ASSURING GROUND-BASED DETECT AND AVOID FOR UAS OPERATIONS

Ewen Denney and Ganesh Pai, SGT / NASA Ames Research Center, Moffett Field, CA
Randall Berthold, Matthew Fladeland, Bruce Storms and Mark Sumich
NASA Ames Research Center, Moffett Field, CA

Abstract

One of the goals of the Marginal Ice Zones Observations and Processes Experiment (MIZOPEX) NASA Earth science mission was to show the operational capabilities of Unmanned Aircraft Systems (UAS) when deployed on challenging missions, in difficult environments. Given the extreme conditions of the Arctic environment where MIZOPEX measurements were required, the mission opted to use a radar to provide a ground-based detect-and-avoid (GBDAA) capability as an alternate means of compliance (AMOC) with the *see-and-avoid* federal aviation regulation. This paper describes how GBDAA safety assurance was provided by interpreting and applying the guidelines in the national policy for UAS operational approval. In particular, we describe how we formulated the appropriate safety goals, defined the processes and procedures for system safety, identified and assembled the relevant safety verification evidence, and created an operational safety case in compliance with Federal Aviation Administration (FAA) requirements. To the best of our knowledge, the safety case, which was ultimately approved by the FAA, is the first successful example of non-military UAS operations using GBDAA in the U.S. National Airspace System (NAS), and, therefore, the first non-military application of the safety case concept in this context.

Introduction

In 2010, the National Aeronautics and Space Administration (NASA) determined that expanding the utility of Unmanned Aircraft Systems (UAS) was critical for advancing the agency's goals in Earth System Science. Towards this end, in part, and to better understand ocean and ice characteristics in the Pacific sector of the Arctic Ocean, in areas known as Marginal Ice Zones (MIZ), NASA's Science Mission Directorate funded the Marginal Ice Zones Observations and Processes Experiment (MIZOPEX). The effort, which concluded in late 2013, contributed to NASA's Earth science goals through measurements that are directly relevant to improving Earth system models, improving our understanding of fundamental phenomena, and characterizing the change in the key components of the Earth system. Besides its science objectives, one of the goals of MIZOPEX was to demonstrate the operational capabilities of UAS when deployed in harsh environments and when tasked with challenging mission profiles. For example, the MIZOPEX required continuous observations of the ocean surface, subsurface and atmospheric conditions, extensive airborne mapping of large surface areas over the Arctic Ocean, and repeated visitations to locations over drifting ice packs.

UAS operations in the NAS requires authorization from the Federal Aviation Administration (FAA), through the issuance of a *Certificate of Authorization* (COA), applicable to public entities such as NASA, or a *Special Airworthiness Certificate* (SAC), which applies to all other entities. The national policy document[1], N8900.207 [1], which details the guidelines for operational approval also sets forth certain system and operational requirements that must be met before a COA/SAC can be issued. The *observer requirement* is one relevant example, where UAS operations conducted under visual flight rules (VFR) must use visual observers (VOs) that can be ground-based or airborne in dedicated chase aircraft. The underlying rationale is to comply with the so-called *see-and-avoid* requirements of the Federal Aviation Regulations (FARs), i.e., 14 CFR Part 91, Subpart B, §91.111, §91.113, and §91.115. Effectively, the role of a VO is to scan the area of UAS operations for potentially conflicting traffic, and to assist the pilot-in-command (PIC) with navigational awareness, so as to avoid collision hazards [1].

Due to the extreme nature of the weather conditions and the location for MIZOPEX, the mission opted to use a ground-based air-defense radar, instead of surface-based or airborne VOs, to provide a *detect-*

[1] Now superseded by the new policy document N8900.227, which retains the elements of N8900.207 referenced in this paper.

and-avoid (DAA)[2] capability to comply with the see-and-avoid requirements of the FARs. The UAS operational approval guidance [1] requires that proponents, i.e., applicants seeking approval of UAS operations, who intend to use an *alternative means of compliance* (AMOC) submit a system safety case assuring that the operations can be conducted safely.

This paper describes our experience with the safety assurance of the MIZOPEX ground-based detect-and-avoid (GBDAA) capability in support of obtaining approval to conduct UAS operations. In particular, we describe how we interpreted the guidelines outlined in the national policy and defined the processes for safety analysis. We also describe how we formulated the appropriate safety goals, identified and assembled the relevant safety verification evidence, and documented the operational safety case in a format compliant with FAA recommendations, in particular Appendix D of N8900.207 [1]. To the best of our knowledge, our safety case (which was ultimately approved by the FAA) is the first successful example of deploying GBDAA for civil UAS operations in the NAS, and, therefore, the first non-military application of the safety case concept in this context. Finally, based upon our previous work, we describe an alternative, but compatible safety case model.

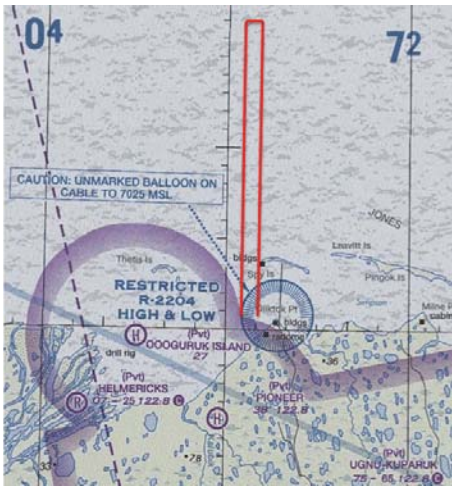
Background

We describe, in brief, the MIZOPEX concept of operations (ConOps), the GBDAA system, and the corresponding safety assurance requirements that were to be met for obtaining operational approval.

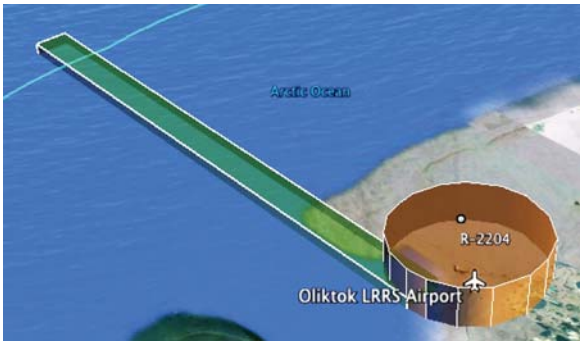
Concept of Operations

For the success of the MIZOPEX mission, multiple UAS, i.e., NASA's Sensor Integrated Environment Remote Research Aircraft (SIERRA) UAS and the University of Alaska Fairbanks' Insitu ScanEagle UAS, were required to be operated with different science instrumentation payloads over the relevant MIZ in the Arctic ocean. Consequently, each UAS was required to safely transit, multiple times[3], through the portion of the NAS between the base of operations (i.e., from U.S. airspace over Oliktok point, Alaska) and the identified MIZ (located under international airspace).

The inbound and outbound flights for both aircraft occurred through a *transit corridor* (TC), located in Class G and E airspaces. The TC (Figure 1(a)) began from Oliktok point at its southern end, where it also overlapped with a portion of the enclosing restricted airspace R-2204, extended to 2,000 ft. in height from the surface, and was 1 nautical mile (NM) wide by 17 NM long. In particular, it extended 16 NM into U.S. airspace, due north from Oliktok point, and an additional 1 NM into international airspace (Figure 1(b)). The restricted airspace R-2204, together with the TC formed the *operational volume* of airspace for the mission.



(a) 2-D airspace sectional showing the transit corridor extending due north from Oliktok point



(b) 3-D visualization of the transit corridor overlapping the restricted airspace R-2204 at the southern end, and extending beyond U.S. airspace in the northern end

Figure 1. MIZOPEX Transit Corridor

[2] At the time, the terminology used referred to a *sense-and-avoid* (SAA) capability, which has been updated in this paper to the currently used terminology, i.e., detect-and-avoid (DAA).

[3] The SIERRA UAS undertook two sorties per day, whereas the ScanEagle UAS undertook one sortie per day for the duration of the MIZOPEX mission.

The unmanned aircraft (UA) were to be launched after establishing that the airspace was all clear, i.e., no incursions were predicted to occur into the airspace covered by GBDAA surveillance, during UA transit. Only one UA was permitted to enter the TC at any give time. During outbound flight, the UAs were tasked to enter the TC at Oliktok point, and proceed to international airspace at their respective cruise speeds. Cruising altitude was weather dependent for VFR flight, and ranged between 1,000 ft. and 1,500 ft. mean sea level (MSL). After exiting the TC into international airspace, the UAs operated as State Aircraft under *due regard* rules for MIZOPEX data collection. Re-entry into the TC from the north and the subsequent inbound transit back to base also required a clear airspace, again established through surveillance using the GBDAA equipment (described next). After entry into the TC, were an incursion to be detected and predicted to intercept the TC, avoidance procedures (described subsequently in this paper) appropriate to the UA location (relative to the mid-point of the transit corridor) and heading (inbound or outbound), would be initiated to minimize the chance of a mid-air collision (MAC). Contingency procedures (also described subsequently) were also defined for off-nominal situations, such as loss of communication links, or loss of the GBDAA capability.

MIZOPEX UAS operations were divided into nine phases: (1) preflight; (2) taxi and takeoff; (3) outbound entry into the TC; (4) transit through the TC; (5) outbound exit from the TC; (6) MIZOPEX measurement; (7) inbound entry into the TC; (8) inbound exit from the TC and landing; and (9) postflight. Of these, eight phases (i.e., phases 1 – 5, and 7 – 9) concerned operations in the NAS and were in the scope of the required GBDAA safety case, whereas the safety of flight during phase 6 in international airspace was addressed through range safety, and was out of scope for this work.

GBDAA System Description

To ensure the safety of flight during transit, the GBDAA equipment, which was collocated with the UAS ground control stations (GCSs), consisted of an intermediate range, pulse Doppler, air-defense radar and a customized, dual-redundant, radar display system (RDS). The radar, operating in the X-band, utilized pencil-beam antenna technology over a detection range of approximately 40.5 NM, an elevation range from -10º to +55º, to provide 360º azimuth coverage at a scan rate of 2s, over a three dimensional hemispheric surveillance volume. The RDS processed the positional data of airborne targets obtained from the radar, to provide the UA pilots with situational and navigational awareness.

The radar system (i.e., the radar and the RDS) was the primary means to (a) monitor the airspace including and surrounding the TC up to an altitude of 10,000 ft. MSL, and (b) detect potentially conflicting air traffic (i.e., manned, general aviation aircraft, or rotorcraft) sufficiently early, so as to determine how operations would commence, continue, and/or to inform decisions to initiate any avoidance maneuvers. Avoidance was to be accomplished through procedural means, which included tasking the UAs to change altitude, heading and speed, as appropriate. In turn, the latter relied on the airworthiness of the UAS, in particular reliable communication links between the GCS and the air-vehicles.

The GBDAA crew consisted of the Pilots-in-command (PICs) and the GCS Operators (GSCOs) for the two UAs, a NASA Range Safety Officer, a NASA trained RDS operator, and a contracted radar operator. The primary responsibility for monitoring lay with the RDS operator, with defined procedures to call out airspace status to the PICs and GCSOs. However, owing to collocation of the RDS and the GCSs, the PICs and the GCSOs also had the ability to see the radar display independently, for decision support. The radar operator was responsible for addressing any technical issues with the radar.

Requirements for Operational Approval

As per our understanding of the national policy for UAS operational approval, N8900.207 [1], the (implicit) requirements for obtaining regulatory approval were concerned with providing assurance that (a) the GBDAA system would allow UAS operations in the TC to be conducted at an acceptable level of safety; and, additionally, (b) that this AMOC would maintain the existing level of safety for the other stakeholders of the affected airspace.

Formally, the FAA requires that such assurance be supplied in the form of an acceptable system safety case, which outlines the associated hazards, risks, and risk mitigations. The national policy also specifies the minimum information comprising a safety case, and Appendix D of the policy document de-

scribes (at a high-level) the expected content, together with the FAA's preferred format. In brief, the safety case expected is a type of safety risk management document that should address: details about the system and environment, including existing procedures, operations, roles and responsibilities; the intended changes to the system, e.g., the introduction of new equipment; hazard and risk analyses (of the proposed changes) including details of the assumptions made, the criteria for categorizing hazards, the levels of initial and residual risk, hazard mitigations, risk treatment and hazard tracking; details of safety risk management planning; UAS capabilities and airworthiness information, etc. For more details on FAA safety case requirements, we refer the reader to [1]. In addition to submitting a safety case, the national policy contains other explicit requirements, e.g., concerning the COA process, UAS pilot qualifications, etc., which were also to be fulfilled for operational approval. The scope of our work was, primarily, the safety case for the GBDAA capability.

Safety Assurance Approach

As mentioned in the previous section, the main goal of the safety case, as per our interpretation of the national policy, was to show that UAS operations in the TC using GBDAA would pose an acceptable level of safety risk for the airspace under consideration. This required us to demonstrate that:

- During nominal operations, the radar system could reliably, and sufficiently early, detect/track intruder aircraft predicted to intercept the TC, so as to permit the PICs or GCSOs to initiate the appropriate procedures and/or avoidance maneuvers to ensure the continued safety of flight during transit; additionally, under the assumptions made and given the performance limits of the UAS, avoidance maneuvers would reliably avoid the intruder aircraft; and
- During both nominal and off-nominal operations, there were procedures and controls established to acceptably mitigate newly identified hazards to flight safety, i.e., any hazards introduced by the GBDAA capability were also appropriately mitigated.

In short, the safety case relied upon assuring that GBDAA performed reliably, and that the hazards posed by using GBDAA instead of VOs, as well as any contingencies, were appropriately managed.

Nominal Operations

For assuring the safety of nominal operations, in particular UA flight through the TC, we considered the radar detection performance and defined avoidance measures for each phase of operations, based upon the position and heading of the UA relative to the mid-point of the transit corridor, and the position, heading, and speed of the intruder aircraft.

Detection Requirements

The requirement for acceptable radar detection performance was that radar coverage would be sufficient and that the radar could, indeed, detect and track intruder aircraft in its surveillance volume. For UA transit operations, the air traffic to be detected (and, potentially, to be avoided) was primarily non-cooperative general aviation (GA) aircraft, rotorcraft, and tethered balloons.[4] Cooperative air traffic, i.e., those aircraft equipped with a Mode 3/C transponder, was considered not to be a threat to safe operations, since such traffic is required to be provided with separation services from Air Traffic Control (ATC). Additionally, air traffic detected above 10,000 ft. MSL were not considered to pose a safety risk, due to the relatively low altitude at which UAs would transit, i.e., no higher than the ceiling of the TC (2,000 ft. MSL).

Sufficiency of Radar Surveillance Coverage

The criterion for sufficiency of radar coverage was that the radar should able to detect an intruder aircraft traveling at a worst-case maximum speed such that, after detection, the time taken to complete an avoidance maneuver would be less than the time the intruder aircraft would take to intercept the TC. Our safety case showed that this criterion was acceptably met, by reasoning about the amount of overlap between the radar surveillance volume, and the *threat volumes* of the airspace surrounding the TC, as follows.

---

[4] There are 6 private/public use airports and heliports in the vicinity of Oliktok Airfield, which were considered to be the source of the majority of the air traffic expected to be encountered during MIZOPEX UAS operations. Additionally, the U.S. Department of Energy's Atmospheric Radiation Measurement Climate Research Facility operates tethered balloons at Oliktok airfield for scientific measurements.

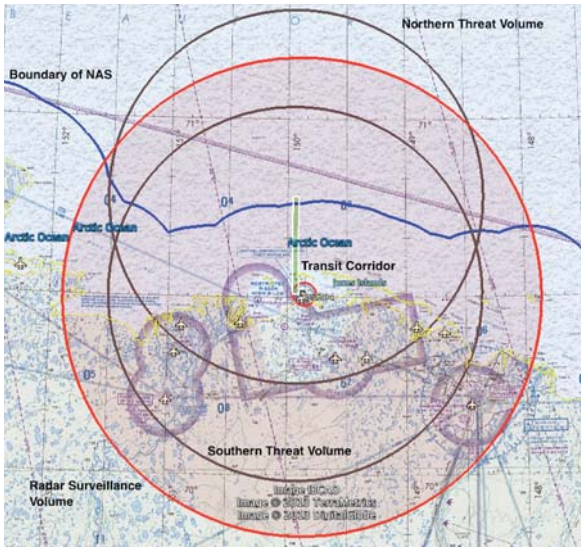


Figure 2. Surveillance and Threat Volumes

The SIERRA and the ScanEagle UAs had a cruise speed of 57 NMPH and 48 NMPH respectively, with each having a maximum speed of 80 NMPH. Accounting for headwind speeds up to 10 NMPH the maximum speed that each UA could attain is 70 NMPH. In cruise, the ScanEagle would take about 1200 s to transit the length of the TC in the NAS, i.e., 16 NM, inbound or outbound. Thus, in cruise, the UAs were at most 600 s from exiting the transit corridor either by continuing if past the halfway point, or turning back if before the halfway point.

However, at a speed of 70 NMPH, the flight time from the midpoint of the TC to either end is 411.4 s. An additional 30 s was added to this time if the UA was required to make a 180º turn to return to base. Thus, an avoidance maneuver which would require the UA either to dash to one end of the TC from the mid-point, or make a turn and return to base, to avoid a potential MAC would require 441.4 s. This calculation assumed that the UAs would not be climbing or descending in the TC.

We defined the threat volumes to transit operations as two overlapping cylinders centered at either end of the TC (Figure 2), with a height of 10,000 ft. MSL. The airspace was a combination of class G and E within the threat volumes. The radii of the cylinders were determined from the time it would take an intruder aircraft to intercept the UA at either end of the transit corridor, if it was detected when the UA is near the midpoint of the corridor, i.e., 8 NM from either end.

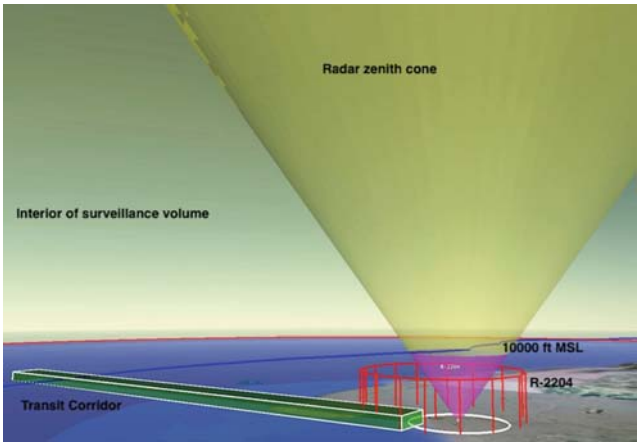


Figure 3. Radar Coverage of TC and Zenith Cone

Although most non-cooperative aircraft in the airspace surrounding the TC were likely to have speeds less than 180 NMPH, we assumed a worst-case maximum ground speed of 250 NMPH to provide a safety margin. Based on our analysis of local air traffic, we considered this to be a reasonable assumption. At this speed, the distance travelled by an intruder aircraft in 441.4 s is 30.65 NM. We added an additional 1 NM as a margin of safety resulting in threat airspace volume radii of 31.65 NM.

Since the radar was to be installed at the ground level, in its normal surveillance mode of 0º to +22º elevation range, the radar had sufficient coverage to monitor the entire TC into international airspace and could detect aircraft operating up through Class A airspace at its maximum detection range (Figure 3). To detect aircraft at altitudes up to 10,000 ft. MSL near the southern entrance of the TC, i.e., at Oliktok airfield, the radar was tilted to its maximum elevation of +55º.

Note that radar surveillance completely covered the southern threat volume but did not fully cover the northern threat volume (see Figure 2). Additionally, the surveillance volume excluded the radar zenith cone (a.k.a. the radar *cone of silence*) directly above the radar, as shown in Figure 3. In this figure, the altitude of the restricted airspace R-2204 is 7,000 ft. MSL, and the intersection of 10,000 ft. altitude with the zenith cone results in a cone radius of 1.51 NM (shown as the circle projected to the surface). Thus, aircraft in these exclusion zones would not be detected in time to safely execute an avoidance maneuver. These conditions were identified and addressed in our hazard analysis (described subsequently in this section).

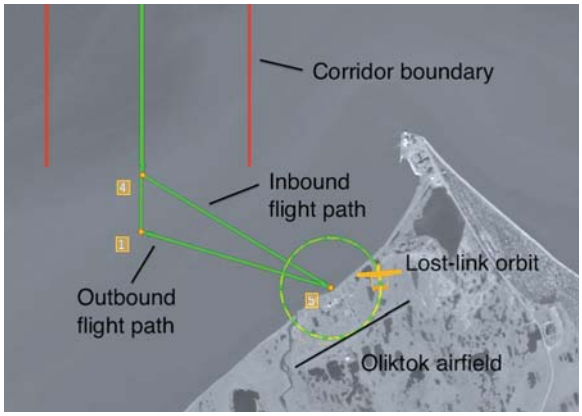


Figure 4. Waypoints at Oliktok

Verification of Radar Coverage

Flight tests were conducted at different altitudes in the range from 1,000 – 10,000 ft. MSL, with a manned GA aircraft, representative of the traffic expected to be encountered, to (i) characterize and confirm the detection/tracking range, (ii) verify that the radar actually performed according to our analysis of airspace coverage and manufacturer specifications, and (iii) identify shadows caused by any structural or geographic obstacles near the radar installation site.

Consequent to these tests, the radar was located at the west end of the runway at Oliktok airfield, far enough away from the location of the hangar, to reduce the blockage of the radar signal. Additionally, flight testing established that in operation, the radar surveillance range was 33 NM (instead of the specified range of 40.5 NM), and that the strongest detection/tracking performance was shown for those targets which had a velocity component towards or away from the radar (perpendicular to the antenna). Since the radar surveillance volume was still large enough to cover the threat volumes, and because flight paths determined to represent a threat to transit operations would have a velocity component that the radar could detect/track, the radar was considered to provide sufficient detection coverage.

Avoidance Procedures

Due to the reduction in the surveillance range, as the flight tests showed, there was a shorter timeframe for the RDS operator to decide if a detected intruder aircraft would, in fact, intercept the TC. Therefore, the approach towards avoidance was primarily to restrict transit operations to the specific time windows when (i) no incursions into the threat volumes were detected after monitoring the airspace continually for a specified duration, and (ii) incursions were predicted to be unlikely to occur subsequently. After confirming that the airspace is clear, the UAs were launched and tasked for waypoint-based flight where, effectively, after takeoff, the UA would proceed to pre-determined waypoints en-route.

Altogether, 5 waypoints were defined: 3 at the southern end of the TC (Figure 4), and 2 at the northern end (not shown in the paper). Two of those waypoints were also the *loiter/lost-link orbit* locations (e.g., waypoint 5 in Figure 4), i.e., locations where the UAs would standby in a holding pattern until either the GCSOs could clear their flight to the next waypoint, or the autopilot determined a lost-link event. The loiter/lost-link orbit altitude was set to 2,000 ft. MSL in the north, and at 400 ft. MSL in the south. For MIZOPEX UAS operations, waypoints could be thought of as locations at which UAs transitioned from one flight phase to the next, and where a transition required an "all-clear" airspace status.

For example, as shown in Figure 4, to transition from the loiter orbit at waypoint 5 (e.g., in the *taxi and takeoff* flight phase[5]) to enter the TC at waypoint 1 (i.e., the *outbound entry into the TC* phase), the RDS operator was required to call out an "all-clear" status for the airspace, after which the GCSO would direct the UA to ascend from 400 ft. MSL to the cruising altitude. On the other hand, were an incursion to be detected, the UA would continue in its holding pattern at waypoint 5 until such time as the RDS operator determined that the airspace was clear of hazards. The operating (and avoidance) procedures were identical for inbound entry into the TC, i.e., from the northern end, with the exception of the loiter waypoint and altitude (waypoint 2, at 2,000 ft. MSL), and entry into the TC requiring a descent to the cruising altitude.

Upon detecting an intruder aircraft during the transit phase, the avoidance procedures to be invoked were dependent upon the position and heading of the UA relative to the mid-point of the TC, the speed, altitude and heading of the intruder aircraft, and the predicted location of intercept with the TC. In particular:

[5] Waypoint numbers reflected identifiers rather than an order of locations during operations. Thus, waypoint 5, rather than waypoint 1, was the first waypoint after takeoff.

(i) *UA heading outbound*: If the predicted location of the intercept with the TC was in the forward path of the UA, then irrespective of whether the UA was in the northern or southern half of the TC, the avoidance maneuver was to turn around and return to waypoint 5, then enter the loiter orbit (see Figure 4), and await an all-clear airspace to resume outbound transit. If the predicted location of the intercept was behind the UA, when the UA was in either half of the TC, then no avoidance was required and the UA would continue outbound.

(ii) *UA in the southern half of the TC, heading inbound*: If the predicted location of intercept with the TC was in the forward path of the UA, active avoidance was required, where the UA would continue inbound, but by descending in altitude and at its maximum ground speed. Although this maneuver presented a comparatively high residual risk, the rationale for its use is as follows: it was adjudged to be unlikely that the intruder aircraft would also descend. Additionally, the airspace analysis included safety margins in the estimation of the threat volume radius ensuring that, at the time the intruder aircraft intercepts the TC, there would continue be lateral separation of at least 1 NM. For a predicted intercept with the TC at a location behind the UA, avoidance required accelerating to the maximum ground speed while continuing inbound.

(iii) *UA in the northern half of the TC heading inbound*: If the intruder aircraft was predicted to intercept the TC in the forward path of the UA, the UA would be tasked to turn around, return to the northern loiter/lost-link orbit (waypoint 2), and await an all-clear airspace to resume inbound transit. For an intercept with the TC predicted to occur behind the UA, the UA would continue inbound at its maximum ground speed.

The preceding discussion addressed the mitigation of existing hazards, i.e., those that would have been mitigated using see-and-avoid. Next, we describe the identification and mitigation of hazards introduced by using GBDAA in lieu of VOs.

GBDAA Hazard Analysis

Process

We performed a hazard analysis using the applicable processes and methods (as recommended in [1], [2], [3]), to provide assurance that the hazards introduced by the GBDAA capability were adequately identified and addressed through the appropriate mitigation/contingency measures. In particular, we used a combination of Preliminary Hazard Analysis (PHA) [4], and Functional Hazard Analysis (FHA) [5] for hazard identification and to analyze safety risk. PHA was used to give a broad coverage of the potential hazards that may be encountered during (nominal and off-nominal) operations, while FHA is similar in format and intent, but orthogonal in scope. To focus the analysis, we also formulated a concept of *GBDAA hazard*, adapting the definition of hazard from [2].

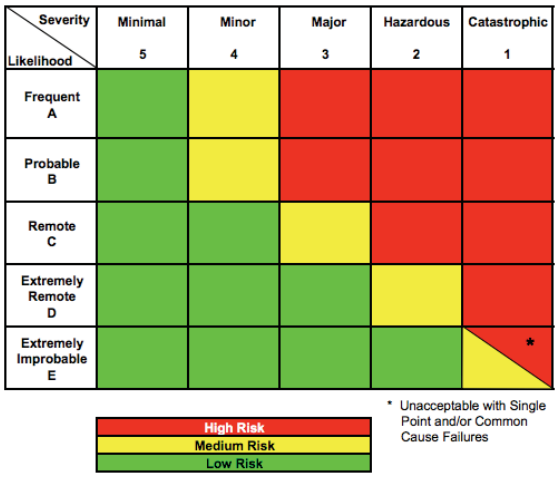


Figure 5. Risk Matrix for Hazard Analysis

Specifically, a GBDAA hazard is a (known or unknown) state of the GBDAA system, (which may or may not be a deviation from its required operational state), one or more (known or unknown, credible, and worst-case) environmental conditions, and/or their combinations, which has the potential to result in an undesired event. The concept acknowledges that there may be unknown hazardous states or conditions, and the challenge of safety analysis is to identify all the relevant hazards (i.e., as many as reasonably possible), assess their risk, and reduce their risk to acceptable levels through hazard mitigation.

For the purposes of hazard identification the GBDAA system included the radar, the RDS, the GCS and control links, the supporting power systems, as well as the crew operations. The environment was considered to be as everything that was not a part of the GBDAA system, i.e., the weather conditions, the operating location, and the air traffic in the operational airspace volume, etc. To identify and formulate hazards, we systematically traversed the GBDAA functions, and brainstormed about the environmental conditions.

Table 1. Identified MIZOPEX GBDAA Hazards

Hazard	Risk Level	
	Initial	Residual
Loss of the radar to detect and track air traffic in the surveillance volume	High	High / Medium
Loss of the radar display system (RDS) to display air-traffic or correctly interpret radar signals	High	Medium
Loss of command and control links	High	Medium
A non-cooperative aircraft on an intercept course at high-speed, originating from the threat volume not covered by the surveillance volume, when the UA is in the transit corridor	High	Medium
Intruder aircraft in the radar zenith cone prior to UAS operations	High	Medium

Risk analysis involved the assignment of a likelihood and severity to the identified hazards in order to provide a *risk level*, i.e., a measure of the risk used to determine its acceptability. Figure 5 shows a classic risk matrix used to allocate the risk level of a hazard. In our case, *High Risk* hazards were unacceptable, whereas *Medium* or *Low Risk* hazards were acceptable. Also, as seen in Figure 5, likelihood ranged from *Frequent* to *Extremely Improbable*, whereas severity ranged from *Minimal* to *Catastrophic*.

The lack of operational data for GBDAA use in UAS operations in the specific airspace under consideration, necessitated the use of qualitative definitions for likelihood and severity, which we adopted from [2]. The main stakeholder that we considered for elaborating each severity class was the airspace user, since the focus was non-cooperative air traffic, with the operations occurring in Class G and E airspaces. For the same reason, ATC was not considered as a stakeholder in characterizing the severity classes.

Assumptions

A number of assumptions were made during hazard identification, some of which were previously made for the safety assurance of nominal operations, while some others were made to eliminate specific scenarios that could be normally hazardous but judged not to apply to the MIZOPEX operations.

For example, cooperative air traffic and traffic in Class A airspace, was assumed to be managed and separated by ATC, and therefore not to pose a threat to operations. The worst-case ground speed for the air traffic expected to be encountered (i.e., non cooperative) was assumed to be 250 NMPH. Cargo aircraft flights occurred between the airports near Oliktok, that were capable of flight at 250 NMPH (or greater) in Class E airspace, but were assumed to be unlikely to venture towards the TC based upon the history of their air routes taken. Additionally, it was assumed that intruder aircraft would maintain relatively consistent ground speeds with no significant increases that could decrease their time of intercepting the transit corridor. Hazards arising from human factors were not considered in the analysis as they were assumed to have been addressed through NASA crew training requirements. Additionally, UAS airworthiness and the related hazards were not considered in the analysis, as they were assumed to have been addressed separately as part of the NASA processes for airworthiness, flight safety and flight readiness reviews [6].

Finally, flight hazards to UAS operations in international airspace were not considered in the analysis. As mentioned earlier, after exiting the TC into international airspace, the UAs operated as State aircraft under due regard rules. Safety of these operations, together with the effects to the people on the ground, UAS crew and the UAS system were considered as part of Range Safety Analysis as per NASA procedural requirements [7].

Identified Hazards

Based upon the concept of GBDAA hazard, as given earlier, we identified 5 classes of a combination of system states and environmental conditions that were hazardous (Table 1). Considered in conjunction with the eight operational phases and the UA heading (inbound/outbound), and eliminating those scenarios that were either precluded through nominal operations or determined not to pose risks, there were 26 known (new) scenarios that had the potential to result in a MAC. Of these, two were worst-case scenarios:

A. Loss of the radar system when the UA is heading inbound in the TC; and
B. Detection of an intruder aircraft (traveling at 250 NMPH, and predicted to intercept the TC) at the surveillance volume boundary that intersects with the northern threat volume when the UA is in the TC.

The determination of initial risk levels for loss of the radar and RDS was based upon their specifications of mean times between failure (MTBF), whereas the likelihood of loss of the command and control links was estimated based upon previous operations of the SIERRA UAS. Air traffic density and other air traffic data, such as the average monthly traffic for the airspace surrounding Oliktok airfield was largely unavailable except for the data from the U.S. Department of Transportation's Bureau of Transport Statistics. While this was insufficient to obtain an accurate estimate of the likelihood of encountering air-traffic during transit operations, it was sufficient to provide an initial likelihood for the purposes of allocating a risk level to the relevant hazards.

Hazard Mitigation

Mitigations for the identified GBDAA hazards were largely procedural, and were implemented by the GBDAA crew, except for those initiated by the UA autopilot. Additional mitigation measures were also used that involved (a) the use of redundancy in some system components, (b) coordination and communication with the relevant airspace stakeholders/users to improve deconfliction in the airspace during transit operations, and (c) equipage onboard the UAs to enable their detection and tracking by ATC and by other aircraft. Altogether, the mitigation measures provided defense in depth.

Procedures

A variety of procedures were in place to assure that nominal operations would ensure safety during transit. For example, a daily flight "Go/No-Go" decision would be made after reviewing the weather and confirming that requirements for flight in VFR were met. In particular, operations in the TC required a visibility of approximately 2–3 NM and a 1,000 ft. ceiling. Additionally, it was also decided to conduct flight operations in visual meteorological conditions (VMC), to give manned GA aircraft the opportunity to see-and-avoid the UAs[6]. Similarly, all operations would only commence after verifying that the radar system is fully functional and operating normally. As mentioned earlier, only one UA would be cleared to fly through the TC at any time. Procedural mitigations for the identified hazards, and off-nominal operational scenarios were integrated into the operating procedures, and the application of such procedural mitigations depended upon the phase of flight in which hazards occurred.

For example, loss of the radar/RDS at any stage of outbound flight, excepting after exiting the TC into international airspace would either preclude UA operations (in the *pre-flight*, and *taxi and takeoff* phases), or would require the UA to turn around and return to base (in those phases where the UA was already airborne). If radar coverage were to be lost during inbound flight—one of the two worst-case scenarios—the mitigation measure was to continue inbound at the commanded altitude and speed. Additionally, loss of radar surveillance required notifying the ATC, so that it could track the UA and alert any surrounding traffic. Loss of the radar system when the UAs were in international airspace was not a concern as radar tracking would not be required at that point.

Upon loss of the command and control links the hazard mitigation procedure in all flight phases was for the UA to (a) proceed to the loiter/lost-link waypoint, and orbit in a holding pattern until links were re-established; and additionally, (b) notify the ATC at Deadhorse and the air route traffic control center (ARTCC) at Anchorage of the lost link, and declare an emergency. For all flight phases, excepting for operations in international airspace, the loiter/lost-link orbit/waypoint was at the southern end of the TC (waypoint 5, as shown in Figure 4). If command and control links were lost during MIZOPEX measurement operations (in international airspace), the UA would proceed to the loiter/lost-link waypoint at the northern end of the TC (waypoint 2), and orbit in a holding pattern until either (a) links were re-established, or (b) an on-board mission timer, typically set to 5 hours, expired. Upon occurrence of the latter, the UA would enter the TC, descend to its cruising altitude and proceed inbound to the southern

[6] In the remote scenario that such an aircraft was not detected by the radar and all other mitigations also failed.

loiter orbit (waypoint 5), and then autoland. The autopilot onboard the UAs were programmed to automatically trigger these procedures upon loss of all control links.

With multiple UAs in international airspace, there was a possibility that both could lose link and return to the loiter/lost-link orbit at the north end of the TC simultaneously. To preclude a MAC between the two UAs in this scenario, the flight paths of each UA was preset to be separated by 1 NM horizontally and by 500 ft. vertically. Furthermore, the mission timers for each UA were staggered by more than 20 minutes to prevent both UAs from entering the TC simultaneously, upon expiry of the mission timers.

An identified worst-case scenario was when the UA was in the TC (heading northbound or southbound), and a non-cooperative intruder aircraft was to be detected, traveling at high speed, predicted to intercept the TC, and originating from a location in the northern threat volume not covered by radar surveillance, i.e., any location between NNE and NNW of the TC. The mitigation for this contingency required (a) increasing UA ground speed to its maximum speed and a dash to the nearest end of the TC, (b) active avoidance, including changes in heading, and altitude if there was a chance for the UA to be overtaken by the intruder. We note, however, that this worst case scenario was determined to be highly unlikely to occur, since the intruder would have to originate from the portion of the threat volume in international airspace and outside the air-defense identification zone (ADIZ). As a matter of procedure, the threat aircraft would have been required to seek prior permission from ATC to enter U.S. airspace, at which point they would be alerted of MIZOPEX UAS operations and directed to alter their course.

To mitigate the hazard posed by an aircraft in the zenith cone of the radar, VOs were to be utilized at Oliktok airfield prior to takeoff, to verify that no aircraft are operating in the zenith cone.

Redundancy and Equipage

In addition to procedural mitigations, redundancy in some GBDAA components was utilized to minimize the likelihood of component loss, and thereby manage some of the causes of hazard occurrence. For instance, each UA had (triple) redundant command and control links: a 2.4 GHz radio control (RC) link or a backup 900 MHz link could be used to operate the aircraft from the GCS, or using a manual, hand-held controller. Over the horizon control, (in international airspace), was through an Iridium satellite communication (SATCOM) link, which served as a backup to the RC links. Additionally, the RDS and the power supply (to the radar, RDS and the GCS) were dually redundant to reduce the chance of loss of these components. To improve the ability of the ATC to detect the UAs and track them in flight, each UA was equipped with a Mode C altitude-encoding transponder. Communications with ATC involved the use of a mobile phone.

Coordination and Communication

Communication and coordination with airspace stakeholders is a key tool to avoid hazards arising from airspace conflicts and in planning for a deconflicted airspace [8]. As part of the safety assurance process, the MIZOPEX mission manager developed formal relationships with local airspace stakeholders, such as the ATC authority at Deadhorse, personnel from airports/heliports near Oliktok, and others[7], early during the planning phase of the mission, to inform them of the intended operations. During the mission, the mission manager also held daily preflight briefings on the operations, and communicated status updates. Communication with the stakeholders also involved being updated of their intended changes in air traffic. A flight coordination procedures checklist was created specifying the required information coordination actions and the crew members to whom the responsibilities were allocated.

After finalizing the flight plans, stakeholders were notified of the area of operations by radio, e-mail, and notices to airmen/mariners (NOTAMs and NOTMARs). After UA entry into the TC, the PICs were in contact with the ATC as required. Additionally, periodic transmissions were made on the common traffic advisory frequency (CTAF) to alert nearby aircraft of the location and altitude of the UAs during transit flights. Furthermore, airports near Oliktok that were equipped with automatic terminal information service (ATIS) capabilities included a warning about UAS operations in the TC and in the restricted airspace R-2204. Finally, an altitude reservation (ALTRV) was coordinated with Anchorage ARTCC, to inform any Instrument Flight Rules (IFR) traffic of the location of UAS operations in the TC.

[7] Such as air-taxis, and Oil & Gas companies that have airborne operations in the area.

Discussion

Safety Case Structure

The safety case that we submitted to the FAA (as part of the COA process, and to meet the requirements for obtaining operational approval) was a report in the preferred format specified by the FAA (see Appendix D in [1], for details). Abstractly, the structure of this report could be thought of as comprising the required *core content* and a *safety management plan*.

Core Content

The core content of the safety case contained the analysis described in the previous section. In summary, we provided a detailed description of: (i) the existing system; (ii) the proposed changes to the existing system, i.e., the introduction of the GBDAA capability, the concept of operations, analysis of the airspace, crew responsibilities, and procedures; (iii) the analysis and results of hazard identification, and risk assessment, along with the mitigations identified; and (iv) the assumptions made.

Safety Management Plan

The MIZOPEX safety management plan included activities to monitor and track hazards (as well as air traffic). The data to be gathered included data obtained from the flight tests verifying radar coverage, data obtained about air traffic (such as traffic volume, patterns, and transponder codes) in and around the TC during the course of the MIZOPEX mission. The intent of these activities was to validate/update the assumptions made and the understanding of the threat and surveillance volumes, to detect new hazards that may not have been considered in the initial safety analysis, and to update the safety case to be consistent with actual operations and observations. Additionally, the safety management plan included an identification of the affected stakeholders and organizations, and the steps taken to communicate information about the UAS operations in the TC, so as to coordinate operations.

An Alternative Model for Safety Cases

Some of the authors of this paper (Denney and Pai) have previously worked on the creation of safety cases in the context of UAS safety assurance [9], [10], [11]. The notion of a safety case used in their work is compatible with the FAA preferences for the content and format of a safety case, but organizes the information in the form of *structured arguments*. This alternative notion of safety case has been put forth in other safety-critical domains [12] (where they are referred to, more generally, as *assurance cases*), as well as in aviation [13], and may utilize graphical notations such as the Goal Structuring Notation (GSN) [14].

Augmenting Safety Cases with Argumentation

An *argument* is a connected series of propositions used in support of the truth of an overall proposition. The latter is usually referred to as a *claim*[8], whereas the former represents a *chain of reasoning* connecting the claim and the evidence. Applied to the domain of safety assurance, a safety argument comprises explicit safety claims, a chain of reasoning that develops those claims and the items of evidence to substantiate the claims made. In addition, a safety argument can typically contain the ways in which the stated safety goals will be developed and substantiated, the relevant context and assumptions, along with the justifications for their use.

Safety cases can, then, be thought of as structured arguments that assimilate the body of evidence and the reasoning required to conclude[9] that a system will be safe for a defined application and operating environment. Indeed, argument-based safety cases are intended to be explicit about safety goals, evidence and the underlying reasoning. In contrast, we believe the focus of the safety case format in [1] is on presenting a compendium of evidence, and the reasoning that ties the evidence presented to the safety claims made may be (often) implicit. We emphasize that argumentation would augment and enhance, rather than replace, the present format preferred by the regulator. Additionally, we note that argumentation is suitable for the core content, and that safety cases represented as arguments would continue to require (and supply) a safety management plan to update the argument and keep it consistent with the system as actually operated.

Graphical notations such as GSN (Figure 6) can be used to create *argument structures*, i.e., diagrams that explicitly document the elements and structure of an argument [14]. These largely serve as an index into the assimilated safety information with the latter being linked from the graphical elements.

---

[8] Reflecting that which we would like to conclude.
[9] Or convince and communicate to the relevant stakeholders.

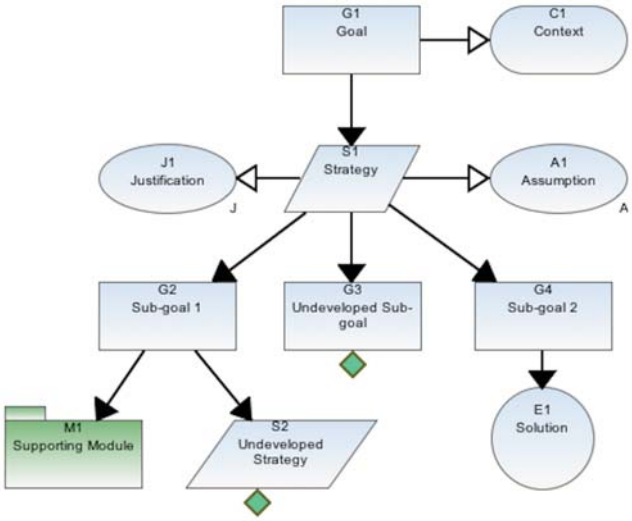


Figure 6. GSN for Safety Argumentation

In brief, as shown in Figure 6, GSN provides a graphical syntax of nodes and links to represent the main elements of a (safety) argument. The nodes are: *goals* (containing safety claims), *strategies* (describing how claims are developed), *contexts, assumptions*, *justifications*, and *evidence* (with their intuitive meanings). Nodes are linked through either a support relationship (the filled arrowhead link, meaning "*is supported by*") or a contextual relationship (the hollow arrowhead link, meaning "*in context of*"). GSN also provides additional node annotations to indicate incompleteness (a diamond annotation, meaning "to be developed"), structuring mechanisms such as *modules*, which may contain other argument structures, and abstraction mechanisms such as patterns [15]. For more details on the notation, refer to [14].

Application to MIZOPEX GBDAA

Now, we briefly illustrate the use of structured argumentation by applying it to the GBDAA safety case. Figure 7 lays out a high-level argument structure for GBDAA safety assurance. Here, we stress that the safety case is not just the argument structure but also (not shown in the figure) all the relevant information linked from the nodes, and the safety management plan.

The initial *root* claim (i.e., the goal node G1) is identical to the stated goal of our submitted safety case, i.e., that GBDAA for MIZOPEX (UAS) operations provides an acceptable level of safety during transit through the NAS. The claim is made in the context of the applicable regulations, the GBDAA system, the ConOps, the airspace for operations, and the characterization of the TC to clarify precisely what the claim means, and the conditions under which the claim should be interpreted. To show that this claim can be accepted, we can apply: (i) an argument of hazard mitigation, and (ii) an argument of compliance to the applicable regulations (represented using the strategy nodes S2 and S4, respectively). The former is further developed in a module addressing the compliance of DAA with the regulations (module node DAA), whereas the latter results in a sub-claim about the mitigation of all the identified hazards (goal node G3). In turn, this sub-claim is developed in separate modules, each addressing a class of hazards (i.e., the module nodes HazH1H2Mit, HazH3Mit, and HazH4Mit, respectively, in Figure 7).

It is easy to see that this argument structure is similar to the structure that we used in this paper in discussing our approach to GBDAA safety assurance. We believe that such graphical argument structures would be intuitively easier to comprehend and, possibly, also to evaluate (although more research is required to substantiate this belief). More recently, we have supplied GSN arguments with formal semantics [15], making them more amenable to automated analysis, such as querying [16], verification, transformation, and report generation. We also believe that these capabilities will present substantial advantages during the creation, management and evaluation of safety cases.

Conclusion

One of the challenges in our efforts to create an acceptable safety case has been the nascent nature of the guidelines in the national policy for UAS operational approval as well as the absence of successful precedents (for civil UAS operations). There have been other contemporaneous examples of the use of radar as an AMOC in UAS operations primarily driven by the U.S. Military. Our work was guided by a draft concept of employment (CONEMP) for ground-based sense and avoid (GBSAA) operations being conducted by the U.S. Air Force at Cannon Air Force Base [17]. Later (after approval of our safety case), we became aware that the U.S. Navy was developing a safety case for a GBSAA concept for use at the Cherry Point Marine Corps Air Station concurrently with our efforts [18]. To the best of our knowledge, however, our safety case was the first successful example of civil UAS operations with GBDAA in the NAS, authorized by the FAA.

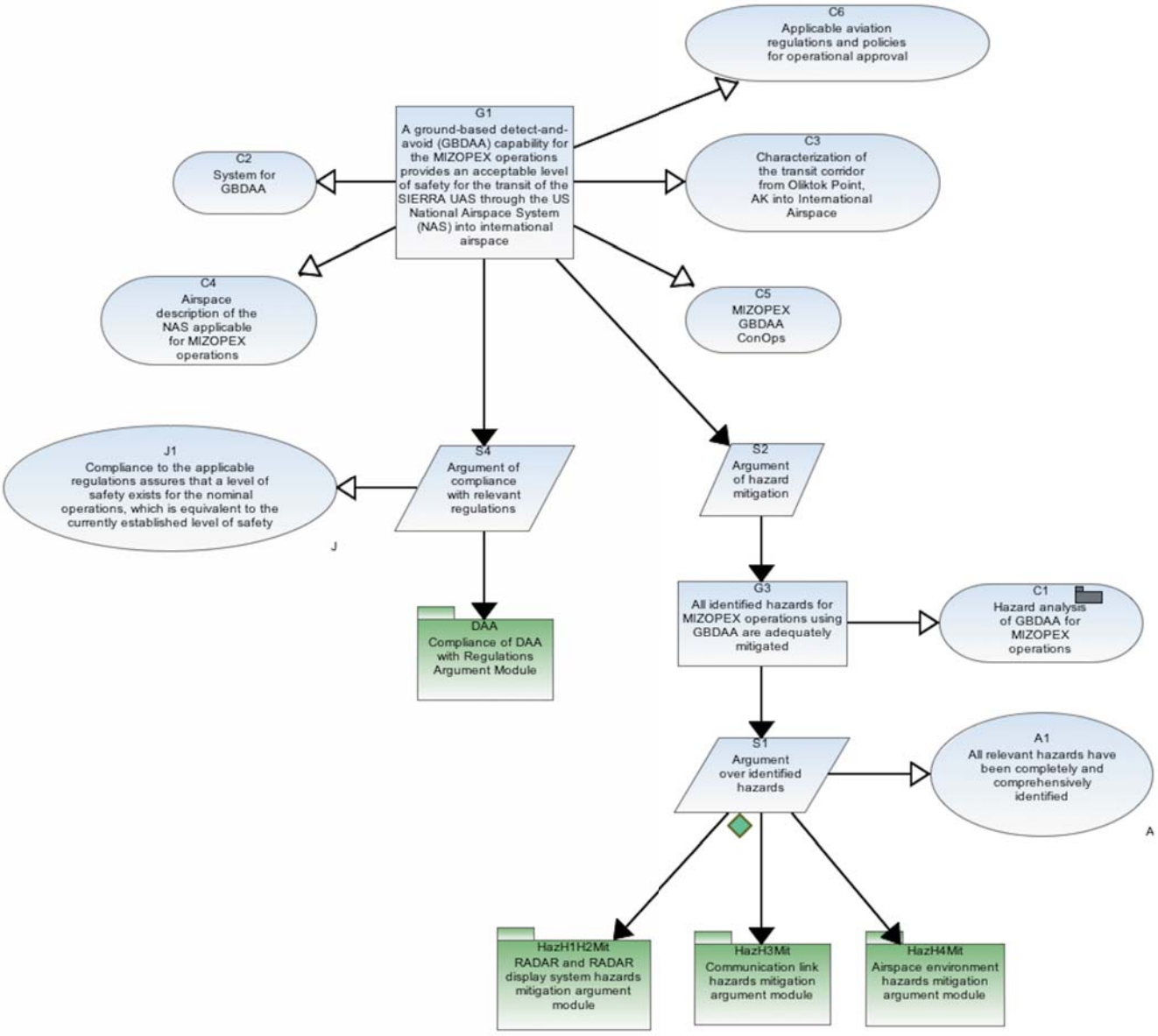


Figure 7. High-level GSN Argument (GBDAA)

References

[1] FAA Unmanned Aircraft Program Office, 2013, Unmanned Aircraft Systems (UAS) Operational Approval, National Policy N8900.207, US Department of Transportation.

[2] FAA Air Traffic Organization, 2008, Safety Management System Manual, Ver. 2.1, FAA.

[3] Dezfuli, H., A. Benjamin, C. Everett, C. Smith, M. Stamatelatos, and R. Youngblood, Nov. 2011, System Safety Handbook, Vol. 1, System Safety Framework and Concepts for Implementation, Ver. 1, NASA/SP-2010-580, NASA.

[4] U.S. Department of Defense, May 2012, Standard Practice, System Safety, MIL-STD-882E.

[5] S-18 Committee, Dec. 1996, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, ARP 4761, Society of Automotive Engineers (SAE), Inc.

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

[7] Office of Safety and Mission Assurance, Sep. 2010, Range Flight Safety Program, NPR 8715.5A, NASA.

[8] Interagency Aviation Management Council, Jul. 2003, Interagency Airspace Coordination Guide, Office of Aircraft Services, U.S. Department of the Interior, and the Forest Service, U.S. Department of Agriculture.

[9] Denney, E., G. Pai, and J. Pohl, Jul. 2012, Heterogeneous Aviation Safety Cases: Integrating the Formal and the Non-formal, 17th IEEE International Conference on the Engineering of Complex Computer Systems (ICECCS 2012), IEEE, pp. 199 – 208.

[10] Denney, E., G. Pai, and I. Habli, Jun. 2012, Perspectives on Software Safety Case Development for Unmanned Aircraft, 42nd Annual IEEE/IFIP International Conference on Dependable System and Networks (DSN 2012), IEEE, pp. 1 – 8.

[11] Denney, E., and G. Pai, Sep. 2014, Automating the Assembly of Aviation Safety Cases, IEEE Transactions on Reliability, IEEE. (*To appear*)

[12] U.S. Food and Drug Administration, Apr. 2010, Guidance for Industry and FDA Staff – Total Product Life Cycle: Infusion Pump – Premarket Notification [510(k)] Submissions.

[13] European Organisation for the Safety of Air Navigation, Nov. 2006, Safety Case Development Manual, ed. 2.2, DAP/SSH/091, EUROCONTROL.

[14] Goal Structuring Notation Working Group, Nov. 2011, GSN Community Standard ver. 1. [Online]: http://www.goalstructuringnotation.info/

[15] Denney, E., and G. Pai, Sep. 2013, A Formal Basis for Safety Case Patterns, 32nd International Conference on Computer Safety, Reliability and Security (SAFECOMP 2013), LNCS 8153, pp. 21 – 32.

[16] Denney, E., D. Naylor, and G. Pai, Sep. 2014, Querying Safety Cases, 33rd International Conference on Computer Safety, Reliability and Security (SAFECOMP 2014), LNCS 8666, pp. 294 – 309. (*To appear*)

[17] Jella, C., Mar. 2013, Draft Concept of Employment (CONEMP) Ground Based Sense and Avoid Operations at Cannon AFB, NM, Ver. 3.2, U.S. Department of Defense.

[18] Spriesterbach, T. P., K. A. Bruns, L. I. Baron, and J.E. Sohlke, 2013, 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, pp. 572 – 583.

Acknowledgements

This work was supported in part by the UAS Integration in the NAS Project under the Integrated Systems Research Program of the NASA Aeronautics Research Mission Directorate (ARMD), in part by the NASA Science Mission Directorate (SMD) Earth Science Division and Airborne Science Program, as well as the NOAA UAS Program. We also thank Francis Enomoto, who contributed to the airspace analysis.

Disclaimer

The opinions expressed in this paper and any errors are those of the authors, and do not reflect the views of SGT Inc., NASA, or the U.S. Government.

Email Addresses

Ewen Denney: ewen.denney@nasa.gov

Ganesh Pai: ganesh.pai@nasa.gov

Randall Berthold: randall.w.berthold@nasa.gov

Matthew Fladeland: matthew.m.fladeland@nasa.gov

Bruce Storms: bruce.l.storms@nasa.gov

Mark Sumich: mark.sumich@nasa.gov