering a feasible and validated point-design that places demands on advanced vehicle concepts and onboard vehicle autonomy to meet requirements and address challenges. The NASA SAFE50 reference design study seeks to establish, analyze, and validate an end-to-end reference design for fully-autonomous large-scale UAS operations. This study seeks to extend current framework design under NASA's UTM project at TCL-3, establishing a consistent design and complete-vertical solution from high-level traffic management down to vehicle sub-system level requirements. This study focuses on developing a realistic point-design in the larger trade space that meets challenges through placing demands on advanced onboard vehicle-level autonomy. The system design is constrained to assume today's technology and today's infrastructure, must be realizable and implementable within the resources of this study, must minimize changes to the rest of the UTM system, must minimize the number requirements, must maximize flexibility, and must deliver a set of generalized vehicle-agnostic requirements. Requirements, constraints, and architecture design choices must be justifiable through traceability flow-down from higher-level design elements. This study establishes a reference design architecture for an advanced fully-autonomous vehicle system in this point-design that meets a methodically derived set of validated requirements that could potentially allow TCL-4 capable operations with minimal changes to an existing TCL-3 UTM system. Verification and validation of the SAFE50 reference design study occurs through simulation and flight-testing of hardware prototypes. This project seeks to deliver a validated realistic point-design and reference systems design study as an informed decision-point for future broader investigation of the larger system design trade space.

This paper addresses risk to people and property from high-density low-altitude UAS operations over densely-populated urban environments within the context of the NASA SAFE50 reference design study and the SAFE50 autonomy architecture. The proposed method includes (1) a generalized risk-analysis framework, and (2) a conceptual flight control system for active risk awareness and mitigation in autonomous UAS operations. The proposed risk-analysis framework extends probabilistic risk models presented in the literature. The framework is flexible, allowing for conservative offline analysis and satisfaction through restricted flight conditions, as well as active online satisfaction through active risk-mitigating flight control. Metrics are proposed for risk assessments and establishment of minimum level of acceptable risk. Contingencies and failures are a part of the analysis framework and include recommendations for early life-cycle certification-phase requirements. Satisfaction of safety requirements can be achieved through many possible methods, including by UAS manufacturers during the design, development, and certification phase, and by UAS operators through operational restrictions, flight plan design parameters, and selection of appropriate contingency functions during flight operations. The risk analysis framework presents a general system appropriate for evaluating flight operation risks in many environments.

The proposed conceptual flight control system establishes a method to allow satisfaction of risks formulated under the proposed risk-model framework that addresses the challenges faced in these urban settings. The presented conceptual flight control system expands the operational envelope within the proposed framework through active automated risk sensing and flight vehicle control. The active control concept requires onboard sensors to monitor the ground around and ahead of the vehicle and detect dynamic ground objects – such as people, cars and animals – that are put at risk by the vehicle as it operates. This active control concept continuously generates trajectory plans that

satisfy a minimum required level of safety. Approved vehicles must also maintain awareness of risk caused by likely failure conditions and the off-nominal behaviors that can result. Through the proposed framework and control system, this paper seeks to demonstrate a feasible method for airspace control that enables access to a larger portion of the urban airspace.

II. Background

Aircraft risks are commonly assessed as a function of likelihood and consequence, such as through a risk matrix to establish risk criticality [8][9][10]. Risk criticality can be reduced to manageable levels in two ways: (1) reducing the likelihood of occurrence of some risk-associated event, and/or (2) reducing the severity of the consequence associated with the occurrence of a risk-associated event. Unfortunately, a problematic characteristic of modern small UAS are high reported failure rates and high system fragility [11]. System failure is common for small UAS and often leads to catastrophic results, such as loss-of-control leading to unplanned flight termination. The uncertainty in the resulting aircraft behavior under failure leads to identification of a large area of high-risk on the ground surrounding planned operational areas of for small UAS.

A commonly utilized mechanism to assure safety and mitigate risk to ground assets due to nearby UAS flight operations is to require assured physical/spatial separation between the two, as illustrated in Figure 2. Segregated operations, i.e. the assurance of physical separation between UAS and assets, provide a simple, straight-forward, analyzable method to assure safety and provide manageable risk. For instance, FAA Part 107.39 states: "No person may operate a small unmanned aircraft over a human being" [12]. Similarly, the current NASA UTM system risk management and safety assurance is provided through enforcing the requirement that a physical spatial separation must be maintained at all times between the UAS and ground assets such as people and property [3].

Geofencing is a common segregation-based mitigation strategy. Geofencing defines boundaries around critical assets that vehicles cannot operate within. These areas often include airports, military bases, critical infrastructure, and areas of high population such as urban areas. Risk criticality is managed despite a high probability of UAS failure by focusing on ensuring a low consequence. UAS are allowed to crash often, but must be operated safely away from anything of value on the ground. This approach, however, assumes low risk criticality in all likely failure conditions. An associated requirement is the analysis of failures, establishment of contingency, and development of mitigations to show geofence boundaries will not be violated in likely failure cases.

While geofencing functionality is a common feature in most commercial UAS flight control systems (FCS), many of these systems are not reliable enough to ensure geofence conformance to the level required for segregation-based mitigation. From a risk analysis standpoint, a low-severity consequence cannot be assured in the worst-case, coupled with high likelihood for failure of the geofence system. For instance, an existing UAS flight control system may not provide the onboard fault-monitoring and contingency control functionality needed to detect and address failures that, in the worst case, result in geofence boundary violations. There are a number of ways designers can address this, such as providing higher-reliability in the FCS, adding system redundancies, utilizing vehicle system health monitoring, applying resilient control strategies, adding contingency management functions to the FCS, or by moving approved UAS operations areas further away from ground assets with larger conservative safety separation zones.

Safe flight-terminating control has also been utilized in the literature for safety-assurance. For instance, today's hobby-grade UAS have difficulty meeting requirements to safely operate in any populated setting. For these low-reliability systems, secondary "safe-ditch" control can be applied, such as the NASA Safe2Ditch flight system [13][14]. The Safe2Ditch system conceptualizes an independent flight-certified monitoring and flight termination system for hobby-grade UAS. The Safe2Ditch system monitors a vehicle's flight status and vehicle health, and will override the vehicle's flight control system as necessary to ensure conformance to operating within approved safe operational flight areas. For instance, the Safe2Ditch system can turn off power to the onboard propulsion system in a multi-copter vehicle platform in response to an impending violation of the operational boundary, ensuring flight termination occurs within the approved operations areas. Alternatively, the system can provide input into the existing FCS to ensure forced/controlled flight termination in pre-established low-risk areas. Such segregated ditching strategies ensure vehicles remain well-clear of ground assets through ensuring the worst-case flight termination response to any failure that endangers range-safety, and they ensure terminal ground-impact occurs within established operational area that must be clear of ground assets. Such approaches, however, would not be appropriate for flight within densely-populated urban environments; flight termination over the operational area becomes the highest-consequence event to avoid due to risk to ground assets, and generally, much higher-levels of reliability and certifiability will likely be required for UAS operating within these environments. While the conceptual approach in

this paper is applicable to UAS in general, addressing the specific issue of existing low-reliability and hobby-grade systems is beyond the scope of this paper.

Flight planning to avoid overflight of populated areas has also been utilized to address UAS ground-risk in the literature, such as [15] and [16]. Several approaches utilize population density databases for offline and online (real-time) flight planning to avoid overflight of regions with high population densities. This was applied in [15] to flight planning for a high-altitude long-endurance (HALE) UAS, with static gross-area assumptions of population over large spatial regions. Populated regions were identified in the population database, and 'keep-out' zones were established considering the performance of the fixed-wing aircraft. Flight plans were generated by hand to ensure the UAS did not fly into any keep-out regions. Contingency plans were created for every leg of the flight plan, identifying safe alternative landing site runways closest to each flight segment. Approval had to be established with each alternative landing site operator for use of their runways for remotely-piloted UAS landing before the flight plan was submitted and approved by the FAA. This approach was also applied to automated re-planning for emergency landing of a small multicopters in urban environments [16]. Unfortunately, the population database approach is difficult to apply to densely-populated dynamic urban regions. Urban areas lack population sparsity, and at the fine-granularity needed for highly-constrained spaces characteristic of urban environments, the population density will be non-stationary and difficult to predict. Urban areas fluctuate in density throughout the day and are unpredictable in a smaller localized region, when the population at risk may be orders of magnitude smaller than the accuracy of a population database. For instance, a specific UAS flight plan may need to overfly several sections of pedestrian sidewalks to conduct a door-step to door-step flight plan, but the risk analysis shows the vehicle cannot safely overfly even a small number of people. Population databases cannot predict movement and provide time-based individual location to the needed level of granularity. The alternative approach presented here applies the notion of real-time flight planning to avoid overflight of dynamic ground assets. Instead of a statically defined population density database, however, this paper conceptualizes a flight system that actively monitors and adjusts flight plans in response to ground assets identified within the range of onboard flight sensors in real-time, adjusting flight behavior to overfly temporarily unoccupied ground-surface regions, and maintaining conformance within pre-approved flight volumes within these urban environments.

III. Use-Case Scenario

A. Nominal Ground-Risk Mitigating Control Case

Consider the following motivating use-case scenario. A small unmanned aircraft plans to operate above a city street with a ground-speed velocity of 30 feet per second at an altitude of 200 ft above ground level. The desired flight plan flies along a street with both parallel and perpendicular intersection of pedestrian sidewalks and crosswalks.

An Off-Nominal Failure Mode (ONFM) model – consisting of the set of failure modes, probabilities, ground-hazard mapping functions, and contingency action plans – must be developed by the UAS manufacturer during the design and certification phase of the UAS system. The ONFM model identifies the set of off-nominal failure modes that could likely occur during flight and that would result in off-nominal behavior. For the motivating use-case, consider the following simplified set of failures in the ONFM model:

1. complete power failure,
2. single motor failure,
3. emergency low-battery level,
4. loss of GPS position input to the Inertial Navigation System (INS).

For each failure mode i, the manufacturer has specified a probability of occurrence (P_i), a forward-prediction ground-area hazard region mapping (G_i), and a backward-prediction 'do-not-fly' area region mapping (D_i). The G_i region identifies the ground area at risk should failure mode i occur in the given flight condition. The mapping G_i maps a vehicle velocity, position, and altitude above ground level (AGL) to a ground surface-area region. The backward-prediction 'do-not-fly' volume D_i specifies a conservative 3-D spatial volume that the vehicle must avoid entering that would result in a high-level of ground risk to a set of ground-surface locations associated with identified ground assets, should the associated failure mode i occur in the given flight condition. D_i maps the cruise ground-speed velocity, AGL altitude, and ground asset locations to a 3-D volume.

Associated with each failure mode in the ONFM model is an associated contingency action plan. In this simplified use-case consider the following contingency actions. For failure 1, complete power failure, the resulting behavior is an uncontrolled ballistic trajectory. For failure 2, single motor failure, the vehicle systems will identify the failure in real-time and quickly switch to a degraded flight control mode with loss of control of yaw-rate; an immediate emergency landing will then be planned/executed at a sufficiently safe obstacle-free location surrounding the vehicle. Throughout flight, the vehicle must continuously verify a sufficiently-safe location exists in case this contingency plan is executed. For failure 3, emergency low-battery level, the vehicle must proceed immediately to the closest alternative landing site. The vehicle must continuously evaluate low-battery levels with conservative power-consumption estimates to the nearest alternative landing site. For failure 4, lost GPS, the system must switch to a LIDAR-based SLAM navigation system that requires AGL altitude be at or less than 150-feet.

The manufacturer has developed and certified the UAS vehicle system configuration that includes an onboard ground-risk mitigation system (GRMS). The GRMS includes forward-looking remote sensors, processing capabilities, and incorporates the ONFM model. The GRMS receives the vehicle state from the onboard INS and trajectory plans from the onboard flight planning system. The GRMS outputs constraints to the flight planning system in the form of 'do-not-enter' regions.

During flight execution in cruising flight, the GRMS sensors identifies two groups of pedestrians on a sidewalk 400 feet ahead of the vehicle, with the first set of pedestrians directly under the planned flight trajectory.

In response to this event, the GRMS performs the following actions. First, the GRMS updates an internal dynamic ground hazards environment map to reflect the sensor updates. This map is responsible for maintaining all ground hazards identified in the system, both in real-time and prior to flight. If this hazard was not previously identified, the GRMS registers a new hazard in the hazard map. The GRMS then updates the position of the registered hazard based on the latest sensor readings. Next, based on the updated environment hazards map, the GRMS updates the location of a safe land-immediately landing site to meet requirements for the contingency action plan identified for ONFM failure 2. The safe land-immediately site is passed to the planning system as an alternative landing site target. Next, the GRMS evaluates the probabilistic ground risk associated with the current flight plan. The GRMS integrates the ground risk differential metric mappings G_i from the ONFM model over the planned trajectory to compute a composite risk metric. If the planned trajectory is unacceptable in terms of risk, it notifies the Autonomous Flight Executive module that immediate contingency actions need to be taken. Next, the GRMS computes a revised set of conservative 'do-not-fly' regions that the vehicle must avoid. These regions are computed from the updated hazard locations in the environment hazards map, and processed against the ONFM model's volume prediction (D_i) mappings. The 'do-not-fly' regions are sent to the flight planning systems as constraints for planning and trajectory generation.

The onboard autonomous flight planning system operates concurrently at two rates. A low-frequency higher-level flight planner generates flight plans to the established destination site and alternative landing sites, checking against operational volume constraints currently approved by the UTM system, and against environment maps that include both static and dynamic obstacles. Dynamic obstacle constraints include the "do-not-fly" constraint volumes provided by the GRMS. The set of alternative landing sites includes the feasible land-immediately site that is dynamically updated by the GRMS. The resulting flight plans are expanded to larger operations volumetric constraints surrounding the feasible plans. A Decision Making Module (DMM) evaluates the potential set of flight plans generated by the high-level planner and selects the most appropriate plan for execution. The DMM passes the selected plans and volumetric constraints to the local planner, which serves as a higher-frequency lower-level trajectory generation system. This trajectory generation system is responsible for producing smooth feasible trajectories satisfying the higher-level volumetric constraints, will check against any updates to the do-not-violate constraint volumes from the GRMS, and will check against other dynamic constraints (such as provided by a dynamic air-to-air see-and-avoid system). If the lower-level system fails to find a feasible trajectory compliant with a higher-level plan and the dynamic constraints, the Decision Making Module will select a different plan. If no feasible flight path plan can be found to the destination location, an alternative plan is selected to one of the alternative landing sites.

The GRMS evaluates the currently planned flight trajectory which overflies the first set of pedestrians, and calculates a risk severity metric for the trajectory. The resulting trajectory risk matrix is unacceptably high, indicating the trajectory is no longer safe to continue along.

The GRMS notifies the Autonomous Flight Executive, which instigates replanning of the higher and lower level planning systems. The higher-level mission planning system determines a nominal path still exists. The planner expands the nominal path plan to find a larger encompassing volume that still satisfies all constraints. The planner also generates a set of alternative plans, repeating this process for designated alternative landing sites. The nominal

plan is selected by the DMM and passed to the lower-level local planner. The local planner generates a trajectory that meets the constraints of the higher-level planner and other dynamic obstacles.

Through this process, the UAS autonomy system has determined a new, feasible, and safe plan. The new plan adjusts the trajectory to guide the aircraft between the two groups of pedestrians, avoiding direct overflight of either groups, and satisfying a maximum ground-risk metric constraint.

As the plan is executed, the movement of the two groups of pedestrians is sensed and tracked by the GRMS. The local planner responds at a high-frequency with adjustments to trajectories that reflect changing DGO locations. The high-level planner continues to re-evaluate plans against higher-level mission objectives at a lower-frequency. This repeats until the vehicle safely navigates past the ground obstacles.

B. Contingency Scenario Use-Cases

Contingency scenarios are defined as branches from the nominal use-case scenario presented above. Consider the case when a very large group of pedestrians have gathered on an intersecting crosswalk that blocks all safe paths from the current vehicle location to the vehicle destination along the nominally desired path.

The GRMS system updates using the same sequence specified in the nominal use case. The GRMS identifies pedestrian locations and updates the hazard map, then finds and updates the location for a safe land-immediately site per ONFM model requirements. The GRMS will then compute the composite risk metric for the current plan and trajectory. In this scenario, the resulting risk metric is higher than the allowable maximum allowable risk threshold, and the Autonomous Flight Executive module is notified that immediate contingency actions need to be taken. Next, GRMS processes the environment map and ONFM model D_i mapping to computes a revised set of conservative 'do-not-fly' regions that the vehicle must avoid. In this case, these volumes will block all paths to the destination in the nominal plan within the approved operational volume constraints.

The planning system will generate a new set of plans. DMM has currently selected a plan generated by one of the planners in the high-level planning system. Two cases may then occur.

In Case 1, consider the existence of alternative paths within the approved UTM volumes that provides a route around the blocked volume. If alternative path volumes exist, the high-level planner will find a new adjusted path through the alternative volume. For instance, during the initial pre-flight planning process, an offline pedestrian density database might have shown the suggested path has high potential risk, and an alternative plan was generated with higher pedestrian density aversion through inclusion in the mission cost function used to generate optimal plans in the mission planner. Both the alternative path and nominal paths would be used to submit an approved operational volume with alternative path plan volumes. When the mission planner is invoked during flight, the adjusted path will in this case require the vehicle to backtrack and navigate through the alternative plan volume.

In Case 2, consider the case where no alternative paths can be found to the destination within the approved UTM volumes. A number of actions could possibly take place at this point.

In Case 2.a, the vehicle performs a safe loiter behavior while new alternative plans are generated and submitted to the UTM system. Once approved, the vehicle can then proceed along the nominal use-case scenario to the destination. The safe loiter behavior may include climbing in altitude within the approved volume to improve expected air-ground link. Note that executing a safe loiter and mid-flight UTM renegotiation may not be a desired or acceptable behavior for many flight operation scenarios. The decision to invoke this behavior may include consideration of high-level mission objectives, energy required for transitioning between cruise and loiter, energy consumption expected during loiter, the condition of the air-ground communication link, risks analysis of a prolonged loiter, design complexity, etc. Ground operators will also be notified for possible human intervention.

In Case 2.b, if the conditions in Case 2a are not satisfied or an alternative plan cannot be negotiated, the vehicle executes a contingency plan to a predefine alternative landing site. Note that the mission planner concurrently generates plans to the destination site as well as all alternative landing locations. The flight executive and/or DMM in this case is responsible for selecting the best alternative landing site plan.

In Case 2.c, if the conditions for Case 2a and Case 2b are not satisfied, for instance if the pedestrians have also blocked paths to alternative landing sites, the vehicle will perform enter a safe loiter. The GRMS and planning systems will continue to track changes in ground-object locations. If a path opens up to either the destination or an alternative landing site, the DMM/executive will switch back to a nominal operating mode described in the use case. Ground operators will also be notified for possible human intervention.

In Case 2.d, onboard energy levels fall below a safe threshold to complete any plan. Whenever onboard energy levels fall below this threshold, a land-immediately emergency contingency is engaged. An emergency transmission is sent to surrounding vehicles and through the air-ground link the UTM system. The GRMS has identified the safe landing zone destination. The DMM/executive instructs the planning system to utilize the plan to transition to the landing site location, then transition to an actively controlled landing flight phase to allow safe landing in an uncontrolled emergency location. The specification of the actively controlled landing flight phase is addressed in the SAFE50 reference design study.

In Case 3, consider the contingency scenario when a sudden large-scale influx of new ground objects is detected over the entire sensor cover area, preventing identification of any safe land-immediately sites. In this scenario, the steps outlined in the nominal use-case can proceed as specified, noting that a large risk metric will be evaluated for each failure mode in the ONFM model that require a land-immediately contingency action. The cost-model composite trajectory metric evaluation will include higher risk probabilities across all trajectory plans (nominal and alternative) due to the risk of the land-immediately failure. Two conditions may occur.

In Case 3.a, the planning system generates a plan with acceptable level of risk, and this plan is selected and executed as specified in the process described in the contingency Case 1.

In Case 3.b, the GRMS fails to find a safe land-immediately location, and the planning system fails to find an acceptably safe plan to any landing sites. This case requires further evaluation and future analysis. Generally, a contingency must be established to meet acceptable risk evaluation through the risk model as the condition for certification. The mitigation approach will likely be specific to the vehicle and supported operations model established by the manufacturer.

In Case 4, consider the effect of GPS navigation system failure. The contingency action plan identified in the ONFM for this scenario requires the onboard navigation system to monitor the integrity of the GPS/GNSS derived position estimate, and switch to a LIDAR-based SLAM position estimate. However, the LIDAR-based SLAM estimate requires navigation closer to the ground with sufficient number of features to maintain tracking. In this motivating use-case scenario, a maximum AGL altitude of 150 feet is utilized as this constraint. The modification to expected flight altitude will affect the risk model through the ONFM mappings D_i and G_i, which take the flight condition as an input. The lower altitude will have beneficial impacts to the D_i and G_i mappings, as lower-altitude results in a smaller risk-hazard area on the ground and smaller "do-not-fly" constraint volume.

In order to satisfy minimum/maximum safety threshold requirements, UAS manufactures have many possible design option to improve safety as evaluated in the proposed risk model. For instance, the probabilistic likelihood of a complete loss of power can be reduced through addition of power-system redundancy. The consequence of a single-motor failure can be reduced by providing more control margin to allow reconfiguration or resilience that can maintain full control of the vehicle under a single-motor failure. The altitude for supported operations can be reduced for multicopter vehicle to reduce the hazard-impact area and energy at impact. Alternatively, for fixed-wing UAS, the supported cruise altitudes can be increased to allow a larger controlled glide area in response to propulsion system failures. Fixed-wing platforms would result in different ONFM model mappings for ground-area hazards and "do-not-fly" constraint volumes (D_i and G_i). Intelligent vehicle health management, redundancies, or resilient control functionality can be incorporated into vehicle system designs to provide safer contingency plans with reduced consequence severity or likelihood probabilities. The design mitigation possibilities for risk mitigations follows the standard formal aircraft systems engineering methodology, for instance as specified in [9] and [10].

IV. Approach

The objectives for this project are as follows:

1. Develop use-case scenarios for nominal and contingency operations that describe functionality of the system, and that allow derivation of lower level systems requirements.
2. Extend the SAFE50 reference design and autonomy architecture to utilize onboard real-time autonomy for dynamic ground risk mitigation
3. Develop risk analysis framework, models and definitions
4. Evaluate risk model and control system on the SAFE50 reference design
5. Develop reference implementation integrated into SAFE50 architecture

6. Implement use-case scenarios and contingency scenarios
7. Verify and validate in simulation
8. Develop generalized vehicle-level requirements

A general requirements architecture for vehicle-level autonomy supporting operations in high-density low-altitude urban area were derived in the NASA SAFE50 reference design study [5] and elaborated in [7]. The requirements can be conceptually categorized in the illustration in Figure 3. The concepts introduced in this paper for dynamic ground-risk mitigation address the requirements highlighted in this figure.

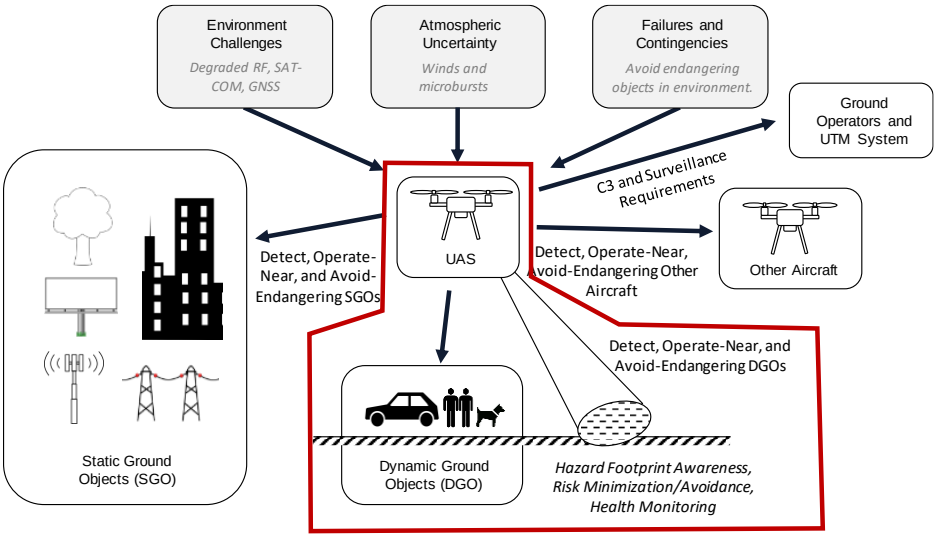

Figure 3. Requirements for Dynamic Ground Risk Mitigation with the SAFE50 Autonomy Architecture.

The high-level SAFE50 reference autonomy architecture was modified as shown. This architecture support communication and data-flow requirements derived from the use-case scenarios.

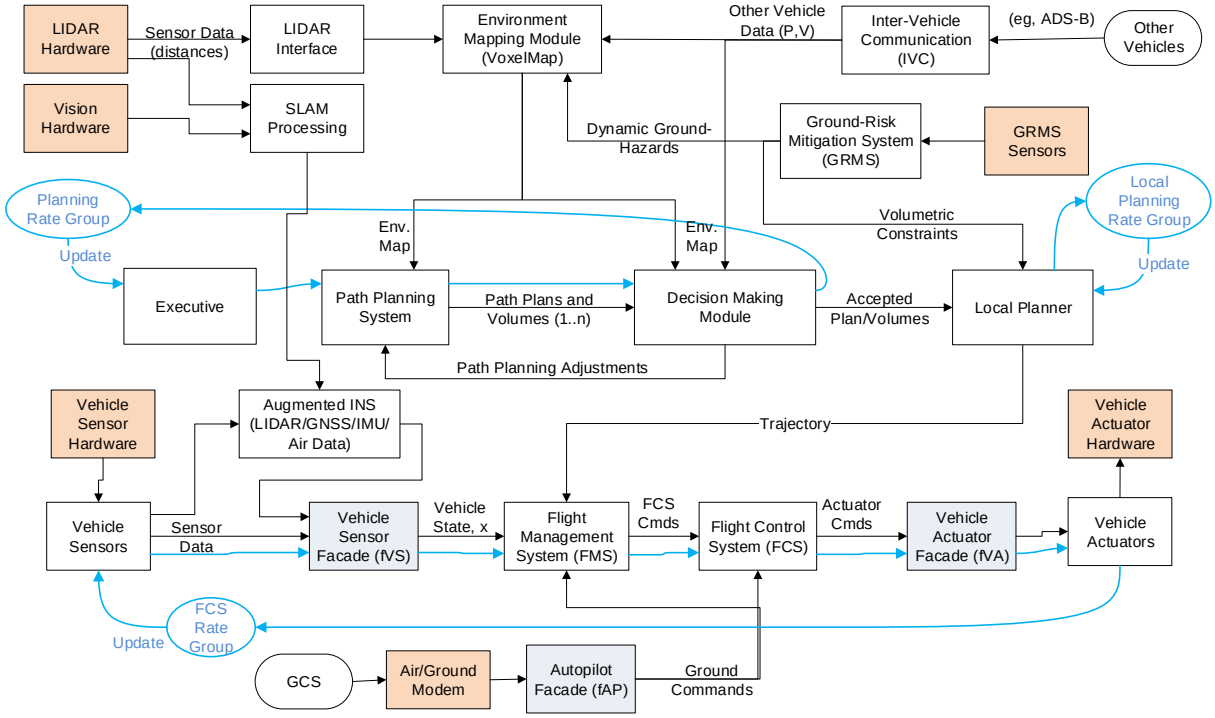

Figure 4. GRMS Integration in the SAFE50 Autonomy Architecture

1. Requirements Derivation

The GRMS use-case scenarios were analyzed to derive system level functional requirements on the vehicle design and reference architecture. The Level 1 and Level 2 components of the requirements architecture are illustrated in Figure 5. The Level 2 components are described below.

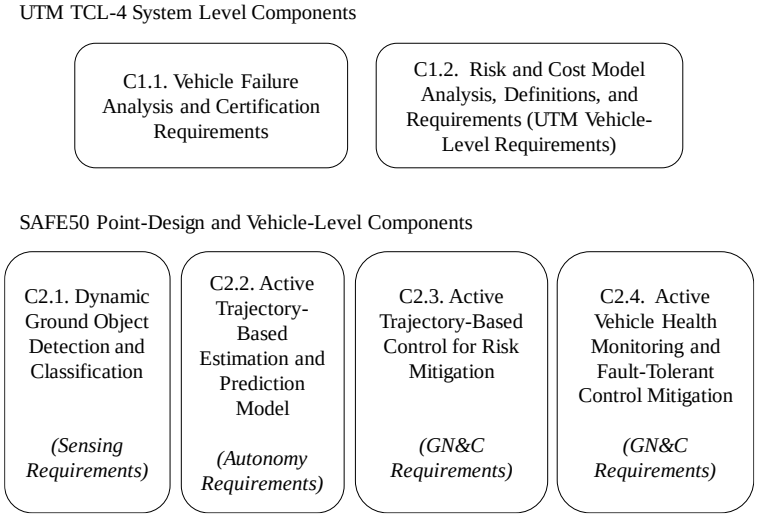

Figure 5. Level 1 and Level 2 Requirements Architecture.

C.1.1. Vehicle Failure Analysis and Certification Requirements

The requirements under C1.1 support the Off-Nominal Failure Mode (ONFM) model. Details of the ONFM were provided in the use-case description. This model consists of a set of failure modes and associated risk-model data elements. The components of the ONFM model are (1) enumeration of off-nominal failure modes, (2) probabilistic likelihood of occurrence, (3) a ground-hazard mapping function, (4) a "do-not-fly" constraint volume mapping function, and (5) contingency action plans.

The following are notes on the C1.1-level requirements.

- UAS manufacturers must develop a ONFM model supported by a formal risk analysis
- UAS manufactures must document and present ONFM model as part of the certification process from the appropriate certification authority.
- Vehicle-specific ONFM models provide additional requirements for configuration-specific vehicle subsystems, including but not limited to the GRMS.
- UAS manufacturers must identify likely failure modes in the ONFM model that can result in off-nominal behavior. (Off-nominal behavior refers to any deviation from the expected nominal system behavior.)
- ONFM model requirements support verification, validation and certification for UAS manufacturers through appropriate certification authorities. This is part of the certification required to access urban environments under the SAFE50 reference design.
- The risk model is general and can be applied to analyze a wide class of vehicle configurations and operations. For example, the risk model supports analysis of simple low-reliability UAS configuration that operate in unpopulated areas away from people/property.

C1.2. Risk and Cost Model Requirements

The following are notes on the C1.2-level requirements.

- The risk and cost models are failure-based and captured in the OFNM model requirements.
- UAS manufacturers must perform analysis of each failure mode that includes the following

- Risk analysis;
- Probabilistic likelihood of occurrence;
- Contingency actions requirements;
- Behavior response models under failure and contingency.

- Manufacturers must provide a ground-area hazard region mapping (G_i) for each failure mode i. This mapping captures the behavioral model estimation of a ground area at risk to a specified severity under a failure mode. The ground surface-area region produced by the G_i behavioral map is expected to be a function of the vehicle parameters, vehicle state at the time of failure, mission parameters, and ground model.
  - The G_i ground-area hazard region metric evaluates to a differential risk metric that can be integrated over ground-risks identified with the resulting region, then integrated over a trajectory or flight plan, then combined with the metrics from all OFNM failure modes to produce a composite safety metric of a specified given trajectory.
- Manufacturers must provide a backward-prediction 'do-not-fly' area region mapping (D_i). This mapping captures the behavioral model estimation of a conservative 3-D spatial volume that the vehicle must avoid entering that would result in a level of ground risk higher than a specific threshold. D_i mapping domain includes the inputs to the G_i mapping, with additional parameters to characterize the trajectories being evaluated and ground-hazard characteristics (e.g., location, shape, size).
  - The 3-D volumes returned by D_i (in the range of D_i) must sufficiently bound all possible starting conditions in the domain of D_i that will result in a ground risk evaluation above the specified threshold for the given ground-hazard locations, as evaluated through integration of the associated G_i mapping over a given input trajectory.
- The risk model specified here is flexible and extend commonly used risk management processes in the aerospace industry. Manufacturers have flexibility in the method by which the safety metric is satisfied. The reference architecture implementation described here in the GRMS system is one such method utilizing onboard real-time ground-risk sensing and control.

C2.1 Dynamic Ground Object Detection and Classification

The requirements for dynamic ground object detection and classification are assigned to the GRMS systems and associated GRMS sensors. The detection geometry is shown in Figure 6, specifying the distance/range of sensing required as a function of the inputs to the behavior models. These inputs include the flight conditions shown, such as velocity v and AGL altitude h.

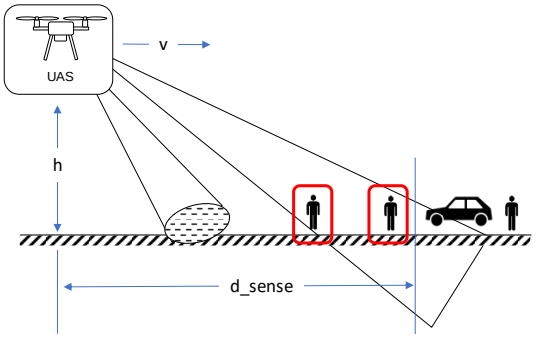

Figure 6. Detection Geometry Definitions

The following are notes and excerpts from the C2.1-level requirements.

- The GRMS must process sensor input to detect and identify dynamic ground objects (DGOs).
- The GRMS must be able to track individual DGOs over time.

- Additional GRMS functionality will assist reducing risks evaluated through the risk model. Useful capabilities include classification of DGOs, state-estimation of DGOs, or the development of DGO behavioral models to assist in forward prediction in the risk behavioral model evaluation.
- The GRMS must maintain positions of all identified DGOs in an environment hazards map structure. In the reference architecture, common voxel-map data structure is utilized to store both static and dynamic ground objects, and is implemented in the Environment Mapping Module.
- The GRMS should provide functionality to remove stale DGO's from the environment map. A supporting use-case needs to be developed and analyzed to determine the necessity of this functionality and derive specific requirements.

C2.2. Active Trajectory-Based Estimation and Prediction Model

Each failure mode must be accompanied minimally by the two behavioral mapping functions. These represent the minimum necessary requirements for behavioral models in the OFNM to support risk model assessment and prediction.

An alternative approach to specifying failure behavior would be to develop detailed trajectory models for each failure mode with some mechanism for incorporating expanding uncertainty bounds over time, such as through the addition of stochastic uncertainty on a dynamics model. This would produce less-conservative risk estimates, in turn resulting in a larger/expanded flight envelope for safe operations.

C2.3. Active Control for Risk Mitigation

The following are notes on C2.3-level requirements.

- The GRMS must perform real-time evaluation of the risk model as specified in the use-cases.
- The GRMS must provide a dynamic ground hazard map to the mission planning system.
- The GRMS must provide a set of 'do-not-fly' volume constraints to the planning system (mission planning system and local planning system).
- The control functionality required to achieve risk mitigation is distributed to the planning, decision-making, and execution control modules. The architectural components and associated requirements for the existing SAFE50 architecture are specified in [7].
- A base set of requirements for sizing the requested UTM volumes are specified in [7]. In addition, the UTM volumes must provide sufficient space for UAS to operate over anticipated dynamic ground object distributions given the desired throughput. For instance, given expectations of ground objects density and coverage, the size of the UTM volumes should be sufficient to allow a target number of UAS to successfully navigate through the environment, with enough space to adjust trajectories to find feasible navigation paths.

C2.4. Active Vehicle Health Monitoring and Fault-Tolerant Control Mitigation

The specific reference design implementation outlined in the use-case description includes requirements for vehicle health monitoring and fault-tolerant control. Note that the requirements for C2.4 are optional design choices made in the UAS design process. UAS designers must develop a specific solution that meets the risk-based model requirements. The method by which the risk model requirements are satisfied are up to the designer.

For instance, designers may choose to incorporate vehicle health management functionality for detection of failures and control system robustness/resilience to accommodate failures. These additions will reduce the risk model likelihood and consequence estimates while providing better off-nominal behavior that will allow for an expanded envelope of safe operating conditions. Designers may choose to incorporate an active GRMS system as described in this reference architecture for improved analysis and estimation of ground risk in the risk model. Alternatively, designers may choose to conservatively reduce the operational envelope to achieve satisfactory levels of safety as evaluated in the risk model with a simpler system design.

V. Conclusion

Enabling safe routine access for high-density UAS operations over densely-populated urban environments at low-altitude requires addressing the issue of risk and safety associated with flight of UAS over people and property. Existing mechanisms established to assure UAS operational safety in less-populated environments cannot be easily applied over these environments, such as methods that require separation between the UAS operations and nearby ground assets. Expanding flight operations to these urban environments requires development of alternative strategies for risk and safety assessment with mitigation strategies that allow flight operation over static ground assets and property, such as buildings and roadways. Further, the framework must allow flight operations in close proximity to dynamic ground objects such as people and automobiles. The framework must allow UAS flight operational areas to overlap the dynamic ground objects movement areas.

This paper presented a conceptual risk-based assessment framework and a reference implementation that satisfies the requirements for these environments. The implementation utilizes a conceptual flight control system for active risk awareness and mitigation for autonomous small UAS operations. This study was conducted as part of the NASA SAFE50 reference design study, with the reference implementation incorporated into the SAFE50 autonomy architecture. The proposed risk-analysis framework utilizes a probabilistic risk model with risk management strategies commonly used in the aviation industry. The framework is flexible, placing no restrictions the UAS system design space, but rather placing requirements on minimum levels of risk and safety as specified in the risk model framework. To demonstrate this approach, a reference UAS design is presented utilizing advanced onboard autonomy to allow high-density urban operations. Contingency and failure analyses are key components of the analysis framework. Risk evaluation includes analysis across likely failures that result in off-nominal behaviors. This framework is also conducive to incorporation within a formalized certification process. The risk framework is currently being explored by analyzing a proposed architecture for active ground-risk detection and flight control mitigation. This approach addresses many challenges faced in the urban operations scenario. The active control concept requires onboard sensors to detect, identify, and track dynamic ground objects, such as people, cars and animals around and ahead of the vehicle. The ground-risk mitigating flight system satisfies ground risk requirements through imposition of volumetric constraints to the online path planning and local trajectory generation systems in the SAFE50 autonomy architecture. The resulting plans and trajectories generated by these systems will be guaranteed to satisfy requirements for acceptable levels of ground-risk. Through the proposed framework and control system, this paper has outlined a concept for management of ground-risk that seeks to enable access to a large portion of the urban airspace. The ground-risk framework outlined in this study is presented at a conceptual level. This framework is being further developed and refined as it is applied to real-time evaluation in the ground-risk mitigating control system. The risk models will be further defined and evaluated against the use-case scenario condition. The control systems concept is currently being incorporated into the NASA SAFE50 reference design study. This paper presented the current design and integration in the SAFE50 autonomy architecture. Development of the framework and control system is continuing under the SAFE50 project, with planned activities to conduct simulation evaluation against the use-case scenarios.

Acknowledgments

The authors would like to thank our collaborators and colleagues in the NASA UAS Traffic Management (UTM) project and the Intelligent Systems Division at NASA Ames Research Center.

References

[1] Federal Aviation Administration (FAA). FAA Aerospace Forecast: Fiscal Years 2017 to 2037. FAA TC17-0002. United States Department of Transportation. Washington, DC. 2017.

[2] Federal Aviation Administration (FAA). Unmanned Aircraft Systems (UAS) Traffic Management (UTM) Concept of Operations. United States Department of Transportation. Washington, DC. May 18, 2018.

[3] Kopardekar, P., Rios, J., Prevot, T., Johnson, M., Jung, J., & Robinson, J. (2016, June). Unmanned Aircraft System Traffic Management (UTM) Concept of Operations. In AIAA 2016 Aviation Forum. 2016.

[4] NASA Ames Research Center. NASA UTM Executive Summary: TCL 3 Media Day. June 2018.

[5] Ippolito, C. A.; Krishnakumar, K.; Stepanyan, V.; Chakrabarty A.; Baculi, J. (2019). SAFE50 Reference Design Study for Large-Scale High-Density Low-Altitude UAS Operations in Urban Areas. In 2019 AIAA Modeling and Simulation Technologies Conference. San Diego, CA. Jan 2109.

[6] Clothier, R. A., Walker, R. A., Fulton, N., & Campbell, D. A. (2007). A Casualty Risk Analysis for Unmanned Aerial System (UAS) Operations Over Inhabited Areas. Twelfth Australian International Aerospace Congress, 2nd Australasian Unmanned Air Vehicles Conference, 19-22 March, Melbourne.

[7] Ippolito, C. A.; Krishnakumar, K.; Stepanyan, V.; Bencomo, A.; Chakrabarty A.; Baculi, J. (2019). An Autonomy Architecture for High-Density Operations of Small UAS in Low-Altitude Urban Environments. In 2019 AIAA Modeling and Simulation Technologies Conference. San Diego, CA. Jan 2109.
[8] Federal Aviation Administration (FAA). Risk Management Handbook. FAA-H-8083-2. United States Department of Transportation. Washington, DC. 2009.
[9] National Aeronautics and Space Administration (NASA). NASA Risk Management Handbook. NASA SP-2011-3422, Version 1.0. November 2011.
[10] National Aeronautics and Space Administration (NASA). NASA Systems Engineering Handbook. NASA SP-2016-6105 Rev 2. Feb 17, 2017. Available at http://hdl.handle.net/2060/20170001761.
[11] Next Generation Air Transportation System Joint Planning and Development Office (JPDO). Unmanned Aircraft Systems (UAS) Comprehensive Plan: A Report on the Nation's UAS Path Forward. September 2013. Accessible from http://www.jpdo.gov/.
[12] Federal Aviation Administration (FAA). Operation over Human Beings. FAA 14 CFR Part 107.39. Washington, DC. 2018
[13] Vanian, J. NASA's New Tech Could Help Drones Safely Land During Emergencies. Fortune Magazine Website. http://fortune.com/2017/05/28/nasa-drone-crash-land-software/. Published May 28, 2017.
[14] Adams, E. New NASA Tech Tells Drones When They're Broken—And Helps Them Land. Wired Magazine. https://www.wired.com/story/nasa-drone-safe2ditch/. Publish June 20, 2017..
[15] Ambrosia, Vincent G., Steven Wegener, Thomas Zajkowski, D. V. Sullivan, S. Buechel, F. Enomoto, B. Lobitz, S. Johan, J. Brass, and E. Hinkley. "The Ikhana Unmanned Airborne System (UAS) Western States Fire Imaging Missions: From Concept to Reality (2006–2010)." Geocarto International 26, no. 2 (2011): 85-101.
[16] Olson, Isaac J., Alec J. Ten Harmsel, and Ella M. Atkins. "Safe landing planning for an energy-constrained multicopter." In Unmanned Aircraft Systems (ICUAS), 2014 International Conference on, pp. 1225-1235. IEEE, 2014.