NASA/CR–20230013203

ATM-X Urban Air Mobility
Assistive Detect and Avoid for UAM Operations Safety Evaluation Metrics

Victor A. Carreño
Compass Engineering, San Juan, Puerto Rico

December 2023

NASA STI Program Report Series

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA scientific and technical information (STI) program plays a key part in helping NASA maintain this important role.

The NASA STI program operates under the auspices of the Agency Chief Information Officer. It collects, organizes, provides for archiving, and disseminates NASA's STI. The NASA STI program provides access to the NTRS Registered and its public interface, the NASA Technical Reports Server, thus providing one of the largest collections of aeronautical and space science STI in the world. Results are published in both non-NASA channels and by NASA in the NASA STI Report Series, which includes the following report types:

- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA Programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA counterpart of peer-reviewed formal professional papers but has less stringent limitations on manuscript length and extent of graphic presentations.

- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.

- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.

- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or co-sponsored by NASA.

- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.

- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services also include organizing and publishing research results, distributing specialized research announcements and feeds, providing information desk and personal search support, and enabling data exchange services.

For more information about the NASA STI program, see the following:

- Access the NASA STI program home page at http://www.sti.nasa.gov

- Help desk contact information:

https://www.sti.nasa.gov/sti-contact-form/ and select the "General" help request type.

NASA/CR–20230013203

ATM-X Urban Air Mobility
Assistive Detect and Avoid for UAM Operations Safety Evaluation Metrics

Victor A. Carreño
Compass Engineering, San Juan, Puerto Rico

National Aeronautics and
Space Administration

Langley Research Center
Hampton, VA 23681

December 2023

Acknowledgments

Prepared for Langley Research Center under Contract 80LARC17C0004.

Available from:

NASA STI Program / Mail Stop 148
NASA Langley Research Center
Hampton, VA 23681-2199
Fax: 757-864-6500

Abstract

This document satisfies ATM-X UAM Task UID 989 "Evaluation Report on Tactical Separation Provision Services with Advisory Detect and Avoid Safety Metrics". The first version of this document was delivered to the UAM team on October 3, 2022, for initial revision and comments. This current version incorporates all the comments received and is being delivered to the UAM subproject for a final revision before is submitted to satisfy the L1 milestone deliverable.

Table of Contents

Table of Figures

1 Purpose of this Document

This document explores the role that “assistive” Detect and Avoid (DAA) will play in the integration of piloted Urban Air Mobility operations in the NAS. DAA alerting and maneuver guidance in the cockpit will enhance the pilot’s traffic situational awareness and contribute to an overall system of hazards mitigation strategies to maintain safe and efficient aircraft operations. This document is not a safety assessment of an operational concept because there is not, yet an industry and government accepted Operational Services and Environment Definition (OSED) for Urban Air Mobility. This document explores safety metrics that will lead to operational and other requirements that will be necessary to meet required safety levels. Assumptions are made on the operations, the environment, the operators, the vehicles, and the equipment on-board the future vehicles. Probabilities used for the causes in the fault trees and probabilities used for the mitigations in the event trees are estimates based on current historical data, conditions, and assumptions. As the Urban Air Mobility concept of operations evolve, these probabilities and other factors will need to be updated accordingly.

2 Introduction

Aircraft operations in the National Airspace System (NAS) must meet a Risk Level as specified in the FAA ATO Safety Management System (SMS) manual [1]. When new operations are proposed in the NAS, approval of these operations require a safety process also defined in the SMS manual. This process generally involves the development of an Operational Services and Environment Definition (OSED), a review process, the formation of a safety panel, identification of hazards, analysis and assessment of hazards, identification and development of mitigations, development of monitoring procedures, and an approval process.

Detect and Avoid (DAA) is defined as “the capability of an unmanned aircraft to remain well clear from and avoid collisions with other airborne traffic” [3] and was developed to provide remote pilots of unmanned aircraft an alternative means of compliance with see and avoid (SAA) regulations. DAA systems use sensors such as radars, lidars, electro-optical cameras, Automatic Dependent Surveillance (ADS), among others, to determine the location and velocity vector of a traffic aircraft. Based on the projected trajectories of the aircraft, the DAA system determines if a conflict exists, and computes possible resolution maneuvers to prevent collisions.

Assistive DAA for piloted aircraft is intended to augment the pilot’s ability to “see and avoid” (SAA). As a safety enhancement, assistive DAA will likely depart from established industry standards (i.e., DO 365x) specifications and intended use. For example, Assistive DAA should be complementary to SAA and advisory rather than prescriptive. Alert and maneuver guidance structures may need to be simpler, well clear volumes may be smaller, and different maneuver guidance options may be needed for terminal area operations. Approval of assistive DAA capabilities for traditional piloted operations in the NAS may fall under the NORSEE (Non-Required Safety Enhancing Equipment) Circular guidelines, which describes a standardized approval process of NORSEE in general aviation (GA) and rotorcraft fleets [7].

Assistive DAA for UAM operations is intended to enhance collision avoidance safety over SAA alone in higher density UAM VFR operations and will need to be included in determining the calculated level of safety required for the operations. In this case, a NORSEE approval process may not suffice, and a full System Safety Assessment (SSA) process will be required. The SSA will need to examine the safety risk associated with the use of a DAA capability by an on-board pilot operating in VMC (Visual Meteorological Conditions) under VFR (Visual Flight Rules).

3 Safety of Operations

The United States Federal Aviation Administration has implemented a Safety Management System (SMS). The objective of the SMS is to provide safe and efficient airspace operations. The SMS manual [1] provide guidance in the implementation of the system. Per the SMS manual: “The SMS is a formalized and proactive approach to system safety.” “The Air Traffic Organization (ATO) SMS is an integrated collection of principles, policies, processes, procedures, and programs used to identify, analyze, assess, manage, and monitor safety risk in the provision of air traffic management and communication, navigation, and surveillance services.”

A fundamental part of the SMS process is “Identifying and Addressing System Vulnerabilities.” To that effect, the SMS establishes the concept of “Hazard Defenses.” Within this concept, there are the sub-concepts of “fault-tolerance,” “fail-safe,” and “error tolerance.” These concepts are rooted on the idea that humans will inevitably commit errors and systems will fail. When errors are committed and systems fail, the overall operations should be sufficiently robust as to not create unacceptable hazards and effects.

The following is an example of an airspace operation where three possible designs structures are used. The operation is a simple crossing of routes. There are two routes, alpha and beta which cross. Alpha route goes from south to north and bravo route goes from west to east, see Figure 1. Alpha route starts at waypoint TANGO and bravo route starts at waypoint RIVER.

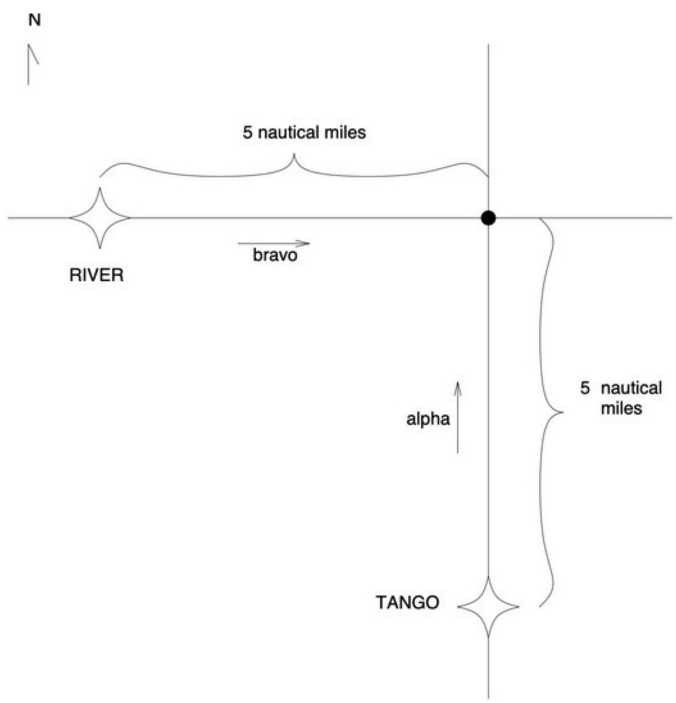

Figure 1: Operation example, crossing routes

3.1 Design Structure 1

In the first design structure, aircraft operating on alpha must be at 2,500 feet MSL (feet above Mean Sea Level). Aircraft operating on bravo must be at 2,000 feet MSL. In order to remain well clear, flight crews operating on these routes must be familiar with the altitude restrictions, have a properly functioning altimeter calibrated to the prevailing barometric pressure, and maintain the required altitude. When a conflict develops because flight crews deviate from the altitude restriction, the flight crews will rely on SAA and assistive DAA to remain well clear.

3.2 Design Structure 2

In the second design structure, both routes are at the same altitude of 2,000 feet MSL. There is a timing scheme such that aircraft are de-conflicted before entering the routes at waypoints. There are altitude and speed restrictions on the routes. Aircraft cannot be faster than 150 knots or slower than 80 knots. When an aircraft enters alpha at waypoint TANGO, another aircraft cannot enter bravo at RIVER for the next 150 seconds. This timing, when there is no wind, will allow one aircraft to pass in-front of the other by one nautical mile in the worst case. In the presence of wind, an additional buffer must be put in place so as to not decrease the distance at crossing. These operations will require that there is a scheduling system that can communicate time entry restrictions to the aircraft, that the scheduling system has an accurate reading of wind speed and direction, that the flight crews are familiar with the operational procedure, that they adhere to the timing restrictions, that the aircraft have a properly functioning speed indicator, that the flight crew maintain the speed restrictions, and that the flight crew do not deviate from the route. When the timing scheme fails to maintain conflict free operations, the flight crews will rely on SAA and assistive DAA to remain well clear.

3.3 Design Structure 3

In the third design structure, both routes are at the same altitude of 2,000 feet MSL. Aircraft rely on SAA and assistive DAA to remain well clear of each other. Aircraft enter the routes without any synchronization and if a conflict is detected, they maneuver on the horizontal domain to remain well clear. These operations require visual scanning for traffic aircraft, ADS-B (Automatic Dependent Surveillance-Broadcast) transmitter and receiver (ADS-B out and ADS-B in or another method of detection such as on-board radar or lidar) a Detect and Avoid system, a properly functioning altimeter encoder, internal or external GPS receiver for ADS-B vector data, the flight crew correctly following traffic advisories from the DAA system, and sufficient airspace to the right and the left of the route to be able to maneuver horizontally.

These three design structures have different levels of fault-tolerance, fail-safe, and error tolerance. The design structures go from the most robust to the least robust. The first design structure is the most robust because a conflict will only exist when one or more flight crews are unable to maintain the altitude restrictions. The DAA system will be a mitigation to possible pilot deviations.

In the second design structure, the operation depends on a scheduler, the performance of the aircraft, wind, and other factors to have a conflict free operation. In general, it will be more difficult to adhere to timing restrictions than to altitude restrictions. The DAA system will be a mitigation to the inability of an aircraft to meet the time crossing restrictions.

In the third design structure, conflicts will be a nominal operation and the number of conflict per flight-hour will be expected to be higher than in design structures 1 and 2. SAA and DAA will be the mechanism to remain well clear.

3.4 Identifying Causes, Conditions, and Effects

For a given Operational Services and Environment Definition (OSED) which includes the concept of operation, airspace density, design structure, etc. the number of conflicts per flight-hour could be estimated using a fault tree. The fault tree is a collection of operational errors, design errors, system failures, and abnormal events. They are combined in a tree using logic gates. Figure 2 is an example of a fault tree. It is important to note that depending on the concept of operation and the airspace design structure, there could be conflicts without the presence of errors, failures, and/or abnormal events. A conflict could be a nominal operational condition. This is the case for the Design Structure 3 in sub-section 3.3.

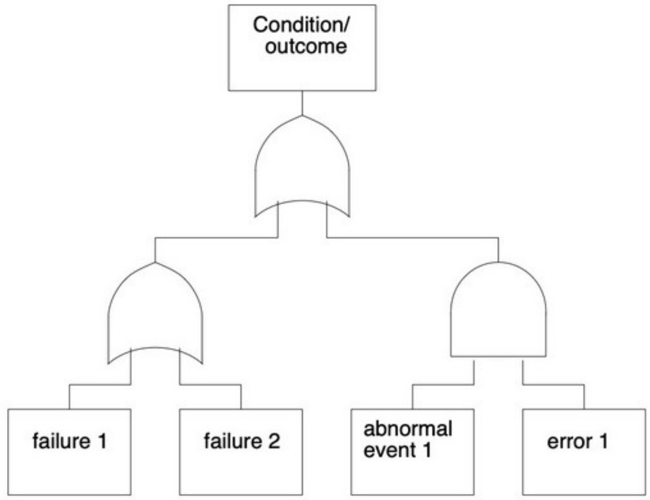

Figure 2: Fault tree generic example

In this generic example, there are AND gates and OR gates that lead to the condition/outcome. In the fault tree, the OR gate means that either event could lead to the condition/outcome. For example, failure 1 or failure 2 will lead to the condition/outcome. An AND gate means that both events must be present simultaneously for the condition/outcome to occur such as in abnormal event 1 and error 1.

The rate of traffic conflicts per flight-hour for a given operation, airspace, and traffic density will depend on the design structure as illustrated in the design structure examples 1 to 3. The requirements placed on DAA deconfliction will depend on the rate of traffic conflicts per flight-hour.

The design of the airspace and procedures not only affect the rate of conflicts but also the type and geometry of the potential conflict. For example, in terminal area, airspace generally consists of arrival flows and departure flows. Aircraft arrive in a sequence and depart in a sequence. This arrangement minimizes the possibility of aircraft having a head-on or crossing encounter. As a result of the established flows, when there is a breakdown in strategic deconfliction or airspace procedures, the DAA deconfliction will rarely have to deal with head-on or crossing encounters which are the most difficult to resolve due to the fast closure rates and in the case of head-on, the smaller visual area presented to the flight crews.

Similarly, in en-route airspace, airspace designs and procedures aim to reduce the frequency of head-on and crossing encounters. An example of a procedure to minimize head-on encounters is the requirement that VFR (Visual Flight Rules) aircraft flying more than 3,000 feet above the surface (and below 18,000 MSL (Mean Sea Level)) operate at a designated altitude (14 CFR 91.159). For an aircraft on a magnetic course of zero through 179 degrees, at any odd thousand-foot MSL plus 500 (3,500, 5,500, 7,500...). For an aircraft on a magnetic course of 180 through 359 degrees, at any even thousand-foot MSL plus 500 (4,500, 6,500, 8,500...).

A condition in an operational environment could be identified as a hazard "...if this condition leads to injury, illness, or death to people; damage to or loss of a system, equipment, or property; or damage to the environment." If a condition/hazard exists, the effects could be estimated using an event tree. The event tree is a probabilistic estimation of possible effects. Figure 3 shows an example in which a 6 faced die will be rolled and the effect/outcome will be a number from 1 to 6.

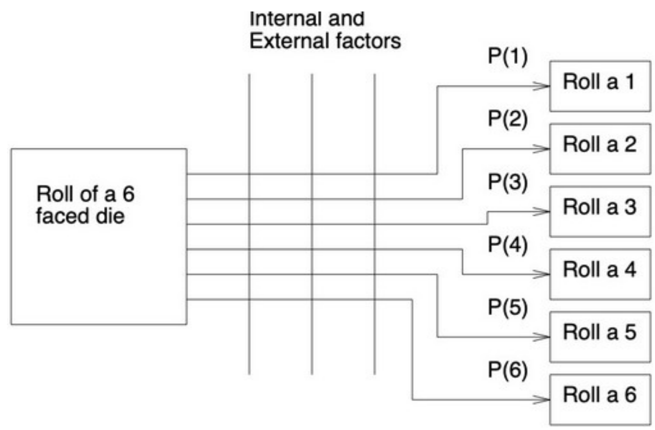

Figure 3: Event tree example

The branches from the left box to the right boxes represent the probability that the condition will lead to the right box effect/outcome. The lines crossing from top to bottom are internal and external factors that can affect the probabilities of the effect/outcome. In the safety analysis, these internal and external factors are called internal and external mitigations. To each of the effects, a level of severity is assigned based on criteria shown in Section 4.

The overall safety of the system will be the result of a combination of factors leading to possible losses of separation and/or losses of well clear. The airspace design, air traffic density, the effectiveness of procedures and strategic conflict management will drive the requirements for DAA deconfliction. The combination of the factors leading to a traffic conflict and the mitigation impact resulting from DAA deconfliction procedures, systems, and operators must achieve the required Safety Risk Level.

4 Levels of Hazard Severity

An excerpt of the severity table from Safety Management System (SMS) manual pertaining only to flight crews and aircraft proximity is summarized in Table 1.

TABLE 1. SMS ABBREVIATED HAZARD SEVERITY CLASSIFICATION

	Hazard Severity Classification				
Applies to	Minimal 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
Flight Crew	Pilot is aware of traffic. Compliance greater than or equal to 66 percent	Aircraft is in close enough proximity to require specific action. Low risk Analysis Event*	In close enough proximity on a course of potential collision. Medium risk Analysis Event*	Near mid-air collision. Proximity of less than 152 meters (500 feet).	Mid-air collision

The Risk Analysis Event (*) severity indicators used in the calculations are defined in the SMS manual and include aircraft proximity and rate of closure, as well as ATC (timely) mitigation and pilot (timely) mitigation. The definition of severity shown in Table 1 is mostly applicable to aircraft operating under air traffic control. However, it shows, in the risk analysis events, that both distance between the aircraft and closure rate are considered in the determination of severity.

When two or more aircraft are involved in an encounter where their routes or trajectories are in conflict, a DAA deconfliction procedure will take place to prevent a loss of separation (LOS) or a loss of well clear (LoWC). Depending on the initial geometry and state of the aircraft and the mitigation effectiveness of the deconfliction procedure, the outcome of the encounter can have different levels of severity. Figure 4 depicts the level of severity including no loss of separation or well clear.

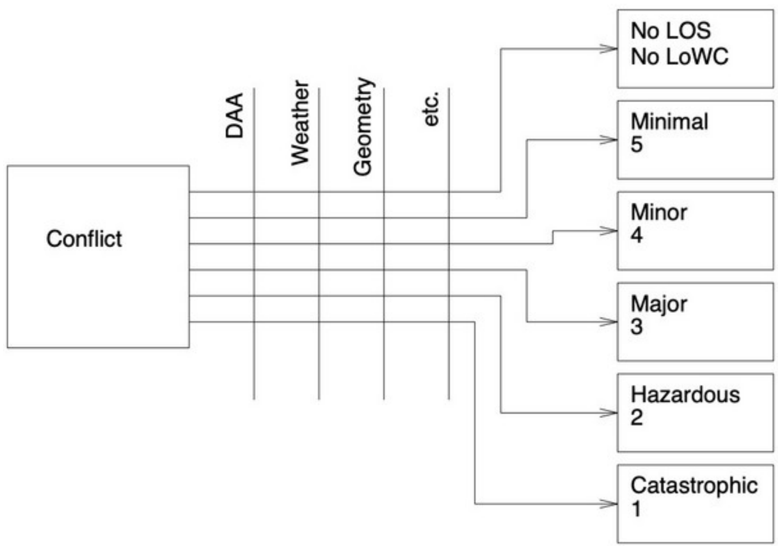

Figure 4: Effectiveness of tactical deconfliction

Analysis, Monte Carlo simulations, human in-the-loop experiments, and flight tests can be used to evaluate the effectiveness of tactical (DAA) deconfliction. For a given scenario or initial condition, it is possible to estimate the likelihood (probability) of an outcome of a given severity for the DAA deconfliction system. Monte Carlos simulations are especially useful for these evaluations given that thousands of scenarios can be explored, and randomness can be used to evaluate large number of possibilities.

5 Conditional Probability Estimation

This section estimates the conditional probability that given an encounter where a conflict exists, the outcome will result in no LOS/no LoWC. It also estimates the probability that a LOS/LoWC occurs for the 5 levels of severity. A conflict is defined as a state where the aircraft are not in a LOS/LoWC but are projected to be in a LOS/LoWC in the future. To estimate the outcome probability, conflicts are divided into 3 scenarios.

1. Aircraft are on a common route in the same direction
2. Aircraft are on a common route in opposite direction
3. Aircraft are on crossing routes

The following assumptions are used in the next subsections to estimate the conditional probability of the outcomes:

Assumptions 1. Aircraft operate under Visual Flight Rules (VFR) without radar services (Air Traffic Control (ATC) services). There are no separation provisions from ATC.
Assumptions 2. All aircraft are navigating using GPS navigation equipment with WAAS (Wide Area Augmentation System) which provides a required accuracy of 7.6 meters laterally and vertically at least 95% of the time.
Assumptions 3. When a conflict exists, aircraft will have sufficient room in the operational airspace to maneuver and stay well clear.
Assumptions 4. The aircraft do not have intent information. That is, neither aircraft has the flight plan of the other aircraft and an aircraft following a route or flight plan can change direction, speed or altitude without the knowledge of the other aircraft.
Assumptions 5. Aircraft are equipped with ADS-B out and ADS-B in.
Assumptions 6. The aircraft transponder (ADS-B out) and the aircraft ADS-B receiver (ADS-B in) are two separate units without a single point of failure. This assumption is critical for the construction of the OH1b fault tree. If the aircraft transponder and the ADS-B receiver are the same unit on an aircraft, then failure of this unit will prevent the aircraft from seeing other aircraft and being seen by other aircraft. Many installations on current General Aviation aircraft have these functions integrated into a single unit.
Assumptions 7. Aircraft follow the right-of-way rules as stated in 14 CFR 91.113. When an aircraft has right-of-way, it will delay the implementation of the avoidance maneuver an additional 5 seconds.
Assumptions 8. Aircraft are equipped with assistive detect and avoid (DAA).
Assumptions 9. The speed of the aircraft vary from 0 to 90 knots.
Assumptions 10. When the aircraft are in the take-off and landing configuration, the minimum speed is 0 knots, and the maximum speed is 45 knots.
Assumptions 11. When the aircraft are on cruising mode, the minimum speed is 45 knots and the maximum 90 knots.
Assumptions 12. Aircraft size vary from 9 to 12 meters in length and width.
Assumptions 13. The protected volume (well clear volume WCV) is 243.84 meters (800 feet) horizontally and 137 meters (450 feet) vertically (for both terminal and en-route airspace).
Assumptions 14. When a conflict exists and the on-board DAA does not provide alerting and guidance, if the flight crew visually acquires the traffic aircraft, it will maneuver to stay well clear or regain well clear 1 second after visual acquisition.
Assumptions 15. When a conflict exists and the on-board DAA system provides alerting and guidance, the flight crew nominally will implement the guidance after a random delay (unless there is an error by the flight crew). The random delay has a Rayleigh distribution with mean 5 seconds and sigma 3.989.
Assumptions 16. No terrain or weather awareness was implemented in the simulation.
Assumptions 17. Only pair-wise encounters were implemented (as per test vectors in DO365)
Assumptions 18. Flight crews are appropriately trained to respond to DAA guidance correctly and in a timely manner.

5.1 Common Segment in the Same Direction (overtake)

Figure 5 shows an illustration of two aircraft on a common segment and going in the same direction.

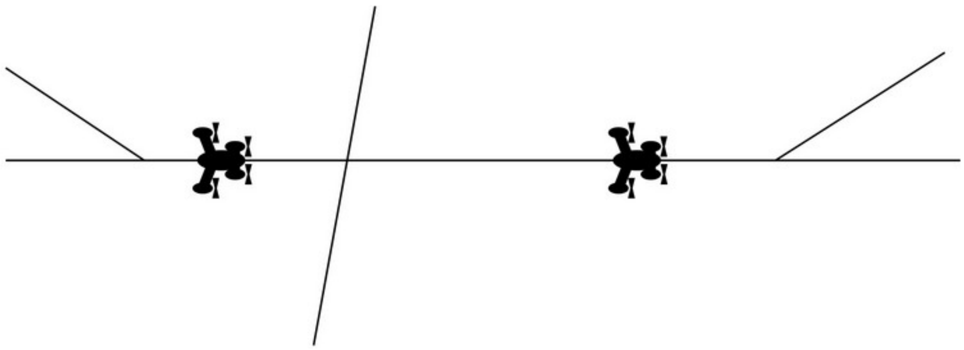

Figure 5: Common segment, same direction

The lines in the figure represent the route structure. The aircraft are on a common segment in the same direction. Aircraft on a common segment in the same direction will only have a conflict when the air speeds of the trailing aircraft is greater than the leading aircraft. Based on Assumption 11, the maximum closure rate for aircraft in the same direction is 45 knots. Simulation experiments show that for overtaking scenarios and under nominal conditions and the assumptions above, the aircraft will remain well clear.

5.2 Common segment in opposite direction (head-on)

Figure 6 shows an illustration of two aircraft on a common segment and going in opposite directions.

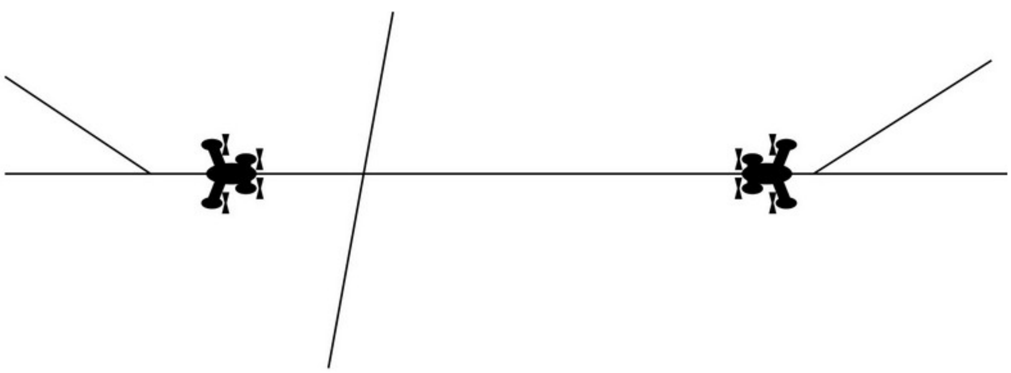

Figure 6: Common segment opposite direction

The aircraft will be in conflict as long as they have non-zero speeds.

5.3 Crossing

Figure 7 shows a crossing scenario. The scenario used in the calculation of the probabilities in the following section uses a 90-degree crossing angle and initial conditions that put the aircraft in conflict.

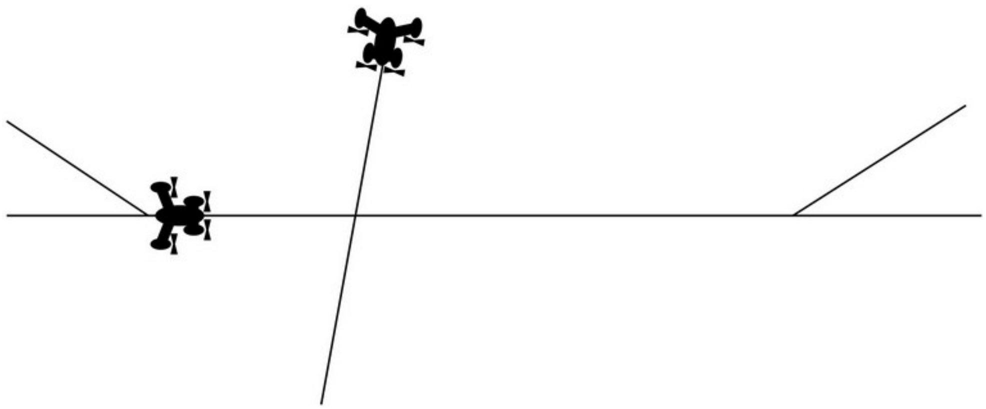

Figure 7: Crossing

The conditional probability of a loss of well clear is based on non-nominal conditions. The following section presents fault trees which estimate the probability that, given a conflict, the Detect and Avoid system will be ineffective in solving the conflict.

6 Causes and Fault Trees

This section contains the potential basic causes and abnormal event that could render the DAA deconfliction ineffective in solving a conflict. This list is a high level conceptual list and likely not all inclusive because, as stated in Section 1, an accepted Operational Services and Environment Definition does not exist at the time of this work. The majority of details regarding structures, implementations, and procedures are not available for analysis. Table 2 contains a list of causes. The columns represent the cause number, description, explanation of the cause, and an estimated probability of the cause occurring. These probabilities are estimated using known historical operational data. The probabilities are likely to change as new operations and new technologies are introduced in the NAS.

Table 2. Basic Causes and Abnormal Events

No.	Description	Comments	Rationale/ Frequency per flight hour
C-1	Surveillance failure to survey a threat	A temporary outage of an ADS-B source is generally caused by non-hardware mechanism such as multipath reception, airframe blockage, interference, or capacity overload. ADS-B signals can be received from a 200 nautical miles radius.	1.73E-3 ADS-B out equipped aircraft can transmit on 978 MHz or 1090 MHz. From [2], the probability of interference due to capacity overload on the 978 MHz frequency is 0.005 for 10 aircraft, 0.03 for 100 aircraft, and 0.12 for 300 aircraft. Reference [2] does not give details of the meaning of “probability of interference.” It is assumed for the purpose of estimating a frequency per flight hour for this cause that the

			probability refers to the probability per sample. In UAM operations, it is likely that the airspace density is high and 300 aircraft in a 200 nautical miles radius is very likely. There are two other factors to be considered in the estimation of the probability of interference: 1. aircraft in conflict will be proximate to each other and the signal strength will be higher than aircraft far away. 2. Interference will be an intermittent issue that will have some drop-off samples and then re-acquire. The frequency per flight hour for this cause is the probability that there is a loss of 3 consecutive samples from the traffic aircraft and 300 aircraft in the reception volume of the ownship. 0.12x0.12x0.12 = 1.73E-3
C-2A	False or misleading information from ownship	One or more components of the DAA equipment produces erroneous information and PIC is unaware. The PIC of the UAS is using incorrect information to make decisions to stay well clear. Components of the DAA equipment include the traffic display, the processing unit, the software, the interconnections, the ADS-B receiver, the ownship GPS source, the pressure encoding transducer, etc. Sub-causes of this cause could include mis-configuration of the DAA equipment or other software related issue.	1.00E-05 Design assurance level of C based on Technical Standard Order (TSO) for DAA equipment for Unmanned Aerial Systems.
C-2B	False or misleading information from traffic aircraft	There are 2 main factors that can contribute to false or misleading information: 1. The position report supplied to the ADS-B or transponder is erroneous; 2. The report is corrupted during encoding and transmission. The source of the position for the ADS-B is GPS for horizontal position	1.24E-06 For ADS-B equipped aircraft, the integrity of a GPS source with RAIM is 1.24E-06 per flight hour. RTCA DO-242A, 3.3.6.5 The integrity of the ADS-B System shall (R3.39) be 1.0E-6 or better on a per report basis. The

		and pressure encoding transducer for altitude. A general accepted method of determining erroneous information from corrupted messages is that there are 3 consecutive corrupted reports. RTCA DO-242 specifies the integrity of ADS-B reports as 1.0E-06 or better per report. However, there have been observed instances of aircraft reporting erroneous position due to ADS-B equipment software, design, and/or installation errors [3]. The equipment exhibiting this behavior do not meet the Technical Standard Orders for ADS-B equipment. The equipment manufacturers are in the process of addressing this issue.	probability of 3 consecutive corrupted reports is 1.0E-06x1.0E-06x1.0E-06 = 1.0E-18. The probability of 3 consecutive corrupted reports in a sequence of 3,600 reports is 3.6E-15. The reported errors affecting some aircraft in the NAS has occurred 5 times in the year 2016. Extrapolating to 100 percent equipage rate, it is expected that there will be 47 position error events every year. Based on these observations and extrapolation [3], the probability is estimated at 1.24E-06.
C-3	Pilot In Command (PIC) late, does not implement, or misinterprets guidance	The PIC could be untimely in implementing the guidance. PIC could be distracted and not detect the alerts. PIC could also incorrectly implement the guidance.	4.0E-5 There is no operational data or human in the loop experiment to estimate the probability of this cause. In past Safety Risk Management analysis (for example, In-Trail Procedure), the probability of the flight crew erroneously implementing the procedure has been estimated at between 1E-05 to 3E-05 with the probabilities for each of the elements of the erroneous part of the procedure. As a conservative estimate, the probability is set to 4E-05.
C-4	Traffic aircraft maneuvers unexpectedly	The PIC of the ownship correctly follows DAA equipment guidance to stay well clear but traffic aircraft maneuvers putting the two aircraft back in a loss of well clear trajectory. This cause assumes that the ownship does not have knowledge of	0.5 UAM aircraft are expected to follow their flight plans and be within the route structure. Depending on how the conflict resolutions are prioritized, a traffic aircraft maneuver might or might not present a problem. For

		the intent of the traffic aircraft.	example, if the resolution maneuver is to slow down, then the traffic aircraft departing the route or turning to a different segment at an intersection will not be a conflict issue. However, if the resolution maneuver is to overtake the traffic aircraft, then a turn by the traffic aircraft will generate a new conflict. An aircraft turning at an intersection is likely and the estimated probability is 0.5 per flight hour.
C-5	The traffic aircraft unexpected maneuver causes a loss of well clear	The unexpected maneuver of the traffic aircraft affects the avoidance maneuver performed by the ownship.	2.50E-02 (overtaking) 1.63E-02 (head-on) 1.57E-02 (crossing) The probability is obtained from simulation runs in which a conflict encounter is considered. The encounter lasts 200 seconds which is slightly more than the time to Closest Point of Approach between the aircraft. During the encounter, the ownship will maneuver to avoid the loss of well clear. The avoidance maneuver of the ownship is heading change priority. That is, the ownship will attempt to solve the conflict using a heading change. If that is unsuccessful, the ownship will try vertical change and then horizontal speed change. At some random time between 0 and 200 seconds, the traffic aircraft maneuvers to a random heading, vertical speed, or horizontal speed. The implementation of the avoidance maneuver by the ownship has a pilot implementation delay. This delay is random for each run with a value selected from a Rayleigh distribution with mean = 5.0 seconds and sigma = 3.989 seconds. 100,000 simulation runs are performed for each scenario to obtain the values.
C-6	DAA equipment	The DAA equipment on-board	1.00E-04

	failure	the aircraft or one of its components fails. This includes the ADS-B In receiver.	GPS avionics must meet an unavailability threshold of 1.0E-04 flight-hour.
C-7	ADS-B transponder or GPS source failure	The surveillance equipment on the aircraft stops broadcasting.	1.00E-04 GPS avionics must meet an unavailability threshold of 1.0E-04 flight-hour.
C-8	Traffic aircraft does not maneuver	In an encounter where a conflict exist, both aircraft are assumed to be DAA equipped and both aircraft are expected to maneuver to stay well clear. If the traffic aircraft has bad information from its own aircraft, the other aircraft is transmitting bad information, DAA equipment on-board fails, or the other aircraft does not broadcast its state, then the traffic aircraft cannot maneuver.	2.11E-04 C-2A OR C-2B OR C-6 OR C-7

The causes from Table 2 are represented in fault trees with the calculation of the overall probability. The causes are divided into temporary and persistent. A temporary or delayed cause will cease to exist during the encounter. A persistent cause is expected to last throughout the encounter.

6.1 Common segment in the same direction (overtake)

Figures 8 and 9 show the fault trees for the temporary and persistent causes. The values in the fault trees reflect the common segment in the same direction case (overtake).

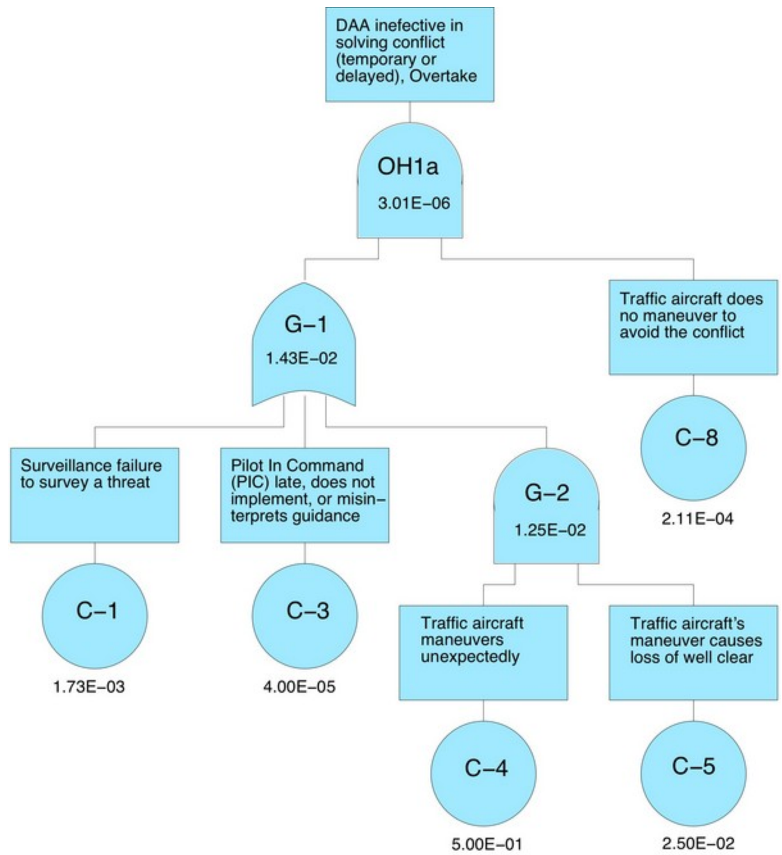

Figure 8: Detect and Avoid ineffective in solving a conflict, temporary or delayed, same direction (overtake)

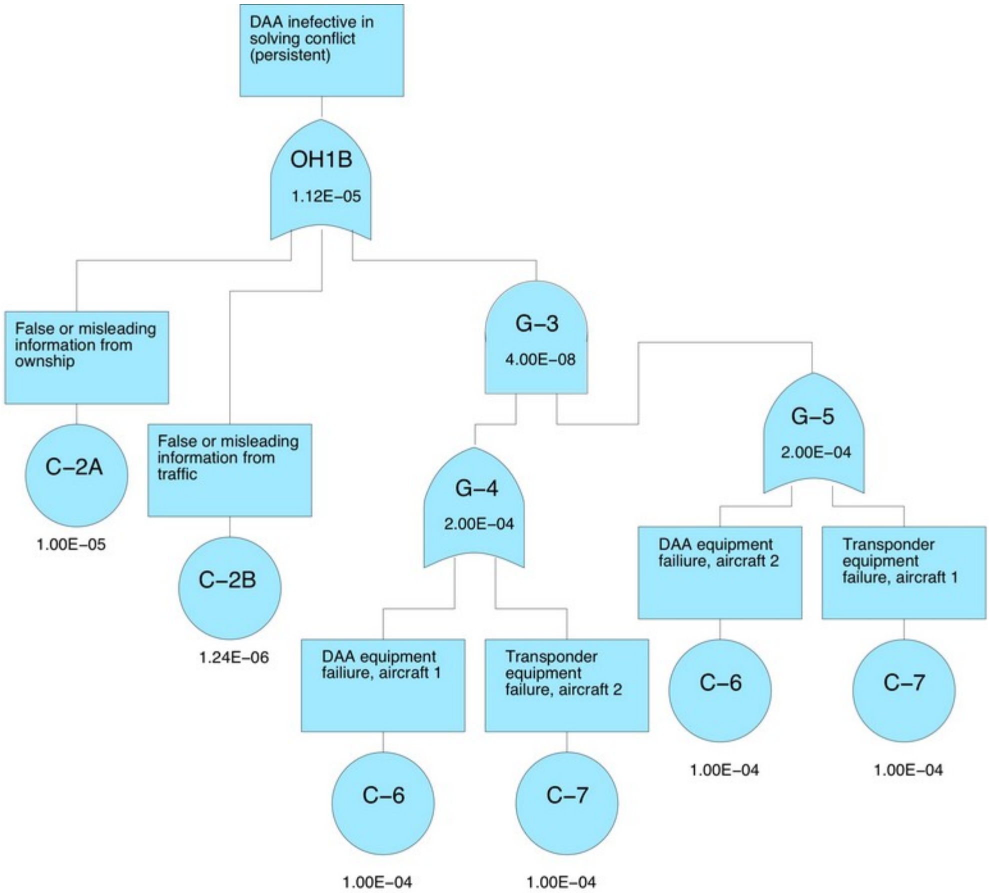

Figure 9: Detect and Avoid ineffective in solving a conflict, persistent, same direction (overtake)

6.2 Common segment in opposite direction (head-on)

Figure 10 shows the fault tree for the temporary causes for the head-on case. The fault tree for the persistent causes is the same as the one for the overtaking case, Figure 9.

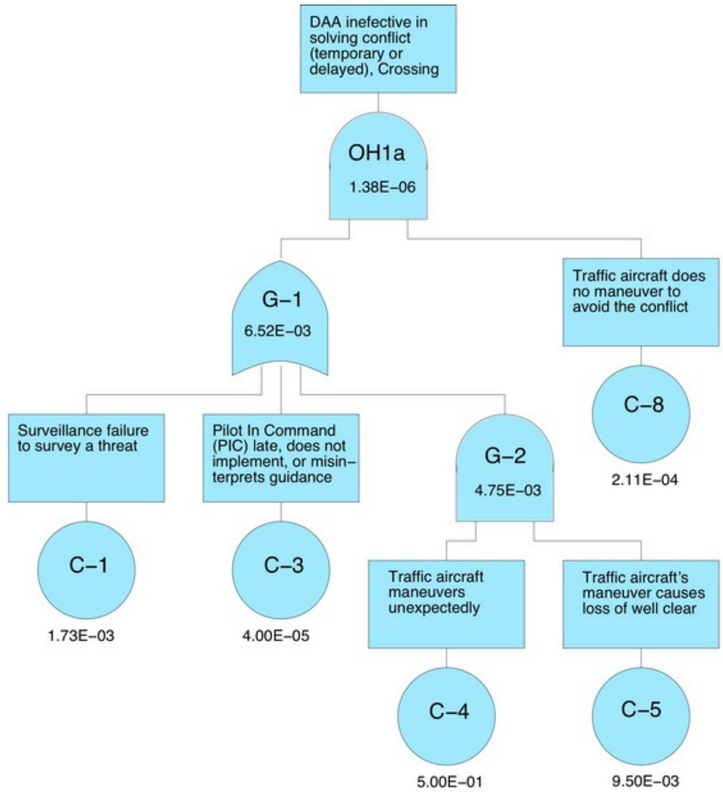

Figure 10: Detect and Avoid ineffective in solving a conflict, temporary or delayed, opposite direction (head-on)

6.3 Crossing

Figure 11 shows the fault tree for the temporary causes for the crossing case. The fault tree for the persistent causes is the same as the on for the overtaking case, Figure 9. The scenario used to generate the value for the C-5 node puts the ownship to the right of the traffic aircraft which means that the ownship has the right-of-way.

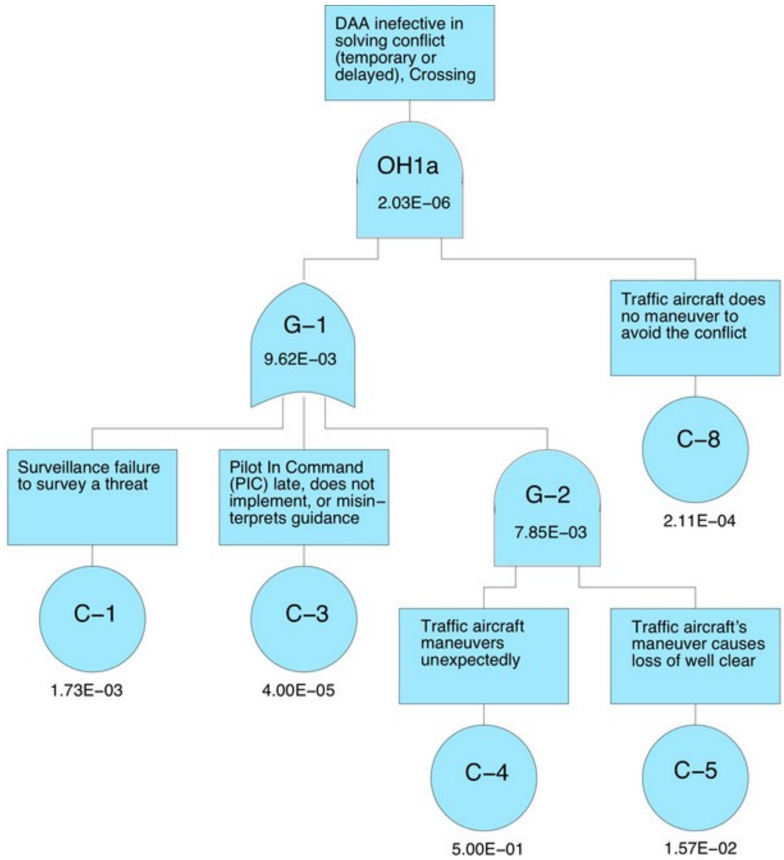

Figure 11: Detect and Avoid ineffective in solving a conflict, temporary or delayed, crossing

Given that the Detect and Avoid system is ineffective in solving a conflict, the severity of the outcome is estimated using Event Trees. The following section present Event Trees that estimate severity and overall likelihood of the hazard.

7 Event Trees

Given that the Detect and Avoid system has failed to maintain the aircraft well clear of each other, the severities and likelihoods of the given severities are estimated using Event Trees. The event trees contain Mitigation Means which are barriers that will reduce the severity or eliminate the effect of the failure on the outcome of the event. Table 3 contain a list of the mitigations. This list is likely not all inclusive due to the lack of an accepted Operational Services and Environment Definition.

Table 3. List of mitigation means

Mitigation Means	Description and likelihood rationale	Likelihood
MM.1	One of the aircraft in the encounter departs the segment following its flight plan which eliminates the conflict. The estimated value is based on short air-taxi operations in urban areas with short segments. This value will need to be revised when more information of the structure	0.5

	of the operations is known. The given value is considered a "place holder."	
MM.2	This mitigation is for the common segment, same direction (overtake) scenario. This mitigation applies to situations where one or both aircraft loses and then regains the surveillance of the other aircraft and it is late in implementing the resolution guidance. The value for this mitigation is estimated using Monte Carlo simulations. Both aircraft are equipped with Detect and Avoid. The guidance is produced with a 6 second delay. After the flight crew receives the conflict alert and guidance, the guidance is implemented with an additional random pilot's implementation delay. The random delay has a Rayleigh distribution with a mean of 5.0 seconds and sigma of 3.989 seconds. Because it is assumed that the aircraft are navigating using GPS (Section 4, Assumption 4), the initial condition for the simulation in each run places the aircraft plus or minus 10 meters from the segment center line.	Severity 5 9.999E-01 Severity 4 1.0E-04 Severity 3 0.0 Severity 2 0.0 Severity 1 0.0
MM.3	This mitigation is for the common segment, same direction (overtake) scenario. When one of the aircraft maneuvers unexpectedly, the Detect and Avoid guidance being implemented by the other aircraft could become ineffective. However, the DAA equipment will update the guidance and the flight crew will implement the new guidance reducing the severity and/or collision. The value is estimated using Monte Carlo simulation where one aircraft maneuvers at random during the encounter. The random maneuvers are: Turn right 0 to 90 degrees; Turn left 0 to 90 degrees; Slow down or speed up from the current speed to a speed between 45 and 90 knots. Climb or descent at 0 to 700 feet per minute. The random maneuver could occur at any time between the beginning of the encounter to a few seconds after the Closest Point of Approach.	Severity 5 9.94E-01 Severity 4 5.10E-03 Severity 3 6.00E-4 Severity 2 1.00E-04 Severity 1 0.0
MM.4	This mitigation is for the common segment, same direction (overtake) scenario. The flight crew of the trailing aircraft visually acquires the leading aircraft and performs a maneuver to maintain well clear, regain well clear, reduce the severity of the encounter, and/or avoid a collision. The value for this mitigation is estimated using a visual acquisition algorithm and simulation runs. The visual acquisition algorithm is based on an MIT Lincoln Laboratory algorithm developed in the 1980's [4]. Because this is a common segment, same direction scenario, only the trailing aircraft has an opportunity to visually acquiring the leading aircraft. The probabilities are based on this geometry.	Severity 5 9.99E-01 Severity 4 8.00E-04 Severity 3 0.0 Severity 2 1.00E-04 Severity 1 0.0
MM.5	This mitigation is for the common segment, opposite direction (head-on) scenario. One or both aircraft loses and then regains the surveillance of the other aircraft. It is similar to MM.2 but with the Monte Carlo simulations performed for the common segment, opposite direction scenario.	Severity 5 9.999E-01 Severity 4 0.0 Severity 3 1.00E-04 Severity 2 0.0 Severity 1

		0.0
MM.6	This mitigation is for the common segment, opposite direction (head-on) scenario. When one of the aircraft maneuvers unexpectedly, the Detect and Avoid guidance being implemented by the other aircraft could become ineffective. However, the DAA equipment will update the guidance and the flight crew will implement the new guidance reducing the severity and/or collision. See MM.3 for more details.	Severity 5 9.90E-01 Severity 4 1.80E-03 Severity 3 1.60E-3 Severity 2 5.40E-03 Severity 1 7.00E-04
MM.7	This mitigation is for the common segment, opposite direction (head-on) scenario. The flight crew of one or both aircraft visually acquires the other aircraft and performs a maneuver to maintain well clear, regain well clear, reduce the severity of the encounter, and/or avoid a collision. This mitigation is similar to MM.4 which contains more details on how the probabilities are obtained.	Severity 5 4.45E-01 Severity 4 9.51E-02 Severity 3 1.28E-01 Severity 2 3.31E-01 Severity 1 9.00E-04
MM.8	This mitigation is for the crossing scenario. One or both aircraft loses and then regains the surveillance of the other aircraft. It is similar to MM.2 but with the Monte Carlo simulations performed for the crossing scenario.	Severity 5 8.74E-01 Severity 4 1.02E-01 Severity 3 1.45E-02 Severity 2 9.20E-03 Severity 1 0.0
MM.9	This mitigation is for the crossing scenario. When one of the aircraft maneuvers unexpectedly, the Detect and Avoid guidance being implemented by the other aircraft could become ineffective. However, the DAA equipment will update the guidance and the flight crew will implement the new guidance reducing the severity and/or collision. See MM.3 for more details.	Severity 5 8.73E-01 Severity 4 1.27E-1 Severity 3 6.37E-04 Severity 2 0.0 Severity 1 0.0
MM.10	This mitigation is for the crossing scenario. The flight crew of one or both aircraft visually acquires the other aircraft and performs a maneuver to maintain well clear, regain well clear, reduce the severity of the encounter, and/or avoid a collision. This mitigation is similar to MM.4 which contains more details on how the probabilities are obtained.	Severity 5 4.58E-01 Severity 4 9.50E-02 Severity 3 1.10E-01 Severity 2

		3.37E-01 Severity 1 2.00E-04

7.1 Common segment in the same direction (overtake)

The following Event Trees estimate the severity and probability of effect using the Mitigation Means that apply to this case.

OH1a. DAA ineffective in solving conflict (temporary or delayed), overtake

Relevant Hazard	Hazard Likelihood	MM.1 The leading or trailing aircraft departs the route and the conflict no longer exists.	MM.2 After dropping the leading aircraft for a few seconds, the aircraft is reacquired and the flight crew implements the resolution to try to stay well clear.	MM.3 The unexpected maneuver of the traffic aircraft leads to the given severity level.	Severity	Severity Rationale	Probability of Effect (Pe)
OH1a	X	5.00E-01					
		5.00E-01				No LoWC	5.00E-01
3.01E-06	X		9.999E-01		5	Minimal	5.00E-01
			1.00E-04		4	Minor	5.00E-05
		5.00E-01	0.00E+00		3	Major	0.00E+00
			0.00E+00		2	Hazardous	0.00E+00
			0.00E+00		1	Catastrophic	0.00E+00
				9.94E-01	5	Minimal	4.97E-01
				5.10E-03	4	Minor	2.55E-03
		5.00E-01		6.00E-04	3	Major	3.00E-04
				1.00E-04	2	Hazardous	5.00E-05
				0.00E+00	1	Catastrophic	0.00E+00
	Hazard Does Not Occur 1-X					No Safety Effect	

US Risk Likelihood P(OHi) x Pe)	FAA SMS Safety Target	FAA SMS Safety Target Met?
0.00E+00	1.00E-09	Yes
1.51E-10	1.00E-07	Yes
9.03E-10	1.00E-05	Yes
7.83E-09	1.00E-03	Yes

Severity	Probability of Effect (Pe)
1	0.00E+00
2	5.00E-05
3	3.00E-04
4	2.60E-03

OH1b. DAA ineffective in solving conflict (persistent), overtake

Relevant Hazard	Hazard Likelihood	MM.1 The leading or trailing aircraft departs the route and the conflict no longer exists.	MM.4 The trailing aircraft visually acquires the leading and maneuvers to remain well clear, regain well clear, and/or avoid a collision.	Severity	Severity Rationale	Probability of Effect (Pe)
OH1b	X	5.00E-01				
		5.00E-01		5	Minimal	5.00E-01
1.12E-05	X		9.99E-01	5	Minimal	5.00E-01
		5.00E-01	8.00E-04	4	Minor	4.00E-04
			0.00E+00	3	Major	0.00E+00
			1.00E-04	2	Hazardous	5.00E-05
			0.00E+00	1	Catastrophic	0.00E+00
	Hazard Does Not Occur 1-X				No Safety Effect	

Risk Likelihood P(OHi) x Pe)	FAA SMS Safety Target	FAA SMS Safety Objective Met?
0.00E+00	1.00E-09	Yes
5.60E-10	1.00E-07	Yes
0.00E+00	1.00E-05	Yes
4.48E-09	1.00E-03	Yes

Severity	Probability of Effect (Pe)
1	0.00E+00
2	5.00E-05
3	0.00E+00
4	4.00E-04

7.2 Common segment in opposite direction (head-on)

The following Event Trees estimate the severity and probability of effect using the Mitigation Means that apply to this case.

OH1a. DAA ineffective in solving conflict (temporary or delayed), opposite direction (head-on)

Relevant Hazard	Hazard Likelihood	MM.1 The leading or trailing aircraft departs the route and the conflict no longer exists.	MM.5 After dropping the traffic aircraft for a few seconds, the aircraft is reacquired and the flight crew implements the resolution to try to stay well clear.	MM.6 The unexpected maneuver of the traffic aircraft leads to the given severity level.	Severity	Severity Rationale	Probability of Effect (Pe)
OH1a	X	5.00E-01					
		5.00E-01				No LoWC	5.00E-01
1.38E-06	X		9.999E-01		5	Minimal	5.00E-01
			0.00E+00		4	Minor	0.00E+00
		5.00E-01	1.00E-04		3	Major	5.00E-05
			0.00E+00		2	Hazardous	0.00E+00
			0.00E+00		1	Catastrophic	0.00E+00
				9.90E-01	5	Minimal	4.95E-01
				1.80E-03	4	Minor	9.00E-04
		5.00E-01		1.60E-03	3	Major	8.00E-04
				5.40E-03	2	Hazardous	2.70E-03
				7.00E-04	1	Catastrophic	3.50E-04
	Hazard Does Not Occur 1-X					No Safety Effect	

US Risk Likelihood P(OHi) x Pe)	FAA SMS Safety Target	FAA SMS Safety Target Met?
4.83E-10	1.00E-09	Yes
3.73E-09	1.00E-07	Yes
1.17E-09	1.00E-05	Yes
1.24E-09	1.00E-03	Yes

Severity	Probability of Effect (Pe)
1	3.50E-04
2	2.70E-03
3	8.50E-04
4	9.00E-04

OH1b. DAA ineffective in solving conflict (persistent), same segment, opposite direction (head-on)

Relevant Hazard	Hazard Likelihood	MM.1 The leading or trailing aircraft departs the route and the conflict no longer exists.	MM.7 One or both aircraft visually acquires the other and maneuvers to remain well clear, regain well clear, and/or avoid a collision.	Severity	Severity Rationale	Probability of Effect (Pe)
OH1b	X	5.00E-01				
		5.00E-01		5	Minimal	5.00E-01
1.12E-05	X		4.45E-01	5	Minimal	2.23E-01
		5.00E-01	9.51E-02	4	Minor	4.76E-02
			1.28E-01	3	Major	6.40E-02
			3.31E-01	2	Hazardous	1.66E-01
			9.00E-04	1	Catastrophic	4.50E-04
	Hazard Does Not Occur 1-X				No Safety Effect	

Risk Likelihood P(OHi) x Pe)	FAA SMS Safety Target	FAA SMS Safety Objective Met?
5.04E-09	1.00E-09	No
1.85E-06	1.00E-07	No
7.17E-07	1.00E-05	Yes
5.33E-07	1.00E-03	Yes

Severity	Probability of Effect (Pe)
1	4.50E-04
2	1.66E-01
3	6.40E-02
4	4.76E-02

7.3 Crossing

The following Event Trees estimate the severity and probability of effect using the Mitigation Means that apply to this case.

OH1a. DAA ineffective in solving conflict (temporary or delayed), crossing

Relevant Hazard	Hazard Likelihood	MM.1 One of the aircraft departs the route and the conflict no longer exists.	MM.8 One or both aircraft loses the other aircraft for a few seconds, the aircraft are reacquired and the flight crew implements the resolution to try to stay well clear.	MM.9 The unexpected maneuver of the traffic aircraft leads to the given severity level.	Severity	Severity Rationale	Probability of Effect (Pe)
OH1a	X	5.00E-01					
		5.00E-01				No LoWC	5.00E-01
2.03E-06	X		8.74E-01		5	Minimal	4.37E-01
			1.020E-01		4	Minor	5.10E-02
		5.00E-01	1.45E-02		3	Major	7.25E-03
			9.20E-03		2	Hazardous	4.60E-03
			0.00E+00		1	Catastrophic	0.00E+00
				8.73E-01	5	Minimal	4.37E-01
				1.27E-01	4	Minor	6.35E-02
		5.00E-01		6.37E-04	3	Major	3.19E-04
				0.00E+00	2	Hazardous	0.00E+00
				0.00E+00	1	Catastrophic	0.00E+00
	Hazard Does Not Occur 1-X					No Safety Effect	

US Risk Likelihood P(OHi) x Pe)	FAA SMS Safety Target	FAA SMS Safety Target Met?
0.00E+00	1.00E-09	Yes
9.34E-09	1.00E-07	Yes
1.54E-08	1.00E-05	Yes
2.32E-07	1.00E-03	Yes

Severity	Probability of Effect (Pe)
1	0.00E+00
2	4.60E-03
3	7.57E-03
4	1.15E-01

OH1b. DAA ineffective in solving conflict (persistent), crossing

Relevant Hazard	Hazard Likelihood	MM.1 One of the aircraft departs the route and the conflict no longer exists.	MM.10 One or both aircraft visually acquires the other and maneuvers to remain well clear, regain well clear, and/or avoid a collision.	Severity	Severity Rationale	Probability of Effect (Pe)
OH1b	X	5.00E-01				
		5.00E-01		5	Minimal	5.00E-01
1.12E-05	X		4.58E-01	5	Minimal	2.29E-01
		5.00E-01	9.50E-02	4	Minor	4.75E-02
			1.10E-01	3	Major	5.52E-02
			3.37E-01	2	Hazardous	1.68E-01
			2.00E-04	1	Catastrophic	1.00E-04
	Hazard Does Not Occur 1-X				No Safety Effect	

Risk Likelihood P(OHi) x Pe)	FAA SMS Safety Target	FAA SMS Safety Objective Met?
1.12E-09	1.00E-09	No
1.88E-06	1.00E-07	No
6.18E-07	1.00E-05	Yes
5.32E-07	1.00E-03	Yes

Severity	Probability of Effect (Pe)
1	1.00E-04
2	1.68E-01
3	5.52E-02
4	4.75E-02

8 Severity Definition

The FAA ATO Safety Management System (SMS) manual defines severity as follows:

"Severity is the consequence or impact of a hazard's effect or outcome in terms of degree of loss or harm."

The SMS manual further defines Severity in the following categories:

- ATC Services
- Unmanned Aircraft Systems
- Flying Public
- NAS Equipment
- Flight Crew

Table 4 is a reproduction of Table 3.3 of the SMS Manual containing the hazard severity classification.

Table 4. Hazard Severity Classification

Effect On: ↓	Hazard Severity Classification *Note: Severities related to ground-based effects apply to movement areas only.*				
	Minimal **5**	**Minor** **4**	**Major** **3**	**Hazardous** **2**	**Catastrophic** **1**
	CONDITIONS RESULTING IN ANY ONE OF THE FOLLOWING:				
ATC Services	A minimal reduction in ATC services CAT D Runway Incursion[1] Proximity Event, Operational deviation, or measure of compliance greater than or equal to 66 percent[2]	Low Risk Analysis Event severity,[3] two or fewer indicators fail CAT C Runway Incursion	Medium Risk Analysis Event severity, three indicators fail CAT B Runway Incursion	High Risk Analysis Event severity, four indicators fail CAT A Runway Incursion	Ground collision[4] Mid-air collision Controlled flight into terrain or obstacles
Unmanned Aircraft Systems	Discomfort to those on the ground Loss of separation leading to a Measure of Compliance greater than or equal to 66 percent	Low Risk Analysis Event severity, two or fewer indicators fail Non-serious injury to three or fewer people on the ground	Medium Risk Analysis Event severity, three indicators fail Non-serious injury to more than three people on the ground A reduced ability of the crew to cope with adverse operating conditions to the extent that there would be a significant reduction in safety margins Manned aircraft making an evasive maneuver, but proximity from Unmanned Aircraft remains greater than 500 feet	High Risk Analysis Event severity, four indicators fail Incapacitation to Unmanned Aircraft System crew Proximity of less than 500 feet to a manned aircraft Serious injury to persons other than the Unmanned Aircraft System crew	A collision with a manned aircraft Fatality or fatal injury to persons other than the Unmanned Aircraft System crew
Flying Public	Minimal injury or discomfort to persons on board	Physical discomfort to passenger(s) (e.g., extreme braking action, clear air turbulence causing unexpected movement of aircraft resulting in injuries to one or two passengers out of their seats) Minor injury to less than or equal to 10 percent of persons on board[5]	Physical distress to passengers (e.g., abrupt evasive action, severe turbulence causing unexpected aircraft movements) Minor injury to greater than 10 percent of persons on board	Serious injury to persons on board[6]	Fatal injuries to persons on board[7]
NAS Equipment	Flight Crew inconvenience Slight increase in ATC workload	Increase in flight crew workload Significant increase in ATC workload Slight reduction in safety margin	Large increase in ATC workload Significant reduction in safety margin	Large reduction in safety margin	Collision between aircraft and obstacles

Effect On: ↓	Hazard Severity Classification *Note: Severities related to ground-based effects apply to movement areas only.*				
	Minimal **5**	**Minor** **4**	**Major** **3**	**Hazardous** **2**	**Catastrophic** **1**
	CONDITIONS RESULTING IN ANY ONE OF THE FOLLOWING:				
Flight Crew	Pilot is aware of traffic (identified by Traffic Collision Avoidance System traffic alert, issued by ATC, or observed by flight crew) in close enough proximity to require focused attention, but no action is required Pilot deviation[8] where loss of airborne separation falls within the same parameters of a Proximity Event or measure of compliance greater than or equal to 66 percent Circumstances requiring a flight crew to initiate a go-around	Aircraft is in close enough proximity to another aircraft (identified by Traffic Collision Avoidance System resolution advisory, issued by ATC, or observed by flight crew) to require specific pilot action to alter or maintain current course/ altitude, but intentions of other aircraft are known and a potential collision risk does not exist Pilot deviation where loss of airborne separation falls within the same parameters of a Low Risk Analysis Event severity Reduction of functional capability of aircraft, but overall safety not affected (e.g., normal procedures as per Airplane Flight Manuals) Circumstances requiring a flight crew to abort takeoff (rejected takeoff); however, the act of aborting takeoff does not degrade the aircraft performance capability	Aircraft is in close enough proximity to another aircraft (identified by Traffic Collision Avoidance System resolution advisory, issued as a safety alert by ATC, or observed by flight crew) on a course that requires corrective action to avoid potential collision; intentions of other aircraft are not known Pilot deviation where loss of airborne separation falls within the same parameters of a Medium Risk Analysis Event severity Reduction in safety margin or functional capability of the aircraft, requiring crew to follow abnormal procedures as per Airplane Flight Manuals Circumstances requiring a flight crew to reject landing (i.e., balked landing) at or near the runway threshold Circumstances requiring a flight crew to abort takeoff (i.e., rejected takeoff); the act of aborting takeoff degrades the aircraft performance capability	Near mid-air collision results due to a proximity of less than 500 feet from another aircraft, or a report is filed by pilot or flight crew member that a collision hazard existed between two or more aircraft Pilot deviation where loss of airborne separation falls within the same parameters of a High Risk Analysis Event severity Reduction in safety margin and functional capability of the aircraft requiring crew to follow emergency procedures as per Airplane Flight Manuals	Ground collision Mid-air collision Controlled flight into terrain or obstacles Failure conditions that would prevent continued safe flight and landing

Effect On: ↓	**Hazard Severity Classification** *Note: Severities related to ground-based effects apply to movement areas only.*				
	Minimal **5**	**Minor** **4**	**Major** **3**	**Hazardous** **2**	**Catastrophic** **1**
	CONDITIONS RESULTING IN ANY ONE OF THE FOLLOWING:				

1 – Refer to the current version of Order 7050.1, *Runway Safety Program*.

2 – Proximity Events and Operational Deviations are no longer used to measure losses of separation, but they are applicable when validating old data. The minimal loss of standard separation is now represented as a measure of compliance of greater than or equal to 66 percent.

3 – Risk Analysis Event severity indicators are as follows:

a. Proximity. Failure transition point of 50 percent of required separation or less.

b. Rate of Closure. Failure transition point greater than 205 knots or 2,000 feet per minute (consider both aspects and utilize the higher of the two if only one lies above the transition point).

c. ATC Mitigation. ATC able to implement separation actions in a timely manner.

d. Pilot Mitigation. Pilot executed ATC mitigation in a timely manner.

4 – Ground Collision. An airplane on the ground collides with an object or person.

5 – Minor Injury. Any injury that is neither fatal nor serious.

6 – Serious Injury. Any injury that: a. Requires hospitalization for more than 48 hours, commencing within seven days from the date the injury was received;

Results in a fracture of any bone (except simple fractures of fingers, toes, or nose);

Causes severe hemorrhages, nerve, muscle, or tendon damage;

Involves any internal organ; or

Involves second or third-degree burns, or any burns affecting more than five percent of the body's surface.

7 – Fatal Injury. Any injury that results in death within 30 days of the accident.

8 – Refer to Order JO 8020.16, *Air Traffic Organization Aircraft Accident and Incident Notification, Investigation, and Reporting*, for more information about pilot deviations.

Table 4 above is intended for operations where aircraft are receiving radar and separation services from Air Traffic Control (ATC). The severities used in the calculations presented in Section 7 of this paper are based on a severity metric from RTCA Special Committee SC-228.

The definition of severity uses a mathematical notion of Well Clear and Loss of Well Clear (LoWC). The exact definition of Well Clear, Loss of Well Clear and Severity can be found in [5] and [6]. The definition uses three components to determine a severity in the range of 0 per cent to 100 per cent with 0 the least severe and 100 the most severe. The three components used are:

1. Horizontal Proximity (tau MOD) (Dynamic component of severity)
2. Horizontal Miss-Distance (HMD)
3. Vertical Distance

The scale of the SC-228 definition of severity has been mapped to the SMS classification of severity as shown in Table 5.

Table 5. Mapping from SC-228 severity to SMS severity

SC-228 Severity Levels	SMS Severity Classification
>0%-17%	5, Minimal
>17%-33%	4, Minor
>33%-47%	3, Major
>47%-94%	2, Hazardous
>94%-100%	1, Catastrophic

9 Risk Level

A loss of separation (LOS) or a loss of well clear (LoWC) event will have different severities depending on all the factors that could lead to the LOS or LoWC. The severity of a LOS are defined by guidelines found in the FAA ATO SMS manual. The severity of LoWC has been defined for Unmanned Aerial Systems (UAS) by the RTCA Special Committee SC-228. The severity of an event is classified in the SMS manual as follows:

- Level 5, Minimal Severity
- Level 4, Minor Severity
- Level 3, Major Severity
- Level 2, Hazardous Severity
- Level 1, Catastrophic Severity

Whether a system meets the required Risk Level depends on how often each of these events occur. The SMS manual contains a risk matrix which defines the risk level. The risk matrix is reproduced in Figure 12.

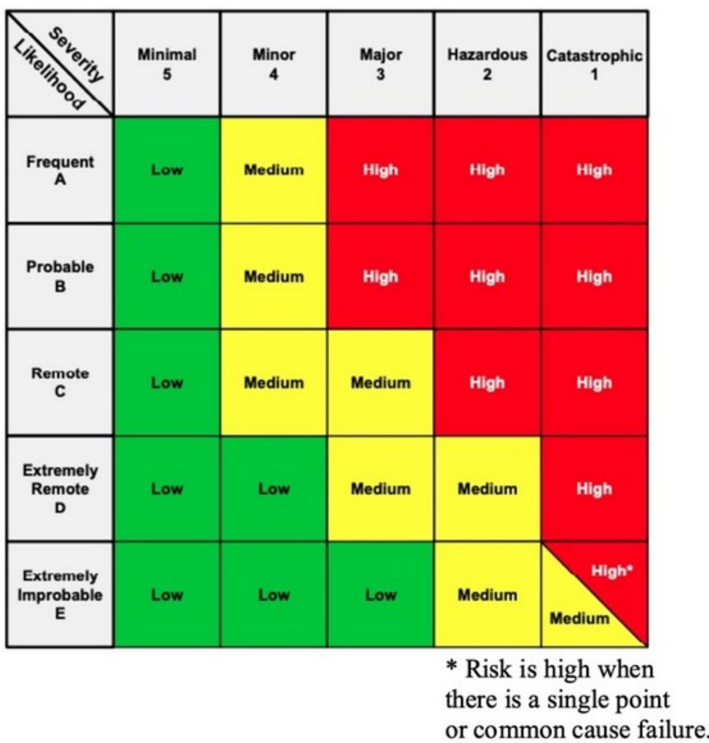

Figure 12: SMS risk matrix

The likelihood or frequency of occurrence are defined in Table 6.

Table 6. Likelihood/Frequency of Events

	Expected Occurrence Rate
Frequent A	Probability >= 1 per 1,000 Probability >= 1.0E-03
Probable	1 per 1,000 > Probability >= 1 per 100,000

B	1.0E-03 > Probability >= 1.0E-05
Remote C	1 per 100,000 > Probability >= 10,000,000 1.0E-05 > Probability >= 1.0E-07
Extremely Remote D	1 per 10,000,000 > Probability >= 1,000,000,000 1.0E-07 > Probability >= 1.0E-09
Extremely Improbable E	1 per 1,000,000,000 > probability >= 1 per 10^{14} 1.0E-09 > Probability >= 1.0E-014

The SMS manual describes the levels of risk as follows:

High Risk. This is unacceptable risk, and the NAS change cannot be implemented unless the hazard's associated risk is mitigated to medium or low. Existing high-risk hazards also must be reduced to medium- or low-risk hazards. The predicted residual risk must be monitored and tracked in relation to the safety performance targets. The predicted residual risk must be confirmed with objective evidence suggesting an impact to the hazard's causes or effects.

Medium Risk. Although initial medium risk is acceptable, it is recommended and desirable that safety requirements be developed to reduce severity and/or likelihood. The risk must be monitored and tracked in relation to the safety performance targets. The predicted residual risk must be confirmed with objective evidence suggesting an impact to the hazard's causes or effects.

Low Risk. This is acceptable risk without restriction or limitation. It is not mandatory to develop safety requirements for low-risk hazards; however, develop a monitoring plan with at least one safety performance target.

10 Results

The fault and event trees give the severity and likelihood of a loss of well clear event for the three scenarios. Table 7 shows a summary of the severity and likelihood of each of the scenarios and two cases.

Table 7. Summary of results

Scenario/Case	Severity	Likelihood (Probability)
Common segment, same direction, temporary	2, Hazardous	1.51E-10
Common segment, same direction, persistent	2, Hazardous	5.60E-10
Common segment, opposite direction, temporary	1, Catastrophic	4.83E-10
Common segment, opposite direction, persistent	1, Catastrophic	5.04E-09
Crossing, temporary	2, Hazardous	9.34E-09
Crossing, persistent	1, Catastrophic	1.12E-09

From Table 7 and the risk matrix of figure 12, it is possible to classify the safety risk. Table 8 shows the safety risk classification for the scenarios and cases.

Table 8. Safety risk

Scenario/Case	Safety risk
Common segment, same direction, temporary	Medium
Common segment, same direction, persistent	Medium
Common segment, opposite direction, temporary	Medium*
Common segment, opposite direction, persistent	High
Crossing, temporary	Medium
Crossing, persistent	High

* Risk is high when there is a single point or common cause failure.

From Table 8, it can be seen that there are two scenarios/cases that have a high safety risk. Per the description of High, Medium, and Low safety risk in Section 9, this risk is unacceptable. Further mitigations will be needed if this operation is to be implemented.

10.1 Possible Mitigations

Mitigations could be identified to reduce the severity or likelihood of the scenarios/cases with high safety risk. Possible mitigations could be:

- Designing an operational environment where the conflicts to be resolved by Detect and Avoid on-board the aircraft have an occurrence rate that brings the likelihood of these events to an acceptable level. This could be achieved with strategic deconfliction, limiting the airspace density, and other methods.
- Designing an operational environment where there are no nominal scenarios with head-on or crossing encounters. This could be achieved by not having bidirectional routes and by having routes where crossings are 500 feet or more apart vertically.
- Having redundant Detect and Avoid capabilities on-board. However, this will not mitigate some of the causes such as frequency saturation and frequency interference.
- Having redundant components for the Detect and Avoid system such as altitude encoding and pitot-static system. This will reduce the most probable cause of erroneous information being used for the ownship and being transmitted to traffic aircraft.
- Having a separate collision avoidance system on-board without common points of failure or common components. The system will have to have different frequencies as the Detect and Avoid system.

11 References

[1] FAA, ATO, Safety Management System Manual, April 2019.

[2] Air Traffic Control Association Institute, Inc.; Air Traffic Control Quarterly, An International Journal of Engineering and Operations, Special Issue, Unmanned Aircraft System Sense and Avoid, Volume 23, number 2/3, 2015.

[3] Surveillance and Broadcast Services Program Office; ADS-B Erroneous Position Hazard Review, February 2017.

[4] J.W. Andrews, “Air-to-Air Visual Acquisition Handbook,” Project Report ATC-151, Lincoln Laboratory, Massachusetts Institute of Technology, 27 November 1991.

[5] V. Carreño, M. Consiglio, C. Muñoz, “Analysis and Preliminary Results of a Concept for Detect and Avoid in the Cockpit,” Proceedings of the 38th Digital Avionics System Conference, San Diego, CA, 8-12 September 2019.

[6] V. Carreño, “Evaluation, Analysis and Results of the DANTi Flight Test Data, the DAIDALUS Detect and Avoid Algorithm, and the DANTi Concept for Detect and Avoid in the Cockpit,” NASA Contract Report, NASA/CR-20205004594, August 2020.

[7] U.S. Department of Transportation, Federal Aviation Administration, “Approval of Non-Required Safety Enhancing Equipment (NORSEE),” Policy No: PS-AIR-21.8-1602, March 2016.