MITRE #: MP060219 Lincoln Laboratory #: 42PM ATC-329

Collision Avoidance for Unmanned Aircraft: Proving the Safety Case

October 2006

Andrew Zeitlin and Andrew Lacher
The MITRE Corporation

Sponsor: Federal Aviation Administration
Contract No.: DTFA01-01-C-00001
Dept. No.: F082 Project No.: 0206FB11-04

James Kuchar and Ann Drumm
MIT Lincoln Laboratory

Sponsor: Federal Aviation Administration
Air Force Contract FA8721-05-C-0002

The MITRE Corporation
Center for Advanced Aviation Systems Development
McLean, Virginia

Lincoln Laboratory
Massachusetts Institute of Technology
Lexington, Massachusetts

1 Introduction and Purpose

Applications for Unmanned Aircraft Systems (UAS) abound from military and homeland security to commercial services. The ability to integrate unmanned and manned aircraft into the same civil airspace is a critical capability that will enable growth in the industry, expansion of applications, and greater utility for UAS operators.

Collision avoidance is emerging as a key enabler to UAS civil airspace access as well an important capability for the integration of manned and unmanned missions in military theaters of operation. UAS collision avoidance capabilities must be interoperable and compatible with existing collision avoidance and separation assurance capabilities including the Traffic Alert and Collision Avoidance System (TCAS) and the requirement for a pilot to see and avoid other aircraft consistent with the right of way rules[1].

The operational and technical challenges of UAS collision avoidance are further complicated by the wide variety of unmanned aircraft, their associated missions, and their ground control capabilities. Numerous technology solutions for collision avoidance are being explored in the community, including research sponsored by the National Aeronautics and Space Administration, the United States Air Force, The Defense Advanced Research Project Agency, and others. The Federal Aviation Administration (FAA) has requested that RTCA, Inc. develop Minimum Aviation System Performance Standards (MASPS) for UAS collision avoidance, referred to as UAS Sense and Avoid.

While the technology research activities are important to the development of these standards, analysis will be required to ensure that the technical solutions provide a satisfactory level of safety. The intent of this paper is to present one perspective on the system safety studies necessary for the community to reach consensus on the appropriate standards -- a necessary step so that a collision avoidance capability for unmanned aircraft can be certified by the FAA.

The MITRE Corporation and Lincoln Laboratory have collaborated on this paper because we believe that it is important to articulate the system safety studies needed. Our two organizations bring a wealth of knowledge and experience associated with the development and implementation of TCAS. We were directly involved and/or closely associated with a significant portion of the system safety analysis that supported RTCA, FAA, Eurocontrol, and International Civil Aviation Organization (ICAO) decisions related to TCAS[2] standards and certification.

Section 2 of this paper describes the safety analysis process. It gives a high level description of each step in the process, with emphasis on issues unique to UAS. Sections 3 through 5 describe selected areas in more detail. Section 3 addresses sensors and algorithms, which are specific aspects of the Concept of Operations. Section 4 describes encounter model development. Sections 5 describes the combination of fault tree

---

[1] Code of Federal Regulations - Title 14 Aeronautics and Space; Part 91 General operating and flight rules; Section 113 Right-of-way rules: Except water operations.

[2] International TCAS is referred to as Airborne Collision Avoidance System (ACAS)

analysis and dynamic simulation to assess UAS collision avoidance performance. Section 6 gives a summary.

2 The Safety Analysis Process

Drawing on TCAS experience, a basic five-step process for analyzing UAS collision avoidance performance has been developed in ICAO and other literature [1-4]. The analysis is based on a comprehensive, statistically-valid set of data describing collision avoidance performance across a wide range of encounter situations. The five steps have been used extensively throughout TCAS development and most recently to assess the performance of TCAS on Global Hawk [5,6]. The five steps are:

1. Develop a <u>Concept of Operations</u> (CONOPS) to provide information, for example, on UAS flight characteristics, the environment in which the UAS will operate, responsibilities of the ground pilot, and communication protocols.

2. Develop an <u>Encounter Model</u> to enumerate the encounter geometries that are expected to occur and their relative frequencies of occurrence.

3. Develop a <u>Fault Tree Analysis</u> to identify all events that could lead to a failure in the end-to-end collision avoidance process and to estimate either absolute or relative system risk.

4. Compute <u>Collision Risk</u> using large numbers of simulated encounters.

5. Conduct <u>Special Analyses</u> to examine, for example, UAS performance in encounters with TCAS-equipped intruders, and encounters with high vertical rates, late maneuvers, or command reversals.

2.1 Concept of Operations

The diversity of UAS and their missions involve a wide-range of system operating concepts. Current unmanned aircraft range in size from small hand launch vehicles weighing only ounces to the Global Hawk weighing over 26,000 lbs with a wing span similar to a Boeing 737. Unmanned aircraft cruise speed, climb rate, and operating altitudes are similarly varied. In addition, some unmanned aircraft operate semi-autonomously with minimal control from the ground, while other aircraft are tele-operated with stick and rudder commands being issued by a ground operator. The link between the ground control station (GCS) and the unmanned aircraft also varies, with some capable of only line-of-sight communications while others have the capability of communicating beyond line-of-sight via satellite or other relay mechanisms.

Algorithms (most likely functioning autonomously) will be needed to ensure that the unmanned aircraft avoids other traffic while also avoiding fixed obstructions such as terrain, obstacles, and political features. The aircraft's navigation function might also be leveraged to avoid fixed obstructions.

System operating concepts must be specified before a safety analysis can accurately determine the likelihood of failures, or the effect of proposed mitigations.

2.2 Encounter Model

Existing collision avoidance safety analyses make use of airspace collision encounter models. These data sets provide representative samples of observed traffic, with statistics mapping the traffic into pre-defined geometric classes of close encounters. Without such a representative traffic sample, it is impossible to determine which types and what frequencies of traffic encounters would occur.

The existing encounter models contain only traffic equipped with an ATC transponder. Onboard pilots are assumed to be able to visually detect and resolve encounters with non-transponding aircraft. The UAS collision avoidance system must be able to sense both transponding and non-transponding traffic. The airspace encounter model is complicated by the need to obtain this additional data, especially since the altitude of this type of traffic may be difficult to estimate. Moreover, since UAS mission locations are so varied, a single model for the national airspace may not be satisfactory. Sub-airspace models may be needed, such as for dense traffic areas; terminal areas including classes B, C and D; remote areas; and high- and low-altitude areas.

If UAS were routinely operated in civil airspace today, the construction of the model including associated encounter geometries and statistical distributions could proceed as with the TCAS modeling approach: by collecting contemporary data and processing it. Instead, the model and subsequent analysis are viewed as a precursor to UAS integrated flight. Since the UAS cannot be observed in the airspace, the only alternative is to postulate likely mission types and locations, and to overlay these among observed manned traffic before processing encounter pairs.

2.3 Fault Tree Analysis, or Hazard Analysis

To prove a safety case, it is necessary to first identify all of the credible hazards falling within the scope of the collision avoidance function. Here hazard is defined as any failure in procedures, communications, equipment, etc., that can lead to potential operational consequences, i.e., in this case, a mid-air collision. The list of hazards depends upon the planned mission of the UAS and upon the system operating concepts.

A fault tree is used to model system failures or hazards. A fault tree analysis is a top-down process which logically derives the failures that could produce the top-level event (collision). The analysis works down through the failures, mitigations, and avoidances involved, and estimates the probability of each. The overall probability of the top-level event must be shown to meet the criticality requirements of the collision avoidance function.

A number of changes to the standard, i.e., manned, collision avoidance fault tree are necessary for UAS. These include the addition of command and control system failure probabilities, failure modes of the sense-and-avoid sensors and processors, and autonomous-response system reliabilities. Examples of standard failures that would be included would be tracker failures (e.g., missing altitude report or loss of intruder track); system component failures (e.g., loss of a traffic display); and improper pilot responses. The incorporation of the fault tree analysis into the safety simulation process is detailed in Section 5, Fault Tree Analysis and Dynamic Simulation.

2.4 Collision Risk

There has been much discussion regarding the concept of "equivalent level of safety" and whether UAS can be shown to achieve a collision avoidance performance equivalent to that of manned aircraft. To do so would require developing a baseline of existing piloted-aircraft see-and-avoid performance, a task that is very difficult. Estimating human visual acquisition is possible, but estimating human reaction timing and maneuver selection, aggressiveness, and ability to adapt to a changing situation cannot be done accurately. Manned aircraft collision risk also varies greatly depending on the types of missions being flown and the airspace being used (e.g., operations in the traffic pattern at an uncontrolled field have significantly higher collision risk than operations in Class A airspace). For this reason, a pure equivalent level of safety analysis is not likely to be feasible.

Two other safety estimation methods are more likely to apply to UAS. First, an <u>absolute risk calculation</u> would evaluate the probabilities of each identified hazard to estimate overall collision risk and compare this risk against a target level of safety. This method is the conventional way of proving the safety of new systems or new procedures. It is consistent with the FAA Safety Management System and the ICAO Airspace Planning Manual [7].

Alternatively, a relative risk calculation would examine the reduction in collision risk attained by equipping a UAS with a collision avoidance system (CAS). This approach was used in certifying TCAS. For TCAS, collision risk is expressed in terms of Near Mid-Air Collision (NMAC) events, defined to occur when separation between two aircraft is less than 100 ft vertically and 500 ft horizontally. The probability of Near Mid-Air Collision, P(NMAC), is estimated with and without a CAS over a wide range of potential encounter situations. The ratio of P(NMAC) with a CAS to P(NMAC) without a CAS is commonly referred to as the risk ratio. A risk ratio less than one indicates a risk reduction; a risk ratio greater than one indicates an increase in risk. A sufficiently small risk ratio might allow a UAS system to be certified even without estimating the overall collision risk or comparing it against estimates of manned aircraft collision risk, but it leaves uncertainty as to the absolute risk that is being proposed, and to the incremental risk incurred by other users of the airspace who might encounter the UAS. Overall, the risk ratio methodology is not considered to be a suitable, comprehensive approach for this analysis because UAS usage involves not only a collision mitigation technology but also introduces an entirely new class of operations.

2.5 Special Analyses

In addition to an estimate of aggregate performance in an airspace, specific problem situations also need to be identified and judged as to their criticality and likelihood. This would include UAS performance in encounters with TCAS-equipped intruders, and encounters involving high vertical rates, late maneuvers, and command reversals. In past TCAS safety studies, specific "stress testing" of the CAS logic was undertaken. This should also be a part of the UAS performance assessment.

It should be noted that other issues may play a significant role in the acceptance of a CAS, including expected nuisance alarm rates or impact on air traffic management. Also, extensive flight testing is required, primarily to support modeling communications latency and availability, sensor performance, automation, human interaction with collision avoidance advisories, and flight characteristics.

3 Sensors and Algorithms

The UAS collision avoidance system, or Sense & Avoid system, needs to operate for hazards within a defined volume of airspace surrounding the UAS. This can be defined in a convenient coordinate system, such as azimuth and elevation angles and range; or range, bearing and relative altitude. The system needs to detect a hazard, determine if a maneuver is required, communicate and execute that maneuver in time to achieve a specified miss distance. These elements represent segments of system design that must be studied together, with their performance allocated between the elements so as to achieve statistically safe operation in the planned operating environment. Therefore, the surveillance system and the threat avoidance algorithms need to be designed cooperatively.

The variety of UAS types is accompanied by a variety of methods under development for sensing non-transponding traffic. Each of these has its own strengths and limitations. The surveillance system, whether consisting of a single sensor or a combination of several, must be characterized in a form suitable for analysis.

Various sensors provide different forms of relative and absolute position data with varying degrees of precision and accuracy. As examples, Mode C and Mode S transponders (queried by TCAS) provide relative range, bearing, and the altitude reported by the traffic. ADS-B provides absolute latitude, longitude, and altitude (usually this is the same altitude reported via the altitude encoded transponder used by TCAS). Some other sensor types may provide azimuth and elevation estimates, possibly with range.

Moreover, the accuracies of measurement dimensions can be quite different among sensors, or even for the same sensor in different conditions. The update rate also is an important element of surveillance system performance. The sensor system field of regard is a design element that could be addressed either by choice of sensor, or by creating an array of sensors with the aim of covering adjacent parts so as to fill the desired volume.

Whenever multiple sensors or sensor types are deployed on a UAS, their data must be selected or combined in some fashion. This process is termed data fusion. Its basic metrics are the probability of detecting desired targets in a timely manner, and the probability of false detections. These metrics are of interest both in the aggregate and for specific cases, so that any geometry that is not well served can be known and understood. The algorithms for data fusion can be complex, as they need to cover every combination of detection and non-detection among the installed sensors, in the presence of multiple targets as well as single or no targets. A substantial effort may be required to collect enough data to fully characterize the sensor combinations. Existing data may be limited, for example including only certain geometries, or certain visibility conditions. Determining the accuracy of fused sensor data and its appropriate use in collision avoidance will be a critical safety analysis task.

The algorithms for Sense & Avoid need to be matched to various characteristics of the sensor system. These include the type and form of data, the data rate, and the accuracy and distribution of data across realistic operating conditions. For example, TCAS provides very accurate range data, but low-accuracy bearing data. ADS-B can provide high-accuracy lateral information, but accuracy and integrity can vary from one target aircraft to another. The TCAS algorithms were tuned to match the performance of its sensor, and would not operate well with ADS-B based sensor data without adjustments, even beyond the conversion of the data into a TCAS-like coordinate system. Sense & Avoid algorithms also need to produce outputs that match the system concept in terms of either alerting a pilot of a need to avoid a hazard, or making a direct input to the UAS flight control system.

When a human pilot is in the loop, the outputs to the pilot need to be informative and useful in terms of timing and update rate. The algorithms need to anticipate a realistic delay before a pilot responds to a maneuver advisory, and they need to be matched to the realistic maneuver capabilities of the UAS. They should not excessively change the maneuver advice, for fear of degrading pilot confidence in the Sense & Avoid system. For the purposes of a safety analysis and certification, assumptions need to be made, with proper validation, concerning the probabilities and timing of pilot response to the advisories. If pilot response subsequently should degrade, the original analysis would become inaccurate.

4 Encounter Model Development

A key component of the safety study process is development of a valid model of the types of close encounters that may occur. Such a model is used to generate millions of representative traffic encounter situations for the inner-loop simulation. The existing models were derived from air traffic radar data so that the encounters have similar characteristics and frequencies as actual encounters occurring in the airspace, but they only encompass transponding aircraft. Models for the United States airspace and an ICAO model are respectively documented in [8] and [9]; several models representing European airspace also exist [10-11].

Each encounter model specifies parameter distributions from which selections are made in every fast-time simulation run. These parameters include the horizontal and vertical miss distance, speeds, headings, and bearing at closest point of approach, plus maneuvers that may take place before the closest point of approach (e.g., a level-off maneuver or turn).

The encounter modeling process begins by collecting thousands of hours of actual air traffic radar data. Radar data was used in the past, but other surveillance technologies could replace radar. Close encounters between aircraft (where a CAS may become involved) are extracted from the radar data using a set of filters. The characteristics of each filtered close encounter are then used to build a statistical distribution describing the likelihoods of various parameter values. When generating encounter scenarios, a separate set of software randomly selects parameter values from these distributions, computes the initial conditions for the simulation, and stores the results in an input file.

Existing encounter models represent situations that have been observed to occur between conventional air traffic. Due to differences in their flight profiles, UAS may experience a different mix of encounter types than conventional aircraft. Global Hawk, for example, flies at a relatively low airspeed and high climb rate, resulting in a steeper climb profile than typically occurs with transport aircraft. It is also more likely that Global Hawk would be climbing or descending through the populated flight levels than cruising there. As a result, encounters with Global Hawk may involve a larger proportion of climbing or descending situations than is reflected in the existing encounter models. A larger proportion of climbing or descending situations impacts the effectiveness of a CAS in resolving these situations, ultimately impacting the risk ratio. There currently are no radar data that include UAS close-encounter events, nor is there an existing non-transponding airspace model. Modeling considerations for UAS are further discussed in [12].

5 Fault Tree Analysis and Dynamic Simulation

It is difficult to assess safety using a single approach. Instead, several tools must be brought to bear, each focusing on a different aspect of the overall system. In particular, the collision risk problem can be partitioned into two regimes: an outer-loop regime that encompasses system failures and events that lead up to a critical close encounter event, and an inner-loop regime that covers the details of what occurs second-by-second in a dynamic analysis of an encounter given the conditions that were defined in the outer-loop regime.

A fault tree is used [13] to model the outer-loop system failures or events that in turn define the environment for a fast-time Monte Carlo inner-loop simulation of a close encounter. For example, the probability that an encounter would occur in visual conditions can be estimated in the fault tree, and P(NMAC) for that type of encounter can be computed in a detailed fast-time simulation. Results are then combined in the fault tree with corresponding performance data and probabilities for other conditions including intruder aircraft equipage, system failures, etc., leading to a global estimate of system safety. Sensitivity studies can then be performed by modifying event probabilities in the fault tree and observing their impact on overall risk without requiring new fast-time simulations.

5.1 Outer Loop: Fault Tree Analysis

The outer-loop analysis is used to define what conditions apply, and how likely those conditions are, in a critical close encounter event. Outer-loop conditions include:

- Altitude of the close encounter
- Characteristics and criticality of the close encounter
- Environmental conditions
- Intruder aircraft equipage (e.g., transponder, TCAS, 100 ft or 25 ft altimeter encoding)
- Sensor or tracker failures
- System component failure
- Command and control system status
- Pilot response to collision avoidance advisories (e.g., standard, fast, slow, or no response)
- Probability of an effect of visual acquisition from the manned aircraft
- Air Traffic Control involvement in resolving the close encounter

The main benefit of fault tree analysis is that it facilitates sensitivity studies. For example, the probability of instrument meteorological conditions can be changed and a new value of P(NMAC) computed without rerunning any simulations. Other studies could include changes in the intruder equipage mix, hardware reliability, or sensor characteristics.

5.2 Inner Loop: Dynamic Simulation

The inner-loop dynamic simulation takes the status of system components and the environment and computes P(NMAC) over a representative range of encounter situations. Because of the need to examine many different situations, it is necessary to run a fast-time Monte Carlo simulation. Four models are essential to this simulation:

1) The encounter model as described above. The characteristics of an encounter directly affect CAS performance – some encounters can be more easily resolved than others.

Thus, it is important to have an accurate model of the types and frequencies of encounter situations so that risk ratios are realistic.

2) CAS sensor characteristics. The capacity to directly measure certain states (e.g., range, azimuth, altitude) affects the ability of a CAS to generate an accurate estimate of miss distance or time to impact. Sensor noise and background clutter in electro-optical systems affect the quality of collision avoidance decisions and false alarm rates.

3) CAS decision thresholds and logic. The sophistication of the algorithms and sensitivity of decision thresholds impact the timing of advisories and the maneuvers that will be used to resolve a close encounter, ultimately affecting the achieved vertical and lateral separation. Interactions between UAS CAS and manned aircraft that have TCAS will be important to explore.

4) Pilot and vehicle response. Once a CAS advisory has been generated, communication and control latencies, coupled with pilot response time (if a human pilot is in the loop) and vehicle control system latency and dynamics, affect when and how the aircraft maneuvers to avoid a collision. Specific data on link performance (dropout rates, latency histograms) would be needed to evaluate expected response characteristics in a human-in-the-loop configuration. It must be stressed that each system configuration may require a different model to be evaluated, e.g., for pilot response, vehicle performance, and link delays.

The CAS sensors, algorithms, and pilot and/or vehicle response need to be modeled in a manner that is compatible with fast-time simulation. Fast-time simulation may be a challenge for some proposed CAS concepts that use video image processing, for example, because generating a simulated video image and running the processing algorithms may be computationally intensive. It may be necessary to develop approximate sensor models that can be used in fast time to estimate when traffic threats would be detected. These models could be based on flight test results that specify expected threat detection ranges, for instance, without running the actual image processing algorithms.

Electro-optical sensors are sensitive to environmental conditions, and any modeling and analysis of their performance needs to take this into account. This in turn requires understanding what types of environments the UAS may operate in, and how likely close encounters may be in those conditions. Accordingly, there is a need to develop a coupled airspace-environmental model. Such a model would provide estimates on the likelihood of an encounter occurring in a given weather condition, and the corresponding sensor performance (e.g., detection range, false alarm rate) in those conditions.

Millions of simulated encounters are generally required to both cover the large number of possible encounter situations that may occur and to generate enough data to ensure that the results are statistically significant.

Additionally, it will be necessary to examine the potential for multiple-aircraft encounters and their effect on safety. Prior TCAS studies, for example, broke multiple-aircraft encounters into two components: the likelihood of a multiple-aircraft encounter, and a study of the criticality of those encounters when they occur. Further examination of the traffic environment is required to estimate how often three or more aircraft may be involved in the vicinity of UAS operations. Simulation of UAS performance in multiple-aircraft situations is needed to ensure that safe resolutions take place and that these resolutions do not induce a chain effect of additional collision avoidance maneuvers in nearby aircraft.

6 Summary

This paper outlines the steps that build the safety case upon which the Sense & Avoid function would be approved. These steps are not insignificant, requiring a thorough concept of operations, new data and models, fault trees tailored for UAS, extensive simulation, and analysis of special cases. System trades may be required to achieve safety targets and other mission needs. The work should be coordinated with the various national and international organizations involved in UAS standards, regulatory, manufacturing, and technology efforts.

References

[1] ICAO, “ACAS Manual”, SCRSP/1-WP/53, Montréal, Canada, 2004.

[2] Kuchar, J., “Modifications to ACAS Safety Study Methods for Remotely Piloted Vehicles (RPVs)”, ICAO SCRSP WG A IP/A/7-281, May 2004.

[3] Kuchar, Andrews, Drumm, Hall, Heinz, Thompson, and Welch, “A Safety Analysis Process for the Traffic Alert and Collision Avoidance System (TCAS) and See-and-Avoid Systems on Remotely Piloted Vehicles”, AIAA 3rd Unmanned Unlimited Technical Conference, Chicago, IL, September 20-23, 2004.

[4] Drumm, Andrews, Hall, Heinz, Kuchar, Thompson, Welch, “Remotely Piloted Vehicles in Civil Airspace: Requirements and Analysis Methods for the Traffic Alert and Collision Avoidance System (TCAS) and See-and-Avoid Systems”, 23rd Digital Avionics Systems Conference, Salt Lake City, UT, October 24-28, 2004.

[5] Kuchar, J. “Safety Analysis Methodology for Unmanned Aerial Vehicle (UAV) Collision Avoidance Systems”, 6th USA / Europe Seminar on Air Traffic Management Research and Development, Baltimore, MD, June 27-30, 2005.

[6] Billingsley, T., “Safety Analysis of TCAS on Global Hawk Using Airspace Encounter Models”, Massachusetts Institute of Technology, June, 2006.

[7] ICAO, “Manual on Airspace Planning Methodology for the Determination of Separation Minima,” Doc 9689/AN-953, Montréal, Canada, 1998.

[8] McLaughlin, M., Safety Study of the Traffic Alert and Collision Avoidance System (TCAS II) – Final Version, MTR97W32, The MITRE Corporation, June, 1997.

[9] ICAO, “ICAO Standards and Recommended Practices – Annex 10, Volume IV, Surveillance, Radar and Collision Avoidance Systems”, Montréal, Canada, 1998.

[10] Miquel, T., & K. Rigotti, 2001, “European Encounter Model”, ACASA/WP1.1/186D, Eurocontrol, Brétigny, France.

[11] Raynaud, B. & Arino, T, “ACAS Safety Analysis post-RVSM Project, ASARP Project”, DSNA, QinetiQ, & Sofréavia, May, 2006.

[12] Zeitlin, A., and M. McLaughlin, “Modeling for UAS Collision Avoidance”, AUVSI Unmanned Systems North America, Orlando, August 2006.

[13] Lebron, J., et al., “System Safety of Minimum TCAS II”, MTR 83W241, The MITRE Corporation, December, 1983.