Safety Considerations for UAS Ground-based Detect and Avoid

Ewen Denney and Ganesh Pai
SGT / NASA Ames Research Center
Moffett Field, CA 94035, USA
{ewen.denney, ganesh.pai}@nasa.gov

***Abstract*—We describe a generic mission concept of low altitude beyond visual line of sight unmanned aircraft system (UAS) operations, in which a ground-based detect and avoid (GBDAA) capability is to be used. First, we discuss some of the variations in the underlying missions and their bearing on providing assurance of safety in operations. Then, drawing upon the experience gained in developing safety assurance cases for many such missions, we summarize the different GBDAA safety considerations pertinent for mission safety. Additionally, we present some of the patterns of safety reasoning that we have used in the safety cases, which take the form of abstract argument structures. The overall goal of this work is to develop an infrastructure that can guide safety assured design of future UAS missions that use GBDAA, while providing rapid feedback on overall mission safety.**

***Index Terms*—Unmanned aircraft systems, Ground-based detect and avoid, Beyond visual line of sight, Safety assurance, Safety cases, Argumentation patterns, Tool support.**

I. Introduction

Safety cases are engineering artifacts detailing the efforts undertaken for safety risk management. In the context of obtaining regulatory approval to conduct UAS operations in civil airspace, they are a requirement of the current process [1] under specific conditions: in particular, when using an alternative means of compliance to the *see and avoid* requirement of the federal aviation regulation 14 CFR 91.113 (b), such as using a ground-based detect and avoid (GBDAA) system with radar, in lieu of visual observers. Over the past few years, we have developed safety cases for a number of NASA UAS operations that have used GBDAA. For instance, one of the safety cases pertained to an Earth science mission involving beyond visual line of sight (BVLOS) UAS flights over parts of the Arctic ocean off the coast of Alaska, through an airspace corridor within the national airspace system (NAS), to and from international airspace [2]. More recently, under NASA's UAS traffic management (UTM) effort [3], the safety cases have addressed UAS missions involving operational concepts of greater complexity, e.g., a combination of both visual line of sight (VLOS) and BVLOS flights using multiple, fixed and rotary wing unmanned aircraft (UAs), over sparsely populated areas.

The Federal Aviation Administration (FAA) guidelines governing the UAS operational approval process [1] specify a preferred format and the minimum required content of a safety case. For instance, details about the system and environment, besides hazard and risk analyses, are required.

An important part of a safety case is a justification for how the specified hazard mitigation measures and safety requirements are expected to reduce risk to an acceptable level. Indeed, such an explanation is also required, as per the FAA guidelines for safety case content [1]. This justification can be given in the form of an *argument*, in the sense of a connected series of propositions used in support of the truth of an overall proposition. A *safety assurance argument* thus makes explicit safety *claims* about a system and justifies how those claims hold, through the *evidence* gathered during design and operation.

In our work, we have found *argument structures* (for example, specified using the Goal Structuring Notation (GSN) [4]) to be useful for organizing and explicitly documenting arguments, including the associated safety rationale, as well as the supporting evidence (see Section V-B1). We have found the advantages of explicit rationale given in this way to be that there is: *i*) an overarching perspective of all the identified safety mechanisms, *ii*) a clarification of how those mechanisms contribute to achieving the overall safety objective(s), and *iii*) a straightforward way to drill down into the details, towards pinpointing where safety measures may be lacking. Indeed, arguments capturing safety reasoning augment hazard analysis worksheets, where this rationale is usually implicit.

Although the FAA guidelines do not require the use of argumentation, its inclusion has not been precluded. Hence, we have begun creating and including GSN argument structures in the safety case reports, using our methodology for developing assurance arguments [5]. Some of those safety cases are currently undergoing review by the FAA.

Future UTM missions will be more complex, and plan to introduce a greater degree of automation, autonomy, and sophistication into the safety systems/procedures whilst also relaxing the prevailing operational restrictions, e.g., on overflight of urban areas, flights within more congested airspace, etc. [3]. Towards supporting that effort—i.e., to develop the safety cases required to obtain FAA approval to access the NAS and conduct those missions—we want to be able to reuse as many applicable safety assets as possible, that have a successful operational history. In conjunction, we also want to create a library of the associated safety rationale to provide assurance of their contribution to safety. We anticipate that such a library will be useful to guide mission design and as a means of rapid feedback on mission safety.

Broadly, our approach is to generalize the specific safety considerations (and the corresponding safety reasoning) that we have gleaned from the prior UAS missions for which we have created safety cases. Since those operations each have their individual (often unique) mission-specific constraints and safety requirements, many of the safety considerations are also tailored to the mission, as is much of the associated safety reasoning. By taking the various operations together, however, we have identified similarities amongst the specific hazard control mechanisms and the applicable safety systems. Based on this, we have additionally developed both domain-independent and domain-specific *patterns* of safety reasoning, which clarify how the identified safety measures contribute to risk reduction. Using our tool, AdvoCATE [6], we have specified these patterns as abstract GSN arguments (i.e., *argumentation patterns*), which make explicit the underlying assumptions, evidence requirements, and dependencies.

In this paper, we first describe a generic concept of operations (CONOPS), giving the scope of the UAS missions being considered, and characterizing the operational context for using GBDAA (Section II). The main focus of the paper (Sections III and IV) is on the safety considerations relevant for ground-based surveillance, avoidance maneuvers, and crew procedures, which collectively comprise the GBDAA concept. Then, we present a selection of the identified argumentation patterns, focusing on those relevant for the safety assurance of GBDAA (Section V). We also discuss the dependencies between the associated capabilities and *a*) other safety mechanisms, such as contingency procedures, *b*) system-specific details, such as the CONOPS, the operating airspace, etc. Finally, we discuss how patterns can be combined to clarify the contribution to system safety.

II. Scope

A. Operational Context

Six types of access profiles broadly characterize how UAS can access and operate in the NAS [8]. In order of increased capabilities required of the UAS, they are: *i*) visual line of sight (VLOS), *ii*) terminal area, *iii*) operating areas, *iv*) lateral transit (corridor), *v*) vertical transit (cylinder), and *vi*) dynamic. Collectively, they provide a framework for incremental access to different airspace classes.

Of these, the *operating areas* access profile primarily concerns access to special use airspace, such as military operations areas (MOAs), and may not be appropriate for civil UAS missions. *Vertical transit* (cylinder) operations are mainly meant to categorize those missions where UAS access the airspace at higher altitudes, e.g., Class A airspace, through a spiral climb, or descend from high altitudes in a spiral descent. Such operations are not in scope for the current work. *Dynamic* UAS operations represent the ultimate goal of routine access to the NAS and is also not in the scope of this paper. Note that since the access profiles are meant to represent increasing capabilities, all those that are not VLOS operations involve UAS operating BVLOS. Thus, we are broadly concerned with a combination of VLOS operations, and BVLOS operations conducted under the terminal area, and lateral transit (corridor) access profiles. Specifically, the emphasis is on multiple, concurrent small UAS (sUAS)[1] operations, which may comprise fixed and/or rotary wing configurations, conducted at low altitudes, e.g., from the surface to approximately $2500\,\mathrm{ft}$ above ground level (AGL).

B. Assumptions and Restrictions

For this paper, we consider the following additional restrictions, though in future (e.g., in the proof of concept demonstrations of UTM) they are expected to be relaxed:

a) Operations occur within a specified *operating range* (OR) that is not within an urban environment. In general, the OR can assume a variety of shapes and sizes, and may include other types of aviation activity. We assume an OR of a polygonal shape on the surface, extending as high as $2500\,\mathrm{ft}$ AGL (for example, see Fig. 1). One consequence of this assumption is that an OR can also be defined for either of VLOS, terminal area, and transit corridor operations.

b) Operations near major airports are not considered, excluding the airspace classes B and C. Thus, depending on the location of the OR, the airspace class associated with the OR may be either of Class D, E, or G. For example, low altitude operations within 4 nautical miles (NM) of an airport with an operating control tower would occur in Class D airspace, whereas the airspace surrounding an airport with no control tower can be Class E, Class G, or a combination of the two.

c) For all access profiles, flights occur over sparsely populated areas, not including heavily built-up areas/trafficked roads.[2] However, the airspace can contain conventionally piloted (i.e., manned) air traffic, and other airspace users.

We also make the following assumptions:

i) Low altitude sUAS operations occur in uncontrolled Class G airspace, where the air traffic to be avoided comprises non-cooperative conventionally piloted aircraft (CPA) or rotorcraft, operating in and around the OR, and that may transit through the OR. Operations are restricted to the daytime, in visual meteorological conditions (VMC), although under the stricter visual flight rules (VFR) of Class E airspace.

ii) Intruders, i.e., aircraft that may pose a threat to the UAs, do not change altitude/heading so as to track them.

iii) The OR may contain obstacles (natural and man-made) that interfere with the normal operations of the GBDAA components. Additionally, the OR may or may not contain sources of electromagnetic interference.

iv) The UAs involved in the flight operations are airworthy and are capable of executing a specified maneuver on demand, within a given time interval, and under the environmental/weather conditions for which they have been designed, or as required for the operations. In general, the level of

[1] Categories I and II, as per NASA classification of UAS [7].

[2] The performance characteristics of the UAs and, more generally, their level of airworthiness will effectively constrain the type, and the location, of the operations that can be conducted. For instance, a lower-level of airworthiness necessitates defining an OR that is sparsely populated (or unpopulated), and that does not contain (m)any built-up areas.

airworthiness limits the avoidance maneuvers/procedures that can be defined/invoked. Moreover, the UAs will fly at some minimum altitude above the tallest obstacle within the OR.

v) Flight plans can include one-way or returning flights, with single or multiple point-to-point segments. The former characterizes a flight profile involving a single takeoff location followed by a flight to a defined landing location (which may be the takeoff location), while the latter entails multiple takeoff and landing locations within a single flight plan.

From the standpoint of airspace and operational safety, flights in controlled airspace are likely to be safer, than in uncontrolled airspace. The rationale is that, in general, the former affords additional safety barriers, e.g., separation services provided by air traffic control (ATC), potentially reducing the likelihood an airborne conflict, and its subsequent escalation into a loss of safe separation, followed by a near midair collision (NMAC), or a midair collision (MAC).

In contrast, aircraft in uncontrolled airspace are not provided separation services, and they may also not be visible to ATC. Consequently, a key component of safety is to *see and avoid* other aircraft when a conflict has been detected. Indeed, one of the current operational constraints for low altitude sUAS operations, is the use of (ground-based or airborne) visual observers (VOs) as the means to comply with the regulations for operating near other aircraft, 14 CFR 91.111, as well as to discharge the 'see and avoid' responsibilities required by the right-of-way rules, 14 CFR 91.113. Thus, the impact of a GBDAA system deployed in uncontrolled airspace in lieu of VOs, is likely to be larger than in controlled airspace.

III. GBDAA Concept and Analysis

Based on the preceding generic CONOPS, in this section we first describe a concept for ground-based detect and avoid (GBDAA) towards supporting BVLOS flight operations with sUAS in low altitude airspace, and outline the elements of this safety system. Then we give examples of the types of analyses required for implementing the concept, and elaborate the associated safety considerations.

A. System Description

The primary use of GBDAA will be for surveillance of the airspace for any non-cooperative, general aviation (GA), conventionally piloted aircraft (CPA), or rotorcraft that may enter the OR. The main goals of the GBDAA concept are to:

a) provide a surveillance capability during all phases of UA flight operations so as to detect and track both cooperative and non-cooperative air traffic that could potentially contribute to a conflicted airspace state when operating with UAS;

b) support both situational and navigational awareness in order to enable informed safety-related decision making in deconflicting the airspace; and

c) provide an airspace conflict resolution and avoidance capability, to maintain the prevailing level of airspace safety.

GBDAA encompasses a broad space of possible solutions, although the key elements comprise the following:

- one or more ground-based sensors, typically radar units, possibly deployed along with one or more automatic dependent surveillance-broadcast (ADS-B) ground receivers (along with supporting equipment, such as antennae, power sources, etc.)
- one or more surveillance displays that provide a visual depiction of the airspace state, with varying levels of integration of the sensed data.
- supporting logic for decision making, which can be automated, procedural, or experience-based.
- possibly one or more visual observers (VOs), to provide supplementary surveillance, e.g., in the radar cone of silence (CoS).
- a suite of conflict resolution/avoidance maneuvers and procedures, issued under the direction of a single safety authority charged with safety-related decision making.
- contingency procedures to address emergencies arising from a compromise of the GBDAA system, and
- supporting crew members, suitably trained and equipped to operate the system, using well-defined procedures addressing both nominal and off-nominal situations.

B. Requirements Analysis

At a minimum, the following aspects need to be considered in determining the functional and safety requirements for a GBDAA concept involving a *single* radar system deployed for surveillance of a polygonal OR (Fig. 2):

a) Surveillance coverage defined in terms of radar range, height, azimuth, and elevation. In turn, this requires an analysis of:

– The airspace of operations, such as an operating range (OR) for terminal area operations, or a transit corridor for lateral transit operations (see Section II).
– The airspace in which other air traffic may pose a threat, for instance by intruding into the OR, i.e., the threat volume (TV).
– The surveillance volume (SV), i.e., the volume of airspace where surveillance coverage is required.

b) The types of intruders to be detected, and their characteristics translated into requirements on the radar cross section (RCS) and radar performance, e.g., update rates, target types and velocity, detection rate and accuracy, tracking rate and accuracy, target resolution and classification, etc.

c) The characteristics of the surveillance display, including display of tracks, azimuth, elevation, height, range, target velocity, etc.

d) The logic used for threat determination and tracking; additionally, the display of threats and alerting mechanisms.

e) Avoidance maneuvers, and the conditions for invoking specific maneuvers.

f) Nominal and off-nominal procedures for the crew using and managing the system.

g) Hazards and failure modes of the system, and the corresponding mitigations.

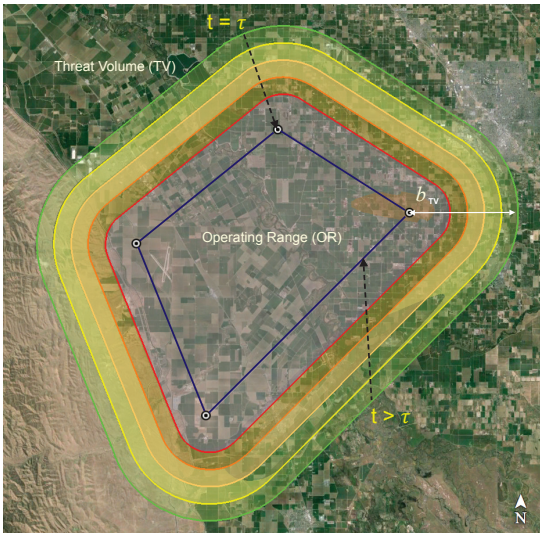

Fig. 1. Threat volume (TV) surrounding a polygonal operating range (OR).

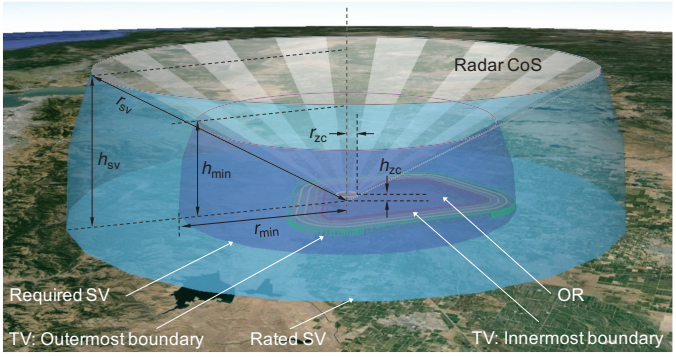

Fig. 2. Surveillance volume (SV) of a single radar enclosing the threat volume (TV) and the operating range (OR). The inner SV represents the *required* extent of coverage, while the outer SV is the rated range for a chosen radar. The cone of silence (CoS), immediately above the radar, is the volume of airspace that is 'invisible' to the radar.

Next, we illustrate some of the associated analyses, in particular the determination of generic requirements for surveillance coverage.

1) Threat Volume (TV): The TV is that volume of airspace where an intruder aircraft traveling along a trajectory whose horizontal component (i.e., its projection to a horizontal plane) is perpendicular to the OR boundary, at a ground speed up to the worst-case maximum, or descending into the OR at a descent rate up to the worst-case maximum, poses a credible collision threat, without any risk mitigation measures in place.

In the worst-case, the minimum time available for a UA to complete avoidance is the time it will take for an intruder aircraft to breach the OR boundary after having been detected at the boundary of the TV. This worst-case applies when a UA is, itself, located at the boundary of the OR where the intruder is predicted to breach it. More generally, the worst-case also applies when the UA arrives at the OR boundary at the same time and location where the intruder is predicted to breach the OR. An appropriate TV is, therefore, one where an intruder aircraft can be detected early enough, i.e., before it breaches the OR boundary, so that sufficient time is available in which to initiate and complete a conflict resolution/avoidance maneuver.

In general, if τ is the response time (in seconds) to complete an avoidance maneuver when the UA is located at the boundary of the OR, and v is the maximum ground speed for the intruder aircraft (in knots) then the outermost boundary of the TV is located at $b_{\mathrm{TV}} = (v/3600)\times\tau = 2.778\,v\,\tau\times10^{-3}$ NM from the boundary of the OR. Likewise if δ is the maximum descent rate for the intruder (in $\mathrm{ft\,min^{-1}}$) then the height of the TV is $\delta\tau$ ft above the ceiling of the OR. Thus, if h_{OR} is the height of the OR above ground level, then the height of the TV is $h_{\mathrm{TV}} = (\delta\tau + h_{\mathrm{OR}})$ ft AGL.

In Fig. 1, the TV comprises concentric projections of the OR such that the outermost projection is located at a distance of b_{TV} NM from the OR boundary, and at a height of h_{TV} ft from the ceiling of the OR. By definition, the dimensions are such that an intruder aircraft at the outermost boundary will require at least τ seconds to reach the OR boundary, whether traveling laterally or descending. Each inner projection represents a constant decrease in τ, and as been color coded as a visual indicator of increasing proximity the intruder to the OR The formulation of the TV in this way represents a tradeoff between obtaining the largest TV size—given the OR, the radar capabilities, the assumptions on intruder ground speed and descent rates, which provide a sufficient response time—and an airspace state where the UAs can continue to remain airborne with manned aircraft in their vicinity.

2) Surveillance Volume (SV): The SV represents the extent of airspace that can be *covered* by the radar system, which has been tuned for detecting targets of a specific radar cross section (RCS). We define a *minimal* SV as one that covers the TV surrounding the OR. For example, given a location for the radar emplacement, the minimal SV can be defined as follows:

i) The ideal SV is a three-dimensional volume of airspace centered at the radar location, and its shape is a hemisphere. However, any targets in the radar CoS which is formed due to the limits of radar elevation coverage, will be invisible to the radar. Therefore, the minimal SV shape is formed by removing the CoS from the ideal SV. The radius of the hemisphere (r_{min}) is the distance of those points on the outermost boundary of the TV that are the farthest from the radar emplacement location. The underlying rationale is straightforward: if the radar range (r_{sv}) is at least as far as the farthest point(s) on the TV, then intruders located at those points, or any other points on the outermost TV boundary—which would then be within radar range—would be detectable.

ii) If ϵ is the elevation angle of the radar (measured in degrees) from the horizon, and assumed to be positive (i.e., the radar is not downward looking), then the CoS is an inverted right cone with an aperture of $(180 - 2\epsilon)°$, centered directly above the radar (see Fig. 2).

iii) The height of the minimal SV, h_{min}, is proportional to the radius of the minimal SV and its elevation angle, i.e., $h_{\mathrm{min}} = r_{\mathrm{min}} \sin\epsilon°$. Note that this height is relative to the

elevation of the radar location, e_r. That is, the theoretical extent of coverage for the minimal SV, i.e., its *surveillance limit*, is up to an altitude of $h_{\min} + e_r$. Moreover, the radius of the CoS where it intersects the TV ($r_{\rm zc}$) depends on the height of the TV above the radar location, $h_{\rm zc}$. That, in turn, is again dependent on the elevation of the radar location. Since the elevations of the radar locations can change, so will the true heights of the SV, the TV, and the radius of the CoS.

3) Surveillance Requirements: In general, the requirement on the radar is for its SV to *cover* the TV and the OR. Based on the preceding analysis, the SV specifications quantify the extent of the required surveillance coverage, in terms of the minimum radar range and the dimensions of its CoS. However, additional analyses also apply. For example,

- the altitude to which surveillance is required, together with the elevation of the emplacement location, contributes to defining the minimum elevation coverage.
- airspace analysis—in terms of the directions from where threat air traffic may originate relative to the OR, together with the radar emplacement location—contributes to defining the extent of the azimuth coverage. Airspace analysis also supplies requirements that quantify performance parameters, e.g., minimum detectable target velocity, radar range and azimuth resolution, detection accuracy, etc.

Furthermore, requirements can arise from interactions and dependencies with other safety systems. For instance, *separation limits/standards* can be defined for segregating multiple UAs. In turn, this provides a performance requirement on the range resolution capability of the GBDAA sensors—i.e., the extent to which the GBDAA sensors can discriminate between UAs and CPA operating in close proximity—so that violations of safe separation can be detected.

IV. Safety Considerations for Implementation

Based, in part, on the preceding analyses, we now describe the considerations for a safe implementation of the GBDAA concept of Section III-A: first, we address each of the broad constituent elements. Then we consider how different access profiles, as well as the variations in specific operations in an access profile, have a bearing on safety and the implementation requirements.

A. Ground-based Surveillance

1) Surveillance Sensors: The types of targets that are assumed to be detected by radar are CPA, unless the radar can be specifically tuned for detecting small slow-moving targets, such as UAs. Hence, surveillance of UAs may also require an alternative system integrated with, or used along with, the radar system and the corresponding display, e.g., an ADS-B receiver and antenna. This type of solution will also require UAs to be equipped with functional and operating ADS-B transponders.

When one radar is used, the CoS immediately above the radar is the volume of airspace where airborne targets will be invisible to the radar. In this case, ground-based or airborne VOs may be used to provide surveillance. Alternatively, additional radar units can be deployed such that the CoS of one is *covered* by another. In such a situation, there are additional constraints/requirements on the radar display.

Radars may or may not be downward looking. In the former case, the height limit is determined by the radar elevation angle below the horizon as well as the range of altitudes where surveillance is required. A radar emplacement location is to be chosen to minimize obstacles and clutter. Similarly, if an ADS-B receiver is used, its location should afford unobstructed radio frequency line of sight to the extent possible.

2) Surveillance Display: The surveillance display system can comprise one or more displays, with a communication network to the surveillance system. Together, it provides a three dimensional (3D) visualization of the various airspace volumes relevant for the intended operations, in particular the threat volume (TV) (see Section III-B) and the OR, so that it can be determined whether or not air traffic detected by the surveillance sensors poses a threat. This system typically ought to provide the ability to determine intruder altitude, location, velocity, heading (possibly for a designated duration) and whether it has breached the TV. The latter may be indicated through an automated altering mechanism.

Depending on the conflict resolution/avoidance maneuvers to be used, the display may, additionally, be required to show which boundary of the TV the intruder has breached. Both the primary and secondary tracks may be shown on a single display and may or may not be fused. If shown on separate displays, the displays ought to be calibrated and correlated to present a consistent picture of the airspace situation. Likewise, downlinked UA data from ground control stations (GCSs) may or may not be integrated. Similarly, when multiple radar units are used, primary tracks will need correlation and/or fusing if a single radar display is being used. If using multiple displays, they ought, again, to be calibrated and consistent with respect to the airspace under surveillance that is common to all radars.

For the purposes of determining system availability, a health status display for the radar/ADS-B receivers is useful so that contingency measures can be invoked in the event of emergency situations, e.g., suspending operations when a radar fails. System reliability may be improved by using redundant radars, while availability can be improved with failover configurations. A primary display is available to the radar operator, i.e., the crew member who is designated to interpret the sensor information. Supplemental displays may be used by other crew members for situational awareness.

B. Avoidance

In this paper, we do not quantify how much time is *sufficient* for completing an avoidance maneuver, and assume that this will be determined externally. In general, however, a *minimum* bound on the avoidance time can be established from a combination of the times to: *i*) detect an intruder, *ii*) track the intruder and establish that it is a threat (i.e., classify the intruder as a credible threat, based upon its trajectory over some minimum interval that confirms that it is on a course to

potentially breach the OR and/or collide with the UA), *iii*) determine an appropriate conflict resolution/avoidance maneuver, *iv*) command and transmit the maneuver to the UA, *v*) process the command and (for the UA to) actuate the maneuver, and *vi*) complete the maneuver given the performance characteristics and environmental conditions, e.g., wind speeds, ending in a safe state.

The definition of avoidance maneuvers and conflict resolution procedures takes vehicle classes (determined on the basis of vehicle performance, communication, and airworthiness) into account. Specific maneuvers are developed through testing and simulation, over a range of environmental conditions, and conflict scenarios. Additionally, the avoidance maneuvers take into account the minimum avoidance time as dictated by the specific surveillance solution. Thus, a suite of avoidance maneuvers can be developed, with an order of preferred execution, i.e., some level of escalation of threat and avoidance that are defined relative to identified contingency locations, including lost-link Points (LLPs), flight termination points (FTPs), and divert/contingency points (DCPs). For example,

- *abort and return to base*, i.e., immediately suspend the current flight plan and return to the takeoff/launch location at the maximum speed;
- *divert and loiter*, i.e., divert to a safe DCP, descending/ascending to a safe altitude, and loiter at that location until otherwise commanded;
- *divert and land*, i.e., suspend the current flight plan, and descend at the maximum descent rate after navigating to a safe DCP;
- *land immediately*, i.e., suspend the current flight plan, and descend at the maximum descent rate from the current location; and
- *terminate*, i.e., immediately shut-off of all propulsion, resulting in a (possibly uncontrolled) descent, while taking measures to halt forward motion.

C. Crew and Crew Procedures

The minimum crew consists of a radar operator (RO), visual observers (VOs), and a safety authority (SA).

i) The RO should be a crew-member who *a*) is familiar with radar surveillance procedures, *b*) has a basic understanding of air traffic management (ATM) with regards to airspace coordination of manned and unmanned flight operations, and *c*) has received sufficient prior training on operating the radar system. The core responsibility of the RO is to interpret the information on the surveillance displays and determine, based upon the encounter geometry, whether or not detected non-cooperative aircraft pose a credible threat. The RO then communicates this information to the authority ultimately responsible for flight safety, who is also charged with safety-related decision making.

ii) VOs are optional and their usage depends on the extent of airspace *not covered* by radar surveillance. If VOs are used, their primary responsibility is to detect any intruders within the radar CoS, as well as any areas of the OR where the GBDAA system is unable to provide sufficient warning, and communicate this to the *pilot in command* (PIC), or more generally provide surveillance information to those with the authority for flight safety and the related safety decisions.

iii) The SA is the crew member who has ultimate authority for the safety of flight operations. This individual can be the *pilot in command* (PIC), or a separate crew member[3] who is not responsible for piloting the UA. The SA determines the exact avoidance maneuvers to be used based upon the airspace situational information communicated by the RO and the VOs.

D. Variations in Access Profiles and Operations

Based on an access profile (see Section II) and the specific operations for a given access profile (or a combination thereof), implementation requirements are likely to change, as are the corresponding safety considerations. Especially, in case of the latter, the variations in operations can expose a GBDAA solution to different hazards that can defeat its purpose.

For instance, terminal area operations within an OR in close vicinity of an active airfield will have different safety implications than operations within an OR that *i*) is well separated from aviation activity, and *ii*) does not include other aviation activity. The rationale is that in the former access profile, there is a greater chance of exposure to intruders than in the latter. Moreover, in the former, if the aviation activity originates within the TV and/or the OR, then the requirement of sufficiently early detection of intruders may not be met with a single radar (if applying the analyses as in Sections III-B1 and III-B2). In this case, a second radar may be required to provide surveillance of the airspace where the threats are situated, or an additional means of surveillance, such as VOs, may be required. Thus, a variation in the access profiles will clearly impact both surveillance and avoidance requirements.

Likewise, for a given access profile, variations in the specific details of the CONOPS/mission profiles also affect GBDAA requirements and its implementation from a safety standpoint. For example, the choice of the emplacement location, in part, together with the size of the OR affects whether or not the radar CoS has a safety impact. In general, an aircraft entering the CoS at a high altitude and descending into the OR at the maximum descent rate and minimum ground speed will be invisible to radar unless it exits the CoS before it descends into the TV. This scenario is especially true for those aircraft descending in a spiral trajectory within the CoS, and for rotorcraft/vertical take-off and landing (VTOL) aircraft that descend vertically (although, by excluding vertical transit access profiles, we somewhat preclude the former). However, the scenario is a threat mainly if the intruder can, in fact, breach the TV and the OR after exiting the CoS. For an OR that is relatively small[4] this scenario is extremely unlikely to occur and, therefore, poses lower risk in comparison to a much larger OR.

Similarly, when the OR is appreciably large, an intruder may continue to be safely separated from the UAs even after

[3]This is the typical approach used when conducting NASA UAS missions.
[4]Specifically, its dimensions are small relative to the glide ratio.

it has breached the OR boundaries. In this case, the OR could be partitioned into smaller *sub-ranges*, each with their own TVs. As consequence, the avoidance maneuvers that can be reasonably utilized are also affected. For instance, in a large OR not including aviation activity, UA flight termination may be a rarity; instead diverting UAs from their flight paths to loiter/land at a designated contingency point is likely to be more frequently utilized. In contrast, in a small OR in a terminal area operation, UA flight termination may often be the maneuver required to result in a safe airspace state.

V. Safety Assurance

A. Overview

We assert the need for explicit safety rationale to be included with the GBDAA solution design and implementation, together with a plan for data collection. The goal of the latter is to support verifying the safety performance of the implementation (e.g., actual radar performance in operation, communication latency between the surveillance system and its displays, surveillance system failures, etc.), and validating the corresponding requirements and the assumptions made, e.g., about air traffic behavior in the airspace of operations, etc. This is consistent with the safety case content as required by the FAA [1]. However, we believe it also goes beyond traditional verification and validation (V&V) by providing explicit justification for the traceability from the V&V evidence to the stated safety objectives. Such rationale can take the form of *structured safety arguments* (described subsequently) embedded into the safety case, which leverages a comprehensive hazard analysis that, in turn, identifies risk mitigation strategies.

GBDAA constitutes two related safety barriers (namely, surveillance, and avoidance) among a *collection* of different safety systems, e.g., separation limits, nominal and emergency procedures, crew communication procedures, etc., that work together to ensure airspace safety during UAS operations. Thus, safety assurance of GBDAA is to be provided in context of these overall measures for system safety, in part because of interactions and potential dependencies between the different safety barriers (see Section III-B3, for an example). The idea is to show not only that the GBDAA design and implementation fulfill the relevant system safety requirements, but also that the system will operate safely in conjunction with other safety barriers. Elsewhere [9], [10], we have proposed how *bow-tie* models can provide an *abstract safety architecture* to support such an assessment.

B. Capturing Safety Rationale

As mentioned earlier, safety rationale represented as an argument can comprise: *i*) explicitly identified (system) safety goals, *ii*) a detailed safety risk assessment from which additional risk reduction barriers, if required, can be identified and derived, and *iii*) structured reasoning with explicit evidence, linked to and justifying how, the identified safety objectives have been met.

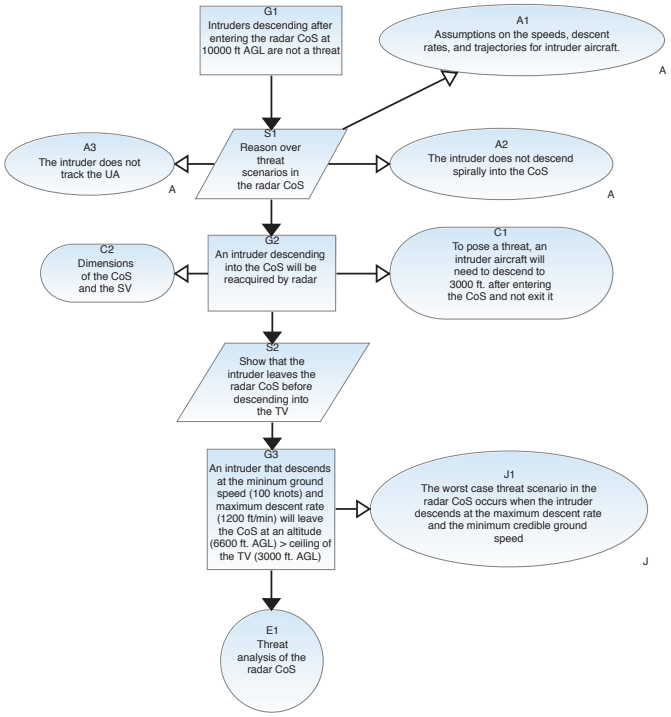

Fig. 3. Example GSN argument fragment capturing safety rationale.

1) Argument Structures: The Goal Structuring Notation (GSN) [4], provides a graphical syntax for a diagrammatic presentation/capture of safety rationale in both an abstract form (i.e., as *argumentation patterns*), and a concrete form (i.e., as *argument structures*).

Fig. 3 shows an example GSN argument, as a directed acyclic graph of different nodes and links. The node types (and corresponding graphical syntax) shown are: *goal* (rectangle), *strategy* (parallelogram), *context* (rounded rectangle), *solution* (circle), assumptions, and justifications (ellipse, annotated with A, and J respectively). The link types '→' and '⇾' represent, respectively, *support* and *contextual* relationships between the nodes. In general, nodes refer to external items including *i*) artifacts such as hazard logs, requirements documents, design documents, various relevant models of the system, etc.; *ii*) the results of engineering activities, e.g., safety, system, and software analyses, various inspections, reviews, simulations, and verification activities including different kinds of system, subsystem, and component-level testing, formal verification, etc.; and *iii*) records from ongoing operations, as well as prior operations, if applicable.

The rationale conveyed by the argument fragment in Fig. 3 pertains to the assertion that an intruder aircraft entering the radar CoS at a high altitude (10000 ft AGL) does not pose a threat (goal G1). The assertion is supported by reasoning over threat scenarios in the CoS (strategy S1), given assumptions on the speed, decent rate, trajectory, and behavior of the intruder within the CoS and relative to the UA (assumptions A1, A2, and A3). That amounts to showing that the intruder will be reacquired by radar (goal G2) given the dimensions of the

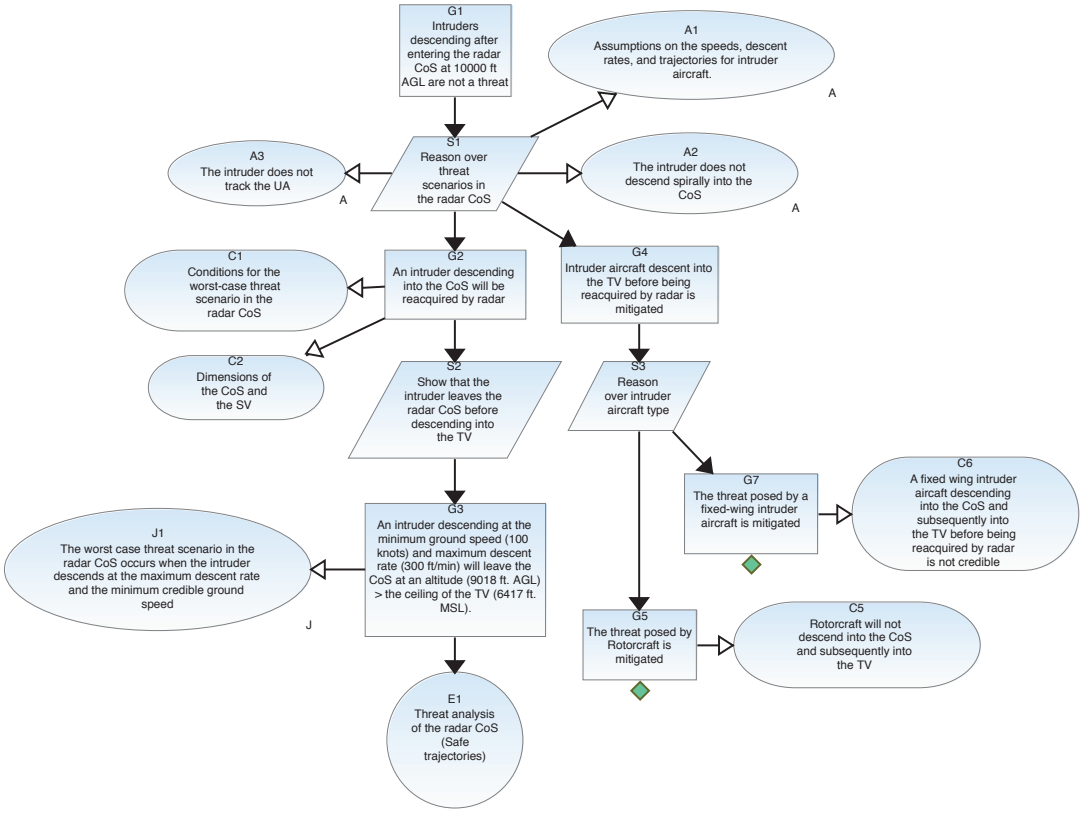

Fig. 4. Example GSN argument fragment for another UAS operation, providing rationale for why threats in the radar CoS have been managed.

CoS, the SV, and the conditions when the intruder will pose a threat (contexts C1 ad C2). The evidence for this claim, in turn, comprises the threat analysis of the CoS (solution E1), which asserts that the intruder will indeed exit the CoS at an altitude greater than the ceiling of the TV (goal G3), given its maximum descent rate and minimum ground speed. The corresponding justification is that this scenario is the worst-case (justification J1). We note that this argument is a fragment of the overall rationale in the safety case for using GBDAA, which we created for an UAS mission whose OR and SV are, respectively, as shown in Fig. 1 and Fig. 2.

Fig. 4 shows another GSN argument fragment, which we created for a different UAS mission (and safety case) that employed GBDAA. Here, we observe that the *leg* of the argument below (and including) goal G2, is similar to the argument in Fig. 3. Specifically, this leg also provides the rationale why an intruder descending into the radar CoS will be reacquired (goal G2), although the supporting evidence (solution E1) and evidence assertion (goal G3) contain the specifics of the applicable mission. Likewise, the elements of context (C1 and C2), justification (J1), and the relevant assumptions (A1, A2, and A3) also contain details pertinent to the applicable operations.

However, there is supplementary rationale (comprising the argument leg including and below goal G4) concerning additional, plausible intruder types and behavior, given the specific access profile and CONOPS. Indeed, the very same GBDAA system has been used in both UAS operations, however there are different safety considerations (and, consequently, differing safety assurance concerns) owing to the variations in the particulars of the mission and the access profile. Specifically, the supplementary rationale is concerned with showing that threats posed by rotorcraft (goal G5), and by fixed-wing intruders (goal G7) are mitigated in the situation where they may exit the CoS but *after* they have already breached the TV. In brief, the substantiation involves demonstrating through analysis that the latter situation can not be a credible scenario given the assumptions on intruder behavior. For the former, the argument relies on an appeal to the communication and coordination procedures in place to achieve airspace deconfliction.

The additional '$\diamond$' annotation on goals G5 and G7 in Fig. 4 is GSN syntax to indicate that the goals need further development (indicated here, since we have not shown the entire argument due to space constraints).

2) Argument Patterns: Fig. 5 gives a fragment of a (domain-specific) GSN argument pattern. As shown, GSN patterns use the same graphical syntax as arguments but have additional constructs and annotations. For instance, nodes have typed parameters, which abstract from the specific details of the rationale. This is given in the description as $\{variable :: type\}$ and visually shown by the node annotation '$\triangle$', indicating that the node can be instantiated. Links have annotations for multiplicity (shown in Fig. 5, as the labeled '$\bullet$' placed on the $\rightarrow$ link), and there is an additional construct

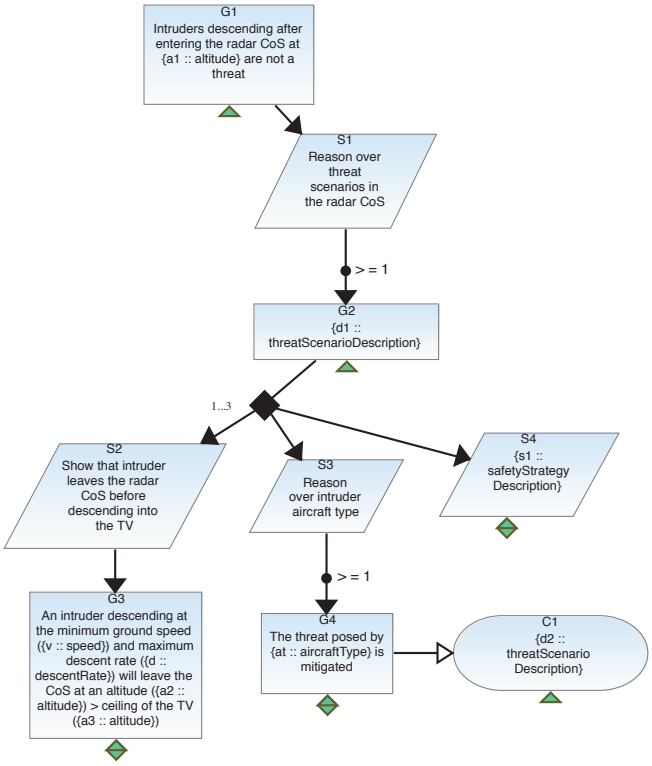

Fig. 5. Example fragment of a domain-specific pattern, in GSN.

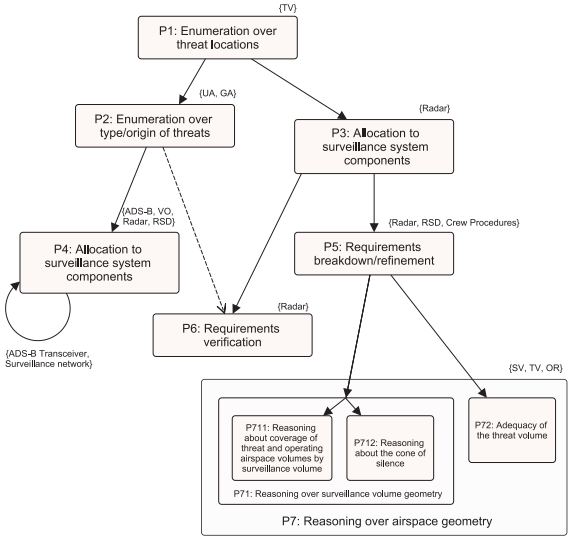

Fig. 6. High-level structure (architecture) of the assurance argument that a GBDAA system satisfies its surveillance requirements

for choices (shown as the filled, annotated diamond in Fig. 5). Choices convey that one or more of the paths specified can be taken upon instantiation. There are additional extensions [11], which we do not describe here due to space constraints.

The GSN argument fragments in Fig. 3 and Fig. 4 are, in fact, different instances of the same argument pattern of Fig. 5. Briefly, this pattern shows the abstract rationale we have used when reasoning about threats posed by intruders entering the radar CoS (goal G1). The approach is to reason about different threat scenarios (strategy S1), the descriptions of which can be enumerated (goal G2). Subsequently, to show that the threat scenarios have been addressed, the following choices exist: either *a*) show that the intruder exits the CoS before descending into the TV (strategy S2), or *b*) reason about the intruder aircraft type (strategy S3), or *c*) any other strategy that applies, based upon the specifics of a mission (strategy S4). The resulting claims (goals G3 and G4) are abstractions of the assertions obtained when the choice is exercised.

Thus, the overall idea here is that the pattern is *instantiated* to make concrete the abstract argument, using specific details for a given mission, CONOPS, access profile, etc. Note that in the pattern here, we have not include the various contextual nodes appearing in the instances: those were added after instantiation, to provide additional clarification of the rationale.

C. Relating Safety Considerations and Argumentation

Structured arguments capturing safety rationale provide a convenient way to justify the GBDAA safety considerations identified earlier (Section IV). Effectively, they provide a way to associate the latter to the wider goal of safe operations. In other words, we can provide rationale (not given in this paper) linking the identified requirements to safety in operations.

One of the (domain-independent) patterns that can be used to create this argument uses *hazard directed* reasoning. The resulting argument enumerates the hazards identified at the system level and provides the reasoning used to arrive at the specific safety considerations. Usually this rationale concerns the mitigation of an identified hazard cause, or a *component* of the hazard. A *risk-driven* argument can also be used, where the identified safety considerations would be shown to reduce some component of the associated safety risk (such as the likelihood of a hazard consequence). Such an argument describes the reasoning underlying bow-tie diagrams, which model how safety barriers prevent a system from transitioning into a hazardous state, or how they recover from the same. Note that the two forms of argument are not mutually exclusive, and address the same safety concerns in different ways.

Effectively this is an *upward* relationship, tying GBDAA requirements to system safety. A *downward* relationship also exists, where the identified safety requirements must be shown to have been met by the GBDAA implementation. Again, structured arguments provide a way to capture this justification, and the broad goal is to show that the concrete GBDAA system properly implements the identified safety requirements.

In general, the safety considerations we identified earlier (Section IV) apply for a class of UAS operations/access profiles where GBDAA will be used. Thus it is intuitive to capture the underlying safety rationale in an abstract form, using argument patterns. We have identified a number of domain-specific and domain-independent patterns to construct these kinds of arguments and that are applicable for justifying GBDAA safety. We have also previously suggested that *pattern compo-*

sition [12] can be used to provide another abstraction—termed *argument architecture*—which gives high-level organization of the overall rationale, and characterizes the reasoning/intent of the various components of the argument.

Fig. 6 shows an example of an argument architecture, capturing the structure of the reasoning why a GBDAA system—utilized in the same UAS mission for which the argument of Fig. 4 applies—meets the surveillance requirements derived from the overall system safety objectives. As shown, each node in the argument architecture is, itself, an abstraction of a GSN pattern and addresses a specific concern: e.g., the node labeled 'P712: Reasoning about the cone of silence' is concerned with the rationale pertaining to the mitigation of the hazards posed when intruders enter the radar CoS. Similarly, each link is a corresponding abstraction of the links between the lower-level pattern nodes. In fact, the pattern in Fig. 5 is a fragment of the complete pattern being abstracted by that node. Moreover, the concrete rationale upon instantiation for a specific UAS mission and access profile will resemble the argument fragments as shown in Fig. 3 and Fig. 4.

We can construct similar argument architectures, patterns, and instances to capture the rationale how the remainder of the GBDAA functions meet their respective safety requirements and contribute to the wider objective of safety during operations. More generally, we hypothesize that we can apply this approach to the overall safety case, to tie together concrete safety requirements, mission requirements, and safety assurance concerns.

VI. Conclusion

The main focus of this paper is on assuring safety when using GBDAA to support sUAS operations, conducted in low altitude uncontrolled airspace, under specific types of access profiles, namely a combination of VLOS, terminal area, and transit (corridor) operations. Based on a generic GBDAA concept, and using the example of surveillance coverage, we have illustrated the derivation of functional safety requirements. Then, we have given an overview of a number of abstract safety considerations for concept implementation. Additionally, our approach to provide assurance (that an implementation not only meets the identified safety considerations but also contributes to overall safety in operations) uses patterns of safety reasoning captured in the form of structured arguments. Moreover, we have illustrated this notion using a specific safety concern—i.e., threats posed in the radar cone of silence—as a driving example, to highlight how an abstract pattern can be instantiated to produce concrete rationale that a given implementation is safe for different missions. As such, we believe the main utility of this work is in creating an infrastructure that can guide safety assured design of future UAS missions using GBDAA.

The perspectives in this paper have been drawn, in part, from our previous experience in creating safety cases for UAS operations using GBDAA [2], and here we generalize those efforts. However, the safety considerations given here are not comprehensive, and more can be done. For example, we have not presented a detailed derivation of the requirements on many related safety aspects, e.g., crew procedures. We have also not discussed detailed sensor specifications, specifications of the threat classification and alerting logic, logic to select an appropriate avoidance maneuver, the implications on vehicle capabilities, and the interplay with other safety barriers. Each of these may need to be considered depending on the level of assurance required, and the complexity of the underlying implementation, e.g., as in the GBDAA systems being developed by the US Department of Defense [13]. In future, we plan to automate the selection and combination of patterns, building on our prior work [12]. There, our goal is to provide an interactive process where the mission and its safety system can be designed in parallel. Our vision is that, based on specified mission characteristics, engineers can avail of rapid feedback on the feasibility of the suggested safety mechanisms.

Acknowledgment

This work has been supported by the SASO project, under the Airspace Operations and Safety Program of the NASA Aeronautics Research Mission Directorate.

References

[1] US Dept. of Transportation, Federal Aviation Administration (FAA), "Flight Standards Information Management System, Volume 16, Unmanned Aircraft Systems," Order 8900.1, Jun. 2014.

[2] R. Berthold, E. Denney, M. Fladeland, G. Pai, B. Storms, and M. Sumich, "Assuring ground-based detect and avoid for UAS operations," in *Proceedings of the 33rd IEEE/AIAA Digital Avionics Systems Conference (DASC 2014)*, Oct. 2014, pp. 6A1–1–6A1–16.

[3] T. Prevot, J. Rios, P. Kopardekar, J. Robinson III, M. Johnson, and J. Jung, "UAS traffic management (UTM) concept of operations to safely enable low altitude flight operations," in *Proceedings of 16th AIAA Aviation Technology, Integration, and Operations Conference*, no. AIAA-2016-3292, Jun. 2016.

[4] Goal Structuring Notation Working Group, "GSN Community Standard Version 1," Nov. 2011. [Online]. Available: http://www.goalstructuringnotation.info/

[5] E. Denney and G. Pai, "A methodology for the development of assurance arguments for unmanned aircraft systems," in *Proceedings of the 33rd International System Safety Conference (ISSC 2015)*, Aug. 2015.

[6] E. Denney, G. Pai, and J. Pohl, "AdvoCATE: An assurance case automation toolset," in *Proceedings of the 31st International Conference on Computer Safety, Reliability, and Security (SAFECOMP 2012)*, LNCS vol. 7613, pp. 8–21, Sep. 2012.

[7] NASA Aircraft Management Division, *NPR 7900.3C, Aircraft Operations Management Manual*, NASA, Jul. 2011.

[8] UAS Task Force Airspace Integration Integrated Product Team, "Department of Defense Unmanned Aircraft System Airspace Integration Plan, Version 2.0," OSD Report RefID: 1-7ABA52E, Mar. 2011.

[9] E. Denney and G. Pai, "Argument-based airworthiness assurance of small UAS," in *Proceedings of the 34th IEEE/AIAA Digital Avionics Systems Conference (DASC 2015)*, Sep. 2015, pp. 5E4–1–5E4–17.

[10] E. Denney and G. Pai, "Architecting a safety case for UAS flight operations," in *34th International System Safety Conference (ISSC 2016)*, Aug. 2016. (to appear)

[11] E. Denney and G. Pai, "A formal basis for safety case patterns," in *Proceedings of the 32nd International Conference on Computer Safety, Reliability and Security (SAFECOMP 2013)*, LNCS vol. 8153, pp. 21–32, Sep. 2013.

[12] E. Denney and G. Pai, "Composition of safety argument patterns," in *Proceedings of the 35th International Conference on Computer Safety, Reliability and Security (SAFECOMP 2016)*, Sep. 2016. (to appear)

[13] T. Spriesterbach, K. Burns, L. Baron, and J. Sohlke, "Unmanned aircraft system airspace integration in the national airspace using a ground-based sense and avoid system," Johns Hopkins APL, Technical Digest Vol. 32, No. 3, 2013.