Some Impacts of Risk-Centric Certification Requirements for UAS*

Natasha A. Neogi, Kelly J. Hayhurst, Jeffrey M. Maddalon, and Harry A. Verstynen

Abstract— **This paper discusses results from a recent study that investigates certification requirements for an unmanned rotorcraft performing agricultural application operations. The process of determining appropriate requirements using a risk-centric approach revealed a number of challenges that could impact larger UAS standardization efforts. Fundamental challenges include selecting the correct level of abstraction for requirements to permit design flexibility, transforming human-centric operational requirements to aircraft airworthiness requirements, and assessing all hazards associated with the operation.**

I. Introduction

Airworthiness certification is one of the most important regulatory approvals typically needed for aircraft to operate commercially in the National Airspace System (NAS). Airworthiness encapsulates the notion that an aircraft meets established design requirements and is in a condition for safe operation. Developing airworthiness requirements for unmanned aircraft systems (UAS) that enable a new range of missions, designs, and operational modes that pose novel risks is a key challenge to the safe integration of UAS into the NAS [1].

NASA recently completed an exploratory research study on risk-appropriate airworthiness requirements for a midsize UAS performing low-risk, precision agriculture application operations [2]. The goal was to facilitate development of airworthiness requirements for a UAS that would not qualify: (a) under the anticipated small UAS (sUAS) rules [3], (b) for an exemption under the FAA's Section 333 [4], (c) under EASA's 'open' category [5], or (d) under current conventionally piloted, civil aircraft standards. The research study employed a hazard-based approach to establish design requirements that would form a mock type certification basis [6] for an unmanned agricultural sprayer. This paper outlines the study's results and describes the broader implications these results may have on UAS design standards and certification processes under more general circumstances.

The next section outlines the precision agricultural research study and summarizes part of the mock certification basis. Section III details the procedure used to evaluate design standards in Part 27 of Title 14 of the Code of Federal Regulations (14CFR) [7] for selection and aggregation into abstracted requirements more appropriate for a UAS platform. Requirements for UAS features needed to perform historically human-centric functions, such as minding operational boundaries (i.e., containment) and avoiding other aircraft and obstacles, are excerpted in Section IV. Related technical work is identified in Section V, with insights and conclusions discussed in Section VI.

* This work is supported by space act agreements between NASA Langley Research Center and Dragonfly Pictures, Inc. (SAA1-17902), and the University of North Dakota (SAA1-17878).

N.A. Neogi, J. M. Maddalon, and K.J. Hayhurst are with the National Aeronautics and Space Administration, Langley Research Center, Hampton VA 23681 USA (corresponding author e-mail: natasha.a.neogi@nasa.gov).

H. Verstynen is with Whirlwind Engineering, LLC, Poquoson, Virginia.

II. Background

UAS intended to operate beyond the limitations imposed on small UAS [3] will likely require some degree of airworthiness certification in addition to operational approvals [1,8]. Airworthiness certification processes for aircraft typically involve compliance with design and performance standards found in 14CFR. These standards include requirements on the aircraft structure, controls, powerplant, electrical and other systems. The requirements are meant to forestall the loss of the aircraft hull, thus protecting all persons onboard. The standards have the additional effect of protecting overflown persons and property on the ground below.

Application of existing airworthiness standards to UAS could be problematic because the hazards mitigated by those standards may not be the same as those for UAS [9, 10]. Risk posed by a UAS is driven by its concept of operations (ConOps), more so than for conventionally piloted aircraft (CPA) whose ConOps is assumed to be the point-to-point transport of goods or persons [5]. The following subsections provide a quick overview of the research study components indispensible to the mock type certification basis.

A. ConOps and UAS Description

The ConOps for the research study targets the precision agricultural application operation. Precision spraying represents a feasible early application for larger UAS (>55 lb) due to the low-risk nature of the operation and strong economic projections [11].

1) Precision Agricultural Application

In the research study, a midsize, remotely-piloted rotorcraft is used to spot treat crops in fields up to 160 acres in rural, sparsely populated areas [2]. Operations can be conducted under daytime, nighttime, and reduced visibility conditions. Operations can also occur within and beyond visual line of sight (VLOS), but always within radio line of sight (RLOS). Operations only occur within Class G airspace [2].

Spray operations are limited to a designated *operational boundary* (Fig. 1, yellow lines) around the field, and an absolute *containment boundary* (Fig. 1, red lines) just beyond the operational boundary. The *containment volume* includes the altitude dimension with the boundaries. A priori knowledge about crop health is used to identify treatment areas (Fig. 1, dashed white lines). The unmanned rotorcraft is expected to operate a few feet above crop height, with a maximum altitude of 400 ft. Constraining the operation to a well-defined volume, restricted in altitude and

inhabitants, is key to limiting operational risk. Procedures or automated systems must be in place to ensure constraints are met [12].

Figure 1. Containment volume bounding spray operation

2) UAS Description and Mission Assumptions

To develop a credible certification basis, a representative example of a UAS that could meet the mission requirements from the ConOps was needed. The platform selected was the DP-14 from Dragonfly Pictures, Inc. [2], a tandem rotor, single turbine, prototype rotorcraft with:

- Maximum Takeoff Weight ≈ 1000 lbs
- Maximum endurance ≈ 2.4 hrs
- Maximim airspeed ≈ 100 kts
- No manual control reversion mode

The goal of the research study was to develop a candidate set of design requirements for a UAS with characteristics and capabilities similar to the DP-14. The design requirements, posed in the form of a mock type certification basis [6], are intended to be sufficient to mitigate hazards arising from the precision aerial application.

B. Approach

Airworthiness standards for new or novel aircraft are typically derived from existing standards, with any additional requirements for unique features incorporated as special conditions. These existing standards (e.g., Part 23, 25, 27, 29 and 33) focus on aircraft systems and equipment, with minimal consideration being given to the operational context of the vehicle. However, UAS enable a wide range of operations and numerous novel design features.

The ConOps and associated operational limitations of a UAS strongly influence the severity of the consequence of its failure. This is especially true for limited-range operations such as those associated with agriculture. Following the development of the ConOps, there were three subsequent major tasks involved in investigating airworthiness requirements for the selected UAS platform: (1) identifying and prioritizing hazards; (2) evaluating the applicability of existing Part 27 regulations; and (3) generating UAS-specific requirements. Figure 2 outlines the research approach taken, including the relevant tasks performed, the products produced by each task, and how these products relate to the content of the mock type certification basis.

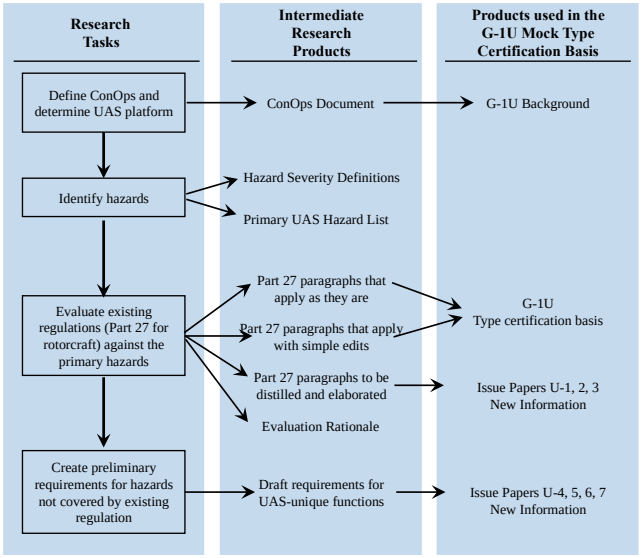


Figure 2. Research Approach Overview

1) Identification and Prioritization of Hazards

The requirements in the mock certification basis were determined by the identified hazards and their associated risks. The first task was to identify hazards that could cause harm to people or property. These include UAS-specific hazards associated with the failure of aircraft functions and operational hazards associated with the mission and crew. Traditional aircraft hazards such as loss of control and loss of navigation were considered. New hazards related to the ConOps, such as loss of containment (i.e., exceeding the virtual boundary for the operation) were also considered. Hazards were then prioritized, with respect to severity and likelihood. The severity definitions as outlined in the FAA Advisory Circulars were tailored for use in this study, leading to the retention of 15 primary hazards to be mitigated [2]. The goal of the hazard assessment for this research was not a definitive assessment of severity for each hazard, but a broader evaluation of whether the potential consequences of a hazard necessitate a design or performance requirement comparable to those in Part 27.

2) Evaluating Applicability of Part 27 Requirements to UAS Platform

The second task was to specify reasonable design and performance requirements for the UAS platform. The Part 27 regulations for normal category rotorcraft provided a practical starting point. Each regulation in Part 27 was evaluated for applicability to the UAS platform and associated ConOps, with respect to the 15 primary hazards. This effort identified Part 27 regulations that apply "as is" to mitigate the primary hazards, those that apply with some simple modifications, and those that may not be applicable at all. The paragraphs accepted "as is" and those that were modified constitute the main set of requirements in the mock type certification basis. A summary of the basis is included in Section II-C.

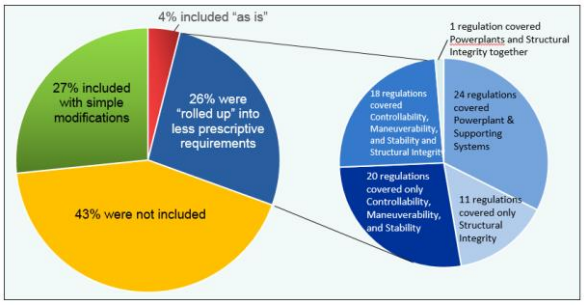
Many other Part 27 paragraphs could not be easily placed into one of those three categories. The relevant content from these Part 27 requirements were generalized or 'rolled-up'

into broad sets of requirements that focus on preservation of the rotor system to prevent harm from release of high-energy debris and explosion. The generalization process is described in Section III.

3) Generating UAS-Specific Requirements

Lastly, the primary hazard list was reviewed to identify hazards for which Part 27 contains no applicable requirements. Four primary hazards that are not covered by Part 27 were identified: (1) loss of vehicle containment (i.e., a failure causing a fly away event where the unmanned aircraft (UA) leaves the operational area); (2) failure to detect and avoid people on the ground; (3) failure of safety-critical command and control (C2) links; and (4) failure to detect and avoid other aircraft. The first three hazards are not addressed in any of the FARs, but the last hazard is related to standards for aircraft operators (Part 91). Section IV describes issues encountered in the development of a selection of these requirements. A summary of the mock certification basis is provided in the next subsection.

C. Summary of Research Study Results



(a) (b)

Figure 3. (a) Disposition of Part 27 Requirements in mock type certification basis (b) 'Rolled Up' Requirements

Current airworthiness regulations in 14CFR Part 27 for normal-category rotorcraft were evaluated to determine their suitability for mitigating hazards for the unmanned agricultural sprayer. Figure 3 illustrates the degree to which the Part 27 requirements were incorporated into the mock certification basis[1].

Many Part 27 requirements are very prescriptive: their constraints and assumptions limit design flexibility. Such requirements relate to issues of: (1) controllability, maneuverability, and stability (CMS), (2) structural integrity (SI), and (3) powerplant and supporting systems (PSS), and are designed to avoid hull loss. The general intent of many requirements in those areas is relevant to unmanned aircraft; those requirements were 'rolled-up'. The 'rolled-up' requirements are a novel feature of the mock certification basis, and are further discussed in Section III.

The Part 27 requirements do not address all of the hazards posed by the unmanned sprayer. Unaddressed hazards included those associated with functions typically performed by a conventional aircraft pilot, including loss of separation from other aircraft and ground-based objects (obstacles and people) and failure to stay within the authorized operational area. Developing design requirements to mitigate those hazards is discussed further in Section IV.

[1] The mock type certification basis, issue papers and any proposed requirements do not represent US Government or FAA policy or guidance.

III. Abstracted Requirements Derived from Part 27 Traditional Areas

The design and operational differences between a medium-sized unmanned rotorcraft and a normal category manned rotorcraft are such that many of the requirements in Part 27 are either not applicable or overly prescriptive for a vehicle that has no humans onboard. The ConOps played an important role in the analysis of hazards and risks, which was the basis for deciding which of the Part 27 requirements may be relevant.

A. Approach

The approach used to derive an appropriate set of vehicle- and ConOps-specific requirements relied on conducting a hazard analysis that identified aspects of the UAS and the operational environment that can compromise safety. Fifteen primary hazards were identified [2], and each Part 27 requirement was evaluated to determine whether it aided in hazard mitigation.

In several instances, many requirements jointly contributed to the mitigation of a single hazard. This was especially true in the areas of CMS, SI, and PSS. In each of those topics, select requirements were aggregated and replaced by more abstract requirements focused on mitigating UAS-specific hazards. Each aggregated requirement emphasizes a safety objective without unduly constraining the UAS design space. For any particular design, an applicant and the regulator would then refine the abstracted requirements into specific, concrete requirements for the UAS presented for certification. The hazard analysis and condensed airworthiness requirements would be supplemented by appropriate operational limitations that would not be part of the airworthiness certification basis, but would be contained in appropriate operational approvals. An example of this approach is provided in III.B.

B. Example of Approach

Consider two sample identified hazards: (1) loss of structural integrity of the rotor system and (2) explosion. Both hazards could result in the release of high-energy debris beyond the containment boundary, consequently harming people on the ground, including UAS crew.

The hazard pertaining to loss of structural integrity of the rotor system can be traced to four primary causal events that should be mitigated or avoided:

- Contact of the rotors with the ground, each other, obstacles, or other parts of vehicle
- Loss of structural integrity of primary structure supporting rotors or critical elements of rotor system
- Loss of structural integrity of rotor drive system
- Sudden engine stoppage resulting in loss of rotor

system integrity

A single Part 27 requirement was included in the mock certification basis to prevent the sudden engine stoppage event:

14CFR §27.917 Design [7]

(a) Each rotor drive system must incorporate a unit for each engine to automatically disengage that engine from the main and auxiliary rotors if that engine fails.

The DP-14 satisfies this requirement by using a clutch, which disengages the rotor from the engine if the engine fails. Mitigating the other three events is less straightforward. An example of the requirements abstraction process is given in III.C.

C. Controls, Maneuverability, and Stability Requirements

A total of 38 individual Part 27 paragraphs were abstracted, either in whole or in part, into an issue paper in the certification basis that describes abstracted requirements for CMS to avoid ejection of high-energy parts. An excerpt from the CMS issue paper is as follows [2]:

The applicant must:

(a) establish controllability and maneuver-ability design margins that prevent contact of the vehicle rotors with the ground, other parts of the vehicle structure, or obstacles in normal and non-normal operations, or any other condition that could compromise rotor system integrity…

An example of a specific prescriptive Part 27 requirement that was 'rolled up' into the abstracted requirement above is as follows [7]:

14CFR §27.51 Takeoff

The takeoff, with takeoff power and r.p.m. <revolutions per minute> at the most critical center of gravity, and with weight from the maximum weight at sea level to the weight for which takeoff certification is requested for each altitude covered by this section—

(a) May not require exceptional piloting skill or exceptionally favorable conditions throughout the ranges of altitude from standard sea level conditions to the maximum altitude for which takeoff and landing certification is requested

…

The CMS issue paper captured many of the Part 27 requirements related to controllability, maneuverability, static stability and piloting requirements. Several of these Part 27 requirements establish characteristics of control systems in terms of pilot handling characteristics, which are not directly applicable or easily translatable into automation requirements.

Note that the CMS issue paper touches on the first causal event (contact of rotors with ground, obstacles, vehicles, etc.), but does not establish a means by which an autopilot can be judged as 'compliant'. The abstract requirement defines a general mitigation whereby a compliant system must establish the appropriate design margins in their control systems (as well as maneuverability guarantees) to explicitly prevent an actuation that leads to the initiating event.

Similarly, CMS requirements related to the design of the rotor drive and structural integrity of the control system elements were 'rolled up' into an abstracted requirement. An excerpt [2]:

The applicant must:

(b) ensure that flight control commands from all sources (stability augmentation system, autopilot etc.) are passed to the appropriate flight control surfaces without hazardous flexure, slop, friction, jamming, interference or other hazards that would lead to loss of rotor system integrity

…

This requirement directly addresses the causal events relating to a loss of structural integrity: either of critical elements of the rotor system and support structure, or the rotor drive system. The relevance of these requirements comes from their ability to mitigate the hazard associated with the ejection of high-energy parts (and not hull loss, as they were originally intended). An example of a specific prescriptive requirement on the control system is as follows [7]:

14CFR §27.685 Control System Details

(e) Control system joints subject to angular motion must incorporate the following special factors with respect to the ultimate bearing strength of the softest material used as a bearing:

(1) 3.33 for push-pull systems other than ball and roller bearing systems.

(2) 2.0 for cable systems.

…

Paragraph §27.685 is geared towards maintaining vehicle hull integrity and protecting any human occupants. However, as hull loss is not a primary concern for agricultural operations, the appropriateness of special engineering design factors should be negotiated with the applicable hazards and risks in mind (e.g., parts ejection). The fact that many of the most prescriptive requirements were abstracted does not mean that they do not apply at all, only that they be considered in their risk-context.

The proposed use of abstracted requirements in areas where current regulations are highly prescriptive is not novel. A similar approach is used for Light Sport Aircraft regulation [13], and the Part 23 Reorganization Aviation Rulemaking Committee is working to replace prescriptive requirements with safety objectives that are design-independent to extend the range of applicability [14]. The novel contribution is that the type certification basis is directly tied to hazards that are relevant to the UAS and its ConOps, forming a risk-centric approach. The correct choice of abstract requirements enables flexibility, while maintaining safety.

The next section addresses further difficulties in choosing the correct level of abstraction to define airworthiness requirements that originate from operational requirements for CPA.

IV. Novel UAS-Specific Requirements

Several hazards whose mitigation are traditionally the responsibility of a pilot were identified during the research study, including: (1) loss of separation with other aircraft, obstacles, or people and (2) failure to confine the operation to the authorized areas (e.g., a fly-away event). There are no airworthiness requirements in Part 27 that address these hazards, since they are traditionally operational requirements (implicit or explicit) [16]. This section examines proposed requirements for functions to avoid obstacles and aircraft (detect-and-avoid functionality), and for a function to limit egress from the operational area (containment functionality).

A. Detect and Avoid (DAA)

The ability of the UAS to detect and avoid other aircraft as well as ground-based obstacles is of paramount importance, even when operations are restricted to a low-altitude containment volume. For a CPA, the onboard pilot performs this function, called 'see-and-avoid', by maintaining situational awareness through looking outside the aircraft's windows. The notion of 'see-and-avoid' is described under several regulations in 14CFR Part 91 [16], most notably as follows:

14CFR §91.113 Right-of-way rules: Except water operations.

(b) General. When weather conditions permit, regardless of whether an operation is conducted under instrument flight rules or visual flight rules, vigilance shall be maintained by each person operating an aircraft so as to see and avoid other aircraft. When a rule of this section gives another aircraft the right-of-way, the pilot shall give way to that aircraft and may not pass over, under, or ahead of it unless well clear.

Other Part 91 operational regulations imply that the pilot must also see-and-avoid ground obstacles. For example, 14CFR Part §91.13 prohibits careless or reckless operations that could endanger the life or property of others, and 14CFR §91.119(d) describes minimum altitudes for rotorcraft operations, provided they do not create a hazard to people or property on the surface.

A UAS must perform an equivalent function, either through airborne or ground-based systems, likely in an automated fashion. Regulatory certification of this function would be expected, as its failure could create a catastrophic hazard. Thus, a function that would conventionally be handled by operational regulation in Part 91, will now be handled for UAS, at least in part, by airworthiness regulation. Note that the 'see-and-avoid' function is specified quite abstractly. Trained human pilots employing 'common sense' interpret it uniformly and execute it well enough to achieve safety. Once this function becomes (partially) automated, these 'common sense' assumptions and pilot insights must become explicit, as overly abstract specifications are no longer adequate.

The mock type certification basis included two issue papers proposing airworthiness requirements for detecting and avoiding aircraft and obstacles. A sample requirement from the issue paper on ground-based obstacle DAA is as follows:

…[The applicant must] Provide a means to detect and avoid persons and objects within the defined operational area during flight operations.

(a) Means of detection will:

(1) have sufficient range in the direction of Unmanned Aircraft (UA) travel to permit a simple avoidance maneuver (e.g., hovering or landing);

…

Note that the detection requirement does not specify whether the detection action is performed by a human or by automation, it merely provides bounds on performance characteristics (e.g., sufficient range in the direction of UA travel). S*ufficient* time is based on the notion that the avoidance action must have enough time to complete its avoidance maneuver.

The proposed requirements were deliberately written in a way so as to guarantee safety without prescribing a particular implementation. Neither the architecture, nor sensors, nor algorithms, nor human-automation function allocation is prescribed by these requirements.

Table 1: Potential Architectures for Ground Obstacle Detection and Avoidance

Architecture	**Ground Based (Ground Control Station)**		**Airborne (UA)**
	Function	**Automation / Human**	**Function**
Ground Only	Sense, Detect, & Avoid,	Y/Y*	None
Ground Decision	Detect & Avoid	Y/Y	Sense
Split 1	Avoid	Y/Y	Sense & Detect
Split 2	Sense & Detect	Y/Y*	Avoid
Air-based	Status	Y/N	Sense, Detect, & Avoid,

* under visual meteorological conditions

Table 1 describes several possible function allocation schemes for the DAA capabilities needed for ground based obstacle avoidance. Broadly speaking, DAA can be broken down into three main functions: (1) obstacle sensing; (2) conflict detection; and (3) avoidance maneuvering. These functions can be allocated to either an airborne agent (e.g., autonomous capability onboard the UA), or to a ground based agent (ground based automation or human). For example, under the Ground Decision architecture, the sensing function is provided by the airborne agent (e.g., LIDAR or camera onboard the UA). The sensing information is then communicated to the ground control station (e.g., via video feed), where the conflict detection

function is performed. Note that this function can be performed either by automation or by a human agent (as indicated by the Y/Y in the Automation/Human column). Similarly, either a human agent or automation can perform the ground-based avoidance maneuver generation function. The sensing function can be performed on the ground by a human agent such as a visual observer or pilot in command (e.g., Ground Only and Split 2 architectures). However, this is only possible under visual meteorological conditions, as is indicated by the asterisk following the Y notation.

In the course of migrating human-centric operational requirements into potential requirements for automation, care must be taken not to over-prescribe the system, thereby eliminating potential architectures that allow a variety of human-machine functional allocations. A high level of abstraction, as well as ambiguous wording (e.g., "sufficient time") is acceptable when the implementation involves a trained pilot. However, concretized requirements are required when this function is implemented through automation to ensure there is no room for ambiguity or unspecified interpretation. This design-agnostic approach, as well as the difficulties encountered in translating human-centric requirements into automation-oriented requirements, is mirrored in an issue paper on containment, discussed in the following subsection.

B. Containment

One of the primary hazards of concern in UAS operation is that of a 'fly-away': that is, the pilot in command of the UA is unable to affect control of the aircraft and the aircraft is no longer following its preprogrammed procedures, resulting in the UAS not operating in a predictable or planned manner. A 'fly-away' could result in the UA entering an area in which it is not permitted to operate, and/or behaving in a manner that is hazardous to other aircraft or persons on the ground. For example, on August 2, 2010, an MQ-8 "Fire Scout" became unresponsive to commands during testing and entered protected airspace around Washington, D.C. [37].

While there is no explicit requirement in 14CFR that states that an aircraft should only operate where authorized, there are Part 91 operational requirements stating where aircraft should not operate (e.g., in restricted areas per Part §91.133) [16]. Thus, there is a recognized concern regarding UAS operations taking place beyond designated operational boundaries, especially due to a loss of the control link [15]. Hence, an issue paper was included in the mock type certification basis that proposed requirements specifically regarding the enforcement of the UA's position with respect to the containment boundary. Note that, like the 'detect-and-avoid' issue papers, the issue paper on containment puts forward suggested airworthiness requirements that were previously proscribed by operational regulation. Difficulties encountered in section IV.A regarding the translation of human-centric requirements into automation-oriented requirements apply.

The issue paper on containment covers a number of important obligations to prevent fly-away events, including knowledge of vehicle position relative to the boundaries, ability to detect impending boundary violations, and the actions needed to prevent exit. For the research study, an independent assured containment system [12], combined with systems and procedures for ensuring that the containment area remains clear of persons, was proposed.

An assured containment system is a *localization* system that acts to keep the UA within given bounds using one or more strategies such as return to containment area centroid, hover, or terminate flight. The *assured* part of the assured containment concept comes from being able to build a safety argument, sufficient for certification purposes, that the UA will remain in a specified area in the presence of common vehicle, autopilot, sensor and actuator failures. Implementing the assured containment system as a separate system isolated from the UA primary avionics facilitates achieving high dependability and might ease certification. It is this system (and component) independence that is the principle difference between geofencing and assured containment. Furthermore, geofencing acts to detect boundary violation on the behalf of the vehicle, while the predictive nature of assured containment can actively keep the vehicle localized or contained within the containment volume.

A partial requirement for the containment function is as follows [2]:

...[The applicant must] Provide a means to detect and avoid transgression of any containment boundaries established for the operation. This includes the following….

(c) Failure of infrastructure not part of the UAS (e.g., Global Positioning System (GPS), cell phone network) must not significantly interfere with the determination of the location of the aircraft.

...

To meet requirement (c), the containment system should not not rely upon GPS or the UA autopilot system and avionics. No single failure in the UA's autopilot system should result in an automatic failure of the containment system. Hence, there should be no critical coupling between the containment system and the UA's primary onboard avionics systems (all flight termination systems are redundant, independent mechanisms). A primary value of the containment concept comes from being able to limit the UA's physical location in the presence of failures in the primary avionics.

An architecture for an assured containment system is proposed in Figure 4, and incorporates an independent system for determining the location of the UA based on three or more low power transmitters prepositioned to provide good multi-lateration geometry over the operational area. The UA contains two receiver/processors preloaded with lateral and vertical containment boundaries. The receiver/processors receive signals from antennas on the vehicle and continuously triangulate to determine current

lateral and vertical position. The current position is differentiated to determine a velocity vector. The position and velocity data are processed to determine a projected time to crossing of the boundary. If the UA has not taken action to adjust its path or speed to stay within the boundaries by the projected crossing time, the proposed containment system forces the vehicle into an immediate landing by closing an emergency fuel shutoff valve. The valve operates completely independently of the UA primary systems, including primary and backup power sources. An activation signal is sent to the operator via C2 datalink and the operator reinforces the automatic action with a command to close the normal fuel shutoff valve.

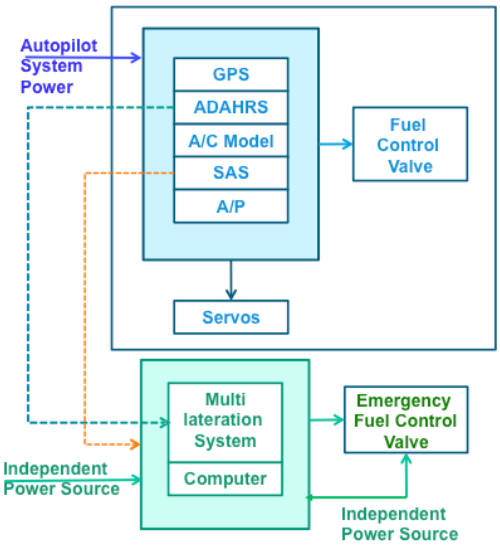


Figure 4: Proposed Containment Implementation

The precision of the vehicle localization system (sensors, filters and positioning algorithms/processors), the fidelity of the algorithm by which impending boundary violations are detected (algorithms and processors), and the means by which avoidance maneuvers are executed (controls algorithms and processors, actuators and communications links/delays) must all be considered in evaluating the assurance case for the containment concept (Figure 4).

A further requirement for containment is:

(g) …containment system design must consider projection of parts that may constitute a hazard to bystanders outside the containment area.

The size and shape of the containment volume is affected by the potential trajectories of parts that may be ejected by the vehicle. Vehicle speed and altitude must be considered in the containment system design since they affect the trajectory of ejected parts. Note that this is the same hazard described in Section III.B-C.

The need for requirements to prevent harm from the release of high-energy parts was not initially obvious. A crash of an unmanned agricultural sprayer within a containment area that has been cleared of people might not be considered a safety concern. However, further consideration of such a crash resulted in identifying hazards related to the release of high-energy parts that could exit the containment area (e.g., rotor blade), as well as hazards related to detecting people who may enter the field during the operation. Hence, a key observation of this work is that mitigations for one hazard may mask or influence another hazard. That is, the CPA mitigation of the hull loss hazard, through the application CMS and SI requirements, acts to mitigate the hazard posed to persons on the ground by the ejection of high energy parts in the event of a crash. Consequently, efforts to mitigate a hazard must ensure that the effects of this mitigation mechanism on all other hazards are clearly understood.

The containment requirements that are proposed allow considerable design flexibility. Thus, under visual metrological conditions, the containment function could be implemented using visual observers stationed along the containment boundary, along with a reliable means of communication, and a remote pilot who can trigger the emergency fuel cutoff valve. Hence, human-automation function allocation is not constrained.

There has been a great deal of fundamental research focusing on the fields of geospatial containment, DAA and CMS functionality. In order to place this work in context, a brief survey is performed in the next section.

V. Related Work

A. *Containment*

A current idea often proposed to control the overflown area of UAS or rockets is that of geofencing [17, 18]. Geofences for UAS are primarily implemented via software in conjunction with the UA's autopilot; thereby using the same sensors, actuators and processor as the vehicle's primary autopilot/control system [19]. The computational platform upon which the autopilot is implemented, as well as the underlying operating system and communications architecture is relevant to the safety of the geofence [20]. Fault tolerance in sensor and actuator architecture and components is also relevant if they impact safety critical functions [21]. Given that many UAS and their autopilots are composed of commercial-off-the-shelf products (some even open source), reaching levels of reliability and design assurance sufficient for airworthiness certification may be difficult to achieve [22-23].

B. *Detect and Avoid*

One of the most restrictive and important issues in the integration of UAS into the NAS is the lack of automated detect and avoid systems for UAS [24-25]. These systems can roughly be divided into ground-based detect and avoid systems, such as [26-27], and airborne ones, such as [28-29]. A radar-based collision avoidance approach is presented in [30] along with potential requirements parameters for UAS.

Vision-based systems are a popular solution to providing detect and avoid ability for small UAS due to size, weight, and power limitations [31]; however, the limited avoidance

time available, unknown object motion (and size) and large relative geometries (scale) create significant observability issues [21]. Automating this process requires balancing expectations on sensor limitations with aviation procedures [22, 31].

C. Controls, Maneuverability and Stability

A primary point of focus for the design of CMS systems for UAS relates directly to trajectory generation for the avoidance maneuver functionality [33]. A UA may need to operate at its CMS limits while generating reasonable trajectories that can be performed effectively without exceeding dynamic range. The authors in [34] propose a receding horizon controller that incorporates obstacle avoidance constraints and waypoint selection, and provides a framework that takes into account dynamic constraints (e.g., turning limits). Similarly, a UAS control framework composed by a trajectory generator and a feedback controller was proposed in [35] for obstacle avoidance. Research groups have presented diverse state-of-the-art approaches that enable impressive UAS maneuverability [36]. However, the majority of these approaches are focused on adhering to physical limits, and do not consider the predictability desired in aircraft avoidance maneuvers in the NAS [23, 31].

VI. Insights and Conclusions

Several insights were gained through the development of the mock type certification basis. Firstly, both the UAS type and operational concept had to be considered in tandem to develop risk-appropriate type certification requirements. A description of relevant aspects of the precision agriculture application concept was necessary to fully identify all of the hazards to be mitigated by the design of the unmanned rotorcraft. This observation is consistent with EASA's proposed framework for UAS operations [5].

Hazardous events such as loss of control do not have the same consequence for many UAS operations as they do for CPA. Hence, conventional standards intended to mitigate such events may not apply in the same way (or at all) for a UAS. Reduction in hazards should not be assumed *a priori*, as different operational models have the potential to introduce new or different hazards that affect requirements for UA systems and equipment. Thus, the operational concept for the UAS will have a direct effect on the airworthiness requirements, and compliance with these requirements affects the economics or practicality of the operation.

Secondly, a key challenge in formulating new requirements (including the 'roll-ups' as well as the novel systems requirements) was attaining the correct level of abstraction required to address the necessary safety issues while not over-constraining the system design. Additionally, tracing individual regulations to the specific hazards they are intended to mitigate is non-trivial. The rolled-up requirements for CMS, SI and PSS were intended to aid the traceability from requirements to specific hazards and also eliminate prescriptiveness. The goal was to pose requirements at a level of detail that addressed the identified hazard but allow for design flexibility on the behalf of the applicant.

The third insight involved re-interpreting human-centric operational requirements, such as those in 14CFR Part 91, into automation requirements supporting airworthiness certification, similar to those in 14CFR Part 27. Generally speaking, humans require only high-level guidance to safely execute tasks such as obstacle avoidance. Training is used to supplement these requirements. However, requirements for an automated system to replicate a human-centric function must be far more explicit. Additional detail is required to concretize operational requirements such that they can be unambiguously and correctly implemented. However, care must be taken to avoid over constraining the system architecture, or imposing a given human-automation function allocation.

The final insight deals with the notion of hazard masking. A single regulation may act to mitigate multiple hazards, just as multiple regulations may be required to mitigate a single hazard. In the research study, the proper implementation of the containment function is fundamental to mitigating the hazard of vehicle 'fly-away'. The use of operational procedures, such as clearing the containment area of people, acts to mitigate the risk to people within the containment area, thereby rendering hull loss within the containment area a low-risk event. Judicious choice of the shape and size of the containment volume with respect to the operational boundaries can act to mitigate aspects of hull loss relating to the ejection of high-energy parts from the containment volume. Thus, while the primary purpose of the containment function is to prevent unintended 'fly-away', the containment system acts to mitigate several additional hazards. This multiple-hazard mitigation (or masking) property requires thorough understanding and documentation of the effect of a mitigation technique on all system hazards, especially in the case of the (future) alteration of mitigation.

In conclusion, the development of risk-centric certification requirements for UAS is challenging, even when leveraging existing regulations that incorporate extensive lessons learned about airworthiness. The process of creating the mock type certification basis for an unmanned agricultural rotorcraft provided valuable insights that could support larger standards development efforts. In particular, there is a fundamental connection between the UAS, its ConOps, and its risk-centric derived certification requirements. Achieving the correct level of abstraction in specifying these requirements, whether it be from aggregating potentially prescriptive Part 27 requirements, or translating human-centric Part 91 operational requirements, is a key challenge in attaining a certification basis that applies to the broadest possible class of UAS.

References

[1] Federal Aviation Administration, "Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap," First Edition, November 2013.

[2] K.J. Hayhurst, J.M. Maddalon, N.A. Neogi, H.A. Verstynen, B. Buelow, and G.F. McCormick, "Mock Certification Basis for an Unmanned Rotorcraft for Precision Agricultural Spraying," NASA/TM-2015-218979, November 2015.
[3] Department of Transportation, Notice of Proposed Rulemaking, Operation and Certification of Small Unmanned Aircraft Systems, Docket No.: FAA-2015-0150; Notice No. 15-01, February 15, 2015.
[4] Federal Aviation Administration, Section 333, [Online]. www.faa.gov/uas/legislative_programs/section_333
[5] European Aviation Safety Agency, Introduction of a regulatory framework for the operation of drones, Advance Notice of Proposed Amendment 2015-10, July 31, 2015.
[6] Federal Aviation Administration, FAA Order 8110.4C, Type Certification, October 26, 2005.
[7] United States Government, (undated), Title 14 Code of Federal Regulations, Electronic Code of Federal Regulation, Part 27—Airworthiness Standards: Normal Category Rotorcraft, [Online], Available: http://www.ecfr.gov
[8] W. Ryan, UAS Certification, "The Path to 21.17(b) Type Certification & Design Standards," Briefing given February 20, 2014.
[9] R.A. Clothier, B.P. Williams, J. Coyne, M. Wade, Mark, and A. Washington, "Challenges to the Development of an Airworthiness Regulatory Framework for Unmanned Aircraft Systems," 16th Australian Aerospace Congress, Melbourne, Australia, February 23–24, 2015.
[10] A. Oztekin, C. Flass, and X. Lee, "Development of a Framework to Determine a Mandatory Safety Baseline for Unmanned Aircraft Systems," Journal of Intelligent and Robotic Systems 65, No. 1-4, pp. 3-26, 2012
[11] D. Jenkins and B. Vasigh, "The economic impact of unmanned aircraft systems integration in the United States," Association for Unmanned Vehicle Systems International, March 2013.
[12] K.J. Hayhurst, J.M. Maddalon, N.A. Neogi, H.A. Verstynen, "A case study for assured containment," ICUAS 2015, pp.260-269, 9-12 June 2015
[13] Federal Aviation Administration, FAA Order 8130.2H, Airworthiness Certification of Products and Articles, Section 6. Light Sport Aircraft Category Airworthiness Certifications, February 4, 2015.
[14] U. S. House of Representatives Committee on Transportation and Infrastructure "Small Airplane Revitalization Act of 2013," (H.R.1848) fact sheet.
[15] Federal Aviation Administration, Notice 8900.227, Unmanned Aircraft Systems (UAS) Operational Approval, Effective 7/30/2013 through 7/30/2014.
[16] United States Government, (undated), Title 14 Code of Federal Regulations, Electronic Code of Federal Regulation, Part 91—General Operating and Flight Rules, [Online], Available: http://www.ecfr.gov
[17] E.M. Atkins, "Autonomy as an enabler of economically-viable, beyond-line-of-sight, low-altitude UAS application with acceptable risk", AUVSI Unmanned Systems 2014, Orlando, FL, pp.200-211.
[18] United States Government, (undated), Title 14 Code of Federal Regulations, Electronic Code of Federal Regulation, Chapter III, Subchapter C, Part 417, Subpart E, Appendix D, Flight termination system design [Online], http://www.ecfr.gov
[19] Ardupoint, (undated), "Simple geofence", copter.ardupilot.com/wiki/ac2_simple_geofence/
[20] K. Bhamidipati, D. Uhlig and N. Neogi, "Engineering Safety and Reliability into UAV Systems: Mitigating the Ground Impact Hazard", University of Illinois, Urbana-Champaign, Urbana, IL, 61822, 2008.
[21] E. N. Johnson and D. P. Schrage, "System Integration and Operation of a Research Unmanned Aerial Vehicle," *Journal of Aerospace Computing, Information, and Communication*, Vol. 1, January 2004, Georgia Institute of Technology, Atlanta, GA, USA.
[22] K. Dalamagkidis, K. Valavanis, and L. Piegl, "On unmanned aircraft systems issues, challenges and operational restrictions preventing integration into the national airspace system," Progress in Aerospace Sciences, vol. 44, no. 7-8, pp. 503-519, Oct-Nov. 2008.
[23] T.L. Martin, D.A. Campbell, "RPAS integration within an Australian ATM system: What equipment and which airspace," ICUAS 2014: 656- 668.
[24] P. Angelov, "Sense and avoid in UAS: research and application," John Wiley & Sons, 2012.
[25] X. Yu, and Y. M. Zhang, "Sense and avoid technologies with applications to unmanned aircraft systems: Review and prospects," Progress in Aerospace Sciences, vol. 74, pp. 152-166, April 2015.
[26] S.R. Herwitz. "Ground-based sense-and-avoid display system (SAVDS) for unmanned aerial vehicles:" U.S. Patent 7,269,513.p2007-9-11.
[27] M. Wilson. "Ground Based Sense and Avoid Support For Unmanned Aircraft Systems", ICAS, 2012
[28] B. Stark, S. Brennan and Y.Q. Chen. "ADS-B for small Unmanned Aerial Systems: Case study and regulatory practices." ICUAS 2013.
[29] C. Geyer, D. Dey, S. Singh. "Prototype sense-and-avoid system for UAVs." Robotics Institute, Carnegie Mellon University, Tech. Rep. CMU-RI-TR-09-09, 2009.
[30] Y. Kwag, C.H. Chul. "UAV based collision avoidance radar sensor." Geoscience and Remote Sensing Symposium, 2007. IGARSS 2007.
[31] K. Valavanis, "Unmanned aircraft systems: the current state-of-the art," Springer, 2013. IGARSS 2007.
[32] A. McFadyen, L. Mejias, "Design and evaluation of decision and control strategies for autonomous vision-based see and avoid systems," ICUAS 2015, pp.607-616, 9-12 June 2015
[33] F. Munoz, E.S. Espinoza, I. Gonzalez, L.R. Garcia Carrillo, S. Salazar, R. Lozano, "A UAS obstacle avoidance strategy based on spiral trajectory tracking," in ICUAS 2015, pp.593-600, 9-12 June 2015
[34] J. Bellingham, Y. Kuwata, and J. How, "Stable Receding Horizon Trajectory Control for Complex Environments," AIAA Guidance, Navigation, and

Control Conference and Exhibit, Austin, Texas, USA, August 2003.

[35] M.B. Milam, R. Franz, and R.M. Murray, "Real-Time Constrained Trajectory Generation Applied To A Flight Control Experiment," IFAC World Congress, pp. 1252-1252, Barcelona, Spain, 2002.

[36] D. Mellinger and V. Kumar, "Minimum snap trajectory generation and control for quadrotors," IEEE ICRA, pp. 2520-2525, May Shanghai, China, May 2011.

[37] E. Bumiller, (2010, August 25). "Navy Drone Violated Washington Airspace", *The New York Times*. Retrieved from http://www.nytimes.com