SAFE50 Reference Design Study for Large-Scale High-Density Low-Altitude UAS Operations in Urban Areas

Corey A. Ippolito[1], Kalmanje Krishnakumar[2]
NASA Ames Research Center, Moffett Field, CA, 94035

Vahram Stepanyan[3]
University of California Santa Cruz, NASA Ames Research Center, Moffett Field, CA, 94035

Anjan Chakrabarty[4], Josh Baculi[5]
SGT Inc., NASA Ames Research Center, Moffett Field, CA, 94035

Enabling safe, routine, and high-density flight-operations of small UAS at low-altitude over heavily populated urban centers presents one of the most challenging goals for emerging Unmanned Aircraft System (UAS) Traffic Management (UTM) system concepts. Low-altitude urban environments, such as within urban canyons, present considerable uncertainties and difficulties. These challenges are exacerbated by a very low risk tolerance, as urban operations by definition involve flight over people, property, and infrastructure. While a significant number of concepts and technologies have been pursued in the literature across many parts of a UTM system, there is significant variability in the design space; assumptions from high-level design choices result in widely-varying requirements throughout the entire traffic system, including at the vehicle-systems level. 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. The SAFE50 study establishes a consistent and complete-vertical design from the high-level traffic management down to vehicle-systems level architectures. This study focuses on a realistic point-design in the larger trade space that meets challenges through advanced onboard vehicle-level autonomy while assuming today's technology and today's infrastructure. This paper presents an overview of the NASA SAFE50 point-design study and presents a summary of the design study elements, including assumptions, concept of operations, system designs, architectures and requirements. The SAFE50 project seeks to validate this reference design through simulation, hardware prototyping, and flight testing. Initial results from simulation and flight testing as part of the verification and validation process are presented for this reference design study.

I. Introduction

The advancement of Unmanned Aircraft Systems (UAS) Traffic Management (UTM) system concepts from segregated flights in lightly-populated areas towards large-scale high-density operations over densely-populated environments presents a substantial increase in complexity and introduces new and difficult design challenges. 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 with significant economic growth potential in this market [1]. However, the problem of determining how to facilitate routine, safe, and fair access to this high-demand airspace remains an open question. Requirements across all parts of a UAS traffic system become more stringent, for instance in terms of reliability, safety, performance, and resilience. The urban environment poses significant new challenges. Risks substantially increase as operations advance to human-safety critical requirement levels involving operations near and around

[1] Research Scientist, NASA Ames Research Center, Moffett Field, CA 94035, AIAA Senior Member.
[2] NASA Ames Research Center, Moffett Field, CA 94035, AIAA Senior Member.
[3] Senior Research Scientist, University of California Santa Cruz. AIAA Senior Member.
[4] Research Engineer, SGT Inc., Moffett Field, CA 94035. AIAA Member.
[5] Systems Engineer, HX5 LLC., NASA Ames Research Center, Moffett Field, CA 94035, AIAA Member.

people, over city infrastructure, and around other airborne vehicles. There is significant variability and degrees of freedom in the design trade space across all elements of the UTM system, there is a large set of stakeholders with competing desires and requirements, there is tremendous variability in the high-level concepts and architecture design choices, there are significant interdependencies and coupling of requirements throughout system design.

The UAS Traffic Management effort at NASA aims to enable access to low-altitude airspace for small UAS [2][3][4]. This goal is being pursued partly through partnerships that NASA has developed with the UAS stakeholder community, the FAA, other government agencies, and the designated FAA UAS Test Sites. NASA is spearheading the development of a UTM research platform that instantiates an application programming interface (API)-based coordination of UAS operations and services into a research software environment. Certain executable research software components are shared with partners under project release agreements. NASA uses the research platform with its partners to test and evaluate increasingly complex UAS operations and associated UTM Technical Capability Levels (TCL). In the current design as of this publication, the UTM system design concept is at TCL-3 capability level, allowing for beyond visual line-of-sight (BVLOS) operations segregated away from people, property, and other air vehicles. The planned shift to TCL-4 capability level includes expanding operations over highly-populated urban environments, high-density operations, higher levels of vehicle autonomy, and inter-vehicle interaction (Figure 1) [4].

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

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. 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.

While autonomous systems research for flight vehicle has been an active field for many decades, there is no general agreement on specific requirements for autonomous systems operating under a UTM system in urban areas, with many differing competing concepts, definitions, ideas for autonomy, and assumptions in the large complex design space. There is a lack of validated concept studies, architectures, rules, and requirements in this regime, particularly that address the full design solution from the higher-level air traffic management level down to the vehicle subsystem level in a formal, methodical, and traceable manner. In this paper, we present the results from the NASA SAFE50 conceptual design and systems study that investigates the trade-space for high-density low-altitude urban UTM operations. This advanced conceptual design study develops a feasible, verified, validated point-design solution. The SAFE50 point-design concept places emphasis on advanced, highly-autonomous, and highly-capable vehicles, and favor intelligent onboard autonomy over direct human control with today's technologies and operating in today's urban environments. This paper describes the SAFE50 systems design study. This paper focuses on a providing a general overview and outline of the design study while highlighting decisions made in the architectural solution. Additional details of the autonomy architecture and components within the SAFE50 reference design study are being published in a companion publication at this conference [5].

II. SAFE50 Reference Design Study

The SAFE50 reference design study was conducted following the conceptual process illustrated in Figure 2. Requirements flow from the concept of operations. Two specific operator scenarios were considered: point-to-point (doorstep-to-doorstep) operations scenario, and emergency response operations scenario. Within each operations operator scenario, a set of off-nominal scenarios were defined. Nominal and off-nominal scenarios were elaborated in terms of use-case descriptions which detailed step-by-step procedures. Additional requirements flowed from analysis of the stakeholders and analysis of the low-altitude urban environment. The requirements flow from these elements are satisfied in the architecture design. The architecture consists of two main models, a functional model and a physical model. Each model contains an architecture specified as a formal leveled hierarchical decomposition. The functional model focuses on functional requirements and sequencing, and includes flight phase decomposition and functional flow block diagram (FFBD) models. The physical model contains a level decomposition of the physical structure of the system, which starts the highest UTM level and breaks down to the vehicle subsystems component level. The physical model breakdown includes a specification of the SAFE50 Reference Design Vehicle and the SAF50 Reference Autonomy Architecture. The physical model breakdown includes both software and systems/hardware. The software system architecture includes flight software configurations and simulation configurations. Simulation configurations include stand-alone simulation, hardware in the loop simulation, batch mode simulation, and UTM lab test integration configurations. Generalized vehicle-level requirements are derived from the reference architecture and organized into function, performance, and equipage requirements.

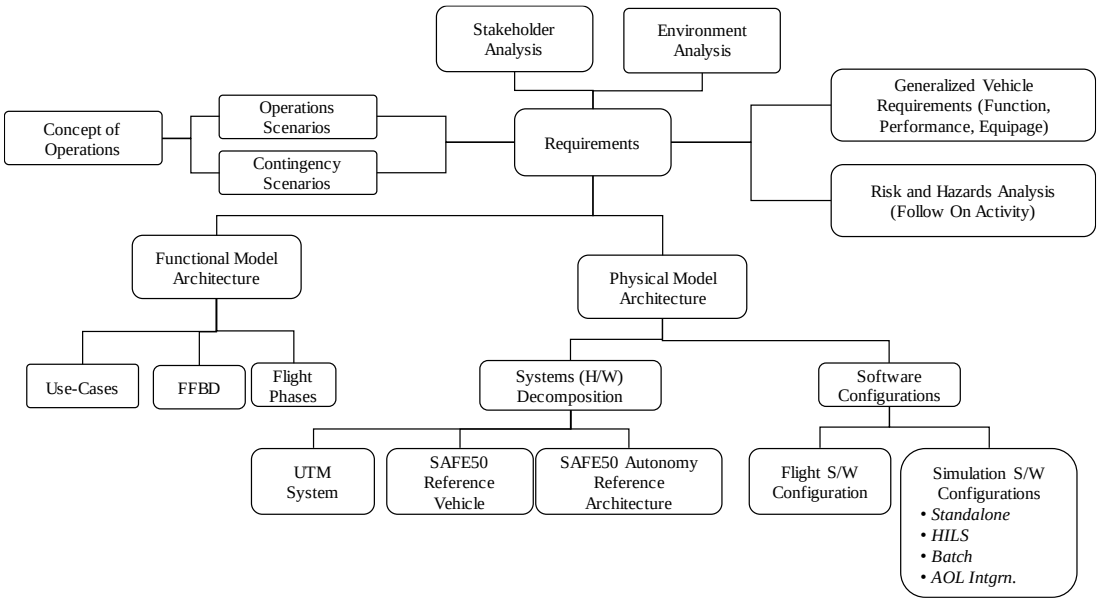

Figure 2. Elements of the SAFE50 Reference Design Study

The SAFE50 reference design study focuses on elaboration of verified and validated vehicle-level requirements. Vehicle system requirements flow from the higher-level system requirements and the rest of the design study elements. Verification and validation of this study occurs through analysis of the reference architecture implementations in flight testing and in simulation testing.

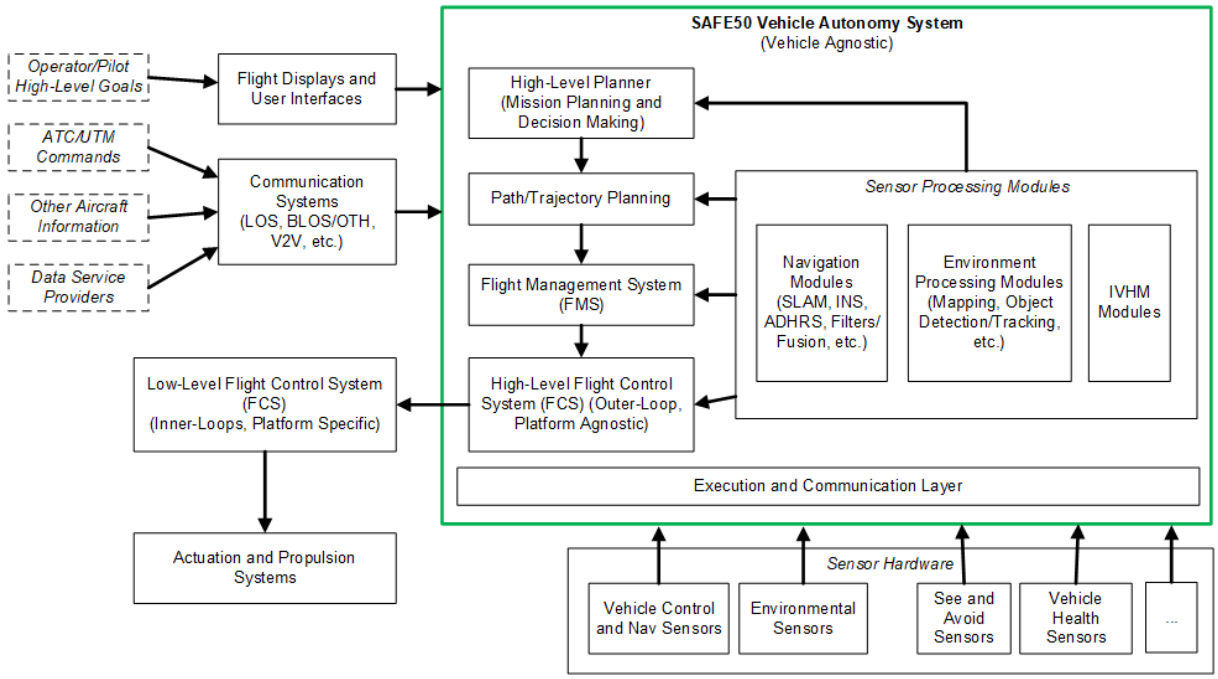

Figure 3. SAFE50 Reference Autonomy Architecture – Concept and Focus

Autonomy can be broadly defined as anything within the look, think, act, and communicate loop for an intelligent system. A conceptual representation of the SAFE50 autonomy reference architecture and the scope of focus for this project is shown in Figure 3. Each vehicle system will require platform-specific subsystems that are certified under the UAS manufacturer's certification processes and are delivered with the vehicle. This includes actuation systems, propulsion systems, and inner-loops for industry standard guidance, navigation, and control (GN&C) systems. For instance, the vehicle may be required to deliver attitude control system modes in the GN&C with certain functional requirements and performance guarantees. The SAFE50 autonomy system conceptually draws a box around the higher-level flight control and flight management systems that are vehicle agnostic. Human interfaces, such as flight displays, are required but outside of this study's main focus. Likewise, while this study specifies requirements for communication systems (e.g., vehicle to multivehicle / V2X must provide certain information to vehicles at a specified distance at a specified rate), elaboration of said specifics (e.g., specification of specific hardware, protocols, packet formats, and communication standards) is beyond the scope of this study. The SAFE50 autonomy system does focus on specification of higher-level autonomy and non-standard aviation system components that are required to meet the system design requirements. The autonomy architecture focus includes mission planning, decision making, mission execution, path and trajectory generation, GNSS-free navigation system components, environment mapping, object detection and tracking, and intelligent vehicle health management (IVHM) functions.

A. Urban Environment

Urban environments contain dangerous and unpredictable atmospheric hazards, characterized by temporally and spatially unsteady wind-fields around complex urban topologies [6]. The Atmospheric Boundary Layer (ABL) is defined as the wind layer that is influenced by surface forcing with time-scales of around an hour or less. The ABL thickness is typically expected to range between 100m to 3,000m, though ABL thickness varies in time and space as a non-trivial function of parameters such as ambient conditions and surface properties [7]. These forcings include frictional drag, evaporation and transpiration, heat transfer, pollutant emission, and terrain-induced flow

modifications. Atmospheric instability occurs when a vertically-displaced air particle accelerates in the direction of displacement which can locally occur within urban environments and may effect vehicle performance [8]. Local wind influences include time-varying influences from local geography. While simple correction models exists for simple larger-scale geographic features, for instance approximations for wind change over hills, these are not trivially applied to urban environments. The ABL structurally is composed of several different layers with different governing characteristics. The Urban Canopy Layer (UCL) is the layer of air in the urban canopy beneath the mean height of buildings and trees that is controlled by microscale processes that rapidly vary in time and space [9]. The Urban Boundary Layer (UBL) is layer above the UCL that is mixture of both UCL forcing below and ABL forcing above that is controlled by local to meso-scale process at temporal and spatial scales larger than the UCL[9]. There are additional atmospheric hazards that impact small UAS in urban environments, including regional weather phenomena, thermals, dust devils, and turbulence. UAS flights within the SAFE50 system design study are expected to be within the ABL, and usually within either the UCL or UBL. The micro-scale rapidly time-varying atmospheric phenomena experienced in urban environments are potentially fatal to small vehicles, and are complex, difficult to predict and detect, and difficult to robustly accommodate on aircraft of this scale [8].

Reliable low-latency communication for high-density operations is not easily achieved. Operation within urban canyons occur in a cluttered radio-frequency (RF) environment with high noise levels, degraded bandwidth and range, line-of-site blockage, and other RF issues such as signal reflection. Flights with any appreciable distance will be beyond both visual line-of-site (BVLOS) and communication RF line-of-sight (RFLOS) from ground operators. While existing 4G cellular communication is commonly available within urban environments, there are well-documented issues with the current cellular networks for large-scale operations which preclude use a reliable low-latency high-bandwidth link for communication, command and control (C3) of UAS. Urban canyon environments are not conducive to utilization of satellite-based communication for over-the-horizon (OTH) communication. Similar, a Global Navigation Satellite System (GNSS) such as Global Positioning System (GPS) will be impacted. Flight operations are expected to occur in a degraded or denied GNSS/GPS condition.

Static ground objects (SGO) pose a hazard at low-altitudes within the urban canyon. Static objects include building structures, towers, billboards, trees, cables, scaffolding, tethered balloons, and power lines. The location of these objects may not be known ahead of time with any given level of certainty or accuracy. Many static objects are difficult to detect, such as power-lines with characteristically long and thin geometry, and are well-document hazards to manned and unmanned aircraft. Likewise, high-density BLOS UAS operations represent a hazard to static objects and urban infrastructure, which is exacerbated by high-failure rates experienced in current commercially available UAS.

Timely detection and response to emergencies and onboard failures, which is critical for safe aircraft operation, will be difficult. Without onboard pilots, the requirement to safely address failures – for instance, to quickly scan the environment and identify safe pedestrian-free landing locations in an emergency – is difficult in densely-populated areas. Dynamic Ground Objects (DGOs) which proliferate in this environment – such as pedestrians and automobiles – are difficult to detect, predict, and avoid. Utilizing current commercially-available sUAS technology for beyond line-of-site urban environments would represent an unacceptably high risk. Risks are assessed in this study as a function of likelihood and consequence. There is a high probability of system failure reported in the literature for the current generation of sUAS. The consequence of failure is also high due to potential for human injury or damage to property.

To summarize, the environment poses a number of challenges:

- Complex dynamic environment with significant uncertainty;
- The presence of dangerous and unpredictable atmospheric hazards, such as unsteady wind-fields and gusts in the atmospheric boundary-layer around complex urban topologies, presence of hazardous adverse weather conditions;
- Difficulties in detecting, avoiding, and mitigating risk to objects, including dynamic ground objects (automobiles and pedestrians), static ground objects (power-lines, towers, structures, overpasses), and other aircraft (manned and unmanned);
- Challenging RF environment with disruptions to wireless communication, impairing air-ground communication and satellite-based communication links;
- Degraded or denied GNSS/GPS conditions;

B. Concepts and Design Study Challenges

The follow lists some of the technical challenges faced in this design study:

- Lack of validated concept studies, architectures, rules, or requirements in this regime that cover the higher-level traffic management level down to the vehicle subsystem level;
- Lack of fundamental physical understanding for how vehicles of this scale behave in these environments, including lack of experimental data, lack of validated flight dynamic models, and insufficient fidelity of existing models;
- Difficulty assuring safety in this environment, e.g. a lack of standardized risk models and definitions, difficulty in establishing acceptable risk postures and safety margins;
- Lack of standardized requirements and an established certification process for autonomous small UAS;
- Large number of stake-holders with competing needs and requirements, and design must address a wide range of concerns (e.g., insurability, noise, privacy, etc.).

The following summarizes challenges with the concept of operations for low-altitude high-density operations:

- Low-altitude autonomous flight is inherently higher risk;
- High-density operations in near proximity to other aircraft;
- Highly-constrained spaces in and around urban canyons;
- Operations beyond RF line-of-site and visual line-of-site from ground operators;
- Mixed operation of manned and unmanned aircraft;
- Separation assurance (SA) and collision avoidance (CA) challenges;
- Flight in urban areas by definition will be over or near people, property, and infrastructure (high-valued assets, higher consequences);
- Ground-based surveillance technologies are difficult to apply to this environment.

Airborne high-density operations require operation in close proximity to other aircraft, both manned and unmanned. Separation assurance (SA) and collision avoidance (CA) between air vehicles in a mixed-use airspace is difficult due to challenges in this environment. Another issue is the difficulty in meeting required autonomous see and avoid (SAA) requirements for vehicles of this scale with current technology. A consideration for sUAS traffic management design is how to assign responsibility for SA and CA, and how to specify SAA requirements that can be realistically met with current technology. The requirement for a sUAS to detect other air vehicles is difficult to achieve with currently technology. Collaborative V2X communication methods have been utilized to assist in the detection problem, such as through the Automatic Dependent Surveillance-Broadcast (ADSB) system on manned aircraft. Separation assurance responsibilities are assigned to regional air traffic controllers for manned aircraft in controlled airspace. Alternatively, autonomous local vehicle-to-vehicle deconfliction (for instance through collaborative V2X communication with a common decentralized onboard avoidance algorithms) have been presented literature for decentralized SA and CA of UAS as an alternative architecture design.

C. Vehicle Level Challenges

The list of vehicle-level challenges includes:

- Low reliability of current small UAS (high likelihood of failure);
- Significant variability in vehicle systems and technologies on the market;
- Significant size, weight, and power (SWaP) limitations for onboard vehicle technology;
- Insufficient precision, accuracy, reliability, and robustness in guidance, navigation and control (GN&C);
- Limited onboard autonomy;
- Inability to see-and-avoid hazards;

- Limited onboard failure accommodation and fragility;
- Degraded navigation system performance in urban environments (GNSS-degraded or denied);
- Degraded air-ground communication without direct line-of-site (low reliability, intermittent connectivity, extended drop-outs, high latency, low bandwidth).

D. Constraints and Assumptions

The set of assumptions and constraints derived in the conceptual design study include the following:

- Vehicles up to 55lbs/87KIAS (possibly extended to small-medium UAS up to 330lbs/200KIAS per [10]);
- Operations occur in low-altitude urban environments, at or below 400 feet;
- Systems are designed using technologies that are available today and infrastructure available in today's urban environments;
- Operations in urban area require overflight over people and property. Autonomous detection and control mitigation systems are required;
- High-density operations allowing concurrent operations of multiple aircraft operated by different operators at any given time in close-proximity to each other;
- Accuracy of closed-loop trajectory prediction and control is low. This is due to an accumulation of sensor uncertainty, navigation uncertainty, control uncertainty, disturbance atmospheric uncertainty, vehicle modeling uncertainty, etc.;
- Routine and responsive operations for operations approval;
- Appropriate size, weight, and power (SWaP) vehicle constraints for a small UAS will be derived from the SAFE50 reference vehicle;
- UAS to USS communication is unreliable;
- Vehicle to multiple vehicle communication is required and must be reliable. This design will assign responsibility of V2X provides cooperative SAA/SA/CA. Failure of V2X must be considered in off-nominal scenarios;
- Flight operations occur entirely beyond visual and RF communications line-of-sight from ground operators;
- Flight operations occur within a GPS-denied or GPS-degraded environment;
- Ground-based surveillance is not likely possible. Separation assurance responsibility is assigned to the onboard vehicle autonomy system in this design study;
- Ground hazards and objects - static and dynamic - are not known with any certainty ahead of time. Vehicle systems will be required to autonomously detect and avoid objects in real-time;
- A cooperative sUAS-to-sUAS SAA/CA/SA design is chosen with direct vehicle-to-vehicle negotiation;
    - Vehicle systems are required to have a common decentralized avoidance algorithm for collision avoidance. Vehicle systems are required to provide V2X communication. USS is responsible for assuring cooperative CA/SA by controlling maximum UAS density allowed in shared operating volumes when approving plans;
- Deconfliction of route is not required in the use-case specifications. However, this can be accomplished through (1) adding an Supplemental Data Service Provider (SDSP) that provides real-time traffic density maps to the UAS from the USS, and (2) adding route optimization in the onboard path planning system, for instance by adding traffic density as a cost function, or adding areas of high traffic density as a constraint volume to be avoided;

- The initial study will assume all aircraft in the vicinity are cooperative and UAS. Future extension to this system design study will consider interaction with non-cooperative UAS and with manned aircraft. However, we will specify UAS have ADSB-in capability to monitor manned traffic.

III. Concept of Operations

E. Generalized Use-Cases

A categorization of general use-cases (GUC) for urban environments was developed from the use-cases presented in Belcastro et al. [11]. This categorization is summarized in Table 1. From this set of generalized use cases, two were selected to be the primary focus in developing the concept of operations: GUC-1, Point-to-point, and GUC-5.1, High-priority point-to-point.

Table 1. Categorization of Generalized Use Cases

ID	Generalized Use Case	Examples
GUC-1	Point-to-point	Package/Cargo Delivery
GUC-2	Patrol	Imaging/Data Acquisition/Survey of Public/Private Land (Terrain Mapping, Land Surveys for Future Construction), Monitoring & Patrol, Broadcasting/Filming
GUC-3	Pursuit	Videography at Public Events (Parades, Festivals), Broadcasting/Filming
GUC-4	Volume occupation	
GUC-4.1	Intra-area	Videography at Public Events (Sporting Events, Fireworks Displays), Infrastructure Inspection (Canals, Bridges, Mines, Onshore Oil and Gas Facilities), Imaging/Data Acquisition/Survey of Public/Private Land (Construction Site Inspection), Broadcasting/Filming
GUC-4.2	Trans-area	Infrastructure Inspection (Railroads, Power Distribution Lines, Oil Pipelines), Broadcasting/Filming
GUC-5	Emergency/High-priority	
GUC-5.1	High-priority point-to-point	Emergency Response, Law Enforcement (Motor Vehicle Accident Response), Package/Cargo Delivery (Delivery of Emergency Medical Supplies), Fire Response
GUC-5.2	High-priority pursuit	Counter UAS Operations (Mitigation of Security Threats & Rogue UAS), Law Enforcement (Aerial Photography for Suspect Tracking)
GUC-5.3	High-priority search/rescue	Search & Rescue (Missing Persons/Airplane/Ship, Survivors from an Accident or Disaster), Law Enforcement (Search and Rescue of Missing Persons)
GUC-5.4	High-priority monitoring/inspection	Security at Public Events (Monitoring/Detection), Disaster Response (Monitoring/Mapping), Emergency Response, Law Enforcement (Crime Scene Investigation, Accident Scene Investigation)

F. Concept of Operations

The SAFE50 design study focused on two primary use-cases. A point-to-point scenario (doorstep-to-doorstep, GUC-1.0) and an emergency response scenario (GUC-5.1). The concept of operations is summarized in Figure 4. The point-to-point scenario was selected as the primary use-case to consider as it represents one of the broadest use-cases in terms of requirement development and elaboration, as solution to this use-case meets most of the functionality required for the system design. The emergency response scenario was selected as the secondary use case to evaluate as it naturally extends the point-to-point use case with the notion of priority access.

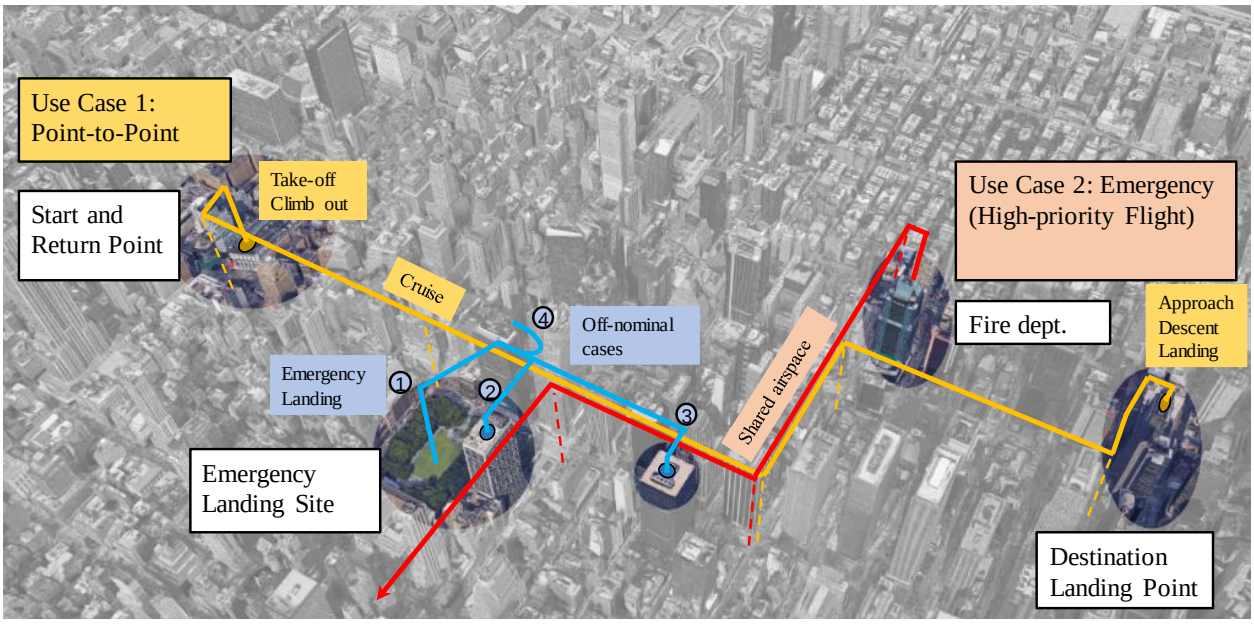

Figure 4. Concept of Operations and Use-Cases

The starting location and destination location are assumed to be any random point in the city. Controlling the location for takeoff and landing is a responsibility assigned to the UAS operators. Takeoff and landing sites must have reliable UAS to UAS ground-element communications. The UAS operator will provide mission objective to the UAS (received by the onboard autonomy subsystem) that minimally includes the destination location and emergency landing locations. The UAS autonomously generates several possible flight plans that include a primary/nominal plan and potential alterative plans. This is illustrated in Figure 5. These potential plans may take into account different high-level objectives for the aircraft, or for instance, might plan to avoid areas where winds or traffic may be high. The UAS must calculate "operational volumes" around the planned trajectory, and then break the volume up into smaller operating volume segments that will be submitted to the UTM system. In addition, the UAS may choose to develop contingency plans in order to meet minimum risk and safety requirements. For example, the UAS may choose to identify emergency landing zones, identify contingency plans to fly to the nearest emergency landing zone should a failure occurs at any point along a planned flight path, and then calculate the volumes that might be entered as a "contingency volume". The UAS will generate a USS flight request that includes operational volumes, contingency volumes, desired take-off time, and a conservative landing time. The UAS can optionally involve human interaction from the UAS operator at any time. The UAS sends the flight request to the USS (UAS to USS communication is relayed through the UAS ground element). If the USS rejects the plan, the UAS is required to generate a new plan, and may take advantage of SDSP information to determine a conflict resolution. The submission process repeats until a plan is approved by the USS. The UAS sends a UTM "all-clear" message after completing a pre-flight process, receives approval from the USS, then can start the mission.

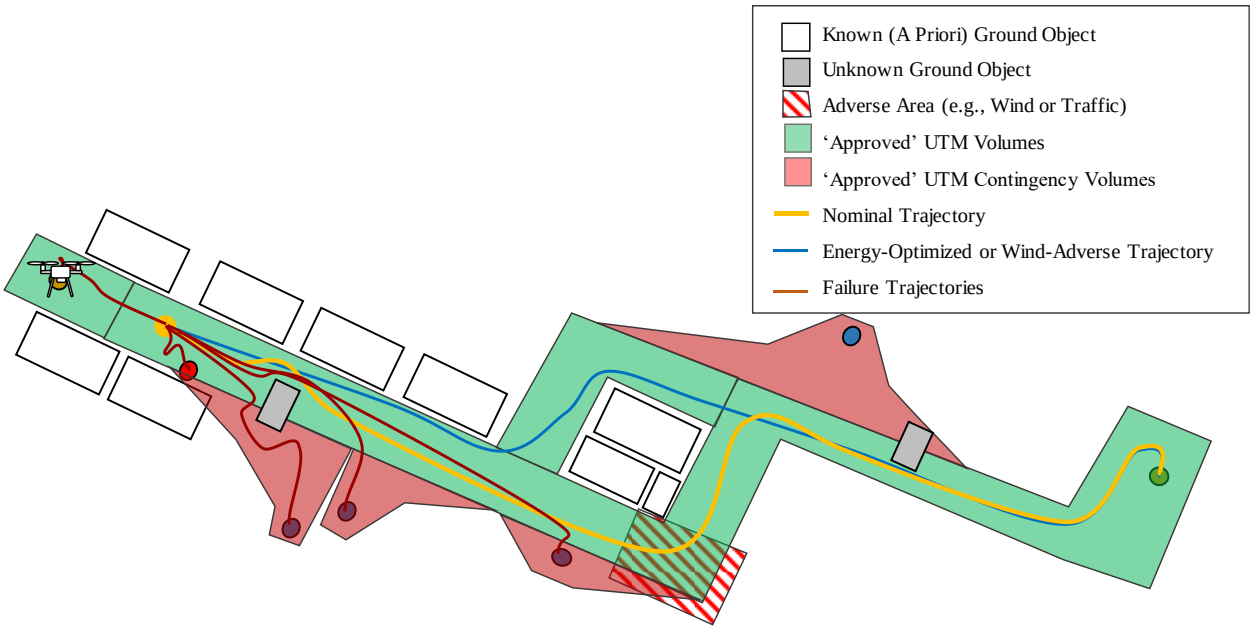

Figure 5. Concept of Operations Illustration

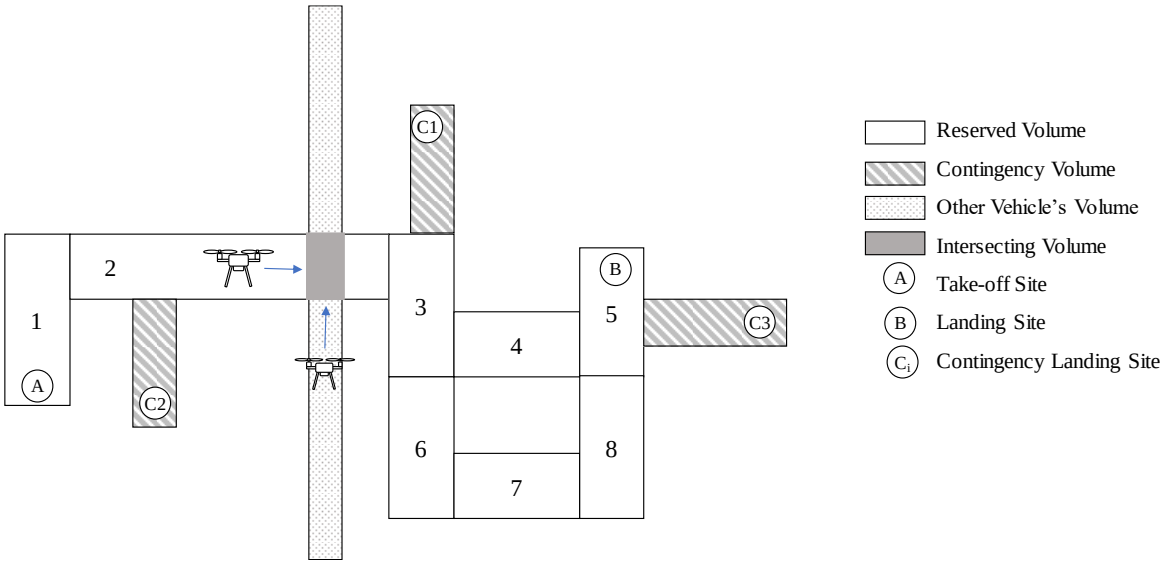

Figure 6. Segmented Volumes and Shared Reservation

An illustration of a segmented volume plan is shown in Figure 6. Once approved, the vehicle will take off and execute the nominal flight plan. When the UAS leaves a volume that it won't return to, the UAS will send a volume clearance notification to the USS and receive acknowledgement. Once the volume clearance notification is sent, the UAS will no longer be approved to enter that volume for the remainder of the approved flight. Note that the air-ground link is unreliable in flight, and there may be delay in releasing volumes. This design choice is conservative in terms of safety/risk violations, but performance and throughput of the UTM network may degrade.

G. Static Ground Object Detect and Avoid (DAA) System, Dynamic Ground-Risk Mitigating Flight Control System

As the UAS executes the flight, the UAS is required to continuously sense and map static ground objects. The UAS must continuously regenerate plans (nominal, alternative, and contingency plans) from its current state to address any unforeseen static objects that enter the periphery of its sensing range. The planning system frequency requirement

is a function of sensing range and parameters such as maximum forward vehicle speed. The UAS must also continuously maintain a safe contingency landing plan for any contingencies that require a 'land immediately' type function or an uncontrolled landing (ditch). For each of these contingency plans, the vehicle must maintain its state to ensure the risk to dynamic ground objects is lower than a specified threshold, as specified by a risk model analysis and ground risk mitigation system.

The UAS is required to continually sense and track dynamic ground objects. The UAS operator is responsible for ensuring ground risks requirements are met based on the ground risk model analysis, manufacturer certification, and manufacturer documentation. Conservative flight plans that always stay away from people/property would satisfy the ground risk requirements, but would not allow access to many areas of the urban space. Alternatively, manufacturers can provide an active ground-risk mitigating flight control system. In the SAFE50 reference design, this system includes dynamic ground object tracking and inputs into a local real-time trajectory planning system. The ground-risk system is responsible for computing sufficient 'do-not-enter' volumes that include all positions that would violate minimum safety threshold requirements determined through evaluation of the ground risk model. The local-planner is responsible for ensuring ground-risks 'do-not-enter' constraints are not violated. Manufacturers are responsible for providing the trajectory models, cost model parameters such as probability of failure, off-nominal behavioral models, and the desired level of continency management and off-nominal control resilience to meet the specifications of the delivered system. Manufacturers are responsible for verification and validation (V&V) and certification of these systems through the appropriate certifying authority stakeholders.

H. Risk-Based Contingency Handling

If a contingency event occurs, the UAS will immediately execute the associated contingency plan, which must always maintain position within an approved operational volume or approved contingency volume. The vehicle will broadcast the emergency event to surrounding vehicles through V2X communication link, and send an emergency notification to the USS when the air-ground link allows. The vehicle will execute either an emergency landing at a designated safe landing location (abort), execute an emergency landing at a safe location determined by the dynamic ground object detection system (land now), or perform a flight termination maneuver (flight terminate) determined by the dynamic ground object detection system. If flight termination is uncontrolled, the UAS should terminate in a safe location as this was the responsibility of the ground risk mitigation system.

I. Overlapping Operations with Collaborative SA/CA

The requirement for high-density operations is met through allowing UAS to overlap operational volumes. This is illustrated in Figure 6. Consider the case where a vehicle requests a volume that is already approved by one or more vehicles. The USS will ensure that all vehicles are equipped with the requisite cooperative SA/CA system, including V2X and avoidance control laws, and the vehicles meet minimum performance requirements. The USS will check for the worst-case overlap conditions if the new plan is approved. The conditions to check depend on the requirements specified by the SA/CA system. In our reference design, the SA/CA system provides provably safe performance when the number of vehicles involved in an encounter and the approved volume is lower than a certain threshold. The USS will check for the number of overlapping plans, and accept plans that are less than this threshold, or reject plans higher than the threshold. This ensures the system will always be in a safe state, as the USS will never approve a plan that violates the SA/CA requirements.

J. Airspace Assignment Study

A study on airspace assignment was conducted to examine the design space in terms of UTM airspace/volume assignments. A summary of this study and results from this study are pending review and publication. Generally, several different potential airspace assignment methodologies were investigated. Figure 7 shows some of these options, including (1) a single-integrated volume around the entire flight plan, (2) segmented volumes, (3) time-based moving volumes based either on highly-reliable communication or highly-reliable trajectory estimation, and (4) predefined volumes provided by the USS system has the UAS must select. Additional temporal variability can be matched with these options, as shown in Table 2. For instance, segmented volumes could be automatically released based on a time-window reservation, could be released by a positive confirmation message from the UAS to the USS, or could be automatically released based on trajectory-estimation and surveillance data from the UAS. A volume-segmentation and release-after-use design choice was selected, as it conservatively provides strong safety guarantees even in worst-case situations, but provides UTM network performance when coupled with the cooperative V2X SA/CA system.

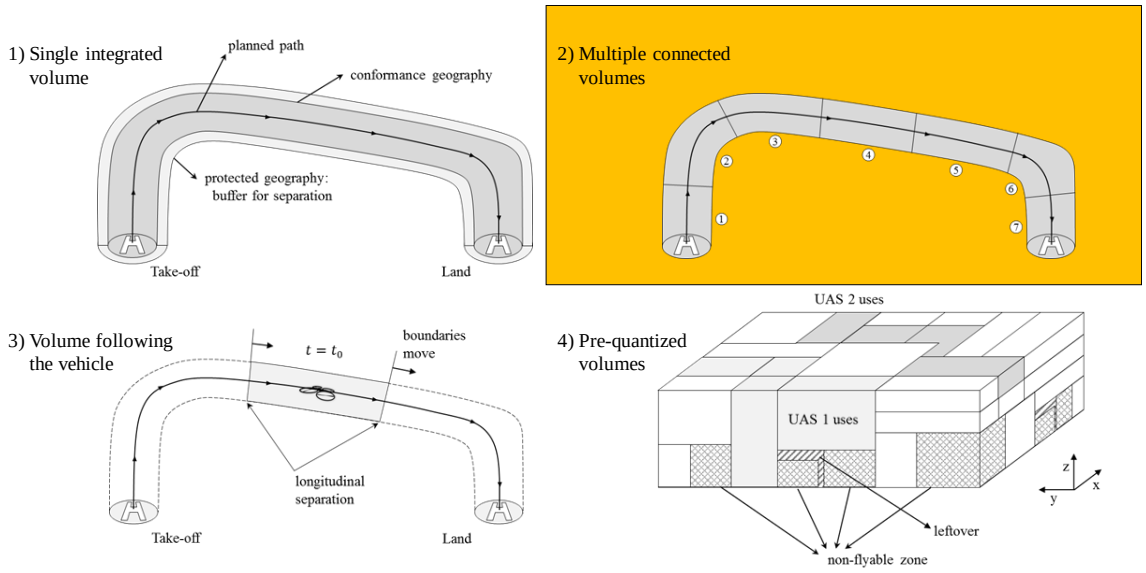

Figure 7. Example Spatial Domain Assignment Trade Space

Table 2. Summary of Preliminary Spatial/Temporal Design Options

Tag	Spatial	Temporal	Pros	Cons
1-1	Single, integrated	Full-time use	Simple creation, Safe, Secured whole path & time	Highly inefficient, Hard management†
2-2	Multiple, divided	Release after use	Simple creation, Little efficient, Safe, Secured path-to-go	Hard management†, Return needs approval
2-3	Multiple, divided	Release-assign	Simple creation, More efficient*	Hard management†, Return needs approval, Non-secured path-to-go
2-4	Multiple, divided	Time windows	Simple creation, More efficient**, Predictable use	Hard management†, Return needs approval, Conditionally secured path-to-go
3-3	Dynamic, continuous	Release-assign	Most efficient*	Hard assignment, Hard management†, Non-secured paths
4-2	Predefined, quantized	Release after use	Little efficient, Safe, Secured path to go	Easy assignment/management††, Return needs approval
4-3	Predefined, quantized	Release-assign	More efficient*	Easy assignment/management††, Return needs approval, Non-secured path-to-go
4-4	Predefined, quantized	Time windows	More efficient**, Predictable use	Easy assignment/management††, Return needs approval, Conditionally secured path-to-go

IV. Requirements and Hazards

K. Stakeholder Analysis

The following stakeholders were identified during the stakeholder requirements analysis phase, as shown in Figure 8. This enumeration of stakeholders is focused on the UAS vehicle system element only. A stakeholder analysis for the entire UTM system is beyond the scope of this study. This list includes the general public, who may be a service requestor for UTM-enabled services but are concerned about issues such as personal safety, noise, and privacy. A set of other service requestors was identified, such as delivery clients for package delivery. The UAS system operator may be a private or public entity. Supplemental Service Data Providers (SDSP) may provide additional services to the UAS, such as weather or traffic maps. The UTM USS provides the majority of UTM services. Regulatory agencies are responsible for establishing regulations regarding UTM/UAS operations, certifying authorities are responsible for defining certification requirements and establishing the certification process, while the UAS system must be maintained in compliance with these certification maintenance requirements. Insurance companies are responsible for establishing the insurance policy requirements and liability. The risk model embedded in the ground-risk mitigation system, as previously described, links a number of stakeholders, including the certifying authority and

insurance companies. A list of additional needs and desires for UAS vehicle-system stakeholders are shown in Figure 9.

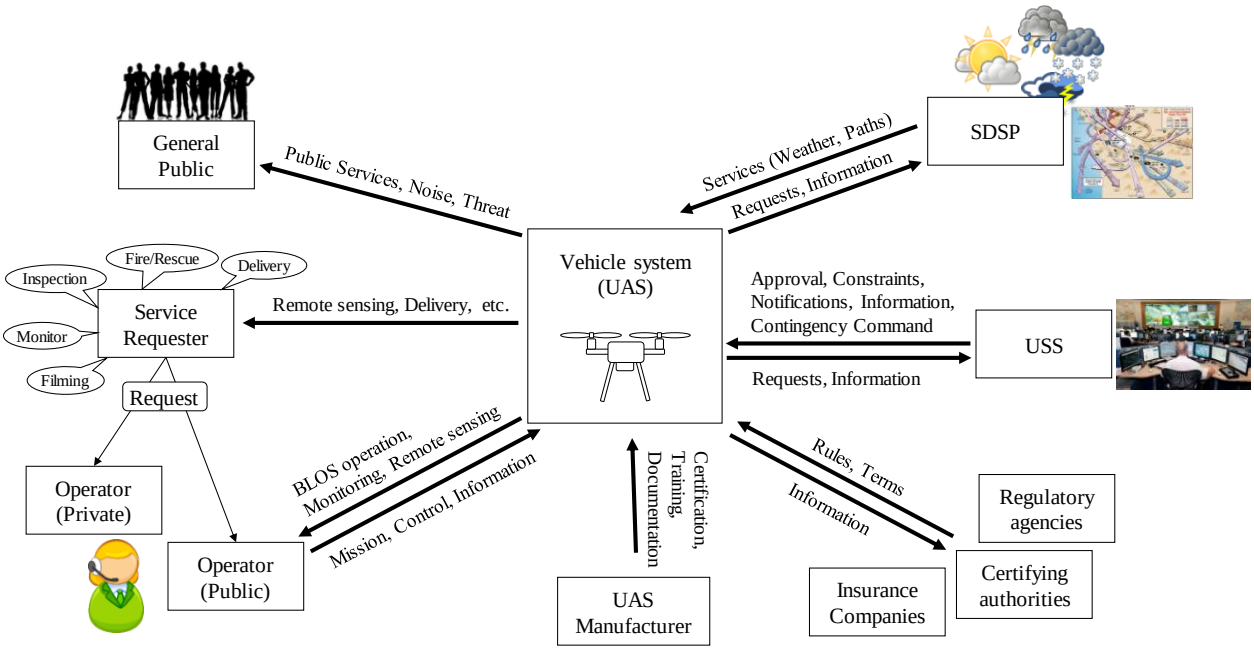

Figure 8. UAS Vehicle-System Stakeholder Model

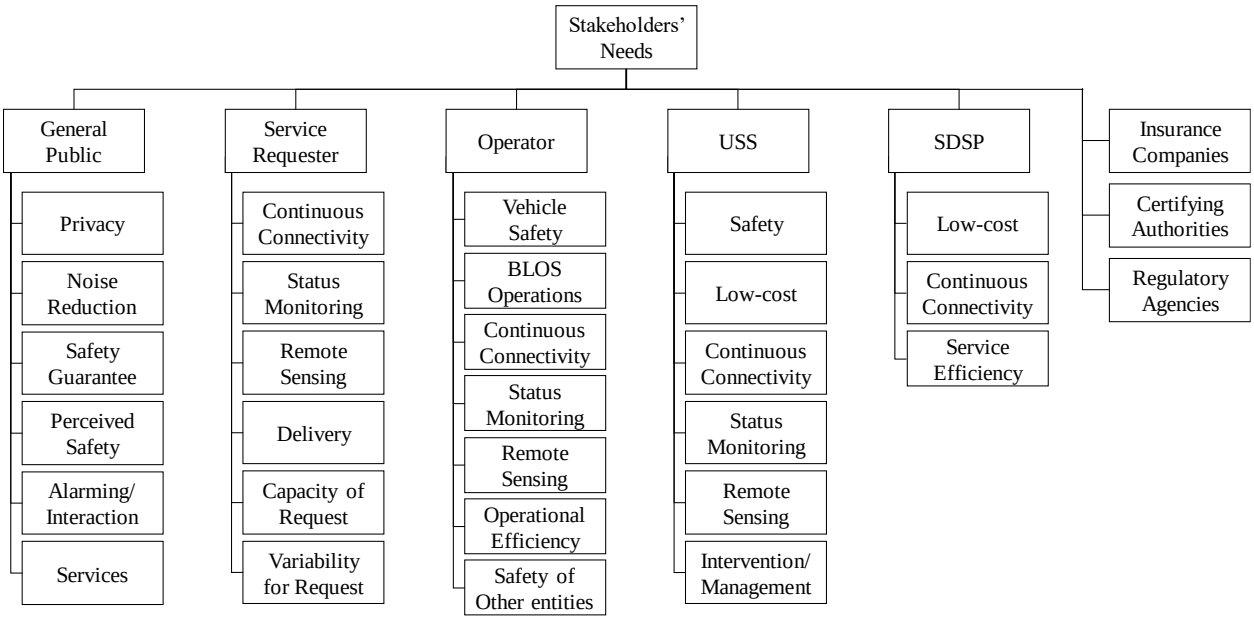

Figure 9. Excerpt of High-Level Stakeholder Needs

L. Risk and Hazards Analysis

A high-level risk and hazards analysis centered on the UAS vehicle system was conducted for this study. This was a vehicle-centric analysis, where scope of the analysis was limited to hazards and risks that are directly related to the UAS vehicle system. A risk and hazards analysis for the entire UTM system beyond the scope of this study. A categorization of entities directly influenced by the UAS vehicle system are shown in Figure 10. Four main categories are the stakeholders identified in Figure 8, other aircraft, dynamic ground objects, and static ground objects. Risk

areas for stakeholders include financial liability, for instance for potential damage caused by approved operations of insured and certified vehicles under established regulations. In this case, if the operator is found to not be at fault, other stakeholders may be held liable or be subject to litigation. Insurance and liability directly impact operational cost models, which are functions of the insurance cost models. The scope of this initial study is limited to cooperative UAS, so UAS present a bi-lateral symmetric risk to other aircraft operating in close proximity. This risk increases as density increases, and can be controlled by the UTM system with existing control mechanisms in the SAFE50 reference design. For instance, USS may reduce the maximum threshold of allowable vehicles in overlap regions to sacrifice UTM network performance for risk minimization.

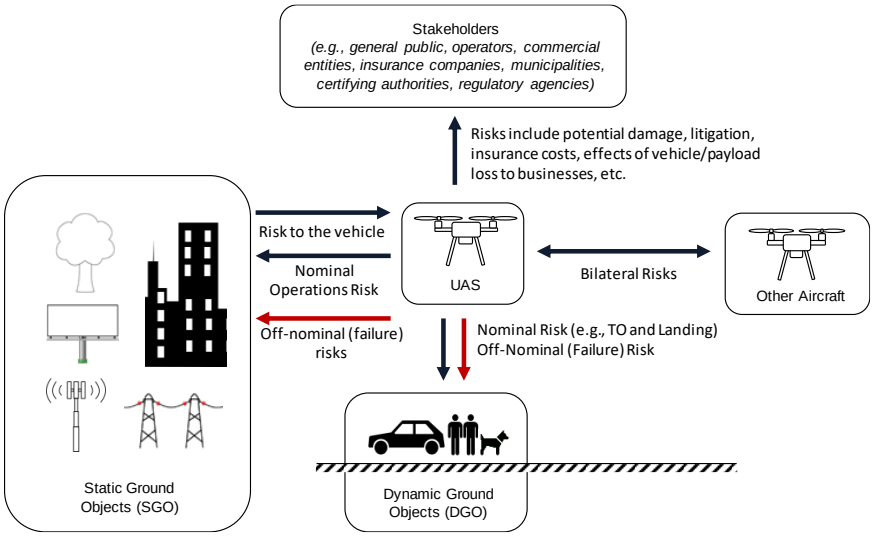

Figure 10. UAS Vehicle-Centric Risks and Hazards

The UAS presents a complex and difficult to mitigate hazard to dynamic ground objects in urban environments. This risk relationship for nominal and off-nominal conditions are described in Section G, and is mapped through the ground risk cost model analysis. Risks are mitigated through passive or active ground risk mitigating flight control. Given the higher safety concerns of dynamic objects, such as a human/pedestrian, and given the assumptions of this system design study, such as requiring landing and takeoff sites be free of obstacles and hazards, in this case dynamic objects pose no measurable hazard to the vehicle and thus risk is unilaterally directed towards the dynamic objects.

The UAS also present a hazard to static ground object. Static objects include critical city infrastructure, such as power-lines and bridges, and private property, such as buildings, towers, and billboards. Implications of collision with a sky-rise building, for instance, may need to consider reporting and filing costs, and expected costs such as costs to perform an external building structural inspection, and measure of expected versus maximum damage. Associated with object risk, we impose a regulatory requirement to mandate reporting of collisions, and the requirement for collection of tamper-free data to support accident investigations.

An excerpt from the risk/hazards list is provided below in Table 3. The final list will be published in an upcoming NASA technical report along with a consequence/likelihood risk assessment.

Table 3. Preliminary Hazards Table, Excerpt

ID	Category	Nominal/ Off-nominal
HZ-1	Static ground object	
HZ-1.1	to Property (public/private)	
HZ-1.1.1	Electromagnetic interference	Nominal
HZ-1.1.2	Collision	Off-nominal
HZ-1.1.3	Fire	Off-nominal
HZ-1.2	to Ground	
HZ-1.2.1	Contamination	Off-nominal
HZ-1.2.2	Forest fire	Off-nominal
HZ-1.3	to Water	
HZ-1.3.1	Contamination	Off-nominal
HZ-1.4	to Air	
HZ-1.4.1	Contamination (fossil fuel)	Nominal
HZ-1.5	from Ground obstacles	
HZ-1.5.1	Effect on flight safety	Nominal
HZ-1.5.2	Reduction of operational efficiency	Nominal
HZ-1.5.3	Limitation to operation space	Nominal
HZ-1.5.4	Collision	Off-nominal

M. Requirement Architecture

The following section summarizes the requirements architecture. A UAS vehicle-centered grouping of requirement sources is shown in Figure 11. These include environmental challenges, atmospheric uncertainty, failures and contingencies (risk), etc. Requirements for hazard footprint awareness and risk awareness were described previously. Additionally, the system design models developed under other parts of the SAFE50 refence design study are considered part of the requirements specification for the system.

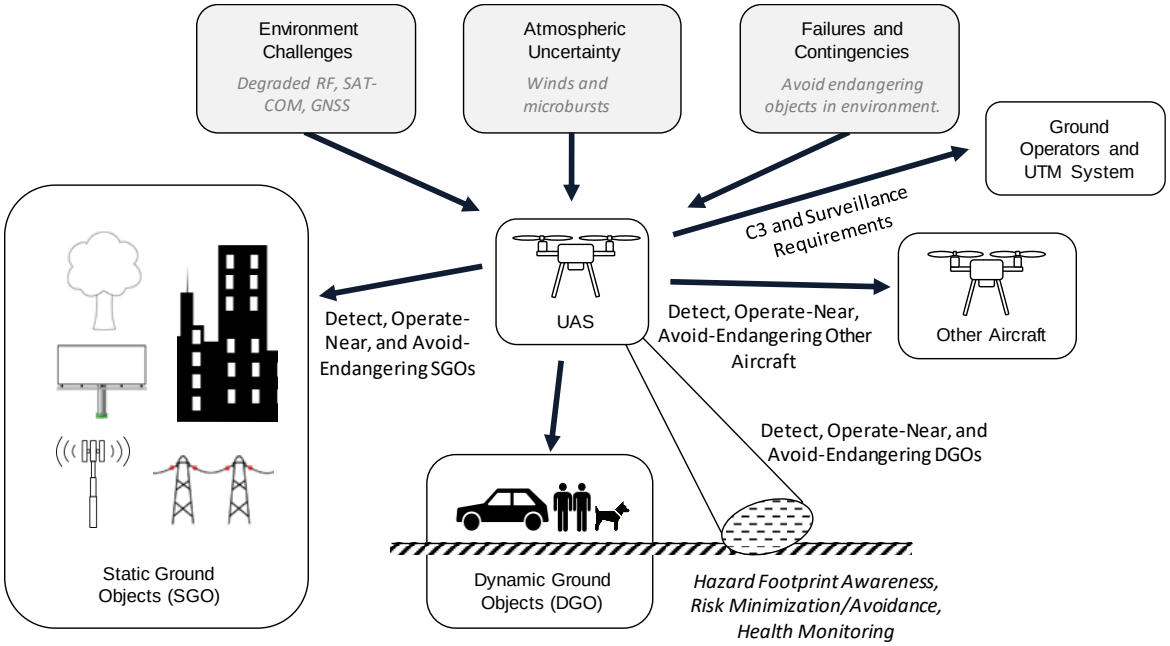

Figure 11. General SAFE50 Vehicle-Level Autonomy Requirements

An excerpt from a mission requirements are shown in Figure 12 and Table 4.

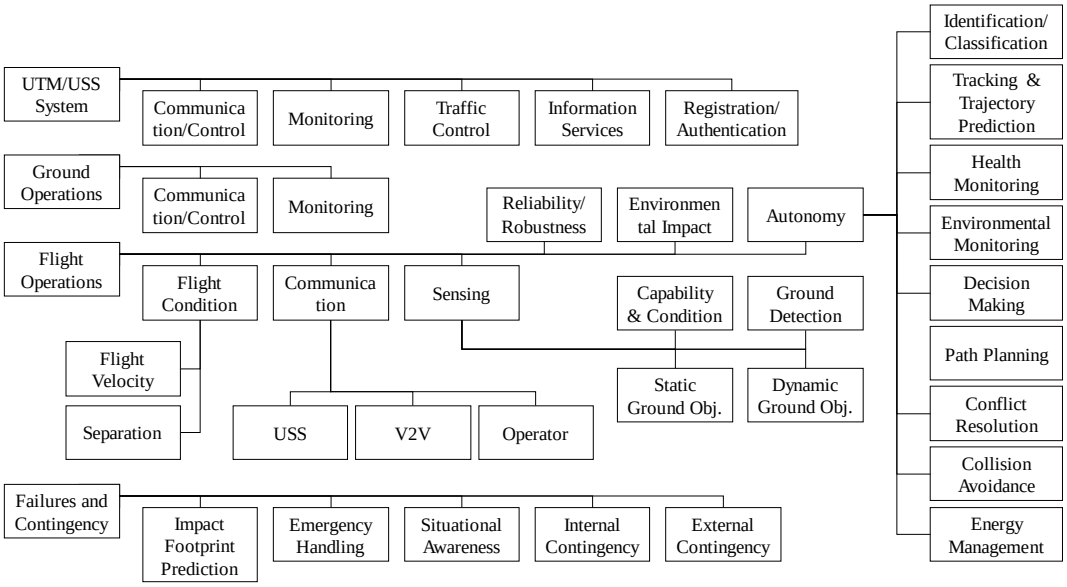

Figure 12. Level 1 Mission Requirements, Excerpt

Table 4. Excerpt from the Mission Requirements Table

ID	Category	Description
MRQ-3	Flight operations	
MRQ-3.1	Flight condition	
MRQ-3.1.1	Flight velocity	A vehicle shall fly at a speed that satisfies all related requirements and guarantees safety of the vehicle and other entities.
MRQ-3.1.2	Separation	
MRQ-3.1.2.1	Aerial object	A vehicle shall keep a safe distance away from known aerial object for preventing possible collision, conflict, or wake interference at the current speed within a time horizon.
MRQ-3.1.2.2	Static ground object	A vehicle shall keep a safe distance away from every static object for preventing possible collision at the current speed or wind sheer.
MRQ-3.1.2.3	Dynamic ground object	A vehicle shall keep a safe distance away from every dynamic object for preventing possible collision at the current speed within a time horizon.
MRQ-3.2	Autonomy	
MRQ-3.2.1	Identification/Classification	A vehicle shall be able to classify ground objects into Vehicle (dynamic), Human/life (dynamic), or Static.
MRQ-3.2.2	Tracking and trajectory prediction	
MRQ-3.2.2.1	Aerial object tracking	A vehicle shall be able to track all known aerial objects, lying near the flight path or in the vicinity of the vehicle.
MRQ-3.2.2.2	Aerial object trajectory prediction	A vehicle shall be able to predict trajectories of all known aerial objects, lying near the flight path or in the vicinity of the vehicle.
MRQ-3.2.2.3	Dynamic ground object tracking	A vehicle shall be able to track all dynamic ground objects in the ground monitoring area.
MRQ-3.2.2.4	Dynamic ground object trajectory prediction	A vehicle shall be able to predict trajectories of all dynamic ground objects lying in the ground monitoring area.
…		

An excerpt from a preliminary list of vehicle sensing requirements are shown in Table 5.

Table 5. Excerpt from Preliminary Vehicle Sensing Requirements List

ID	Required capability/functionality	Required coverage/range of sensors	Possible solutions (sensors)
1	Localization and state estimation of aerial vehicles	All direction and range for possible collision in a time horizon	V2V comm.
2	Identification and classification of aerial vehicles	All direction and range for possible collision in a time horizon	V2V comm.
3	Flight Path clearance (maybe comes from cruise flight phase)	All direction and range for possible collision in a time horizon and in the planned path	.
3.a	Horizontal clearance (aerial, ground static objects)	360deg horizontal & covers the vicinity of all path in a time horizon	V2V comm., 360deg lidar
3.b	Vertical clearance (aerial, ground static objects)	covers the vicinity of all path in a time horizon	V2V comm., lookdown lidar, look-up lidar
4	Detection and ranging of static ground objects	360deg horizon and range up to the braking distance to fully stop + margin (func. of speed) / lookdown, covers footprint and around it (no reasonable range setting yet) (Note that there are 3 types: bulk, vertical pole, horizontal wire)	360deg lidar, lookdown lidar
5	Detection and ranging of dynamic ground objects	Lookdown, covers footprint and around it (no reasonable range setting yet)	Lookdown lidar, lookdown camera (especially for tracking)
6	Identification and classification of ground objects	Lookdown, covers footprint and around it (no reasonable range setting yet)	Lookdown lidar, lookdown camera
7	Ground monitoring (minimize crash impact and secure safe normal/emergency landing)	Lookdown, covers footprint and around it (no reasonable range setting yet)	Lookdown lidar, lookdown camera
8	Ground detection/classification	Lookdown, covers footprint and around it (no reasonable range setting yet)	Lookdown lidar, lookdown camera
9	Landing clearance (maybe comes from landing phase)	Lookdown, covers footprint and around it (no reasonable range setting yet) and 360deg short range sudden approach detection	Lookdown lidar, lookdown camera, 360deg sonar, 360deg lidar
10	Health monitoring of all critical sub-systems. Vehicle providers must provide the definition of the critical sub-systems based on a risk-based analysis.	none	Rely on each subsystem
11	Wind monitoring	none	INS + others, external info.
12	Take-off clearance (maybe comes from take-off phase)	covers the vicinity of all path in a time horizon	Lookdown lidar, lookdown camera, 360deg lidar

V. Functional Architecture

A functional architecture was created to support this systems study. The level 1 functional architecture is summarized in Figure 13. The major flight phases are pre-flight, take-off, cruise, landing, and post-flight.

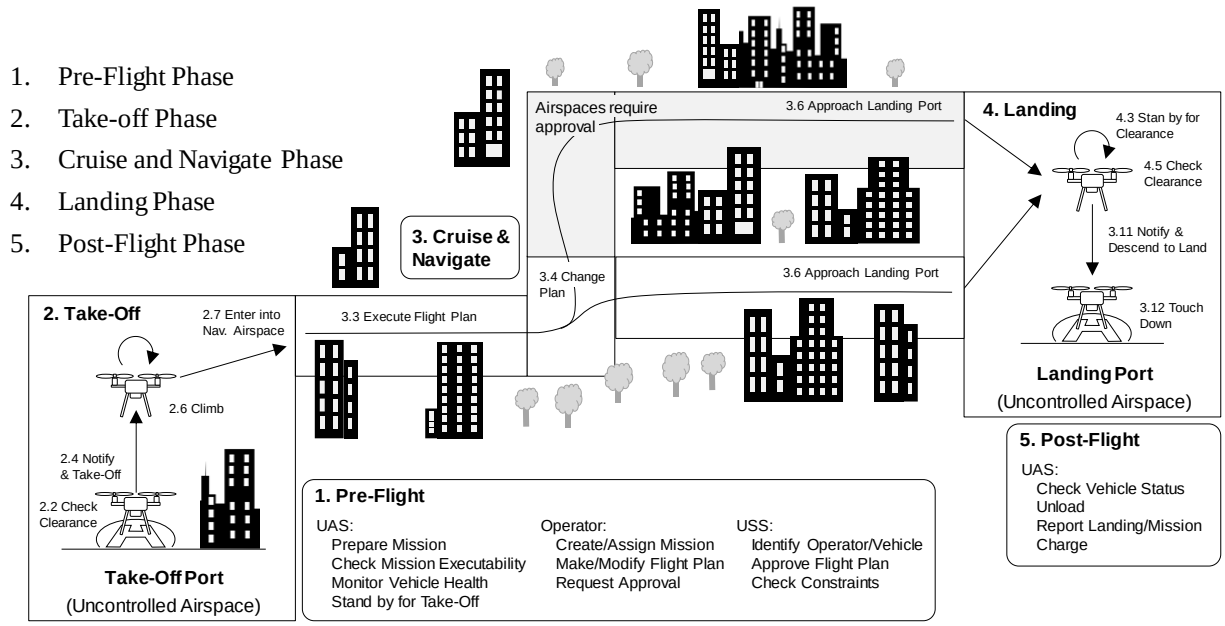

Figure 13. Flight Phase Functional Decomposition

The leveled functional requirements architecture utilizes Functional Flow Block Diagram (FFBD) models to decompose the flight phases. The level 1 FFBD is shown in Figure 14. The 1.0 Pre-Flight Phase function is decomposed to level 2 requirements in Figure 15. This diagram matches the architecture diagram presented in the Physical Architecture section, representing an assignment of function requirements to a physical component in the architecture. For instance, functional requirement 1.15, "Approve Flight Plan", is assigned to the USS component.

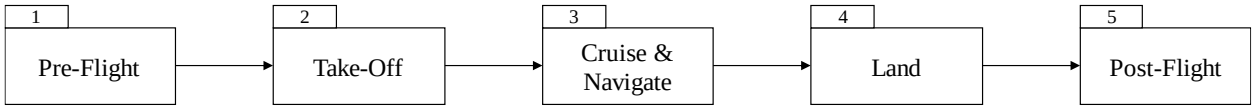

Figure 14. FFBD of Flight Phases for Point-To-Point Use-Case

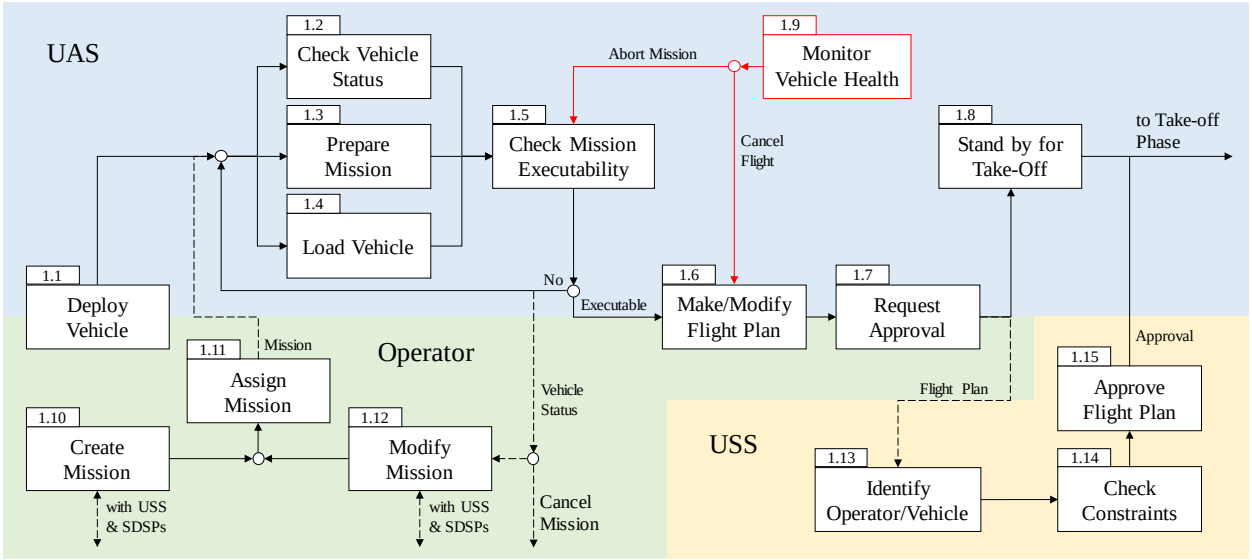

Figure 15. FFBD – 1.0 Pre-Flight Phase

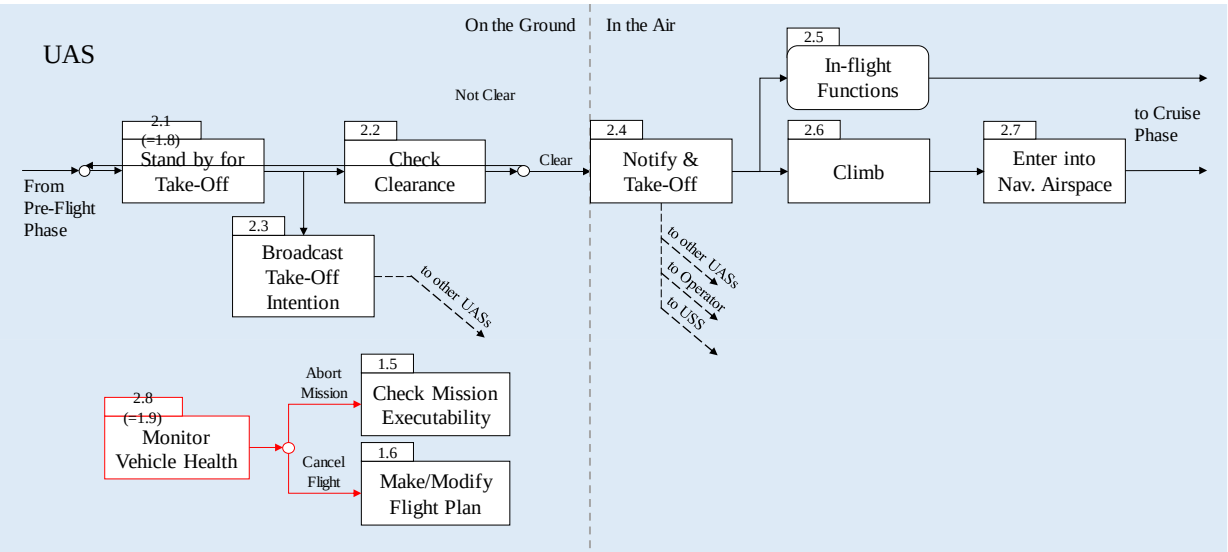

Figure 16. FFBD – 2.0 Take-Off Phase

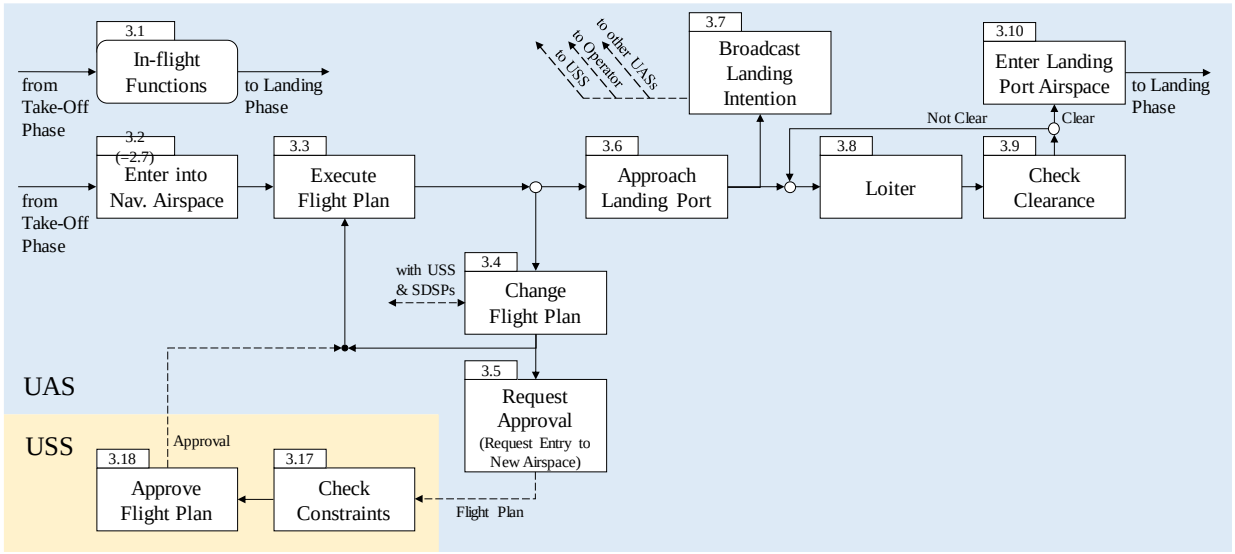

Figure 17. FFBD - 3.0 Cruise and Navigation Phase

FFBD's for phases 2, 3, 4, and 5 are presented in Figures 16, 17, 18, and 19, respectively.

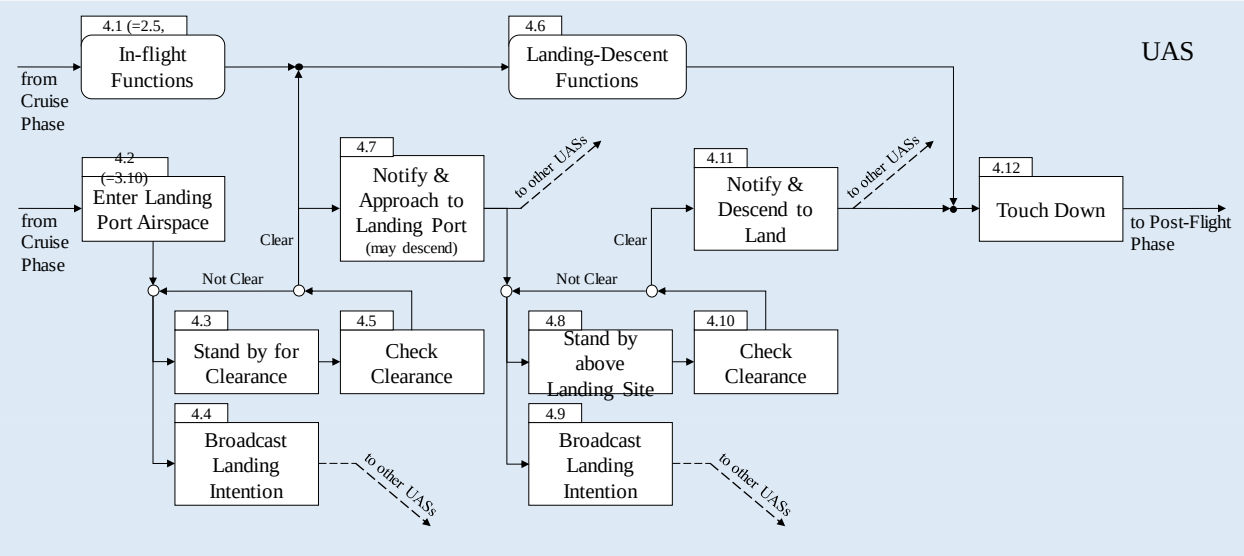

Figure 18. FFBD - 4.0 Landing Phase

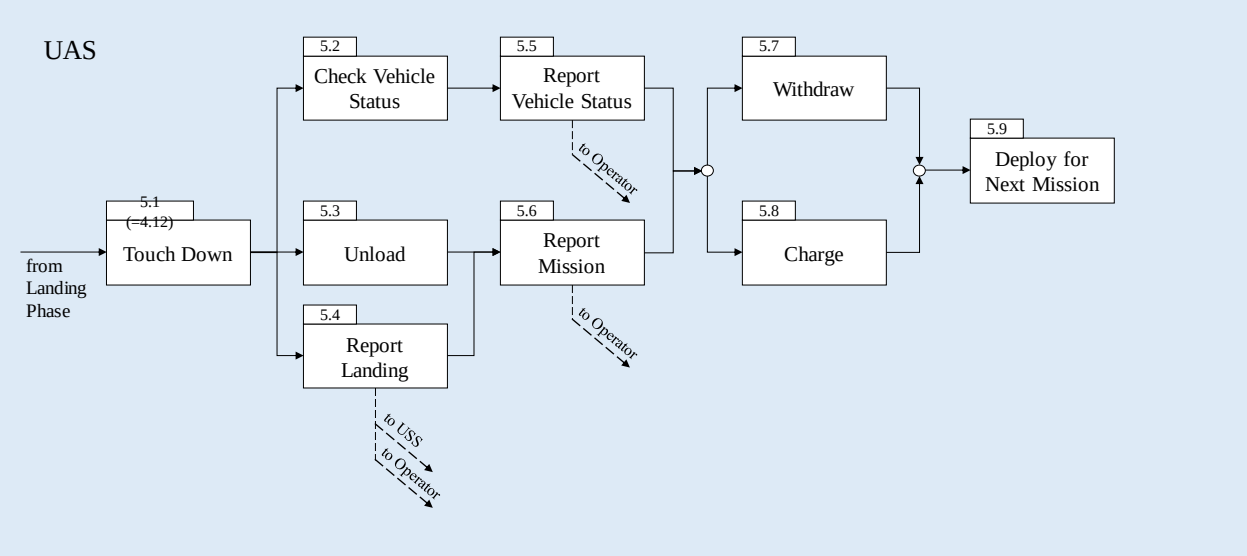

Figure 19. FFBD – 5.0 Post-Flight Phase

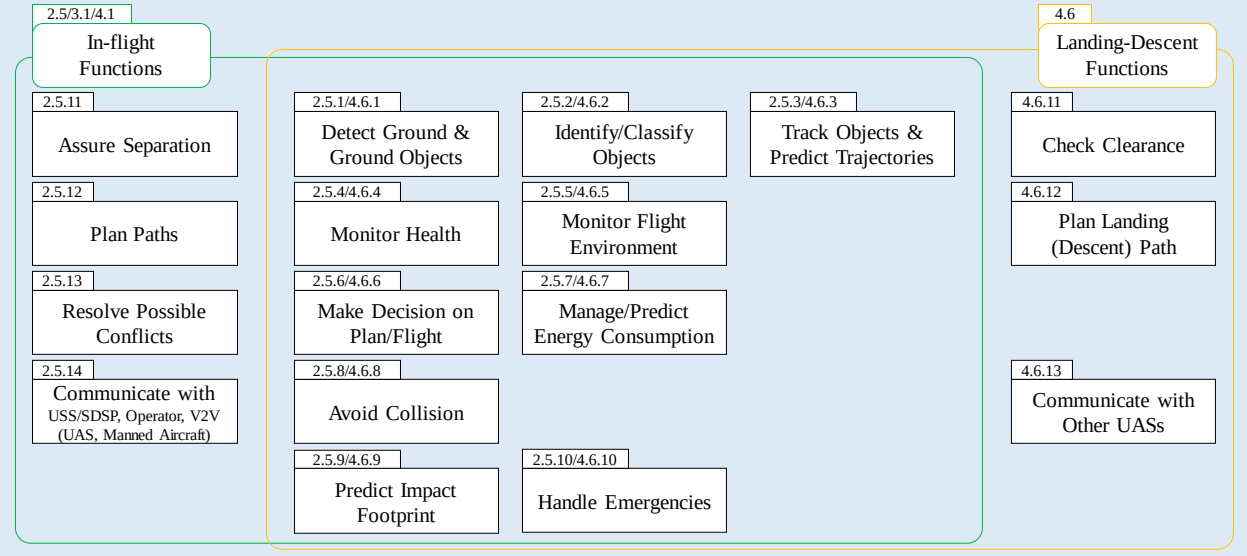

Figure 20. Grouped Functional Requirement Blocks

VI. Top-Level Systems Architecture

The general architecture for the SAFE50 extension of UTM TCL-3 to TCL-4 is presented below. The level 1 architecture is shown Figure 21 and represents the current TCL-3 architecture. The SAFE50 reference design modifies this architecture as shown in Figure 22.

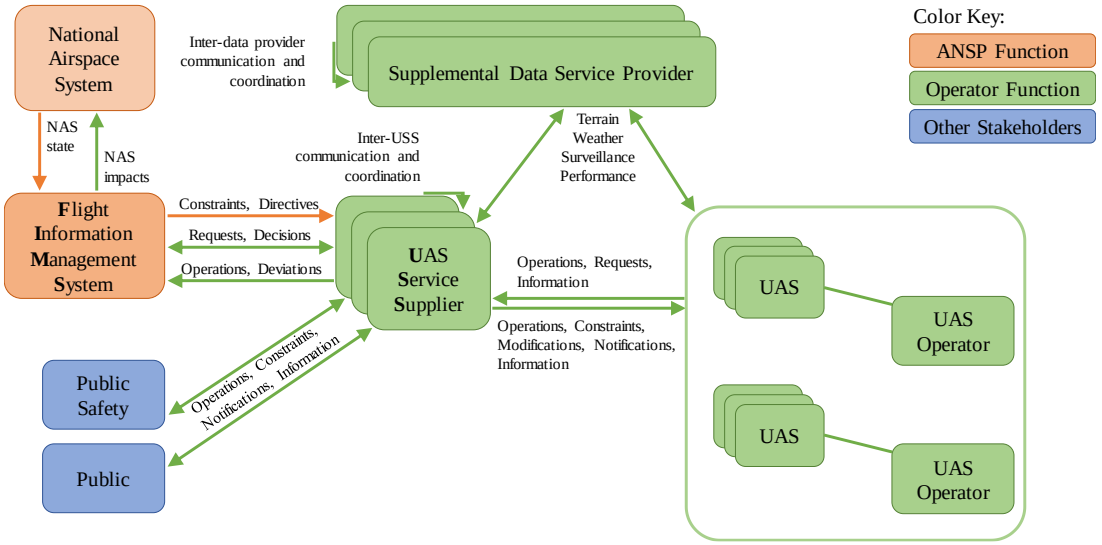

Figure 21. UTM TCL-3 Architecture

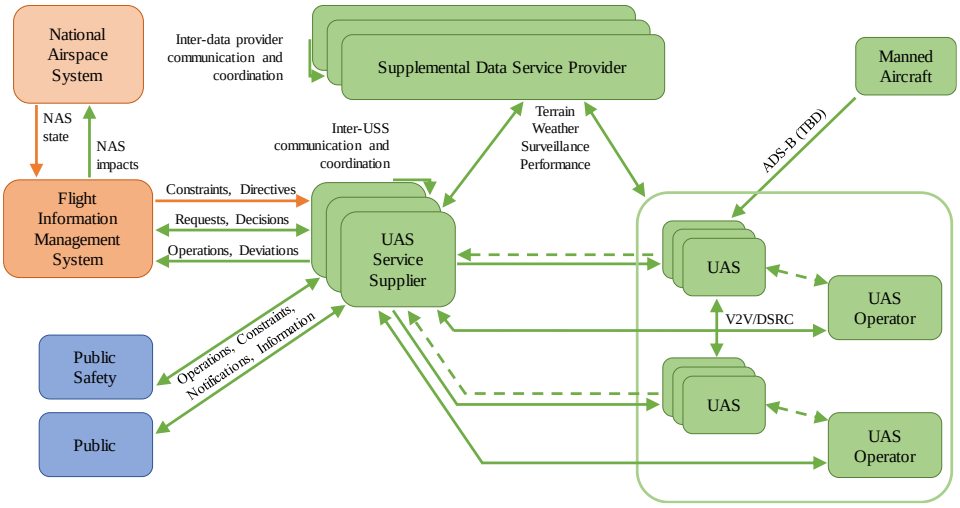

Figure 22. SAFE50 Reference Design - Level 1 System Architecture

The SAFE50 reference architecture further decomposes the UAS vehicle system and the UAS ground element. The architecture for other components of this system were not modified. The level 2 physical architecture, decomposing the UAS airborne and UAS ground elements in the reference architecture, are presented in [13].

VII. Conclusion

This paper presents a high-level summary of the NASA SAFE50 reference design study. This 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.

An overview and background for this system was presented, the high-level system design elements were presented, the assumptions and constraint on the design study described. The unique challenges imposed by this design problem were presented. The concept of operations was presented, with a description of some of the major design features of this study. Requirements were derived as flow down from the mission concepts, elaboration of the scenario and use cases, and captured in the functional architecture. The level 1 systems architecture was presented. The reference architecture documentation continues in the referenced publication.

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. Verification and validation of the SAFE50 reference design study will be achieved through simulation and flight-testing of hardware prototypes, with major V&V activities planned for 2019. Through development of this system design, the SAFE50 seeks to enable access to low-altitude high-density urban environments through advanced onboard UAS autonomy.

Acknowledgments

The authors would like to thank Dr. Dae-Sung Jang, who provided a substantial bulk of the system design effort presented in this paper, Sebastian Hening, and Shankar Sankaraman. The authors would also like to thank our collaborators and colleagues on the NASA UAS Traffic Management (UTM) project.

References

[1] Federal Aviation Administration (FAA). FAA Aerospace Forecast: Fiscal Years 2017 to 2037, US DOT FAA TC17-0002, 2017.
[2] Federal Aviation Administration (FAA). Unmanned Aircraft Systems (UAS) Traffic Management (UTM) Concept of Operations. 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 Aviation Forum.
[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). 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.
[6] Liling Ren, Mauricio Castillo-Effen, Han Yu, Yongeun Yoon, Takuma Nakamura, Eric N. Johnson, and Corey A. Ippolito. "Small Unmanned Aircraft System (sUAS) Trajectory Modeling in Support of UAS Traffic Management (UTM)", 17th AIAA Aviation Technology, Integration, and Operations Conference, AIAA AVIATION Forum, (AIAA 2017-4268)
[7] Stull, R. B. (2012). An introduction to boundary layer meteorology (Vol. 13). Springer Science & Business Media. 2012 Dec 6.
[8] Federal Aviation Administration. (2016). Advisory Circular 00-6B, *Aviation Weather* (FAA-AC-00-6B). Washington, D.C.
[9] Oke, T.R., 1976. The distinction between canopy and boundary-layer urban heat islands. Atmosphere, 14(4), pp.268-277.
[10] National Aeronautics and Space Administration. Aircraft Operations Management. NPR 7900.3D. May 2017.
[11] Belcastro, C. M., Newman, R. L., Evans, J., Klyde, D. H., Barr, L. C., & Ancel, E. (2017). Hazards Identification and Analysis for Unmanned Aircraft System Operations. In 17th AIAA Aviation Technology, Integration, and Operations Conference (p. 3269).
[12] Nehme, C.E., Crandall, J.W., and Cummings, M., "An Operator Function Taxonomy for Unmanned Aerial Vehicle Missions," 12th International Command and Control Research and Technology Symposium, Command and Control Research Program (CCRP), AT&L, DOD, Washington, DC, June 19-21, 2007.
[13] Ippolito, C. A.; Krishnakumar, K.; Stepanyan, V.; Chakrabarty A.; Baculi, J. (2019). An Autonomy Architecture for High-Density Operations of Small UAS in Low-Altitude Urban Environments. 2019 AIAA Modeling and Simulation Technologies Conference.