Detect & Avoid
Design, Test & Evaluation Guideline

Appendix E:
Requirements Validation Guidance

Version 1.0

ID: REVAERO-1462090167-139343

This page is intentionally left blank.

Development and Approvals

Developed	Approved
Mr Tom Putland Senior Research, Regulation, and Product Development Engineer Revolution Aerospace Dr Terry Martin CEO and Co-founder Revolution Aerospace Mr Angus McLaren Senior Systems Engineer Revolution Aerospace	Dr Terry Martin CEO and Co-founder Revolution Aerospace Mr Kristian Cruickshank CTO and Co-founder Revolution Aerospace

Version History

Version	Release Date	Description
1.0	31 January 2024	Initial Release

Contributions

The Guideline has drawn on many different sources of DAA research, development, standardisation, and guidance material across the globe including information produced by the following organisations:

- RTCA
- ASTM
- JARUS
- FAA
- MIT
- EASA

Use and Licensing

Attribution

When attributing this publication (and any material sourced from it), the following wording should be used:

References:

[1] T. Putland, T. Martin, A. McLaren & K. Cruickshank, "*Detect & Avoid Design, Test & Evaluation Guideline-Appendix E,*" Revolution Aerospace, Brisbane, Queensland, Australia, January 2024.

Acknowledgments:

The authors and Revolution Aerospace gratefully acknowledge the following organisational support for completion of the DAA document package:

- Grant funding from the Australian Department of Infrastructure, Transport, Regional Development, Communications
- In-kind Support from the Queensland Government through Trusted Autonomous Systems (TAS), a Defence Cooperative Research Centre funded through the Commonwealth Next Generation Technologies Fund and the Queensland Government.

Disclaimer

Contents

List of Figures

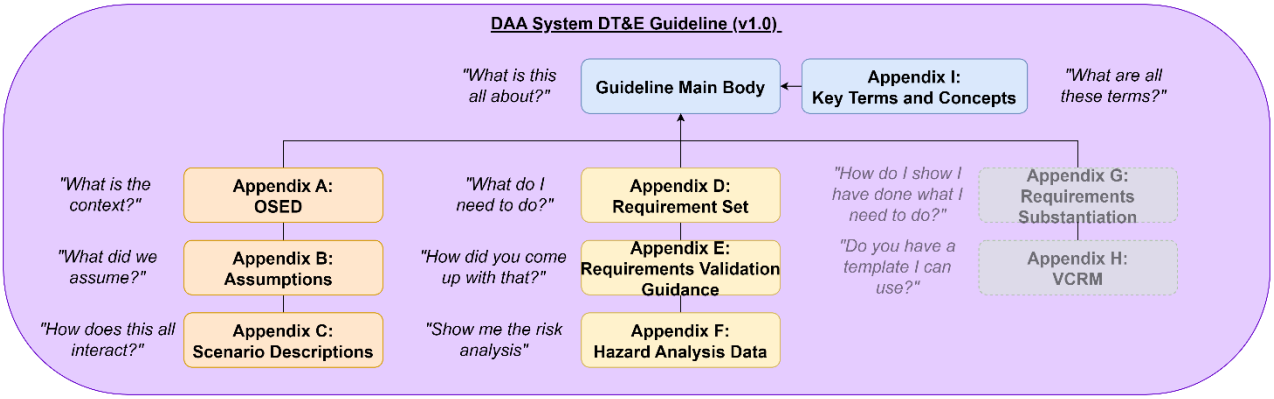
List of Tables

Forward

Figure 1 depicts the placement of the Requirement Set and Requirements Definition documents within the broader structure of the DAA DT&E Guideline, consisting of the Main Body and associated Appendices.

The Requirement Set outlined in Appendix D, constitutes an integral component of the comprehensive DAA DT&E Guideline Package. The aspiration is for these requirements to eventually contribute to the formulation of a future design standard, serving as a foundation for the development and testing of Detect and Avoid Systems. This document elucidates the process of deriving the requirements set, providing the rationale and justification for all safety requirements encompassed in the overall guideline.

Figure 1: DAA DT&E Guideline Document Hierarchy



The development of a DAA System that aligns with these requirements is strongly discouraged until the complete Guideline, along with all Appendices, is published. However, this initial release aims to initiate discussions within the UAS community in Australia and beyond, fostering dialogue on DAA performance requirements and verification. RevAero and TAS welcome commentary on this document and its associated requirements.

1 Introduction

This document outlines the derivation process for a comprehensive set of high-level, functional, safety, and analysis requirements tailored for a Detect and Avoid (DAA) system integrated into Uncrewed Aircraft Systems (UAS).

The primary objective of this Requirements Validation Guidance document is not to furnish a complete safety argument for the design, production, and operation of a DAA-equipped UAS. Instead, it provides a detailed rationale for the derived requirements, establishing a high level of traceability up to globally recognized DAA safety objectives advocated by key regulatory agencies like the FAA and EASA.

Notably, this document includes an assurance argument demonstrating how adherence to the requirement set in Appendix D aligns with the crucial 'Avoid Air Traffic' function. This function is often considered the primary risk control for a UAS to prevent Mid-Air Collisions (MAC) and forms the foundation of high-level safety objectives.

The information presented in this document is particularly useful for designers and operators seeking approval for Beyond Visual Line of Sight (BVLOS) operations in uncontrolled Class G airspace below 10,000 feet Above Mean Sea Level (AMSL) at an Air Risk Class (ARC) of ARC-c. It can be incorporated into their safety case within the application process.

This Requirements Derivation document, along with the resultant Requirements Set in Appendix D, has been developed with reference to the Operational Services and Environment Description (OSED) provided in Appendix A of the Guideline. It's crucial to note that the derived requirements outlined in this document are valid only within the context of the OSED. Any deviations from this context require further safety analysis to assess their impact, subsequently necessitating a re-validation or supplementation of the Requirement Set.

Throughout the document, uniquely identified requirements are consistently carried through to the Requirement Set detailed in Appendix D.

1.1 Overview of Requirements Architecture

This document is structured into three major sections, aligning with the top-down investigation process that has guided the requirements derivation activity:

- **Section 2** Establishes the **hazard and risk context**, articulating the societal expectation of safety that propels the overall need for this endeavour. The high-level detect and avoid objective is then contextualised using the expected operating environment (outlined in the OSED at Appendix A). This section then identifies relevant hazards and hazard models, forming the basis for system-level requirements crucial for subsequent risk assessments**.**
- **Section 3** Utilises the context and core requirements from the previous section to conduct key **hazard analyses**, including an Operational Hazard Analysis (OHA) and a Functional Hazard Analysis (FHA). Controls identified in the OHA

shape requirements across the entire spectrum of operational risk mitigation, while the FHA drives functional and system safety requirements for the UAS and DAA system.

- **Section 4** focuses on **functional requirements validation**, specifically for those requirements derived from the risk analyses conducted above. This completes the Requirement Set within this Guideline, providing the supporting rationale for their creation.

Figure 2 visually illustrates the interconnections between all the sections:

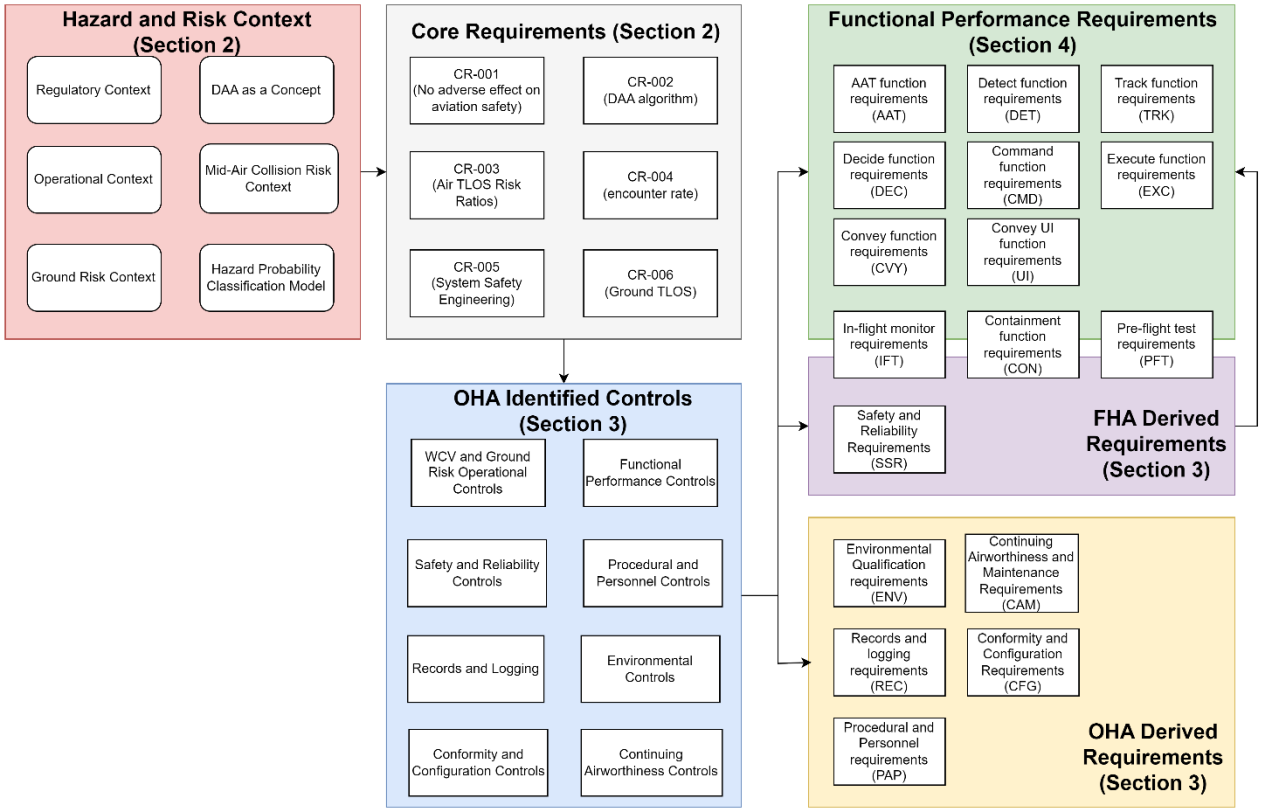


Figure 2: Requirements Derivation and Document Architecture

1.1.1 Key Terms and Concepts

A comprehensive suite of key terms used throughout the Guideline can be found in Appendix I.

2 Establishing the Hazard and Risk Context

The first step in the risk management process is to establish the hazard and risk context. In this document, this will be done through:

- Summarising the regulatory context (Section 2.1), which drives the expectations of aviation safety globally and in Australia.
- Summarising the operational context (Section 2.2), driven by the OSED at Appendix A to this Guideline. This section highlights:
    - the traffic types and characteristics important to DAA,
    - the airspace classes, altitudes, and other aviation related parameters,
    - the expected clutter in the environment, and
    - the expected background environment.
- Reviewing the general concept of Detect and Avoid (Section 2.3) system being used as a mechanism to replace the crewed aircraft equivalence for collision avoidance and separation obligations in uncontrolled airspace.
- Deriving a set of core functions that execute the above-mentioned goals, before identifying how they may fail to support derivation of relevant operational hazards for a DAA system (Section 2.4).
- Determining the risk associated with a Mid-Air Collision (Section 2.5). This includes:
    - the definition of hazard severity for MACs based on accepted conventional aviation hazard severity classifications and the TLOS,
    - the definition and determination of Target Levels of Safety for crewed aircraft based on the regulatory context.
    - providing a means to model events that lead the airspace hazards identified by defining a probabilistic collision risk model, and establishing the key model parameters:
        - Unmitigated probability of causal events leading to a collision
        - Risk ratios as key performance metrics for a DAA system mitigating the risk of a collision
        - The encounter rate (natural and induced).
- Determining the risk associated with ground impact (Section 2.6), including:
    - The hazard severity associated with a ground fatality.
    - Defining a ground risk model, and establishing the key model parameters.

This section of the analysis utilises the discussions on the risk and hazard context to derive high level safety requirements that will be utilised throughout the rest of this Guideline. The outcome of this section is a set of **core requirements**, which provide the necessary traceability to ensure that an acceptable level of safety is met by a compliant DAA system under this guideline.

This section also uses the hazard and risk context identified in the preceding sections as a basis for developing a Hazard Probability Classification Model (Section 2.7), which leads to the determination of Design Assurance Levels necessary to substantiate risk controls against various hazards associated with the DAA system, which will be used for other analyses in this document.

2.1 Regulatory Context

2.1.1 International Regulatory Context

Under the rules developed by the International Civil Aviation Organisation (ICAO), it is a requirement for aircraft bearing the nationality and registration marks of a contracting state to comply with Annex 2 of "*the ICAO Convention*" [1] to the extent that these rules do not conflict with specific Contracting State rules of any overflown territory (Subsection 2.1 of [1]). This usually results in states issuing rules and regulations that align with [1], such that this Annex becomes the rules of the air for most states.

Under Section 3 ("*General Rules*") of ICAO Annex 2 there is an inherent responsibility for a pilot-in-command to avert collisions when they arise. This set of requirements introduces the concept of remaining "well-clear" and giving way to aircraft (that have right of way) in order to reduce the probability of a collision occurring between two aircraft. This results in the following characterisation of requirements:

- Requirement to avoid collisions (note that most states stipulate this as a requirement to "See and Avoid (SAA)" other aircraft).
- Requirement to "Remain Well Clear (RWC)" of other aircraft.
- Requirement to give way to aircraft with the right of way.

These requirements apply to any operation of conventionally piloted aircraft (i.e., VFR, special VFR, or IFR flights) Subsection 2.2 of Annex 2 of [1].

2.1.2 Rules and Regulations for Crewed Aircraft and UAS in Australia

Whilst this Guideline is intended to assist internationally with the design, development, testing and evaluation of DAA systems, the following section focuses specifically on the Australian legislative context for the operation of UAS[1].

For **crewed aviation** in Australia, general flight rules apply under Part 91 of the *Civil Aviation Safety Regulations 1998* (CASR). Under Subdivision 91.D.4.4, requirements are placed on operators of aircraft to avoid collisions by maintaining vigilance to "*see and*

[1]Other countries will need to consider how their own legislative requirements may apply to DAA.

avoid" other aircraft[2], and for "*keeping clear*" of other aircraft[3]. These collision avoidance rules are a significant part of any safety case argument for the operation of an aircraft in Australia (particularly when operating under VFR) and are part of CASA's means of compliance with Annex 2 of the Convention.

For **Australian UAS**, the relevant regulations are found under Part 101 of CASR, and they are specifically exempt from complying with the above-mentioned Part 91 via Regulation 91.030. This means that the crewed aviation regulations for "*see and avoid*" and "*keeping clear*" are not applicable. Instead, UAS are limited in their ability to operate by Regulation 101.073. This requires all UAS operations to be undertaken within the Visual Line of Sight (VLOS) unless the operator holds an approval to operate Beyond the Visual Line of Sight (BVLOS) under Regulation 101.029.

Regulations 101.029 and 11.055 of CASR are interrelated. A BVLOS approval under Regulation 101.029 is subject to Regulation 11.055, which details the considerations CASA must take when issuing such an approval. Key among these is Sub-regulation 11.055(1A) (e), which states that CASA may grant the authorisation only if "**granting the authorisation would not be likely to have an adverse effect on the safety of air navigation.**" This regulation implies that any aircraft operating in Australia under either VFR or IFR, regardless of equipage, are entitled to an acceptable level of safety based on their compliance with the current rules and regulations for operating conventionally piloted aircraft. This key regulatory criterion will be used as the high-level safety goal for a DAA system being operated in Australia under the CASR.

2.1.3 Requirements Generated by Regulatory Context

Table 1: Requirements Generated by the Regulatory Context

Req. ID	Requirement Text	Rationale
CR-001	The DAA system shall provide an equivalent level of safety to other airspace users and people on the ground as is currently expected due to crewed aviation activities in uncontrolled Class G airspace.	From CASR 101.029 and 11.055, the key criterion for granting an authorisation is driven by ensuring that granting the authorisation does not have an adverse effect on the safety of air navigation.

2.2 Operational Context

Appendix A to this Guideline, the Operational Services and Environment Description (OSED) provides a detailed description of the interned operational environment, however in particular, the following key operational characteristics are repeated in Table 2 for convenience:

[2] CASR 91.325.
[3] CASRs 91.330, 91.335 and 91.340.

Table 2: Select, Key OSED Assumptions

OSED Reference	Assumption	Rationale
Ownship Assumptions		
ASSUMP-OSED.3	The DAA System will use an EO/IR detection subsystem.	While there are many possible sensor options for detecting non-cooperative intruders, this safety case, and the broader DAA guideline, assumes that EO/IR is the only feasible current technology to achieve the required declaration ranges for a small SWaP DAA system.
ASSUMP-OSED.5	Aircraft characteristic dimension will not exceed 8m.	For the probabilistic value for a Mid-Air Collision (MAC) on the condition of Near Mid-Air Collision (NMAC) used in this document (i.e. (0.01 derived from [[2]) to be valid the total wingspan of both intruder and UAS must be less than 100ft. By restricting the UAS wingspan to less than 8m (approximately 26ft), the majority of intruder aircraft in uncontrolled airspace will have wingspans less than 74ft (approximately 23 m, almost the wingspan of a Fokker 50 aircraft)
ASSUMP-OSED.6	The Ownship is equipped with ADS-B (In) as a component of the DAA system supporting deconfliction with cooperative Intruders.	It is not expected that all intruders will carry ADS-B (Out). However, when they do, its expected the DAA system shall be capable of receiving ADS-B transmissions.
Intruder Assumptions		
ASSUMP-OSED.14	Intruders are not equipped with any DAA system and therefore will not coordinate DAA functions to stay well-clear from or avoid collisions with the Ownship in nominal operating environments.	The burden of avoiding a potential collision cannot be transferred to other aircraft.
ASSUMP-REQV.1	If an intruder is impacted by the Ownship, both aircraft will have hull losses, and all persons on board the intruder will be fatally injured.	Without more information, it is a conservative assumption that a MAC will result in the worst case consequence. For larger Ownships, it is considered very plausible that this occurs.
Operating Airspace Assumptions		

OSED Reference	Assumption	Rationale
ASSUMP-OSED.21	The UAS will operate in Class G Airspace and will integrate other Class G traffic.	Uncontrolled airspace users are not provided air traffic separation services (although some limited services can be provided if requested of ATC and if ATC are able to accommodate the workload). As it cannot be assumed that any ATC services will be available across the entirety of Uncontrolled Airspace, this affects the severity classification of an aircraft on a collision course without a functioning DAA system. The airspace class also drives the expected mix of aircraft types, encounter rate, and encounter types.
ASSUMP-OSED.26	The UAS will operate in AEC 5 airspace, per the JARUS SORA; namely, class G airspace, outside of airport environments, and over rural areas.	The 'airport environment' is an undefined term qualitatively, capturing the volume around an airport where the airport environment's structure (approach and departure paths, circuits etc.) have a meaningful effect on the nature of aircraft flight paths. Within this region, encounters can be considered "correlated" with one another (and to the airport environment structure). To reduce complexity of this guideline, only uncorrelated encounters, outside of the airport environment, are considered.
ASSUMP-OSED.28	The Ownship may operate up to a ceiling of 10,000ft AMSL.	In many nations, operations within Class G and E airspace are restricted to operating below 250 knots indicated airspeed when below 10,000ft AMSL (specifically ss. 4.02 of Part 91 Manual of Standards for Australia). This ensures that the speed differential between intruder and Ownship is restricted.
ASSUMP-OSED.30	The operation of the DAA system is assumed to be under Visual Meteorological Conditions (VMC). Specifically, Day VFR conditions.	Applicants will be required to demonstrate they can maintain VMC as part of their individual safety case, to a level commensurate with the hazard severity, to the satisfaction of the competent authority.

OSED Reference	Assumption	Rationale
ASSUMP-REQV.2	Well Clear Violation Rate will not exceed 1 encounter per 100 hours (0.01 encounters per hour).	As part of the external event probability equations used to reduce the quantitative probability of failure, a maximum Well Clear Violation rate of 1 per 100 hours is assumed. In order to meet TLOS expectations through the system safety objectives using the risk ratios defined by ASTM and other institutions, this WCV rate must not be exceeded. However, due to recent research by MITRE [3] indicating some variability in encounter rates across uncontrolled airspace, it is the applicant's responsibility to ensure that the operational area/location where the DAA system is deployed does not exceed this encounter rate. To that end, the applicant must demonstrate to the authority how they make that determination, as part of their individual safety case. If this value is exceeded, additional analysis is necessary to re-evaluate quantitative probabilities due to the increase in external event frequency, and the increase in induced detected intruders. It is recommended that the applicant work with the competent authority to make this determination.

2.3 Detect and Avoid as a Concept for Meeting Regulations

To accurately assess the effectiveness of any DAA system, we need to understand the overall concept of its operation. Put simply, we need the DAA system to detect air traffic, and subsequently implement manoeuvres or some other action to avoid it. To ensure this concept is appropriately specified and complete, we must:

- clearly articulate the goals or objectives of a DAA system,
- formally decompose the functionality of the DAA system into functional requirements based on these goals,
- ensure that the specified requirements are comprehensive in achieving the goals whilst ensuring that there are no superfluous requirements, or unintended functions added by implementing the requirements.

There have been many documents written and activities undertaken by the UAS community with the intent of addressing the above. This section will summarise key

documents and findings that underpin a set of DAA objectives and functional decompositions that we feel meet the criteria above and are included as part of this guideline.

2.3.1 Overarching Objectives of a DAA System

In 2013, the Federal Aviation Administration (FAA) SAA second caucus workshop meeting report [2] detailed the following high-level objectives for a sense and avoid algorithm (in order of precedence):[4]

1. Prevent Mid Air Collisions
    a. Avoid collisions.
    b. Reduce risk of collision by remaining well clear.
2. Do No Harm
    a. To airworthiness of Ownship.
    b. To coordination between encountering aircraft.
    c. To interoperability within the National Airspace System (NAS).
    d. To ATC operations.
3. Do Not Impede
    a. Minimise disruption to the NAS.

2.3.1.1 Goal 1(a) – Avoid Collisions

The first listed goal is self-evident, and clearly meets the intended goal of a Detect and Avoid system.

2.3.1.2 Goal 1(b) – Reduce Risk of Collisions by Remaining Well Clear

The second goal is driven by the logical flow of causal events leading to a collision. The greater the range an Ownship is from another aircraft, the less likely it is that a collision event will occur (i.e., all other events are more likely). This is reflected in airspace risk management hazard severity definitions where the severity of a Loss of Separation between two aircraft is less than the severity of a Near Mid-Air Collision between two aircraft, due to the proximity of each aircraft to one another.

2.3.1.3 Goal 2(a) – Do No Harm to Airworthiness of Ownship

This goal is a corollary to the overall intent to improve safety for UAS operations. The safety benefit from the implementation of a Detect and Avoid capability is eliminated if that system degrades airworthiness of the Ownship.

2.3.1.4 Goals 2(b) & 2(c) – Do No Harm to Coordination Between Encountering Aircraft. Do No Harm to Interoperability Within the National Airspace System (NAS)

In the realm of Sense and Avoid systems, these objectives entail ensuring predictability and agreement between aircraft and the Air Traffic Management (ATM) system during manoeuvres. Essentially, this involves establishing universally understood rules followed by all aircraft, fostering reliance on expected behaviours by operators of each aircraft.

[4] Conclusion C 5.1 of [2]

In the specific scenario of operations within uncontrolled airspace below 10,000 feet in the current state of Australian airspace equipage requirements, direct coordination between crewed aircraft systems and the DAA system is unlikely. Moreover, it is anticipated that crewed aircraft may struggle to visually acquire a UAS within the necessary time and range for conflict resolution manoeuvres. Despite these challenges, it remains imperative for a UAS to execute manoeuvres in a predictable and expected manner, adhering to give-way rules as reasonably practicable.

For the purpose of this Guideline, the assumption is made that any intruder aircraft will not coordinate with the UAS (ASSUMP-OSED.14), and the Ownship must prioritize giving way to all aircraft to ensure safety objectives.

It's important to note that above 5,000 feet in uncontrolled airspace and for any IFR aircraft, radio communications become possible (although coordination is not mandated or standardized). While this may contribute to coordination between the two aircraft, it is not considered a required input for the functioning of a DAA system. Instead, it should be viewed as part of broader operational procedures and processes aiding conflict resolution, as outlined in the OSED at Appendix A and the Operational Scenario Descriptions at Annex C to the Guideline.

An additional consideration noted in the FAA report [2] is that interoperability is driven by the harmonisation of any algorithms implemented to avoid other aircraft, and that the standardisation of manoeuvres should be developed and established.

2.3.1.5 Goal 2(d) – Do No Harm to ATC Operations

Whilst this goal is important for operations in the overall NAS, it is not relevant within the context of this Guideline. A key operational assumption within this Guideline (ASSUMP-OSED.28) is that operations are limited *to Class G airspace, below 10,000ft AMSL and outside of airport environment*[5]. In this environment, it is expected that the impact of a DAA system on ATC operations is low and does not warrant further consideration, as ATC are not required to provide separation services in Class G airspace.

2.3.1.6 Goal 3(a) – Minimise Disruption to the NAS

Similar to Goal 2(d), this goal is much more focused on more complex and structured airspace (i.e. operations in controlled airspace under ATC control, or airspace with significant airspace use). Under the operational context of this guideline, this minimisation is only able to be done by minimising the deviation of any manoeuvre to prevent another interaction with another aircraft. Although this should only be undertaken, if possible, as the priority of goals requires the avoidance of the primary threat first.

2.3.1.7 Additional Goal– Do No Harm to 3rd Parties on the Ground

An additional goal must be added to ensure that the DAA system does not create additional hazards for persons on the ground. To be clear, this is not an objective to prevent ground collisions as part of a ground collision avoidance system, but purely an

[5] Specifically, the Assumption identifies Aircraft Encounter Class (AEC) 5, per the JARUS SORA [14].

objective that is intended to prevent unwanted additional ground risk by undertaking a manoeuvre that will cause the aircraft to impact the ground when attempting to satisfy Goals 1a and 1b of the SAA algorithm objectives.

2.3.1.8 Goals Summary

From this discussion we can modify the FAA-derived DAA algorithm objectives to suit the operational context specified for this guideline simply by removing goal 2(c) and 2(d). This is reflected in core requirement 2 (CR-002).

These high-level goals will be used as the basis for evaluating the performance of a DAA system, and result in one of the core requirements for the Requirement Set.

2.3.1.9 Requirements Generated by Detect and Avoid System Goals

Table 3: Requirements Generated by the Detect and Avoid System Goals

Req. ID	Requirement Text	Rationale

CR-002	The DAA system shall attempt to:
	• Prevent Mid Air Collisions:
	  ○ Avoid collisions.
	  ○ Reduce the risk of collision by remaining well clear.
	• Do No Harm:
	  ○ To airworthiness of Ownship
	  ○ To coordination between encountering aircraft
	  ○ To third parties on the ground
	• Do Not Impede:
	  ○ Minimise disruption to the National Airspace System
		These are high level goals of a DAA system, derived from the findings of the FAA Sense and Avoid Second Caucus Workshop [2]. These are the root "goodness" values of the DAA system.

2.4 DAA Functions and Hazards

2.4.1 The Avoid Air Traffic Function

The preceding section outlined the goals or desired outcomes that a Detect and Avoid (DAA) system should aim to accomplish. The focus of this section is to delineate the definition of the functions that must be executed by a DAA-equipped Unmanned Aircraft System (UAS) to realize the aforementioned outcomes.

From the standpoint of systems engineering, any safety-critical aircraft system endeavours to perform "aircraft-level functions." These functions represent the highest level of operation, encompassing the integration of technical systems, personnel, and organizational elements necessary for the safe operation of an aircraft. NASA [4] has

established a hierarchy of aircraft-level functions, providing a structured framework to comprehend these high-level functions, as illustrated in Figure 3:

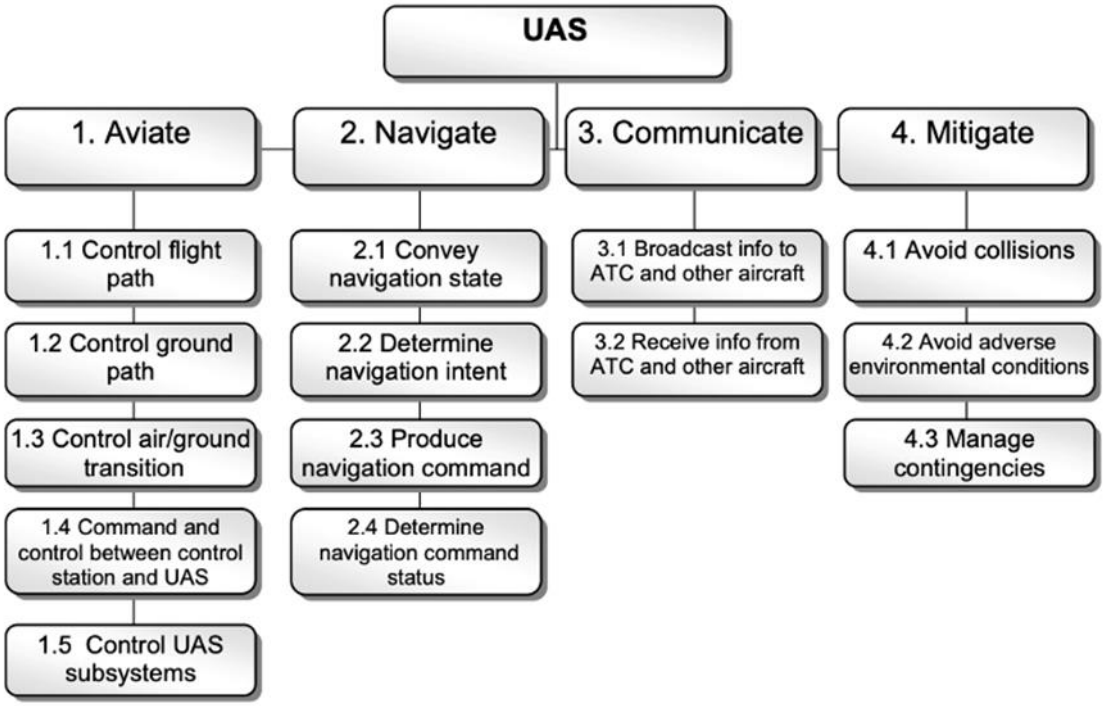


Figure 3: Top-Level UAS Functions, reproduced from [4] with permission from NASA, p.16.

While the terms Detect and Avoid (DAA) or Sense and Avoid (SAA) are universally employed to describe systems implementing traffic avoidance, our functional perspective specifically centres on the aircraft-level function **4.1** "Avoid Collisions," as depicted in the preceding figure. NASA [5] further breaks down this function into several subfunctions, illustrated in Figure 4. When addressing the overarching concept of avoiding air traffic, this guideline specifically refers to the Avoid Air Traffic (AAT) function, denoted as item **4.1.1** in the aforementioned figure. This function is further decomposed by NASA per [4] into several subfunctions, per Figure 4.

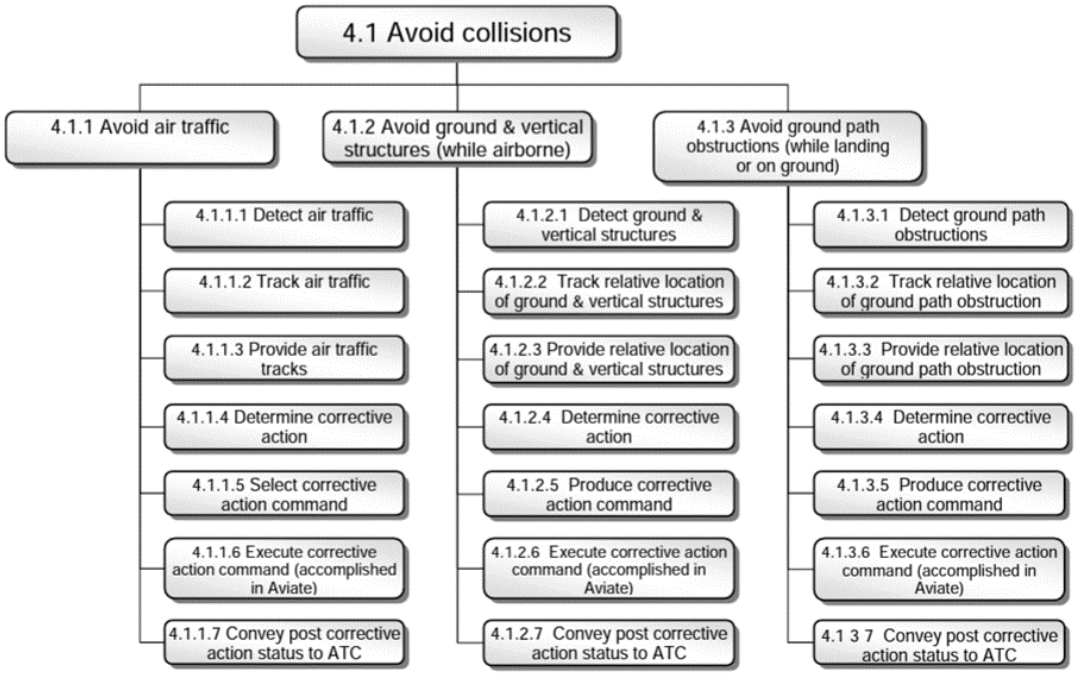


Figure 4: Avoid Collisions Function Decomposition, reproduced from [4] with permission from NASA, p. 19.

The detailed breakdown of item 4.1.1 in the NASA paper and Figure 4 offers a way to further decompose the function into subordinate elements. However, various standards, including JARUS [5], FAA at [2] and ASTM at [6], have presented alternative decompositions of this AAT function.

In this guideline, we propose a distinct set of core functions that **closely align with the JARUS Tactical Mitigation Performance functions**, as outlined in Table 4 below. Notably, our proposal deviates slightly by incorporating a delineation of the core activities that a DAA system must undertake. Additionally, it includes supporting functions to ensure the continued safe functioning of the core functions outlined by FAA and ASTM. Section 3.2.2 provides further detail on this proposal.

Table 4: Core AAT Function Definitions

Core AAT Function	Description
Detect	The Detect Function ingests sense data from the external environment, filters the data as required, and outputs any detected object of interest's data (i.e., an estimate of the detect objects position in space) to the Track Function (via the Convey Function).
Track	The Track Function's purpose is to create, update, and remove tracks (i.e., correlate detect data into identified objects movement in space and time within a range of the Ownship) and then provide tracked objects data (i.e., position, velocity, heading) to the Decide Function via the Convey Function.

Core AAT Function	Description
Decide	The Decide Function's role is to classify and prioritise tracked objects as threats (i.e., may pose a collision risk), and to then, if necessary, calculate the most appropriate alerting and manoeuvre and guidance to the Command Function.
Command	The Command Function's purpose is to issue a manoeuvre command, based upon the received alerting and manoeuvre guidance from the Decide Function. This Command Function can be: • Human induced (i.e., a remote pilot provides the manoeuvre command). • Automated (i.e., the UA commands the aircraft to manoeuvre based on the guidance and alerts the remote pilot to this occurring).
Execute	The Execute Function receives a command and executes the command to physically control the aircraft through the manoeuvre.
Convey	The Convey Function provides the interface between each of the previously mentioned functions and any other UAS functions and ensures all required DAA information is provided to the remote pilot.

These proposed functions still retain a degree of alignment with the NASA subfunctions, as well as those developed by the FAA SAA Workshop and by ASTM. This is illustrated below in Table 5 with some simplifications.

Table 5: Comparison of AAT Functional Decompositions

<table>
<tr><th>Proposed Core AAT Functions</th><th colspan="3">JARUS Annex D to SORA – TMPR Functions [5]</th><th>NASA – FHA [4]</th><th>FAA – SAA Workshop [2]</th><th>ASTM – F3442M-20 [6]</th></tr>
<tr><td>Detect</td><td rowspan="7">Convey</td><td rowspan="3">Detect</td><td rowspan="6">Feedback Loop</td><td>Detect Air Traffic</td><td>Detect</td><td rowspan="3">Detect Function (DF) (7.1)</td></tr>
<tr><td>Track</td><td>Track</td><td rowspan="2">Track</td></tr>
<tr><td></td><td>Provide Tracks</td></tr>
<tr><td>Decide</td><td rowspan="3">Decide</td><td rowspan="4">Determine Corrective Action</td><td>Evaluate</td><td rowspan="4">Alert Function (A1F) (8.1.1)</td></tr>
<tr><td></td><td></td><td>Prioritise</td></tr>
<tr><td></td><td></td><td>Declare</td></tr>
<tr><td></td><td></td><td>Determine</td></tr>
<tr><td>Command</td><td colspan="2">Command</td><td>Select Corrective Action</td><td>Command</td><td rowspan="2">Avoid Function (A2F) (9.1.1</td></tr>
<tr><td>Execute</td><td colspan="2">Execute</td><td>Execute Corrective Action</td><td>Execute</td></tr>
</table>

These defined functions are used as the basis for functional requirements derived across the Guidance Document suite.

2.4.2 Functional and System Representations of UAS Operations

It is crucial to differentiate between the functional and system representations of a UAS operation. Functions refer to tasks, processes, algorithms, or similar elements essential for aircraft operation. Safety-critical functions are those contributing to or controlling system-level safety hazards. In the design of a UAS, safety-critical functions materialize through systems, subsystems, and components. Best practices in system safety and systems engineering involve designing and defining functions to the required level and then allocating aircraft systems (subsystems or components) to these functions, along with defining the interfaces between functions and systems.

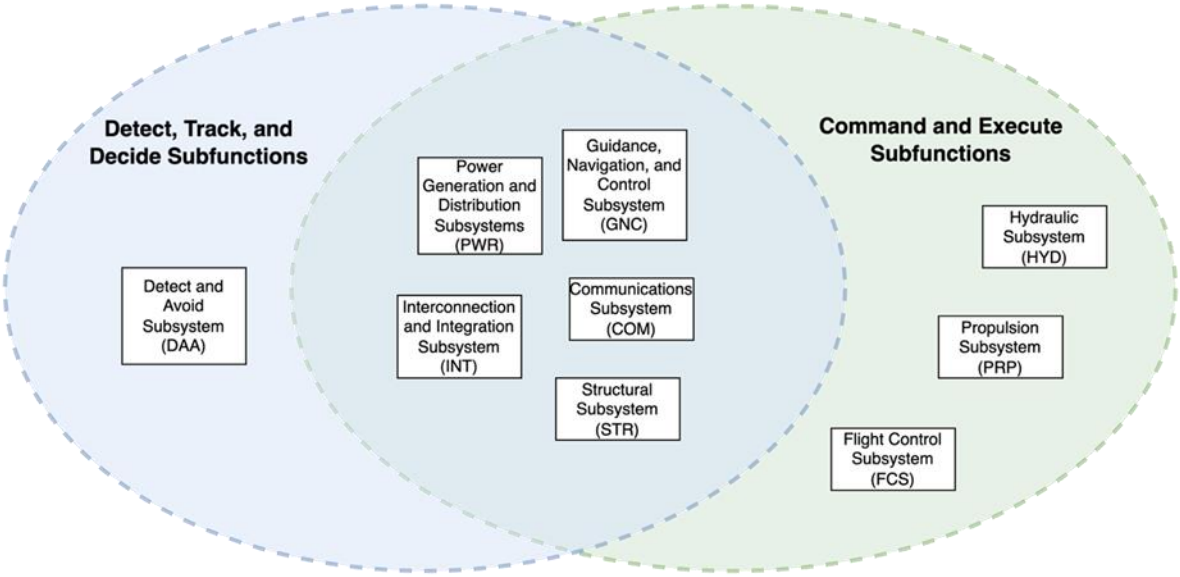


Figure 5: Functions vs Systems

For instance, the AAT functions may find support from a range of DAA and aircraft subsystems, as illustrated in Figure 5. Given that the AAT function involves actions from nearly every subsystem onboard a UAS, specifying the attribution of functions to subsystems can be challenging. For clarity, the following definitions will be consistently used throughout this guideline.

- The **AAT Function**: Encompasses processes and algorithms that implement the desired objectives of a DAA capability, encompassing both core and supporting functions.
- The **UAS**: Represents the remainder of the physical system, including those implementing parts of the AAT function that are not considered part of the DAA system.
- A **DAA equipped UA**: Denotes a **UAS** with a **DAA system** installed, featuring a functioning **AAT Function**.

- The **DAA System**: Comprises additional components and subsystems necessary to be added to a UAS to implement the AAT function [6].

2.4.3 Functional Reliability and System Safety

As described in ARP 4754A [7], a function can fail from two different causes:

1. An error in the development of the function, or
2. Anomalous behaviour of the systems used to manifest a function.

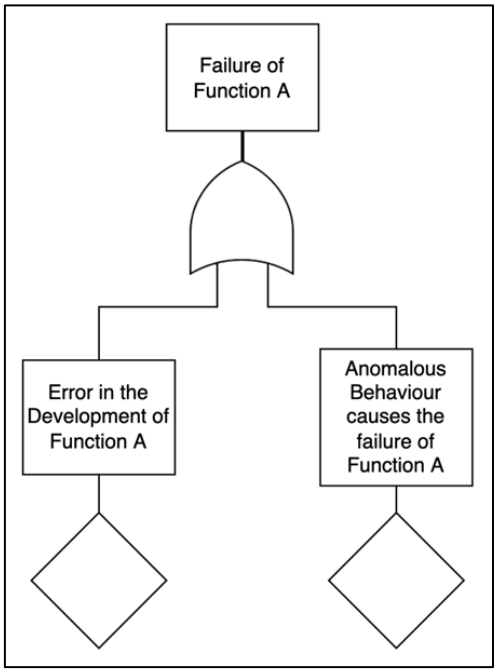


Figure 6: Different Ways in Which a Function Can Fail

This representation will be used to support requirements derivation during the FHA process in Section 3.2.

The first point captures the errors (which cause a loss or malfunction of the intended function) that can be introduced when taking conceptual needs of the system and translating them into written/documented system requirements and then development of the functionality. That is, an error can be introduced into the system requirements themselves at any point during the requirements analysis process.

The second point captures the systemic (i.e., errors in the engineering process) and environmental failures (e.g., random failures, wear-out failures) of systems that can

[6] The specific subsystems and components considered as part of the DAA System will likely vary depending on the UAS to which it is fitted. E.g., a UAS with an incompatible GPS would require a standalone module to be fitted as part of the DAA System, whereas for a UAS with a compatible GPS, the DAA system would not include a GPS, but would interface with the GPS subsystem, which is considered part of the UAS.

cause the loss or malfunction of the function. These two failure paths can be represented using a fault tree, as shown in Figure 6:

2.4.4 An Operational hazard List for DAA Systems

Given the operational context and the concept of a DAA system and AAT function, it is now possible to construct an operational hazard list which will be used throughout this guideline to inform requirements and analyses. The FAA in [8] identified four key hazards associated with a DAA system:

OHAZ-1: Failed or inadequate manoeuvre when one is required.

This hazard is the most obvious one when considering implementing a DAA system, i.e., when it does not have the positive outcome compared to a situation where the DAA system is not used (but no negative outcome). This can lead to a loss of well clear, an NMAC, or in the worst case a MAC and potential ground fatalities.

OHAZ-2: Increased collision risk from manoeuvre.

This hazard is similar to OHAZ-1 a manoeuvre of this nature can lead to a loss of well clear, an NMAC, or in the worst case a MAC and potential ground fatalities. Importantly, this hazard is differentiated from OHAZ-1 due to the increase of the chance of subsequent events compared to OHAZ-1 (i.e., the DAA system manoeuvres in such a way to increase the chance of a loss of well clear, NMAC, or MAC).

OHAZ-3: Secondary effects from manoeuvre.

The key feature of this hazard is worsening safety outcomes due to a manoeuvre that successfully avoids the initial encounter. In particular, the following events are identified:

- A manoeuvre leads to an induced encounter (i.e., an encounter that would otherwise not have occurred but for the execution of the manoeuvre to avoid another aircraft). This encounter could lead to a potential loss of well clear, NMAC or MAC, and then potential ground fatalities.
- A manoeuvre that leads to the Ownship exceeding its flight envelope or some other restriction on its operation, potentially leading to the loss of control of the aircraft (e.g., stall, or structural failure). In this case, the most likely outcome is a ground impact, potentially leading to fatalities on the ground.
- The combination of Ownship position and determined manoeuvre results in controlled flight into terrain of the Ownship, potentially leading to fatalities on the ground.

OHAZ-4: False alerts.

This final hazard is a consequence of trying to implement a detection and classification system. By increasing detection sensitivity to maximise successful detection and tracking of genuine targets, the rate of false detection of targets also increases (and is non-zero). These detections may lead to unnecessary avoidance manoeuvre against a

false target, which could then cause any of the effects listed in OHAZ-1, OHAZ-2, OHAZ-3.

2.5 Mid-Air Collision Risk

This section aims to explore the repercussions of a Mid-Air Collision between two aircraft and initiate the derivation of risk characteristics associated with such collisions. The analysis conducted here serves as the qualitative and quantitative foundation for subsequent safety assessments within this document.

This section begins with defining the qualitative definition of hazard severity related to a Mid-Air Collision aligned with global standards, to allow allocation of design rigour based on the AAT function failure conditions that lead to a Mid-Air Collision.

Following this, Target Level of Safety (TLOS) is defined, distinguishing between predominantly air transport and Instrument Flight Rules (IFR) aircraft, and that of predominantly general aviation and Visual Flight Rules (VFR) aircraft. These TLOS considerations are significantly influenced by the regulatory mandate that "UAS operations shall not have an adverse effect on the safety of air navigation."

With a quantitative determination of acceptable Mid-Air Collision rates established, this section proceeds to articulate a collision risk model. This model facilitates the mathematical representation of the causal chain of events leading to Mid-Air Collisions.

The discussions and conclusions drawn in this section will permeate subsequent analyses, playing a pivotal role in shaping the core requirements of the Detect and Avoid (DAA) System.

2.5.1 Airspace Event Hazard Severity Model

All safety claims should be defensible commensurate with the severity of worst credible failure conditions. Across nearly all industries, as the severity of an event increases, higher certainty of risk control effectives is needed; that is, the rigour of the safety case argument must increase as hazard severity increases.

In the case of a DAA System per this Guideline, the acceptance of residual uncertainty based upon the severity of a hazard should be commensurate with current accepted practices for system safety engineering in aviation. Specifically, airspace event severity levels (consequences) in this analysis should align with internationally agreed hazard severity levels for equivalent risk. This analysis will refer to the Federal Aviation Administration UAS Safety Risk Management (SRM) Policy, Order 8040.6A [9]. This document provides a UAS-specific SRM context for the application of assurance activities based on the severity level of a hazard.

Table C-1 (p. C-1) of the Order details a way to correlate the number of fatalities of an event to the severity. This is reproduced for reference at Table 6, below:

Table 6: Hazard Severity, reproduced from [9], table C-1.

Minimal 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
Negligible safety effect	An expected unintentional effect that includes any of the following: • 1-2 minor injuries • Minor damage to manned aircraft • Substantial damage to unmanned aircraft weighing at least 55 pounds	An expected unintentional effect that includes any of the following: • 1-2 serious injuries • 3 or more minor injuries • Substantial damage to manned aircraft • Hull loss to unmanned aircraft weighing at least 55 pounds	An expected unintentional effect that includes any of the following: • 1-2 fatalities without manned aircraft hull loss • Manned aircraft hull loss without fatalities • 3 or more serious injuries	An expected unintentional effect that includes any of the following: • 3 or more fatalities • Manned aircraft hull loss with at least 1 fatality

It must be assumed that any MAC between the Ownship and an intruder will cause the loss of both aircraft, fatally injuring all people inside the aircraft.

An additional note in [9], for Table C-1 reproduced above, explains that it is possible to classify a mid-air collision as Hazardous, so long as the aircraft is likely to only encounter aircraft with fewer than three people on board.

However, for aircraft with more than three people on board, the hazard severity must be classified as Catastrophic. For the operational context of this Guideline, it cannot be claimed definitively that an encountered aircraft will have fewer than 3 people. Hence, for the purposes of this guideline, a Mid-Air Collision will always be treated as a Catastrophic event.

2.5.2 Target Levels of Safety for Airspace Hazards

A hazard severity metric itself does not fully allow the design of systems that meet these quantitative requirements (alongside other qualitative requirements). We need to understand the acceptable level of rigor required to demonstrate that enough has been done to mitigate an identified hazard.

A Target Level of Safety is a metric that quantifies the maximum allowable level of risk (or conversely, a minimum level of safety assurance) for a given hazard. This quantitative baseline can be used to drive safety analysis and design requirements.

When considering airspace hazards, we are specifically dealing with the hazard of a MAC. To ensure the TLOS is appropriate, it is necessary to recall the regulatory goal to "not have an adverse effect on the safety of air navigation", and so consequently to ensure that incidence rate for MACs between UAS and crewed aircraft is equivalent to that of MACs between two crewed aircraft.

The 2nd Sense and Avoid Workshop used this concept to recommend two different TLOS for different types of airspace (Recommendation 3.3 or R 3.3), based on the type of traffic encountered:

- A TLOS for airspace primarily used by schedule air carriers. This is set to less than 1 MAC per billion flight hours (R 3.4).

- A TLOS for airspace primarily used by general aviation aircraft under VFR. This is set to less than 1 MAC per 10 million flight hours (R 3.5).

As per the OSED Assumption (ASSUMP-OSED.30), this Guideline is scoped to operations in uncontrolled airspace below 10,000ft. Hence the lower TLOS (1 MAC per 10 million flight hours) is the appropriate TLOS to use for the Guideline.

2.5.3 Probabilistic Collision Risk Model

To provide the ability to analyse the causal events that lead to a MAC, this analysis will define various stages of a MAC event in alignment with global concepts.

The majority of collision risk models revolved around three volumetric boundaries that define increasing severity of Ownship and intruder proximity with decreasing physical volume, the Detection volume, the Well-Clear Volume, and the NMAC Volume. These are defined in Table 7 below, in order of increasing severity.

Table 7: Detection, Well Clear, and NMAC Volume Definitions

Term	Description
Detection Volume	An important point in a potential collision sequence is the first point (in either distance or time) prior to impact where the Ownship is able to accurately detect and track an Intruder aircraft. This is called the Detection Range. The volume that encompasses the Ownship up to the max detection range is termed the Detection Volume. When an Intruder is detected and is tracking towards a loss of well clear state, the Ownship should undertake **self-separation** manoeuvres to remain well clear of the intruder. The size of this volume is very much dependant on both the Intruder detection characteristics (passive and active), and the Ownship's means to detect and track these intruders. Developing a Detection and Tracking system, such that the Detection Volume will be large enough to reliably execute manoeuvres in time to remain well clear, is a critical part of DAA System performance. As this is often an output of system design, there can be no quantitative definition given in the Guideline. However, the user of this Guideline will need to define the maximum detection range across the potential encounter angles.
Declaration Range	The declaration range is defined as the distance of an intruder from the Ownship such that the detect and avoid system can in time detect, track, decide on a manoeuvre, and execute the manoeuvre, all while remaining Well Clear from the Intruder. The minimum declaration range would constitute the minimum range at which a well clear can be maintained given the expected encounter scenarios. The declaration range should always remain inside the potential detection volume.

Term	Description
Well Clear Volume	This volume defines the region within which there is a loss of well clear between the Intruder and Ownship. When an Intruder is within this volume, the Ownship should take **collision-avoidance action** to prevent an NMAC. This volume has multiple quantitative definitions, delineated primarily by the TLOS required in the airspace (itself driven by the type(s) of aircraft operating therein). For this Guideline, the TLOS for a MAC has been specified as that associated with predominately VFR and GA traffic (i.e., 1 MAC per 10 million flight hours). The well clear volume for this encounter type is defined purely as a physical distance, specifically as a Horizontal Miss Distance (HMD) of less than 2000ft and a Vertical Miss Distance (VMD) of less than 250ft. These values are used by JARUS [5] and ASTM [6], which both derived the value from Weinert, et al [10]. Note that for encounters with faster moving aircraft (i.e., in controlled airspace) a time value is included as a parameter to the WCV definition, ensuring that there is ample time for the system to undertake any protective action. However, for uncontrolled airspace with slower moving aircraft, incorporation of the closest point of approach is not recommended by JARUS [11].
NMAC Volume	Near Mid Air Collision Volume is defined by a Horizontal Miss Distance of less than 500ft and a Vertical Miss Distance of less than 100ft. This is defined in the Traffic Collision Avoidance System (TCAS) Minimum Operational Performance Specification and adopted by JARUS SORA [5]. When the Intruder and Ownship are within this volume, a NMAC is considered to have occurred. Within this volume it is assumed that **only providence** can prevent a MAC.

A visualisation of the distance between the Ownship and any Intruder aircraft can be illustrated as a series of buffers, or 'pucks', that exists around the Ownship (the UAS), as depicted in Figure 7. As the distance between the Intruder aircraft (the conventionally piloted aircraft) and the Ownship reduces, more of these buffers are violated and the chance of a collision increases:

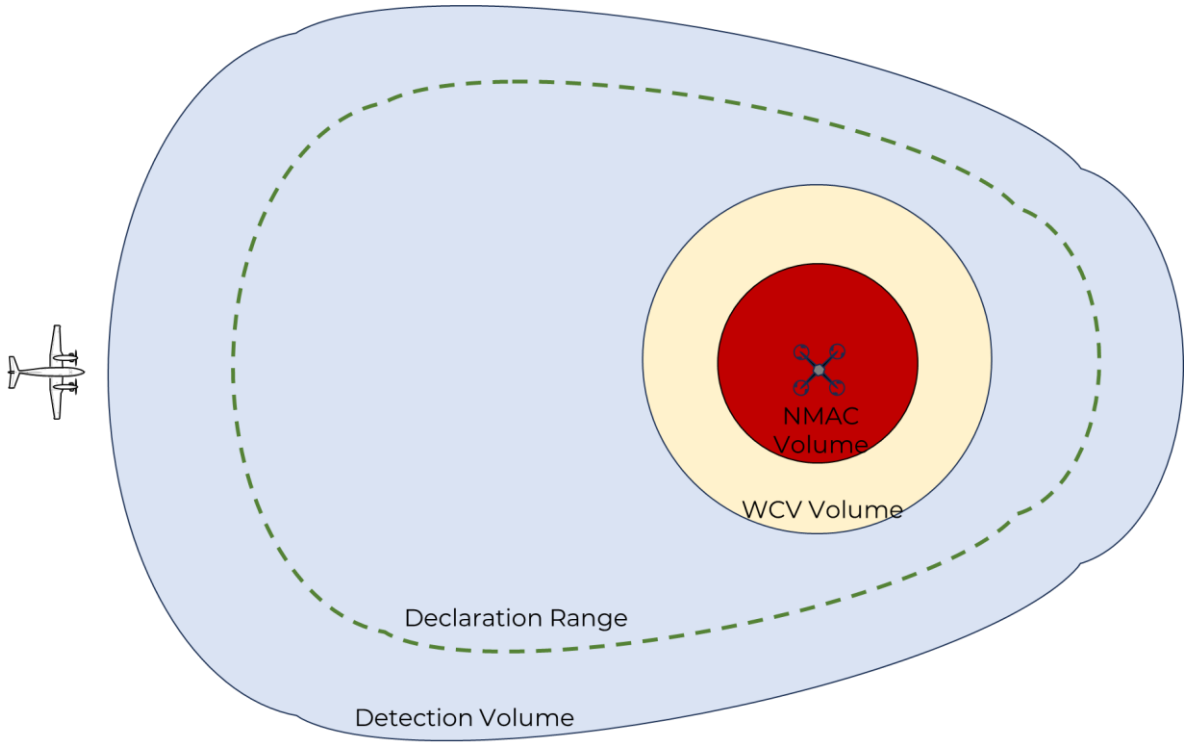


Figure 7: Airspace Volumes Surrounding the Ownship

As these volumes are nested, the chance of a MAC can be expressed in terms of the likelihood[7] of the transition through each of the volumes during an encounter, from the Detection Volume, to WCV, to an NMAC, and then finally to a MAC. The equation is given as:

$$\lambda_{MAC} = \lambda_{WCV} \times P(NMAC|WCV) \times P(MAC|NMAC) \qquad \textit{Equation 1}$$

Where:

- λ_{MAC} is the rate of MACs, usually measured in MACs/flight hour to align with the TLOS described in Section 2.5.2
- λ_{WCV} is the Vell Clear Violation (WCV) rate (i.e., the rate at which aircraft enter within the well clear volume per hour).[8]
- $P(NMAC|WCV)$ is the conditional probability that the two aircraft experience a Near-Mid-Air Collision, given that the intruder aircraft is in the Well Clear Volume. And

[7] More accurately, when examining the general concept of Detect and Avoid, individual likelihood is examined as rates of occurrence over time.
[8] Note that here, the Well Clear Violation rate can also be expressed in terms of the declaration range rate (i.e., the rate at which aircraft enter the declaration range, per hour) via $\lambda_{WCV} = \lambda_{DR} \times P(WCV|DR)$, where $P(WCV|DR)$ is the conditional probability that an aircraft which enters the declaration range transitions to a well clear violation.

- $P(MAC|NMAC)$ is the probability that the intruder and UAS collide with each other in a MAC, given that the intruder aircraft is in the Near Mid Air Collision Volume.

To determine the effectiveness of any DAA solution, it must be compared with the case where the DAA system is not influencing the encounter. These two cases are termed the "*mitigated*" and "*unmitigated*" MAC rates.

2.5.3.1 Unmitigated MAC Rate

The "*unmitigated*" MAC rate defines the various conditional probabilities that exist when there is no DAA system acting to reduce the likelihood of a collision. To differentiate between the two, a subscript "*unmit*" is added to the previous equation's parameters to denote this case:

$$\lambda_{MAC,unmit} = \lambda_{WCV,unmit} \times P_{unmit}(NMAC|WCV) \times P_{unmit}(MAC|NMAC) \qquad \textit{Equation 2}$$

Significant work has been undertaken to understand and model realistic encounters to derive the unmitigated probabilities of transition from one such volume to another. This work is summarised in Table 8 below:

Table 8: Airspace Model Unmitigated Probability Definitions

Term	Description
$\lambda_{WCV,\text{unmit}}$	This is the unmitigated Well Clear Violation rate; defined as: $\lambda_{DR} \times P_{\text{unmit}}(WCV\|DR)$. The unmitigated probability of a transition from the edge of the declaration volume to a Well Clear Violation depends on the size and shape of the Declaration Volume. In the unmitigated case, it doesn't matter what this declaration volume is, as the resultant WCV rate will be unchanged
$P_{\text{unmit}}(MAC\|NMAC)$	For the defined NMAC volume, Weinert et al. [10] determined the probability that a MAC occurs through providence is 0.01 for a combined UAS and intruder aircraft wingspan of less than 100ft. Assuming that most general aviation aircraft wingspans are less than 75ft, this allows the UAS wingspan to be up to 25ft (approximately 8m) and this value to remain valid. For UAS with wingspan exceeding this value, a re-evaluation of this unmitigated probability should be undertaken and employed throughout the rest of this Guideline.
$P_{\text{unmit}}(NMAC\|WCV)$	For the defined Well Clear Volume size (HMD of 2000ft and 250ft VMD), Weinert et al. [10] determined that the conditional probability of an unmitigated NMAC, given a Well Clear Violation, is 10% (0.1). This assumption also underpins the work in JARUS SORA [11] and ASTM [6] for lower risk environments.

2.5.3.2 Mitigated MAC Rate

The second case is the "*mitigated*" case, wherein a DAA system is present and aims to reduce the chance of a collision by:

- **Self-separating** from intruders to decrease the likelihood of a Well-Clear Violation. I.e., reducing $P_{\text{mit}}(WCV|DR)$.
- Conducting **collision-avoidance** manoeuvres when a loss of well clear is experienced to decrease the likelihood of an intruder entering the NMAC volume. I.e., reducing $P_{\text{mit}}(NMAC|WCV)$.
- Lowering the likelihood of a MAC in the event of an NMAC. I.e., reducing $P_{\text{mit}}(MAC|NMAC)$.

Note: it is assumed that once in the NMAC volume, **only providence** can prevent an MAC. However, the preceding actions of conducting self-separation and collision-avoidance have been found [12] to affect the probability of an NMAC transitioning to a MAC. Consequently, this value must still be differentiated from the unmitigated case.

This results in the following equation for the MAC rate with a DAA system on board:

$$\lambda_{MAC,mit} = \lambda_{DR} \times P_{mit}(WCV|DR) \times P_{mit}(NMAC|WCV) \times P_{mit}(MAC|NMAC) \qquad \textit{Equation 3}$$

It is clear here that there are two "opposing forces" that drive the change in the mitigated MAC rate:

- An increasing detection volume, which increases the number of encounters (a bigger volume is more likely to intersect with aircraft) that could lead to a MAC, per flight hour. This value is driven by:
    - The external environment: i.e., where the operation is intended to occur and the density of air traffic in that area)
    - The number of **induced well clear violations**: when the DAA system causes a change in flight route (due to either a true potential MAC or a false alert), it may cause the aircraft to encounter an aircraft it would otherwise not have encountered, potentially artificially increasing the overall well clear violation rate.
- The combination of the mitigated probabilities of transition from a well clear violation to a MAC. These values are driven by the DAA system, which attempts to reduce these probabilities from the unmitigated state. However, this is only true if the system has been designed correctly and is functioning as intended. It is possible that some combination of design errors or reliability issues could cause the DAA system to increase the probability of transition from WCV to MAC.

2.5.4 Defining Risk Ratios

In order to provide a consistent point of comparison between various DAA systems and their effect on the unmitigated rate of MAC, the use of risk ratios have been employed across international standards and analysis of DAA systems.

A risk ratio is simply a comparison of the outcomes of an event when comparing different probabilistic scenarios leading to that outcome. This is usually done by

comparing the probability of a mitigated series of events leading to the outcome to the probability of that same outcome occurring with no mitigation in place.

In the case of airspace risk, the Risk Ratios are defined by comparing the unmitigated outcome of an event in the MAC causal chain to the mitigated outcome of that same event. Specifically, the following three risk ratios are defined:

- The NMAC risk ratio,
- The Loss of Well Clear Risk Ratio, and
- The MAC Risk Ratio.

2.5.4.1 Near Mid-Air Collision (NMAC) Risk Ratio

The NMAC risk ratio is the ratio of mitigated to unmitigated probabilities that an NMAC occurs. The mitigation in this case is a DAA system performing both the separation function (before a WCV) and collision avoidance function (within the WCV before an NMAC). Given that we have defined the detection volume as the volume within which an aircraft can possibly be detected, we can use compare the risk within this volume (mitigated and unmitigated). The NMAC risk ratio is defined using the following equation:

$$RR_{NMAC} = \frac{P_{mit}(NMAC|DV)}{P_{unmit}(NMAC|DV)} = \frac{P_{mit}(WCV|DV) \times P_{mit}(NMAC|WCV)}{P_{unmit}(WCV|DV) \times P_{unmit}(NMAC|WCV)} \qquad \textit{Equation 4}$$

2.5.4.2 Loss of Well Clear (LoWC) Risk Ratio

The Loss of Well Clear (LoWC) Risk Ratio is defined as the ratio of mitigated to unmitigated probabilities that a WCV occurs. The mitigation in this case is the DAA system only undertaking separation. Because the MAC rate equation starts at a Well Clear Violation, the unmitigated probability of a WCV is set to 1 (i.e. a WCV **has occurred**). The LoWC risk ratio is by definition a **subset of the NMAC risk ratio**, focusing only on the probability of a WCV occurring.

We define the LoWC RR using the following equation:

$$RR_{LoWC} = \frac{P_{mit}(WCV|DV)}{P_{unmit}(WCV|DV)} \qquad \textit{Equation 5}$$

$$RR_{NMAC} = RR_{LoWC} \times \frac{P_{mit}(NMAC|WCV)}{P_{unmit}(NMAC|WCV)} \qquad \textit{Equation 6}$$

This metric is used to specifically ensure that a significant portion of the DAA performance concentrates on preventing a LoWC, rather than simply avoiding NMACs as a last resort.

2.5.4.3 Mid-Air Collision (MAC) Risk Ratio

The final risk ratio, the MAC Risk Ratio, only pertains to the effect of a mitigation on a MAC occurring, **on the condition that an NMAC has already occurred**. We define the MAC risk ratio using the following equation:

$$RR_{MAC} = \frac{P_{mit}(MAC|NMAC)}{P_{unmit}(MAC|NMAC)} \quad \textit{Equation 7}$$

2.5.4.4 Use of Risk Ratios

The whole purpose of defining risk ratios is to be able to provide a standardised way to calculate the mitigated MAC rate:

$$\lambda_{MAC,mit} = RR_{LoWC} \times \lambda_{WCV} \times \frac{RR_{NMAC}}{RR_{LoWC}} \times P_{unmit}(NMAC|WCV) \times RR_{MAC} \times P_{unmit}(MAC|NMAC) \quad \textit{Equation 8}$$

If the purposes of equipping a DAA system is to satisfy the TLOS, therefore, the mitigated MAC rate must be below the MAC TLOS:

$$\lambda_{MAC,mit} \leq \lambda_{TLOS} \quad \textit{Equation 9}$$

We can combine and rearrange Equation 8 and Equation 9 to only have the risk ratios on one side of the equation:

$$RR_{NMAC} \times RR_{MAC} \leq \frac{\lambda_{TLOS}}{\lambda_{WCV} \times P_{unmit}(NMAC|WCV) \times P_{unmit}(MAC|NMAC)} \quad \textit{Equation 10}$$

The denominator is just the unmitigated MAC rate. Hence:

$$RR_{NMAC} \times RR_{MAC} \leq \frac{\lambda_{TLOS}}{\lambda_{MAC,unmit}} \quad \textit{Equation 11}$$

This equation allows us to specify the capability of a DAA system that undertakes both separation and collision avoidance using only the TLOS and the unmitigated MAC rate of an area.

Theoretically there are an infinite number of combinations[9] of $RR_{NMAC} \times RR_{MAC}$.

2.5.4.5 System and Logic Risk Ratios

Without further specification, the risk ratios as defined above would be considered "*system*" risk ratios, as they take into account all factors that affect the mitigated versus unmitigated states (i.e., pilot error, failure of DAA systems, unusual or unexpected encounter scenarios). The system risk ratio is, "the total net collision risk benefit. The system risk ratio includes all failure conditions of the system, including system failures".[10]

Another type of risk ratio frequently used, referred to as a "*logic*" risk ratio (Logic RR), only encapsulates the intended functionality of a mitigation. This definition allows for a focus on verification of functional performance in line with XX.1301 requirements (where other safety metrics are captured in other requirements such as XX.1309).

[9] RR_{MAC} is typically not designed for and is a passive benefit gained from applying RR_{NMAC}, so it is assumed to be tied to the RR_{NMAC} value.
[10] See subsection. 3.3.9.1(2) from [8].

Referring to [8], the Logic RR is defined as "*the net collision risk benefit when the system operates as intended or specified; this includes the negative effect of induced collisions.* ***It is typically assumed that the system is operating as intended.***"

What falls within the category of the Logic RR, and what resides outside of the Logic RR, but still within the System RR, is not yet settled internationally. For the purposes of this analysis, a definition is proposed for the components of the Logic RR (see Table 9) derived from a draft ICAO RPASP Paper [13] noting that any changes to this definition in the future could be adapted by adjusting this table and subsequent requirements in this Guideline.

Table 9: Logic Risk Ratio Parameters

Logic Risk Ratio Parameter	Explanation
Expected encounter rates (including induced encounters) and geometries (i.e., Ownship and intruder encounter geometries, with manoeuvrability of each based off the intended operational environment).	The purpose of the Logic RR is to take into account the expected encounter geometries in the airspace being operated within. The encounter set should be sufficiently representative of what a UA in a given area may experience.
Distribution of Cooperative and Uncooperative Intruders.	In any given airspace, there will be a mix of IFR and VFR platforms. In Australia, all IFR platforms require ADS-B (Out) and are therefore electronically conspicuous (in cooperative and uncooperative airspace). Some VFR aircraft may also voluntarily carry and use ADS-B (Out). These VFR aircraft may be detected by the DAA system if the DAA system incorporates ADS-B (In), but it cannot be assumed that VFR aircraft will carry ADS-B (Out).
Expected functional response of DAA system (Detect, Track, Decide) including the time taken to complete these functions.	This caters for the intended function of the DAA system, based off the models/algorithms utilised to achieve the detect, track, decide subfunctions.
Expected functionality of Command and Non-Payload communications (CNPC) system including latency.	CNPC requirements are specified separate to the DAA system. This includes the expected functional performance of the CNPC.
Expected manoeuvrability of Ownship.	Key considerations for the functioning of the UAS are the time taken to generate an avoidance manoeuvre, and the capability of the platform to manoeuvre once instructed.
Expected human response and timing.	The Logic RR takes into consideration the average pilot response, without any consideration for human error.

Logic Risk Ratio Parameter	Explanation
Expected environmental conditions.	This effectively means that the logic risk ratio is only valid within the expected operational environment. This will require that the external environment is well defined and applicable bounds are set. This needs to be considered in the design of the test encounters including aspects such as background lighting and clutter, both above and below the horizon, and intruders of non-interest such as birds and cars.
Expected or nominal False Alerts/False Alarms/False Tracks.[11]	A few risks exist due to the rate of false alerts as part of the nominal functioning of the DAA system. If the number of false alerts is so high that the total number of tracks overwhelm the DAA system, there is a risk that a true detection could be "dropped" or missed. Additionally, false alerts can lead to an increased number of induced well clear violations, reducing the net benefit of the DAA system that should be considered as part of the functional performance.

Parameters considered part of System RR, but not part of the Logic RR are listed in Table 10 below:

Table 10: Additional System Risk Ratio Parameters

System Risk Ratio Parameter (excluded from Logic RR)	**Grouping**	**Explanation**
DAA system failures	UAS System Failure	Once the DAA system has failed in some way, the system is no longer operating as intended and is not captured in the logic risk ratio. This should be covered by system safety analyses.
Loss of CNPC	UAS System Failure	Loss of CNPC is an off-nominal scenario (regardless of if the operation uses automated or manual avoidance input). This should be covered by system safety analyses.

[11] The current entry in this table for the expected or nominal false alarms diverges from the preliminary work by ICAO RPASP paper. This decision has been made because the selection of an operating point on a Receiver Operating Curve, where the coordinates are described by a coordinate pair of Detection Rate and False Alarm Rate are in fact an inherent part of the DAA system functionality, and in turn warrant inclusion in the Logic Risk Ratio. The flow on implications of this finding will be included in the next version update, however readers are cautioned that this must be considered.

System Risk Ratio Parameter (excluded from Logic RR)	**Grouping**	**Explanation**
Failure of the UAS (I.e., manoeuvrability, power)	Safety Performance	Like the DAA system failures and Loss of CNPC, this should be covered by system safety analyses.
Human errors caused by HMI, pilot training and proficiency, human factors etc.	Human Error	As defined by the SAA Second Caucus Workshop [2], the Logic RR will not include human errors. Human error should be included in the System RR including: • Appropriately qualified and competent pilots to reduce the chance of a human error. • Appropriate human-machine interface to reduce the chance of human error due to poor HMI. • Appropriate/clear/effective operational procedures to undertake nominal and off-nominal procedures to reduce the chance of a human error.
Unusual or unexpected encounter rates or encounter geometries	Removal of non-credible encounters	To prevent poor estimation of the real-world performance of the DAA system, encounters that would be physically impossible or incredibly unlikely should be excluded from any estimation of the functional performance. The definition of the encounter set used as part of the functional performance estimation should cover all expected possible encounters during operation. Other encounters will be excluded from any analysis.
Adverse environmental conditions	Environmental definition and durability	Operations outside of the intended operational environment will likely have an adverse effect on the UAS or DAA system. This case will be mitigated through appropriate definition of the intended operational environment, as well as appropriate design to reduce the effect of the adverse environmentt on the UAS.

System Risk Ratio Parameter (excluded from Logic RR)	**Grouping**	**Explanation**
Intruder undertaking avoidance manoeuvres	Non considered as part of analysis	Due to the low conspicuity of the Ownship (partially due to physical characteristics, also due to the rules of the air and equipage requirements), it will be assumed that an Intruder does not undertake any manoeuvre to reduce the chance of a MAC. This assumption may need refinement upon airspace or equipage rule changes that require crewed aircraft and uncrewed aircraft in uncontrolled Class G airspace to coordinate avoidance manoeuvres.

The elements described in Table 10 for System RR are illustrated in Figure 8.

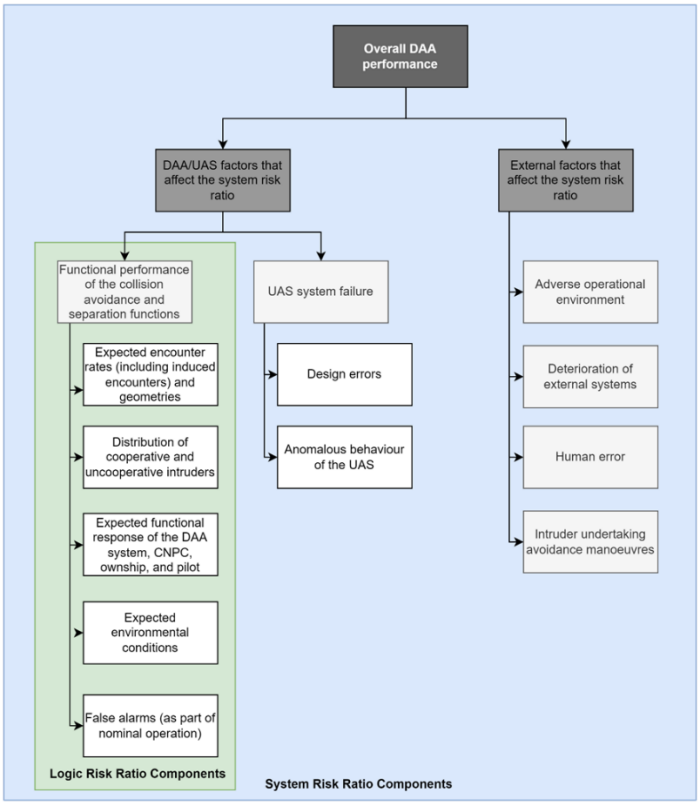


Figure 8: System and Logic Risk Ratio Elements and Categorisation

2.5.4.6 Aviation Standards for System and logic Risk Ratios

Over the last few years, various aviation bodies have begun defining minimum acceptable risk ratio requirements based on classification of airspace traffic types and densities. Inevitably, standards will align, and regulators will begin to accept these standards rather than apply a first principles approach to every application. To that end,

this Guideline will also attempt to align with the most prominent standards relevant to the operational context at the time of publishing.

There are two main standards of note for the operational context of this guideline:

- JARUS SORA v2.0 Main Body Tactical Mitigation Performance Requirements (TMPR) [5]
- ASTM F3442M Standard Specification for Detect and Avoid System Performance Requirements [6].

These standards are partially harmonised, but still lack complete alignment. This section will introduce these bodies requirements for risk ratios, and the context in which they apply, and the differences between them. Finally, a recommendation on the logic and system risk ratios shall be discussed.

2.5.4.6.1 JARUS v2.0 Main Body Tactical Mitigation Performance Requirements

The JARUS SORA provides a holistic process for assessing the risk of a UAS operation and deriving safety requirements necessary to meet a TLOS (the TLOS in this Guideline align with the TLOS defined by JARUS). From the perspective of risk ratios, JARUS defines **system NMAC risk ratios** aligned with "Air Risk Classes", a 4-tiered categorisation of airspace risk:

Table 11: JARUS Mapping, Airspace Risk Classes to System Risk Ratio, [5]

Air-Risk Class	Tactical Mitigation Performance Requirement (TMPR)	TMPR System Risk Ratio Objectives
ARC-d	High Performance	System Risk Ratio ≤ 0.1
ARC-c	Medium Performance	System Risk Ratio ≤ 0.33
ARC-b	Low Performance	System Risk Ratio ≤ 0.66
ARC-a	No Performance Requirement	No System Risk Ratio Guidance: although operator/applicant may still need to show some form of mitigation as deemed necessary by the CAA.

For the operational context of this Guideline, the ARC level is "ARC-c". I.e., operations in uncontrolled airspace above 500ft, in rural areas (see Figure 7 of the JARUS SORA v2.5 Main Body [14]). JARUS also recommends that the LoWC risk ratio should be **at least** the square root of the NMAC risk ratio. Hence, we can create the following table of suggested JARUS requirements:

Table 12: Suggested JARUS Risk Ratio Requirements

Risk Ratio for ARC-c Airspace	System Risk Ratio Value
NMAC Risk Ratio	<0.33
LoWC Risk Ratio	<0.57

JARUS does not stipulate a logic risk ratio but does provide some guidance on the allowable loss of function rate for the tactical mitigation employed. For ARC-c, this rate must be less than 1 loss of function event per 1,000 hours. JARUS does not stipulate any design assurance requirements or human performance guidelines (i.e., human factors and human machine interface factors that affect human performance).

2.5.4.6.2 ASTM F3442M Standard Specification for Detect and Avoid System Performance Requirements

The American Society for Testing and Materials (ASTM) have published ASTM F3442M to specify the performance of a DAA system. This standard applies within the ARC-b (Class 1) and ARC-c (Class 2) bands of JARUS classified air risk classes, focusing primarily on Class E and G airspace above 400/500ft AGL, and stipulates **logic risk ratios** for both non-cooperative and cooperative aircraft, shown below:

Table 13: ASTM Logic Risk Ratio Values

Intruder Aircraft Equipage	Logic Risk Ratios	
	NMAC Risk Ratio	LoWC Risk Ratio
Cooperative (ADS-B Out) Intruder Aircraft	<0.18	<0.4
Non-Cooperative Intruder Aircraft	<0.3	<0.5

ASTM also specify some system performance requirements. For Class 2 aircraft, the loss of function rate shall not exceed 1 event per 1000 flight hours, and the hazardously misleading information rate shall not exceed 1 event per 10,000 flight hours. The derivation of these requirements is from the JARUS TMPR requirements described in the previous section, with some adjustments for hazardously misleading information events.

The ASTM standard provides limited detail on human performance aside from some detail on pilot response models.

2.5.4.6.3 Summary of DAA System Performance Requirements

A summary of the different requirements is provided in the table below:

Table 14: Summary of DAA System Performance Requirements

Parameter		JARUS	ASTM
System Risk Ratios	LoWC Risk Ratio	0.57	-
	NMAC Risk Ratio	0.33	-
Logic Risk Ratios	LoWC Risk Ratio	-	0.5 (non-cooperative) 0.4 (cooperative)
	NMAC Risk Ratio	-	0.3 (non-cooperative) 0.18 (cooperative)
System Reliability Requirements	Loss of Function	1 E-3 per flight hour	1 E-3 per flight hour
	Hazardously Misleading Information	-	1 E-4 per flight hour

2.5.4.7 Additional MAC Risk Ratio Benefit When Complying with ACAS sXu

Recent work by the *Alliance for System Safety of UAS through Research Excellence* (ASSURE) [11] has demonstrated that when using the ACAS sXu algorithm, there is an additional effect on the probability of a MAC given an NMAC.

This study showed that this effect can range from at least one order of magnitude benefit, to over two orders of magnitude benefit. This effect should be considered when calculating the overall effect of the DAA system on the mitigated MAC rate.

2.5.4.8 Induced Well Clear Violations

The final component to the discussion on air risk is the concept of an induced well clear violation. An induced WCV is an interaction with an intruder that only occurs because the Ownship has manoeuvred in response to a prior DAA system alert. Responding to this alert puts the Ownship on a potential WCV heading with a second intruder, where the DAA system may then need to undertake evasive action to prevent a loss of well clear or an NMAC from occurring with this second intruder. This can be caused by either true alerts (see Figure 9 below) or from false alerts.

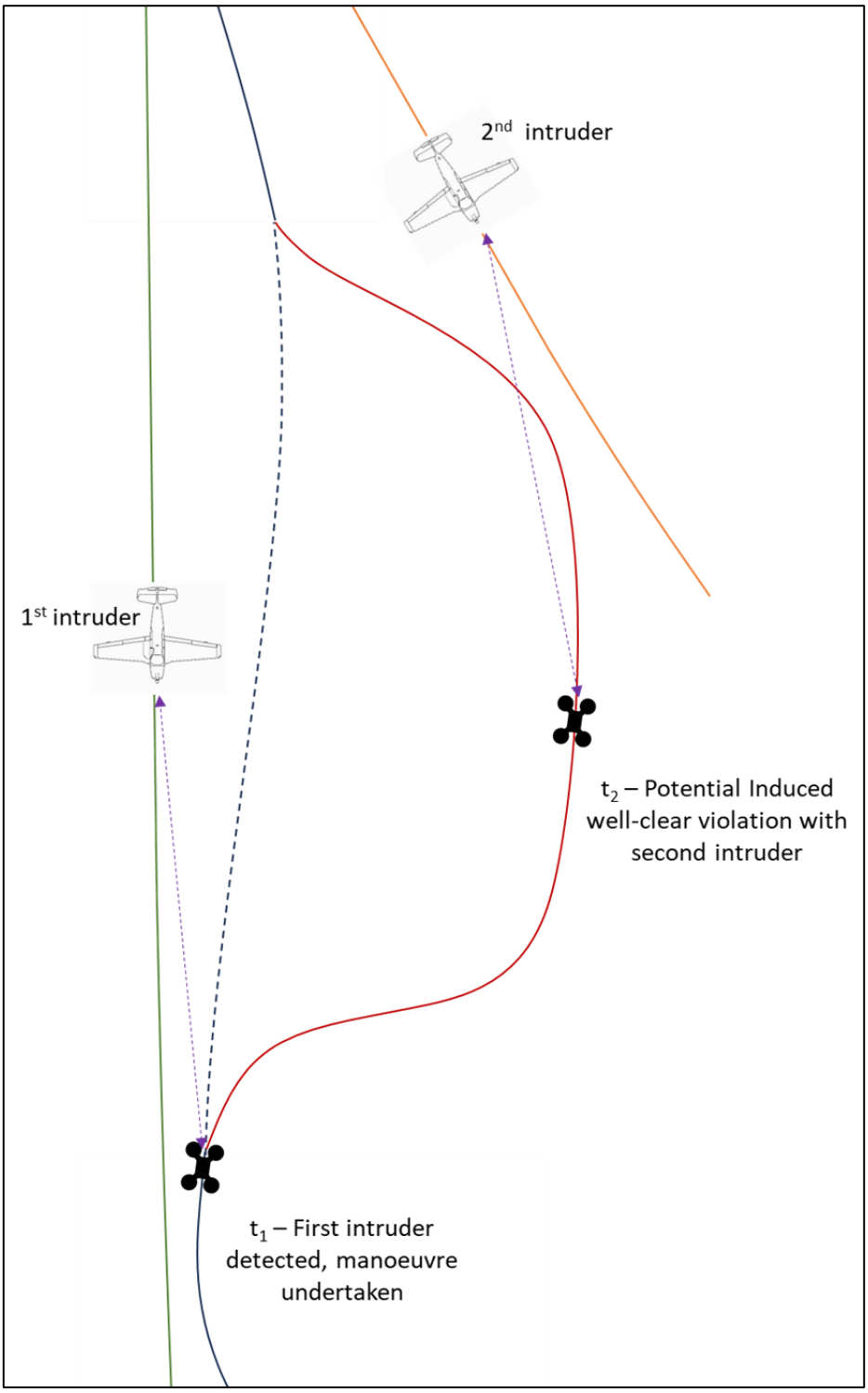


Figure 9: Visualisation of an Induced Encounter:

The total well clear violation rate that an Ownship experiences is driven by a combination of the natural underlying encounter rate and the induced well clear violation rate caused by the implementation of a DAA system:

$$\lambda_{WCV,total} = \lambda_{WCV,nat} + \lambda_{WCV,ind} \qquad \textit{Equation 12}$$

We can separate the induced WCV rate into those caused by true detections, and those caused by false alerts:

- For an induced encounter to occur from a true detection, the following must occur:
    - An actual intruder (induced or natural).
    - The Ownship then needs to undertake avoidance action in response to prevent a loss of well clear, or to avoid an NMAC (i.e., there is a chance the intruder is not detected, and no avoidance action is taken).
    - During the manoeuvre time, another intruder is encountered.
    - This can be expressed as the following equation:

$$\lambda_{WCV,ind|TD} = \lambda_{intruder,total} \times P(manoeuvre|intruder) \times P(ind|manoeuvre) \qquad \textit{Equation 13}$$

- For an induced encounter to occur as a result of a false alert, the following must happen:
    - A false detection is propagated as a true detection through to DAA system.
    - The Ownship determines the need to undertake avoidance action in response to the false alert.
    - During the manoeuvre time, a true intruder is encountered.
    - This is expressed as the following equation:

$$\lambda_{WCV,ind|FA} = \lambda_{FA} \times P(manoeuvre|FA) \times P(ind|manoeuvre) \qquad \textit{Equation 14}$$

Because the calculation of risk ratios is usually undertaken using pairwise interactions between an Ownship/Intruder pair, the induced encounter rate may not be adequately estimated by purely focusing on managing the risk ratio**. It is therefore critical to ensure that induced encounters are covered as part of any safety analysis of a DAA system.**

2.5.5 Summary of Mid-Air Collision Hazard Context

In order to satisfy our higher order objectives (i.e., to meet the TLOS and ensure that there is no adverse effect on the safety of air navigation), it is recommended that the **logic risk ratios from the ASTM standard are utilised**, particularly as JARUS does not provide additional requirements for cooperative aircraft.

It is important to note that the ASTM definition only employs logic risk ratio's, with the assumption that it only applies when the DAA system is working as intended. It does not cater for factors that cause the DAA system not to function as intended.

To accommodate this shortfall in catering for UAS system failure, adverse operational environments, and the deterioration of external systems situations, the FAA Second Caucus Report concluded (Conclusion 4.1 or C 4.1) [2] that "*Existing airworthiness and operational approval processes, in general, are appropriate for fielding of UAS SAA systems.*" Additionally, the use of XX.1309 (equipment system safety) and XX.1301 (equipment functional performance)[12] for DAA systems was considered an appropriate method to ensure safety goals are met and validated appropriately.

It is our view that these engineering processes should take into consideration the hazard severity of a MAC (Catastrophic), the TLOS (less than 1 MAC per 10 million flight hours) and the external event frequencies that lead to a MAC.

The effect of human error very much relies on the required performance of the remote pilot in the DAA system control loop, but should still be driven by aviation best practice for the:

- Design of any human-machine interface, including managing the alerts and situational awareness information provided to the remote pilot.
- Development of processes and procedures to operate the DAA system, including all nominal and off-nominal situations, taking into consideration pilot workload.
- Development of any training material for the purposes of educating and rating pilots to use the DAA system.

The system risk ratios can be estimated using a combination of modelling, analysis, and design review. This value can then be used in conjunction with operational areas encounter rate to determine the mitigated MAC rate, and compared to the TLOS to ensure the higher-level objectives are satisfied.

Finally, the analysis showing satisfaction of the TLOS by limiting the encounter rate subject to the system risk ratio should incorporate induced encounters as a component of the encounter rate.

[12] Note that as part of XX.1301, the function should be established across the intended operational environment, and limits need to be established. This allows for the definition of the adverse environment adequate processes/procedures to ensure the DAA system is not operated outside of these limits.

2.5.5.1 Encounter Set Compilation during Risk Ratio demonstration.

It is important to note that substantiating achievement of the NMAC RR and the LoWC RR performance levels in Table 14 is reliant on having a set of test vectors which includes a pre-ordained proportion of encounters where the intruders are deemed to be electronically cooperative. This may be modified by competent authorities to reflect local distributions of aircraft fitted with this equipment.

the unmitigated conditional probabilities for P (MAC|NMAC) and P (NMAC|WCV), derived by Weinert in [10] are used to back derive allowable encounter rates and ultimately underpin the safety basis for achieving the TLOS.

It is important to note that the encounter set geometries compiled by either competent authorities or presented by applicants for the purpose of demonstrating compliance with Risk Ratio requirements should maintain these probabilities, otherwise the TLOS safety basis has been corrupted.

For instance, and applicant might seek to increase the number of unmitigated WCV's that are simply crossing manoeuvres and don't subsequently migrate to NMACs. Alternatively, there may be similar movements that enter the NMAC volume but don't migrate to MACs.

Accordingly, Competent Authorities should insist that encounter sets maintain the ratios identified for P_{unmit}(MAC|NMAC) and P_{unmit}(NMAC|WCV).

2.5.6 Requirements Generated by Mid-Air Collision Hazard Context

Table 15: Requirements Generated by the Mid-Air Collision Hazard Context

Req. ID	Requirement Text	Rationale
CR-003	The DAA system shall meet all required risk ratio requirements necessary to satisfy the target level of safety in ARC-c Airspace.	The risk ratio is globally accepted metric for assessing the performance of a DAA system. To harmonise internationally, the ASTM risk ratios are the most appropriate ones for use in the operational context of this guideline (uncontrolled class G <10,00ft AMSL)
CR-004	The Maximum allowable encounter rate, including both natural and induced encounters shall be determined.	The ability for a DAA System to meet the TLOS is heavily affected by the encounter rate of the operation. The encounter rate limit should include both natural encounters and induced encounters to ensure the TLOS is truly met. By meeting the target level of safety, we can ensure that the regulatory goal of not having an adverse effect on the safety of air navigation is satisfied for a given pairwise interaction.

Req. ID	Requirement Text	Rationale
CR-005	Hazards associated with development errors and anomalous system behaviour of the AAT function shall be minimised by use of aerospace best practice system safety engineering techniques.	The FAA [2] concluded that aerospace best practice system safety processes (i.e., XX.1301 and XX.1309) are appropriate to manage the safety performance of DAA systems. Utilising the hazard severity of a MAC (Catastrophic), and the TLOS for MACs, an appropriate analogous aircraft category can be derived, and these aviation practices can be applied as if that category of aircraft was being designed.

2.6 Ground Impact Risk Context

In a similar vein to the previous section on the risk context of a MAC, it is important to consider how a DAA system affects 3rd parties on the ground. This section will:

- Define the hazard severity associated with a fatality on the ground caused by an aviation event.
- Define the Target Level of Safety for ground risk, driven from the higher-level regulatory requirements to “not have an adverse effect on the safety of air navigation”.
- Introduce a probabilistic model for calculating the expected fatality rate for third parties on the ground, aligned with JARUS SORA methods.
- Discuss the relative ways in which the use or failure of a DAA System can lead to fatalities on the ground.

Part of this context is be used to generate high level requirements to meet the overall regulatory requirement, whilst other portions are be used as inputs to the operational hazard analysis and functional hazard analysis.

2.6.1 Hazard Severity of a Ground Fatality

This Guideline refers to the JARUS Scoping Paper to AMC RPAS.1309 [15] which is one of the few regulatory references that specifically refers to the hazards associated with ground impact of a UA. Specifically, one or more fatalities on the ground is considered a catastrophic occurrence. This classification will be used throughout the rest of this Guideline.

2.6.2 Target Levels of Safety for Ground Risk

Many efforts have been undertaken to determine the risk that third parties on the ground experience from aviation activities, including by JARUS and the Range Commanders Council [16]. In both cases, the currently expected rate of fatalities on the ground was established to be on the order of 1 fatality per million hours. JARUS specifically notes [17] that his is measured as a rate of risk to a population, and is expressed in fatalities per million **hours**, rather than flight hours.

2.6.3 Probabilistic Model for Ground Fatalities

Draft Annex F to SORA v2.5 provides us with a probabilistic equation that maps the causal chain of events leading to ground impact and potential fatality of third parties on the ground (in a similar way to the previous air risk model did):

$$\lambda_{fatality} = \lambda_{UooC} \times D_{pop} \times A_C \times F_{exp} \times P(fatality|impact) \qquad \textit{Equation 15}$$

Where:

- $\lambda_{\text{fatality}}$ is the expected fatality rate, measured in fatalities per hour (applied to the population density at risk).
- λ_{UooC} is the rate of a UAS out of control event.
- D_{pop} is the population density at risk from the ground impact.
- A_{C} is the critical area of the ground impact, effectively the area within which a fatality will occur to a person.
- F_{exp} is the fraction of exposed people, effectively the converse of the sheltering factor. It expresses the fraction of the broader population considered, that could actually be harmed by the hazard.
- $\text{P}(\text{fatality}|\text{impact})$ is the probability that upon impact, the person(s) impacted are fatally injured. This value is conservatively set to 1 (i.e., any person that is hit is fatally injured).

To ensure that the high-level safety objectives are met, the TLOS for ground risk should always be greater than or equal to the acceptable fatality rate:

$$\lambda_{TLOS} \geq \lambda_{fatality} \qquad \textit{Equation 16}$$

2.6.3.1 MACs and DAA Systems Effect on Ground Risk

From an airspace hazard perspective, there are two pathways that could lead to a ground impact:

- A Mid Air Collision results in debris impacting the ground. In this case, the rate of UAS out of control event is expressed as $\lambda_{\text{fatality}|MAC}$.
- A manoeuvre initiated by the DAA system leads to an aircraft performing controlled flight into terrain. In this case, the rate of UAS out of control event is expressed as $\lambda_{\text{fatality}|DAA}$.

These must be considered together when determining if the TLOS has been met. It is likely that for each type of hazard, some of the underlying parameters (in particular, the critical area) will vary, and will need to be considered individually to determine the overall effect on the TLOS:

$$\lambda_{TLOS} \geq \lambda_{fatality|MAC} + \lambda_{fatality|DAA} \qquad \textit{Equation 17}$$

2.6.3.2 Post-MAC Ground Risk

The expected number of people fatally injured on the ground from debris following a MAC at a point in time can be expressed as:

$$E[fatalities|MAC] = P(T_{mac} = t|T_{mac} \geq t) \times P(GI|MAC) \times P(fatality|GI) \quad \textit{Equation 18}$$

A reasonable, albeit conservative assumption is that if a MAC occurs, both aircraft will impact the ground soon thereafter (i.e. $\mathrm{P(GI|MAC)} = 1$). If we further assume that the hazard rate associated is constant (i.e. exponential probability distribution), and that all impacts are considered fatal, the equation can be simplified to the following:

$$E[fatalities|MAC] = \lambda_{MAC} \times D_{pop} \times A_{C|MAC} \times F_{exp|MAC} \quad \textit{Equation 19}$$

Note that this hazard is itself dependant on a MAC occurring, which sets a ceiling on the likelihood of this happening, equal to the likelihood of a MAC.

2.6.3.3 CFIT Due to DAA Manoeuvre

The potential for a DAA system to malfunction[13] and cause a ground impact provides another pathway to a ground hazard. This contribution to the fatality rate can be expressed using the following equation:

$$\lambda_{fatality|DAA} = \lambda_{GI|DAA} \times D_{pop} \times A_{C|DAA} \times F_{exp|DAA} \times P(fatality|impact) \quad \textit{Equation 20}$$

The ways that a DAA system might malfunction or otherwise behave in an unintended manner, and then subsequently cause a ground impact, can vary substantially across systems. These considerations and their impact on the hazard rate should be considered in any safety analysis.

2.6.4 Summary of the Ground Risk Context

A DAA system must consider the effect of ground hazards to substantiate it supports the top-level requirement to not introduce any adverse effect on the safety of air navigation.

As per the air risk considerations outlined in Section 2.5, the function and performance of a DAA system must also ensure protection of third parties on the ground in accordance with aviation best practice system safety engineering processes.

Utilising the TLOS (1 fatality per million hours), as well as the hazard severity associated with a ground fatality (Catastrophic), alignment with crewed aviation system safety requirements can be undertaken.

[13] Or an unintended behaviour of the DAA system that would not technically be considered a malfunction.

2.6.5 Requirements Generated by the Ground Collision Hazard Context

Table 16: Requirements Generated by the Mid-Air Collision Hazard Context

Req. ID	Requirement Text	Rationale
CR-006	The DAA system shall not cause a hazard to third parties on the ground greater than expected by the target level of safety.	In a similar vein to CR-003, the currently accepted TLOS for third parties on the ground presents us with a metric that, if satisfied by the implementation of a DAA system, will meet the regulatory objective not to create an adverse effect on the safety of air navigation.
CR-005 (repeated)[14]	Hazards associated with development errors and anomalous system behaviour of the AAT function shall be minimised by use of aerospace best practice system safety engineering techniques.	The same justification for aerospace best practice system safety techniques to apply for airspace hazards applies to ground hazards. For the identified hazard severity (Catastrophic) and TLOS (1 fatality per million hours) an appropriate aircraft analogy can be found.

2.7 Hazard Probability Classification Model

The purpose of this section is to derive an equivalent system safety aircraft class (from Part 23) as the basis for system safety requirements for a DAA system operating under this Guideline.

As described earlier, the FAA SAA Workshop [2] provided further clarification on DAA equipment by highlighting a need to comply with FAR/CS XX.1301 and XX.1309 requirements, thereby confirming that DAA equipment must meet both functional and system safety requirements.

Using the principles outlined in XX.1309 and a hazard severity classification of Catastrophic across both air and ground risk, it is possible to apply a similar approach to that found in AC 23.1309-1E [12] to take the assessment of TLOS and hazard severity metrics consolidated in Table 17, and these allow us to determine the subsequent safety class.

Table 17: TLOS and Hazard Severity Metrics

Context	Hazard Severity	TLOS
Air Risk – Mid Air Collision	Catastrophic	1×10^{-7} MACs per flight hour

[14] While CR-005 was generated in the previous investigation into air risk, this investigation provided additional context and expanded the applicable scope of the requirement.

Context	Hazard Severity	TLOS
Ground Risk – Ground Fatality	Catastrophic	1×10^{-6} Ground Impacts per flight hour

To simplify this process, the analysis has not been conducted for ground risk. The rationale is that air risk has a more stringent TLOS and has significantly more impact on the overall systems requirements and will be used throughout this analysis.

Using AC 23.1309-1E [12] we can solicit safety requirements for the DAA equipment by:

- Identifying a TLOS,
- Determining the proportion of the TLOS that results from equipment failing catastrophically (i.e., the top-level catastrophic system failure rate), and
- Identifying the number of catastrophic failure conditions that lead to TLOS and proportioning the allowable top level catastrophic system failure rate to each failure condition.

For Part 23 aircraft, AC23.1309-1E establishes a baseline for Class I aircraft, using the following approach:

- The historical general aviation fatal accident rate was assessed as 1 per 10,000 flight hours (1×10^{-4} pfh).
- Approximately 10% of these accidents were attributable to equipment failures, therefore resulting in an allowable catastrophic failure rate of 1 per 100 thousand flight hours (1×10^{-5} pfh) attributable to all aircraft equipment.
- It was assumed that there are 10 independent failure conditions that can lead to these system failures. This results in a maximum failure rate of 1 per 1 million flight hours (1×10^{-6} pfh) for individual independent failure conditions.

This approach can be applied to the DAA system to derive appropriate system safety requirements, for use within this Guideline:

- The acceptable MAC TLOS for airspace users in uncontrolled airspace is 1 per 10 million flight hours (1×10^{-7} pfh) (which accounts for a portion of the AC 23.1309-1E TLOS for fatal accidents).
- It is reasonable to assume, per the AC, that 10% of the MAC TLOS is attributable to equipment failure. This leads to an allowable catastrophic functional failure rate (due to systems) of 1 per 100 million flight hours (1×10^{-8} pfh).
- In accordance with JARUS [18], it is assumed that an aircraft utilising this DAA system is at Complexity Level 2, i.e. there are 100 independent potential catastrophic functional failure conditions at the aircraft level. It is further assumed that the DAA system only contributes to a portion (10 catastrophic functional failures) of the aircraft level catastrophic functional failures.

Consequently, each of the 10 catastrophic functional failures are equally apportioned the allowable catastrophic functional failure rate due to systems ($1/10^{th}$ of 1×10^{-8} pfh). This results in a catastrophic failure condition probability of 1×10^{-9}, which aligns with Class IV aircraft, per AC23.1309-1E as shown below in Figure 10.

Classification of Failure Conditions	**No Safety Effect**	**<----Minor----->**	**<----Major----->**	**<--Hazardous--->**	**< Catastrophic>**
Allowable Qualitative Probability	**No Probability Requirement**	**Probable**	**Remote**	**Extremely Remote**	**Extremely Improbable**
Effect on Airplane	No effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reduction in functional capabilities or safety margins	Large reduction in functional capabilities or safety margins	Normally with hull loss
Effect on Occupants	Inconvenience for passengers	Physical discomfort for passengers	Physical distress to passengers, possibly including injuries	Serious or fatal injury to an occupant	Multiple fatalities
Effect on Flight Crew	No effect on flight crew	Slight increase in workload or use of emergency procedures	Physical discomfort or a significant increase in workload	Physical distress or excessive workload impairs ability to perform tasks	Fatal Injury or incapacitation
Classes of Airplanes:	**Allowable Quantitative Probabilities and Software (SW) and Complex Hardware (HW) Development Assurance Levels (Note 2)**				
Class I (Typically SRE 6,000 pounds or less)	No Probability or SW and HW Development Assurance Levels Requirement	$<10^{-3}$ Note 1 P=D	$<10^{-4}$ Notes 1 and 4 P=C, S=D	$<10^{-5}$ Note 4 P=C, S=D	$<10^{-6}$ Note 3 P=C, S=C
Class II (Typically MRE, STE, or MTE 6,000 pounds or less)	No Probability or SW and HW Development Assurance Levels Requirement	$<10^{-3}$ Note 1 P=D	$<10^{-5}$ Notes 1 and 4 P=C, S=D	$<10^{-6}$ Note 4 P=C, S=C	$<10^{-7}$ Note 3 P=C, S=C
Class III (Typically SRE, STE, MRE, and MTE greater than 6,000 pounds)	No Probability or SW and HW Development Assurance Levels Requirement	$<10^{-3}$ Note 1 P=D	$<10^{-5}$ Notes 1 and 4 P=C, S=D	$<10^{-7}$ Note 4 P=C, S=C	$<10^{-8}$ Note 3 P=B, S=C
Class IV (Typically Commuter Category)	No Probability or SW and HW Development Assurance Levels Requirement	$<10^{-3}$ Note 1 P=D	$<10^{-5}$ Notes 1 and 4 P=C, S=D	$<10^{-7}$ Note 4 P=B, S=C	$<10^{-9}$ Note 3 P=A, S=B

Note 1: Numerical values indicate an order of probability range and are provided here as a reference.
Note 2: The letters of the alphabet denote the typical SW and HW Development Assurance Levels for Primary System (P) and Secondary System (S). For example, HW or SW Development Assurance Level A on Primary System is noted by P=A.
Note 3: At airplane function level, no single failure will result in a Catastrophic Failure Condition.
Note 4. Secondary System (S) may not be required to meet probability goals. If installed, S should meet stated criteria.

Figure 10: Design Assurance Levels, reproduced from [19], with emphasis added.

Whilst the information is useful the descriptions of failure effects only covers effects for Ownship and does not sufficiently cover of on the broader UAS components, other crewed aircraft, and third parties on the ground, who are all parties of particular interest to this Guideline.

The required development assurance levels and quantitative probabilities of occurrence from AC 23.1309-1E [19] can be combined with the failure effects descriptions from FAA Order 8040.6A [9] to create Table 18 which provides a tailored Hazard Severity Classification Matrix, outlining the acceptability of risk for undesired

airspace events for UAS operations in uncontrolled airspace.[15] Table 18 will be used as a starting point for deriving verification and validation requirements in Section 3 and 4.

[15] Note that this table is specific to failure of the AAT function. It is not for all credible system failure conditions for a UAS.

Table 18: Proposed Severity of Failure Conditions, Required Probabilities, and Development Assurance Levels for DAA

	Hazard Severity Classification				
	Minimal (5)	**Minor (4)**	**Major (3)**	**Hazardous (2)**	**Catastrophic (1)**
UAS Operating in Uncontrolled Class G airspace, <10,000ft AMSL, outside of the airport environment	**Conditions resulting in any one of the following:**				
	• Negligible Safety effect.	• Non-serious injury to 3 or fewer people on the ground. • Hull Loss of UA	• Crewed aircraft making an evasive manoeuvre, but proximity from UAS remains greater than 500ft (WCV). • 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. • Non-serious injury to more than three people on the ground.	• HMD of less than 500ft and VMD of less than 100ft between Ownship and crewed aircraft (NMAC). • 1-2 fatalities onboard crewed aircraft (no hull loss). • Serious Injuries to persons on the ground.	• Collision with Manned Aircraft • 3 or more fatalities onboard crewed aircraft. • Crewed aircraft hull loss. • 1 or more ground fatalities.
	Allowable Quantitative Probabilities (Note 1) and Software (SW) and Complex Hardware (HW) Development Assurance Levels:				
	• No required probability • No Software or Hardware DAL	• $<10^{-3}$ • Primary system: DAL D	• $<10^{-5}$ (Note 3) • Primary system: DAL C • Secondary system: DAL D	• $<10^{-7}$ (Note 3) • Primary system: DAL B • Secondary system: DAL C	• $<10^{-9}$ (Note 2, Note 3) • Primary system: DAL A • Secondary system: DAL B
	Note 1: Numerical values indicate an order of probability range and are provided here as a reference. Note 2: At airplane function level, no single failure will result in a Catastrophic Failure condition. Note 3: Secondary System (S) may not be required to meet probability goals. If installed, S should meet stated criteria				

2.7.1 External Event Probability

The allowable quantitative probabilities of failure, and the required Development Assurance Levels (DAL) outlined in Table 18, rely on the assumption that the system or functional failures directly lead to the consequence (for example the complete failure of a the flight control function on a crewed aircraft will result in a catastrophic outcomes directly). It doesn't provide for the fact external factors, in addition to the functional failure are required.

For example, when dealing with a MAC event, **both the functional/system failure and a collision event** must occur (i.e., the consequence only arises if the two aircraft are on a collision course and the function failed). Therefore, the AAT function can be treated as a protective function as described in Subsection 5.2.4 of [7]. This allows for a reduction in assurance requirements commensurate with the probability of the external event.

This can be represented probabilistically as:

$$P(hazard\ occurs) = P(loss\ of\ protection\ function \wedge external\ event) \qquad \textit{Equation 21}$$

Assuming independence between the external event and the loss of protection function:

$$P(hazard\ occurs) = P(loss\ of\ protection\ function) \times P(external\ event) \qquad \textit{Equation 22}$$

By adopting the system safety objectives for Class IV aircraft, per Part 23, there are clear maximum allowable hazard rates for these events that cannot be exceeded[16]:

$$P(hazard\ occurs) \leq QPF_{hazard\ severity} \qquad \textit{Equation 23}$$

Where the Quantitative Probability of Failure (QPF), aligns with the quantitative numbers detailed in Table 18.

Combining the above equations and rearranging, the following expression shows how to reduce the allowable failure rates based upon the probability of the external event:

$$P(loss\ of\ protection\ function) \leq \frac{QPF_{hazard\ severity}}{P(external\ event)} \qquad \textit{Equation 24}$$

It should be noted that this process cannot be used ad infinitum. As described in Section 5.2.4 of [7], for any external event with a severity classification of major or higher, the DAL level must be at least DAL C.[17]

Given this assessment, functional hazard analyses and associated system safety engineering requirements should take into consideration that the AAT function is a

[16] NOTE: for exponential distribution hazard rates, the hazard rate is constant and equal to the rate parameter. This is also the inverse of the expected value of the distribution

[17] This limit in DAL reduction is driven by guidance developed for passenger transport aircraft. It may not be fully appropriate for the operational context of this Guideline. It is retained in the interests of being conservative. A competent authority may be able to work with the applicant to reduce the minimum DALs from C to D, noting that DAL D represents a significant drop in assurance from DAL C.

protective function, and external events probabilities that need to occur in order for the hazard (a MAC) to occur.

2.7.2 Requirements Generated by the Hazard Probability Classification Model

Using the accommodation for external events and the status of AAT as a protective function, core requirement 5 can be updated, we can update the expectations for CR-005.

Table 19: Requirements Generated by the Hazard Probability Classification Model

Req. ID	Requirement Text	Rationale
CR-005 (repeated)[18]	Hazards associated with development errors and anomalous system behaviour of the AAT function shall be minimised by use of aerospace best practice system safety engineering techniques. The Avoid Air Traffic Function can be considered a protective function, the external event being an aircraft on a collision course.	The same justification for aerospace best practice system safety techniques to apply for airspace hazards applies to ground hazards. For the identified hazard severity (Catastrophic) and TLOS (1 fatality per million hours) an appropriate aircraft analogy can be found.

[18] While CR-005 was generated in the previous investigation into air risk, this investigation provided additional context and expanded the applicable scope of the requirement.

3 Safety Analyses

This second major requirements derivation activity utilises the context described above in an Operational Hazard Analysis (OHA) to classify the risk of hazards and define risk controls that should align with the previous Core Requirements.

This OHA identifies risk controls that will be expanded through the rest of this section, culminating in a completed suite of requirements that provide coverage across all the identified hazards and core requirements derived in Section 2.

To further elicit system performance requirements, a Functional Hazard Analysis (FHA) of the avoid air traffic function is then undertaken, depth of analysis requirements, and some required functional architecture and operational procedures to reduce the analysis requirements absent this functional architecture.

The functional development assurance level of the highest severity hazards necessitates the validation of the functional requirements, which is provided at a high level across the AAT function in Section 4. The relationship between all the requirements is visualised in Figure 11 below:

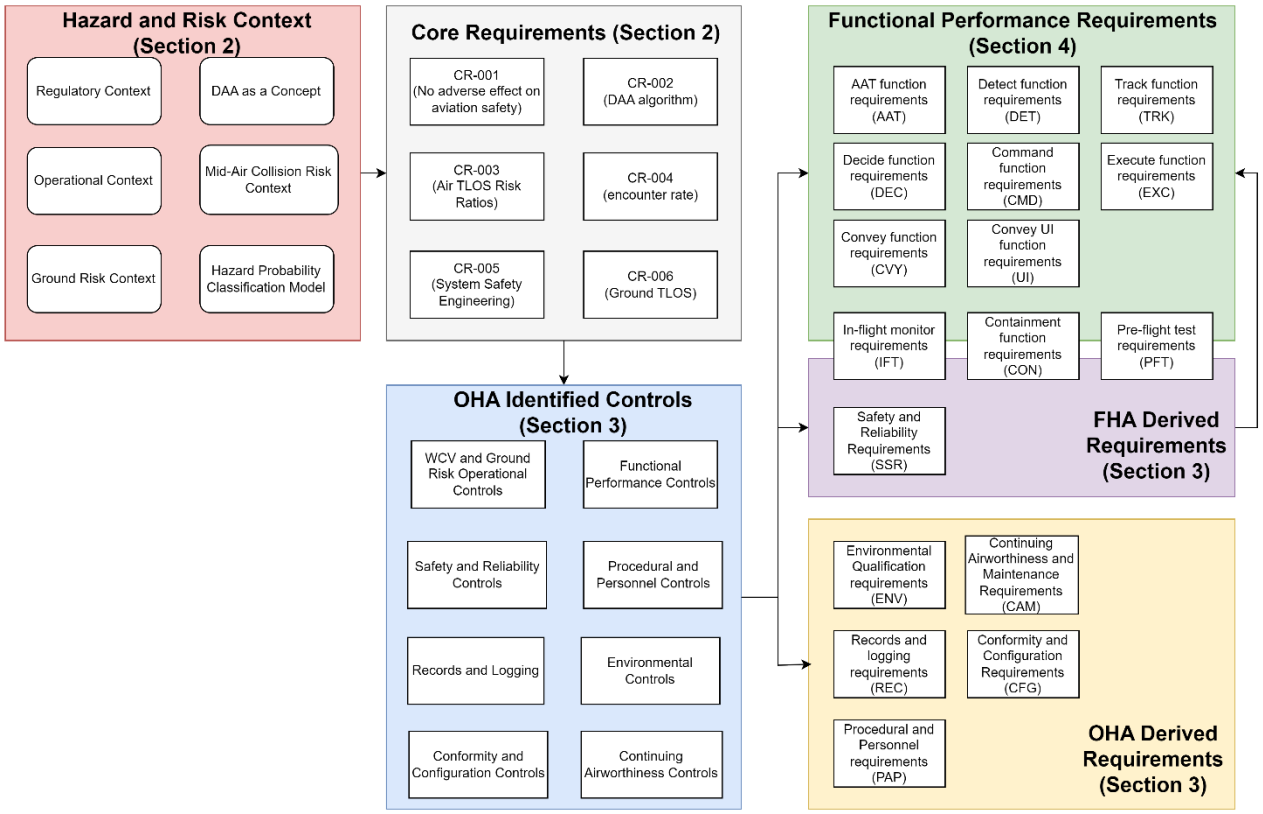


Figure 11: Requirements Derivation and Document Architecture[19]

[19] This figure is identical to Figure 2, it is reproduced here for convenience.

3.1 Operating Hazard Analysis

Utilising the operational hazard list in Section 2.4.4 within the context of the OSED at Appendix A, an OHA has been completed. It was heavily informed by previous work undertaken by the FAA [8] and previous international work. The full OHA can be found in Appendix F of the Guideline. In short, three Catastrophic hazards and one Minor hazard were identified:

- **OHAZ-1:** Failed or inadequate manoeuvre when one is required (Catastrophic).
- **OHAZ-2:** Increased collision risk from manoeuvre (Catastrophic).
- **OHAZ-3:** Secondary effects from manoeuvre (Catastrophic).
- **OHAZ-4:** False alerts (Minor).

For the three catastrophic hazards, these all have the potential to lead to a MAC, and potential subsequent ground fatalities, whereas the minor failure may lead to an unwanted encounter, nuisance alerts and increased distraction to the remote crew.

Sections 3.1.1describe the controls and mitigations identified during the OHA process, and in certain instances, identifies specific derived requirements that are incorporated into the Requirement Set in Appendix D to this Guideline.

3.1.1 WCV and Ground Risk Operational Controls

The following controls were identified to ensure the TLOS is met by controlling the operational WCV rate:

- Operations are restricted to areas where the total allowable WCV rate meets the TLOS (OHAZ-1, OHAZ-2).
- Operations are restricted to areas where the MAC rate and false alert rate have no adverse effect to third parties on the ground. (OHAZ-1, OHAZ-2, OHAZ-3).

These controls are effectively equivalent to the core requirements CR-004 and CR-006, **further solidifying the need for some form of analysis to ensure the maximum allowable WCV rate and underlying population densities overflown** are acceptable for the operation.

3.1.2 System Safety and Reliability Controls

The following system safety and reliability control was identified:

- Verification and validation of AAT function and DAA system design uses aerospace best practice system safety processes, to ensure that design errors and anomalous behaviour of the DAA system are minimised to an appropriate level based on the risk (OHAZ-1, OHAZ-2, OHAZ-3, OHAZ-4).

The System Safety and Reliability requirements ensures that the DAA system functions as intended within the operational environment, meets the necessary level of reliability, and can manage functional and system failures safely.

These controls and mitigations feed into the following Core Requirements:

- CR-002 – By providing the level of validation required to define the functional performance and functional requirements of the AAT function.
- CR-003: – By undertaking system safety analyses allows the quantification of hazard rates and ensures the system will function as required within the intended operational environment. This combined with the logic risk ratios, as well as some human factors analysis, provide assurance that the system risk ratio is adequate to meet the intended TLOS.
- CR-004 – By using the system risk ratio as an input to an analysis of the allowable encounter rate requirements.
- CR-005 – By requiring the combination of design, manufacturing, and conformity to meet aerospace recommended system safety and adjacent practices.
- CR-006 – By implementing safety analysis of the functional performance control to ensure the AAT algorithm considers ground impacts.

System safety and reliability requirements are further derived in Section 3.2 of this document.

3.1.3 Functional Performance Controls

The following functional performance controls were identified by the OHA:

- System is designed and demonstrated to meet functional performance requirements (OHAZ-1, OHAZ-2, OHAZ-3, OHAZ-4).
- Functional design of DAA systems and algorithm:
    - Meet the TLOS, based on the well clear rate and risk ratio performance (NMAC, LoWC, and MAC) of the DAA system (OHAZ-1, OHAZ-2).
    - Meet right of way requirements to prevent confusion or misinterpretation of Ownship manoeuvre by intruder (OHAZ-2).
    - Minimises time between initiation of manoeuvre to return to intended flight path, whilst still ensuring safety of the primary encounter (OHAZ-3).
    - Minimises manoeuvre loads to UA structure by remaining within the intended flight envelope, whilst still ensuring safety of the primary encounter (OHAZ 3).
    - Minimises the number of false alerts through system design whilst still retaining DAA capability (OHAZ-3, OHAZ-4).
    - Takes into consideration the potential for ground impact when determining most appropriate alerting and guidance (OHAZ-3).
- Human machine control interfaces are designed clearly and succinctly, and do not confuse, cause unreasonable fatigue, or contribute to remote crew error that

could adversely affect the safety of the operation (OHAZ-1, OHAZ-2, OHAZ-3, OHAZ-4).

The identified functional performance controls all provide necessary system values and context to support the following Core Requirements:

- CR-002 – by further refining the specific controls that allow the DAA system to meet these high-level algorithm requirements.
- CR-003 – by providing the capability to deliver on the logic risk ratio as required by this requirement, as well as by providing the ability to estimate the system risk ratio using the determined logic risk ratios.
- CR-004 – by providing the capability to quantify the minimisation of the false alert rate, such that the encounter rate (particularly the induced encounter rate) can be estimated.
- CR-005 – functional requirements validation is a key part of the system safety processes mandated in the requirement. These identified functional performance controls provide the first level of decomposition for validation of these requirements later in this Guideline.
- CR-006 – By explicitly taking into consideration ground risk hazards.

Functional performance requirements are further expanded in Section 4 of this document.

3.1.4 Records and Logging Controls

The following recording and logging control was identified:

- System health and all detected encounters are logged to validate system operational performance (OHAZ-1, OHAZ-2, OHAZ-3, OHAZ-4).

This is a derived control, to ensure that it is possible to review and analyse the operational performance of the DAA system, to both capture any undesired behaviour of the DAA-equipped UAS and to allow for the provision of any data for the purposes of any safety investigation.

3.1.4.1 Derived Requirements

Table 20: Records and Logging Requirementsoutlines the derived requirements for Recording and Logging.

Table 20: Records and Logging Requirements

Req. ID	Requirement Text	Rationale
REC-001	The AAT function shall be able to record and log information and data on: • all encounters that occur during operation, and • any incidents, functional failures, anomalies that occur during operation relevant to the DAA system.	This is the initial parent requirement that ensures the DAA system includes record and log information.
REC-002	The AAT function shall be able to log data relevant to all detected intruders during a typical operation.	This requirement ensures that all relevant data as part of any encounter throughout a typical operating is captured.
REC-003	The AAT function shall be able to log system information relevant to any functional failures, incidents, or anomalies that affect the systems that make up the AAT function.	Further to the intruder data, fault and failure data is critical to ensuring continuing airworthiness and to measure the expected in-flight reliability against the estimated design reliability.

3.1.5 Environmental Qualification Controls

The following environmental qualification control was identified:

- Systems are designed and demonstrated to operate as intended, within the intended operational environment (OHAZ-1, OHAZ-2, OHAZ-3, OHAZ-4)

All of the core requirements assume that the system is operated within the intended operational environment. This control requires that the systems are designed and demonstrated to operate as intended within that defined operational environment.

This applies to the integration effort between the UA and the DAA system, as well as the GCS. In general, we can separate the "environment" into the following different categories:

- The sensor environment – i.e. the characteristics of the external environment that are intended to be sensed by the DAA sensors. This guideline will specifically focus on the detector environment, however other conventional sensors do exist (i.e. airspeed indicators, pressure sensors, GPS) and should also be shown to meet required performance.
- The physical environment – i.e. the different characteristics of the external environment that affect the functioning of the physical hardware used onboard the DAA equipped UA. These can be further subdivided into:

- The UA equipped DAA and their effect on one another (i.e. electromagnetic interference from the UA system on the DAA hardware, and vice versa, voltage spikes, vibration)
- The external physical environment (the physical characteristics of the environment external to the UA equipped DAA that can affect either the UA or the DAA system (i.e. temperature, humidity, pressure, precipitation, HF).

3.1.5.1 The Sensor Environment

In order to be able to undertake DAA functions, it is critical that the sensors used are capable of functioning as intended across the entire range of expected sensor environments expected in operation.

The set of environment possibilities have been segregated into the following three categories:

- **Background Lighting and Atmospheric Conditions** – the elements of the background that can affect the capacity of the detector to accurately detect and track intruders of interest. For example, illuminance variation and the corresponding intervening media (the atmospheric effects) can play a significant role in what is received at the sensor. The position of the Ownship and intruder in reference to the sun, and of ground features and any reflected light, can all play a role. Separately, humidity can impact the degree of reflected radiation that is received at the sensor
- **Clutter** – Clutter can take many forms, including those that occur above the horizon (clouds, birds, other aircraft that are not a threat) and below the horizon (whether the area is water (ocean, lakes etc) or land (grass, desert, snow, urban areas and the coinciding elements like cars, boats etc) . All of these impact on the ability of the DAA system to accurately detect and track intruders of interest (i.e. many birds all being detected and tracked at once causing a reduction in functionality of the DAA system).
- **Intruders of Interest characteristics** –the characteristics of the intruders of interest that the sensor is intended to detect to classify intruder parameters (primarily position in 3D space) must be understood across the combination of expected intruder of interest types (and their sense data characteristics), and the expected encounter geometries.

3.1.5.2 The physical environment

Outside of the specific external environment that is ingested by the sensor, it is critical to ensure that the DAA system and the UA are able to function in the expected operational environment. This includes the effect of the UA on the DAA system, and vice versa. Classic environmental qualification requirements should apply as per traditional aviation practices.

3.1.5.3 Derived Requirements

Considering the above, the following environmental qualification requirements have been derived and are included in the Requirement Set:

Table 21: Environmental Qualification Requirements

Req. ID	Requirement Text	Rationale
ENV-001	The DAA system shall be designed and verified for the intended operating environment.	This is the parent requirement for all environmental requirements. The functional design and safety requirements are based on the assumption that they function within the intended operating environment, this requirement ensures that this must be designed for, and verified. In order for this requirement to be met, the design and verification should take into consideration: • The physical environment all the systems involved in the AAT function within. • The possible encounter geometries, and the clutter and background environment the sensor will likely encounter during operation. • The potential interference and effects between the Ownship subsystems.
ENV-002	The physical operational environment (i.e., temperature, pressure, humidity, vibration) that the hardware/software involved in the AAT function is intended to operate within shall be defined and the systems qualified for use in that environment.	The first consideration is the capacity for the systems to endure the intended operational environments effect on the AAT function. The definition is required for both verifying the demonstration of resilience is valid, and to ensure this information is propagated through to the remote pilot.
ENV-003	The environmental conditions for safe operation of the DAA system shall be defined and included in the aircraft's flight manual (or equivalent).	To ensure a remote pilot is able to adhere to any environmental limits, and to plan flights, environmental limits must be included as a supplement to the aircraft's flight manual (or equivalent).

Req. ID	Requirement Text	Rationale
ENV-004	Verification and validation of the DAA system's ability to detect and track intruders shall adequately cover the intended operational environment.	The key external information that the AAT function is attempting to ingest accurately is intruder track data. The previous requirements (ENV-002, ENV-003) are focused on traditional environmental qualification. Because of the unique breadth and variability in the particular sense environment (which may not have a direct, adverse effect on the system function like pressure or temperature do) it is critical that the capacity of the sensor suite to detect intruders (cooperative and non-cooperative) is demonstrated across this environment. This requirement provides a traceable link to the specific requirements ENV-005 and ENV-006.
ENV-005	The encounter set used for verification and validation of the DAA system's ability to detect and track intruders shall adequately cover the expected encounters during operation.	The first key sense environment variable is the encounter set (i.e., all possible encounter aircraft types, speeds, geometries). Any testing suite must adequately cover the potential encounter environment to demonstrate generalisability of any algorithms across this encounter set.
ENV-006	Verification and validation of the DAA system's ability to detect and track intruders of interest shall adequately cover the expected intruder of interest characteristics across the intended operational environment.	In addition to the encounter sets in ENV-005, the capability of the detector to handle the characteristics of the intruder types across the encounter set need to be demonstrated.
ENV-007	The environmental clutter and background for detectors (visual, RF etc.) used for simulation and verification of the DAA system's ability to detect and track intruders shall adequately cover the expected environment during operation.	Particularly for passive sensors like EO/IR detectors, being able to handle all possible variations in clutter (sense information in the same region as potential intruders that could lead to poorer performance) and background (the sense information of the reference or background scene from which intruders or clutter is differentiated). This requirement ensures that these two key variables are covered, and acceptable performance of the sensors is verified.

Req. ID	Requirement Text	Rationale
ENV-008	The DAA system shall not have an adverse effect on the functionality of any UAS systems.	From the perspective of the DAA system (i.e., the additional hardware and software added to the UAS to provide AAT functionality not inherent to the UAS), the UAS itself is a potential source of external interference and hazard. This requirement ensures that the integration between the UAS and DAA system preserves the functioning of the UAS.
ENV-009	The UAS system shall not have an adverse effect on the functionality of the DAA system.	This is the corollary requirement to ENV-007, to ensure that the integration between the UAS and DAA system preserves the functioning of the DAA system.

3.1.6 Procedural and Personnel Controls

The following procedural and personal controls were identified:

- Operational procedures are verified and validated across the nominal states and off-nominal states to allow the safe management of the DAA system and the safety of the UAS operation (OHAZ-1, OHAZ-2, OHAZ-3, OHAZ-4).
- Operational procedures and planning are implemented to ensure that any manoeuvres conducted as a result of potential DAA operation do not cause the UAS to leave the intended operational area (OHAZ-3).
- Remote Pilots are competent to operate the system across all states and modes (OHAZ-1, OHAZ-2, OHAZ-3, OHAZ-4).

3.1.6.1 Derived Requirements

Considering the above, the following procedures and personnel requirements have been derived and are included in the Requirement Set:

Table 22: Procedural and Personnel Requirements

Req. ID	Requirement Text	Rationale
PAP-001	Human errors that can affect the system risk ratio shall be minimised to an acceptable level.	This is the parent requirements that ensures that procedures and personnel controls are included as part of the mitigations
PAP-002	Suitable operational procedures for the use of the DAA system in all nominal and off-nominal situations shall be defined.	In order to ensure remote pilots can manage the DAA system in all nominal and off-nominal states and modes, operational procedures must be developed across all these states and modes

Req. ID	Requirement Text	Rationale
PAP-003	Operational procedures shall include at least: • Pre- and post-flight inspections, • Procedures to cope with unintended adverse operating conditions (e.g., precipitation exceeds allowable operational limits for DAA system), • Normal use of DAA system procedures, • Contingency procedures for DAA system (to cope with abnormal situations), • Emergency procedures (to cope with emergency situations).	This requirement further refines what the operational procedures should include. Heavily influenced by JARUS procedures recommendations.
PAP-004	The adequacy of the Contingency and Emergency procedures shall be demonstrated effective with positive results	Because it can be difficult to analyse the effectiveness of procedures, this requirement ensures that the procedures are demonstrated effective (simulated or flight test).
PAP-005	The UAS-crew user interfaces (UIs) shall be clearly and succinctly presented and shall not confuse, cause unreasonable fatigue, or contribute to remote crew error that could adversely affect the system risk ratio.	The interface between the remote pilot and the UAS/DAA systems is a significant cause of human error. This requirement ensures the minimisation of: • Misinterpretation of DAA information by the remote pilot, • Increased workload and stress on the remote pilot leading to errors or lapses, • Overly confusing or redundant information leading to omission of procedures
PAP-006	The flight crew involved in safety critical operation of the UAS or DAA system used during the avoid traffic function shall be appropriately trained, qualified, and competent to operate the DAA equipped UAS.	This requirement ensures that the appropriate training and qualification of remote pilots who use the DAA system.

3.1.7 Continuing Airworthiness and Maintenance Controls

The following continuing airworthiness and maintenance controls were identified:

- Maintenance schedules and maintenance instructions are available to ensure the DAA system is kept airworthy and safe to fly. (OHAZ-1, OHAZ-2, OHAZ-3, OHAZ-4).

- UAS maintenance is certified by appropriately competent persons (OHAZ-1, OHAZ-2, OHAZ-3, OHAZ-4).

The system safety and reliability controls from Section 3.1.2, as well as the conformity and configuration controls discussed in Section 3.1.8, focus on the design, production, and conformity of the system, representing the contribution to 'initial airworthiness' (i.e., ensuring that an article, such as an aircraft or aeronautical product, is in an initial airworthy[20] state when introduced to service). However, throughout operation, all systems begin to deteriorate from this initial airworthy state.

Maintaining airworthiness requires the implementation of appropriate maintenance scheduling (when to do maintenance), the use of appropriate and accurate instructions for undertaking maintenance activities, and approval from appropriately licenced persons to certify that the maintenance has been undertaken correctly. All these elements are critical to ensuring the continued airworthiness of a DAA equipped UAS. the above controls ensure that the ways in which the system was defined to meet the core requirements initially are not voided by the degradation of systems over time.

3.1.7.1 Derived Requirements

Considering the above, the following continuing airworthiness and maintenance requirements have been derived and are included in the Requirement Set:

Table 23: Continuing Airworthiness and Maintenance Requirements

Req. ID	Requirement Text	Rationale
CAM-001	Continuing airworthiness of the UAS and DAA system shall ensure the ongoing airworthiness of the UAS and DAA system.	Parent requirement to ensure that continuing airworthiness controls are captured.
CAM-002	If necessary, a maintenance schedule shall be developed that ensures the systems that make up the AAT function continue to be airworthy.	This requirement drives the continuing airworthiness management of the DAA system, by requiring a maintenance schedule is developed if necessary.
CAM-003	Any maintenance processes that need to be undertaken shall be defined.	This requirement ensures any maintenance instructions (including defect rectification, troubleshooting) are defined.
CAM-004	Personnel responsible for certifying that maintenance has been completed in accordance with applicable instructions, and responsible for releasing the aircraft will be appropriately competent to complete this task	The last element, ensuring that continuing airworthiness processes are undertaken correctly and are certified by an appropriate person before release to service.

[20] Where airworthy means that an article conforms to its approved design **and** is in a condition for safe operation.

3.1.8 Conformity and Configuration Controls

The following conformity and configuration controls were identified:

- System conformity and configuration is controlled to prevent non-approved configurations from being released to service (OHAZ-1, OHAZ-2, OHAZ-3, OHAZ-4).
- DAA system manufactured in accordance with aerospace best practice manufacturing processes (OHAZ-1, OHAZ-2, OHAZ-3, OHAZ-4).

3.1.8.1 Derived Requirements

Considering the above, the following conformity and configuration control requirements have been derived and are included in the Requirement Set:

Table 24: Conformity and Configuration Control Requirements

Req. ID	Requirement Text	Rationale
CFG-001	The configuration control of software and hardware shall meet appropriate standards to ensure only approved configurations are operated.	This requirement ensures that configuration management is included as a control for all hardware and software involved in the AAT function.
CFG-002	All systems involved in the AAT function shall be manufactured to ensure conformity of the manufactured items to the design at a level commensurate with the risk of the part not being conformant.	To ensure that the physical hardware and software manufactured conforms with the approved design, this requirement is required.

3.2 Functional Hazard Analysis

The full FHA can be found in Appendix F of the Guideline.

As identified by the OHA, a key hazard control for a DAA System is the appropriate functional and safety performance of the AAT function. In general, aviation best practice for the design of a system begins with a Functional Hazard Analysis (FHA). This section of the document provides the results of an FHA for the AAT function as described in Section 2.4 using the TLOS, hazard severity, and external event probability concept discussed in Section 2.5.2, Section 2.7, and Section 4.1 of Annex F to this guideline respectively.

3.2.1 Functional Hazard Analysis – Summary

Four hazards were assessed in the FHA:

- **FHA-001:** Loss of Function (Annunciated) (Minor)
- **FHA-002:** Hazardously Misleading Malfunction – Unannunciated Loss of Function (Major)
- **FHA-003:** Hazardously Misleading Malfunction - Increased Risk of Collision (Major)
- **FHA-004:** Inadvertent Operation Outside of Intended Operational Environment (Minor/Major[21])

Using the external event concept, the following requirements verification means were determined to ensure that these hazards were appropriately managed:

Table 25: Functional Hazards - Severity, Design Assurance Levels, and Verification

FHA Reference	Hazard Severity	DAL	QPF	Verification Means
FHA-001 Annunciated loss of function	Minor	Primary: DAL D Secondary: DAL E	<1×10^{-2} pfh	**FHA with Design and Installation Appraisal** per AC 23.1309-1E, sections 17(a) and (b). Showing that a detectable loss of function can be isolated and that the UAS can safely complete appropriate flight termination procedures. The FHA with Design and Installation Appraisal should show there is appropriate independence between the in-flight detection system and the DAA system such that the cause of a loss of function does not also cause a loss of detection capability. **Note:** if the common failure results in the aircraft crashing into the ground, this may be acceptable from an air risk perspective only, as the aircraft will not continue to pose a MAC threat to other aircraft users.

[21] The Hazard Severity of FHA-004 depends on whether avoidance manoeuvres are commanded and executed by a human Remote Pilot in Command (RPIC), or automatically by the UAS flight control system. These two cases are treated distinctly in subsequent discussions.

FHA Reference	Hazard Severity	DAL	QPF	Verification Means
FHA-002 Unannunciated loss of function	Major	Primary: DAL C Secondary: DAL C	<1×10^{-4} pfh	**Preliminary System Safety Assessment (PSSA-001)**. Demonstrating appropriate functional development assurance of the Avoid Air Traffic function, and pre-flight functional test. Undertaking appropriate software/data development assurance of the avoid air traffic function and pre-flight functional test to minimise systemic development errors. Undertaking appropriate Fault Tree Analyses / Failure Modes and Effects Analyses to show that the appropriate reliability of both of these functions, either through redundancy / independence / separation (**per AC 23.1309-1E, section 17c(4)**), or through a combination of qualitative FMEA/FTA supported by failure rate data to show the appropriate QPF is met (**per AC 23.1309-1E, section 17c(3)**)
FHA-003 Increased Collision Risk from Malfunction	Major	Primary: DAL D Secondary: DAL D	<1×10^{-4} pfh	**See FHA-002** This will be covered in the requirement to ensure that there is no unannunciated loss of function. The key difference is that it assumed that the in-flight detection mechanism cannot detect a hazardously misleading malfunction, and this can only be detected with a functional built-in test undertaken before each flight. **PSSA-001** will need to cater for the hazardously misleading malfunction hazard as well as the unannunciated loss of function hazard.
FHA-004 (RPIC) Inadvertent operation outside of intended operational area	Minor	Primary: DAL D Secondary: DAL E	<1×10^{-2} pfh	If RPIC issues command: **FHA with Design and Installation Appraisal** per AC 23.1309-1E, sections 17(a) and (b). The FHA with Design and Installation Appraisal should show there is appropriate independence between functions/systems intended to prevent inadvertent operation outside of the intended operating environment.

FHA Reference	Hazard Severity	DAL	QPF	Verification Means
FHA-004 (Automatic) Inadvertent operation outside of intended operational area	Major	Primary: DAL C Secondary: DAL D	$<1\times10^{-4}$ pfh	If commands issued automatically: Preliminary System Safety Assessment (**PSSA-002**) Demonstrating appropriate functional development assurance of the Avoid Air Traffic function ensuring operation within the intended operational environment. Undertaking appropriate software/data development assurance of the Avoid Air Traffic function ensuring operation within the intended operational environment to minimise systemic development errors. Undertaking appropriate Fault Tree Analyses/ Failure Modes and Effects Analyses to show that the appropriate reliability of both of these functions, either through redundancy/ independence/ separation (**per AC 23.1309-1E, section 17c(4)**), or through a combination of qualitative FMEA/FTA supported by failure rate data to show the appropriate QPF is met (**per AC 23.1309-1E, section 17c(3)**)

3.2.2 Derived Functional Architecture

Given the above FHA, the following functional architecture has been determined necessary for the AAT function to meet the requirements of the FHA:

- **An independent, in-flight failure detection monitor.** In order for FHA-001 to be legitimately managed (i.e., there is the capacity for detection of a loss of function), as well as to increase the architectural resilience of the AAT function to the functional failure associated with FHA-002, an independent, in-flight failure detection monitor function is required. Alongside this, appropriate procedures and processes are required to ensure that upon detection of a DAA failure, the aircraft can safely end the flight, or return to an operational state.
- **A pre-flight, built-in-test to prevent the commencement of flight with a failed or degraded AAT Function**. Alongside an in-flight fault detection monitor, the ability to detect latent failures that cannot be picked up by the in-flight fault detection monitor should be minimised by the use of a pre-flight built-in-test, that ensures the functionality of the AAT function before flight. Appropriate procedures and processes to ensure the correct functioning and response to the results of the pre-flight test are required alongside this mitigation.

- **An independent, in-flight containment function.** To mitigate FHA-004, an additional function preventing the inadvertent operation of the remainder of the AAT function outside of the intended operational environment is required.

3.2.3 Design Assurance of Neural Networks

While not inherently necessary for the development of an AAT Function, it is highly likely that many DAA Systems will incorporate neural networks in their design, particularly for Detection, Tracking, and Classification of intruder aircraft, and from a range of sensors. For those DAA systems that incorporate neural networks in any portion of the system, for safety-related functions, the implemented network must be assured against a recognised standard or guide to minimise the probability that the neural network will introduce errors into the system's functioning.

EASA recently published the Concepts of Design Assurance for Neural Networks (CoDANN) [20] which explores a potential means of design assurance for neural networks. This domain is relatively immature compared to most aviation domains with guides and recommended practices only being proposed in the last few years. Fundamentally, for a neural network to perform as specified, some form of assurance should be applied to all the elements that make up the design of that network – in addition to being able to statistically verify performance. This is because the complexity of a neural network is so vast that verifying performance, even at high levels of statistical confidence, is unlikely to explore a majority of the functionality embedded in the neural network. The CoDANN Report [20] provides guidance on many topics that contribute to design assurance of neural networks including:

- Dataset management and verification,
- Machine learning model verification,
- Inference stage verification,
- Runtime monitoring,
- Learning assurance artifacts,
- Transfer learning,
- Synthesised data,
- Model evaluation,
- FHA and DAL assignment,
- Common Mode Analysis, and
- Neural network FMEA.

Future iterations of this safety case may specify additional requirements for neural network design assurance.

3.2.4 Derived System Safety and Reliability Requirements

Given the discussion in Sections 3.2.1 through 3.2.3, the following system safety and reliability requirements are derived:

Table 26: System Safety and Reliability Requirements

Req. ID	Requirement Text	Rationale
SSR-001	The functions and systems involved in an annunciated loss of function of the AAT function shall be developed to FDAL D, and a maximum failure rate of less than 1 per 100 flight hours (1×10^{-2} pfh).	Based off FHA-001 outcome. Uses current failure condition assessment criteria (catastrophic MAC) driven by external event probabilities. FHA uses FAA AC 23.1309 [19] as backbone to assessment.
SSR-002	The functions and systems involved in an unannunciated loss of function of the AAT function shall be developed to a Function Development Assurance Level of FDAL C, and a maximum failure rate of less than 1 per 10,000 flight hours (1×10^{-4}4 pfh).	Based off FHA-002 outcome. Uses current failure condition assessment criteria (catastrophic MAC) driven by external event probabilities. FHA uses FAA AC 23.1309 [19] as backbone to assessment.
SSR-003	The functions and systems involved in a hazardously misleading malfunction of the AAT function shall be developed to a Function Development Assurance Level of FDAL C, and the maximum allowable probability of the event shall be less than 1 per 10,000 flight hours (1×10^{-4} pfh).	Based off FHA-003 outcome. Uses current failure condition assessment criteria (catastrophic MAC) driven by external event probabilities. FHA uses FAA AC 23.1309 [19] as backbone to assessment.
SSR-004	The functions and systems involved containing the AAT function to the intended operational environment shall be developed to: a. In the case of a DAA system that requires the remote pilot to manually manoeuvre the UAV, Development Assurance Level D, and the maximum allowable probability of the event shall be less than 1 per 100 flight hours (1×10^{-2} pfh). b. In the case of a DAA system that has the ability to automatically manoeuvre the UAV, Development Assurance Level C, and the maximum allowable probability of the event shall be less than 1 per 10,000 flight hours (1×10^{-4} pfh).	Based off FHA-004 outcome, which was split based on whether manoeuvres were automated or required pilot input Uses current failure condition assessment criteria (catastrophic MAC) driven by external event probabilities. FHA uses FAA AC 23.1309 [19] as backbone to assessment.

Req. ID	Requirement Text	Rationale
SSR-005	The DAA system shall incorporate Loss of Function Detection functionality capable of detecting a loss of the Avoid Air Traffic function while airborne.	Architectural requirement to ensure that there are two independent functions that ensure the AAT function occurs, or the flight managed via contingencies: • AAT function is working. • Detected loss of function, notifying the RP/AP to undertake contingency action.
SSR-006	The DAA system shall incorporate Functional Testing to identify any malfunctioning functions making up the DAA system before flight.	An assumed corollary to the loss of function detection that can occur on the ground before flight. This function test can be used to ensure that at the point of release, the AAT function was operating as intended (i.e., there were no latent failures before this test that are not captured before flight).
SSR-007	The DAA system shall incorporate a means to contain the operation of the DAA system to within the intended operational environment.	Alongside SSR-005 and SSR-006, the other required functional architecture ensures the system does not operate outside of the intended operational environment.
SSR-008	Where the DAA System uses machine learning for any safety-related functions the learning process shall be assured against an authority recognised standard or guide.	Noting the likely use of machine learning of some kind to generate the capability to detect objects, this is a catch all requirement ensures that any use of machine learning is captured using a known or accepted standard for development assurance of a learning process.

4 Functional Requirements Validation

As described in Section 3.2, the completion of the FHA has driven both functional architecture and functional development assurance requirements. This section will first fully define the complete Avoid Air Traffic Function for the purposes of this Guideline, including the additional functional architecture required, as identified in Section 3.2.2.

Subsequently, this section will derive functional requirements for the AAT Function providing traceability to higher level requirements and justification of their derivation and inclusion in the Requirement Set.

With these requirements fully defined and substantiated, an end-user of this Guideline can take the Requirement Set as a comprehensive basis for an AAT Function, and then determine the lower-level subsystem and component requirements, based on their specific design and implementation.

4.1 Defining the Complete Avoid Air Traffic Function

Given the definition of the AAT Function in Subsection 2.4.1 and the additional required safety functional architecture from Subsection 3.2.2, the complete AAT function can be defined here as the set of:

- The **Core** Avoid Air Traffic Functions, which consists of the AAT Function elements that perform the actions of Detect and Avoid and allow the system to meet the high level DAA goal. This consists of:
    - Detect Function (DET)
    - Track Function (TRK)
    - Decide Function (DEC)
    - Command Function (COM)
    - Execute Function (EXC)
    - Convey – Inter-functional (CVY)
    - Convey – UI function (UI)
- The **Supporting** Avoid Air Traffic Functions, which consist of the additional functionalities identified by the OHA and FHA to ensure correct and safe operation of the Core Functions. They are the following:
    - In-Flight Monitor function (IFM)
    - Containment Function (CON)
    - Pre-Flight Test (PFT)

These functions are visualised below in Figure 12:

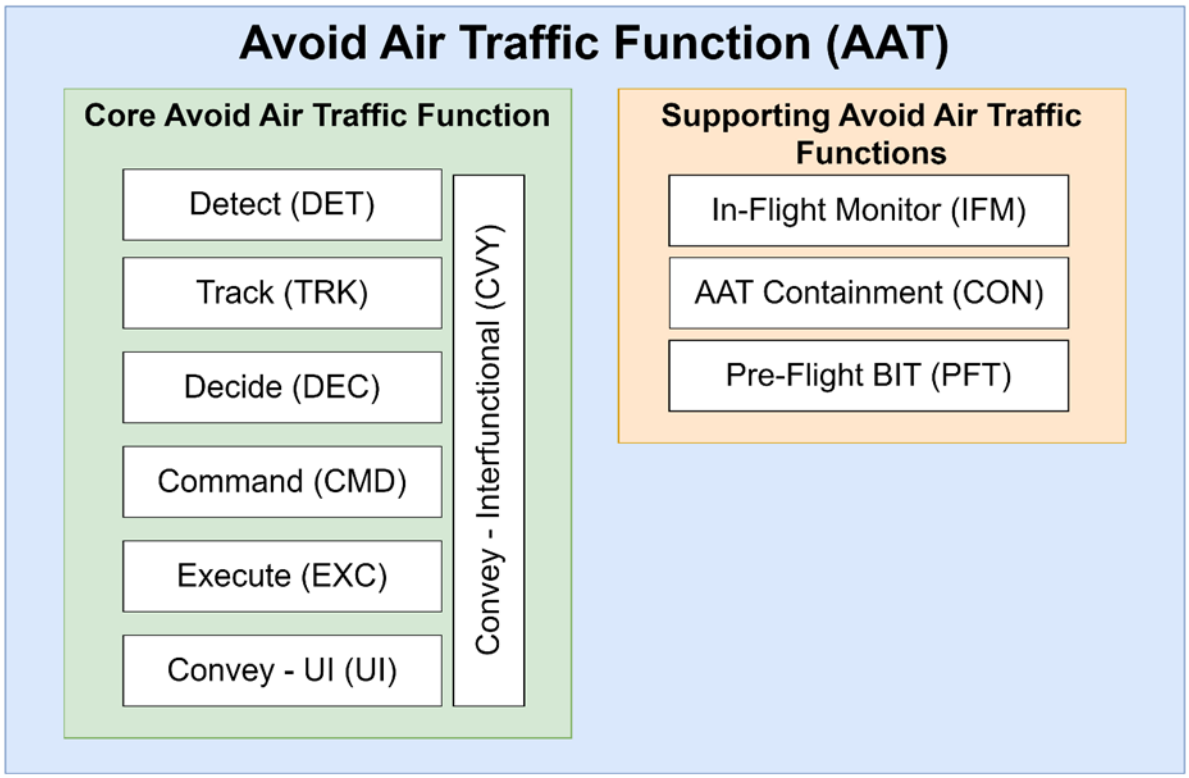


Figure 12: Avoid Air Traffic: Functional Groupings

These functions are defined for the purposes of the Guideline, and the associated Requirement Set, in Table 27 below:

Table 27: Avoid Air Traffic – Complete Functional Definition

Function Name	Category	Description
Detect	Core	This function ingests sense data from the external environment, filters the data as required, and outputs any detected object of interest's data (i.e., an estimate of the detect objects position in space) to the Track Function via the Convey Function.
Track	Core	This function's purpose is to create, update, and remove tracks (i.e., correlate detect data into identified objects movement in space and time within a range of the Ownship) and then provide tracked objects data (i.e., position, velocity, heading) to the Decide Function via the Convey Function.
Decide	Core	The Decide Function's role is to classify and prioritise tracked objects as threats (i.e., may pose a collision risk), and to then, if necessary, calculate the most appropriate alerting and manoeuvre and guidance to the Command Function.

Function Name	Category	Description
Command	Core	The Command Function's purpose is to issue a manoeuvre command, based upon the received alerting and manoeuvre guidance from the Decide Function. This Command Function can be: • Human induced (i.e., a remote pilot provides the manoeuvre command). • Automated (i.e., the UA commands the aircraft to manoeuvre based on the guidance and alerts the remote pilot to this occurring). In the case of an **automatic manoeuvre**, the manoeuvre command is issued to the flight control computer. This is then provided to the Execute Function for implementation. Configured data is also provided to Ownship and the RPS via CNPC link to notify the remote pilot that an automatic manoeuvre is underway and when the manoeuvre is completed. Note it may be that although automatic control is available, the remote pilot can, at any point, interrupt and regain control of the UAS if necessary. It is also possible that an automatic manoeuvre is initiated only if a manual manoeuvre has not been commanded by the remote pilot earlier the latest possible point remain well clear. In the case of a **manual manoeuvre**, the manoeuvre data presented by the Decide Function is acted upon by the remote pilot from the RPS, sending command data over the CNPC link to the flight control system which is then provided to the Execute Function for implementation (this provision of data is completed via the Convey Function).
Execute	Core	The Execute Function receives a command and executes the command to physically control the aircraft through the manoeuvre.
Convey	Core	The Convey Function provides the interface between all of the previously mentioned functions and any other UAS functions and ensures all required DAA information is provided to the remote pilot.
In-Flight Monitor	Supporting	The purpose of this function is to monitor the core AAT functions and the AAT Containment Function during flight, and to detect any failures or faults in these functions. The In-Flight Monitor Function should provide health information to the remote pilot such that they can undertake the appropriate procedures in the event of a fault or failure.

Function Name	Category	Description
Containment	Supporting	The AAT Containment Function is intended to ensure that the AAT only operates within the intended operational environment. This function should take into consideration any: • States or modes that the pilot sets and the expected functionality of the AAT function, • Geographical restrictions implemented by the remote pilot, • Phases of flight within which the AAT function is not intended to operate (i.e., take-off/landing), and • Operation of the AAT function when the system is in a faulty or failed state. It is expected that if the AAT Containment Function undertakes any action, the remote pilot will be notified immediately. It is assumed that alongside any functioning of the AAT Containment Function, there would be appropriate procedures and processes for the remote pilot to undertake to manage any contingency.
Pre-Flight Test	Supporting	The pre-flight built in test is an additional fault detection mechanism that is intended as a functional test of all other functions before flight. This should identify any latent failures or faults that may have occurred in the previous flight or during the time between flights. Additionally, ensuring all systems are functional before flight reduces the time within which a latent failure, particularly one not detectable by the In-Flight Monitor Function, can occur.

4.1.1 Core AAT Function – Relationship to the Core DAA Objectives

At the core of the entire Detect and Avoid problem space, there are several key variables. But potentially, the most critical is **time**. For any (detectable) encounter, there needs to be sufficient time between the initial detection through to the execution of resultant avoidance manoeuvres to remain well clear or avoid a collision. There is a delicate balance between maximising the amount of time before an event (Well Clear Violation, NMAC or MAC), and the capability of a physical system to provide that maximised time.

The maximisation of available time, for a given airspace with known intruder geometries and characteristics, is achieved through the maximisation of detection range. Depending on the detector equipment used, there are various limits to the ability to increase detection range. For EO/IR detectors, this is mostly influenced by instantaneous field of view (the spatial resolution of each pixel) at the range required.

If the Intruder is captured across too few pixels at this range, it may not be able to discriminate an aircraft from other information in that scene. Conversely, radar detection requires that for an increase of the detection range, the power requirements increase to the fourth power.

The time available, based upon the ability to detect an intruder at a given range (at given closure rates/geometries) is needed to facilitate the complete Detect, Track, Decide, Command, Manoeuvre, Convey cycle. Of particular note, the following variables have a significant effect on the time taken to complete this process:

- **Human in the loop decision making time:** This is usually assumed to be on the ranges of 5 seconds or greater, which when dealing with a closure speed of ~200 knots, the distance covered by the two aircraft during the decision time is ~500m (~1500 ft).
- **Manoeuvre time:** This is driven by the turn rate of the Ownship and the speed of the Ownship, which defines the turn radius of any manoeuvre. Fixed-Wing UAS are usually much less manoeuvrable (in classic aviation sense of turn rates and climb/descend rates) than crewed aircraft. Rotorcraft, multi-rotors may have some unique qualities that result in increased manoeuvre capabilities compared to fixed wing UAS.
- **Command and control link latency:** which can add on the realms of 1 or more seconds to any complete uplink-downlink cycle.

The time it takes the Ownship to detect an intruder, associate the detection to a track, determine appropriate alerting and guidance, issue the relevant commands, and execute a manoeuvre, such that the Ownship remains well clear of the intruder, given the likely intruder and Ownship closure rates, is the critical **declaration range**.

The declaration range should be appropriately analysed and defined, given the relevant parameters described above, such that a clear demonstration of an effective detection volume is possible (i.e. the declaration range is nominally inside the detection volume) and the risk ratios are met (both loss of well clear and NMAC risk ratios).

Two examples of encounters that would lead to detected Well Clear Violation are provided below. In both cases, the time (and equivalently distance) taken to complete the detect, track, decide, command, execute cycle (measured as being complete once the aircraft has reached its closest point of approach during the manoeuvre and is Well-Clear).

There are potentially infinite encounters that could exist, and for the i^{th} encounter, the declaration range (to prevent a well clear or an NMAC) can be computed:

$$t_{DR,i} = t_{det} + t_{trk} + t_{dec} + t_{cmd} + t_{exc}$$

$$d_{DR,i} = \left(-\boldsymbol{s_{rel}}(t) \cdot \boldsymbol{v_{rel}}(t)\right)_i \times t_{DR,i}{}^{22}$$

[22] This equation is written for closing velocities between the intruder and Ownship.

In theory, if the AAT function can be shown to be able to complete a manoeuvre to remain well clear within the declaration time across a significant proportion of all encounters, then it will be possible to show the relevant risk ratios are met.

4.1.2 Prevent Mid Air Collisions

The key purpose of the AAT function is to prevent Mid-Air Collisions. By ensuring that the Logic Risk Ratios are met, by definition the AAT function will meet this high-level goal. This applies to both preventing Mid-Air Collisions, and attempting to remain well clear.

The risk ratios are a single number, which seem simple but hide significant complexity underneath them. The purpose of this guideline is to elicit the functional requirements that ensure achievement of the risk ratios (both system and logic) across all potential operational environments to meet this high-level algorithmic goal. All core AAT functions (Detect, Track, Decide, Command, Execute) feed into meeting this algorithmic goal.

4.1.3 Do no harm

4.1.3.1 To Ownship

Protection of the Ownship has both safety and commercial aspects to consider. From a safety perspective, if the Ownship is damaged from the act of undertaking a manoeuvre (either by exceeding the aircraft's flight envelope, or by impacting the ground or ground obstacles), persons on the ground may be harmed. Additionally, if operating at altitude, a damaged UAS crashing to the ground poses an air hazard to those aircraft operating underneath the UA. Commercially, it is not considered viable to destroy the ownship every time a potential collision is detected.

To ensure this requirement is met, it is required that any avoidance manoeuvre guidance (or command) includes consideration of:

- The possibility of the manoeuvre leading to a ground impact, under control from the remote pilot or automated maneouvre;
- The manoeuvre exceeding the nominal flight envelope of the Ownship, causing it to lose control and impact the ground.

Primarily this is goal will need to be met by the Decide and Command core AAT functions, but is influenced by the other functions (i.e. how much time there is to make a manoeuvre can influence how much stress a manoeuvre should place on the Ownship to meet its risk ratio requirements.

4.1.3.2 To coordination between encountering aircraft

Coordination between two aircraft involves the ability of the two aircraft to both predict the other aircraft's manoeuvres during an encounter event, and that the predicted manoeuvre's intent is to protect both aircraft. Although this guideline is intended for uncontrolled Class G operations, with non-coordinating aircraft, there still should be some consideration when determining any avoidance manoeuvres. These may consider:

- The rules of the air, particularly give way rules. Although in ASSUMP-OSED.25, it is assumed that the responsibility for separation and collision avoidance is solely on the UAS, this shouldn't be interpreted as not in any way considering the potential for an intruder to detect the Ownship. To that end, the expected manoeuvre, given the rules of the air, in an encounter scenario, should be considered to prevent confusing an intruder that does detect the Ownship, and attempts to make an avoidance manoeuvre.
- Any future standards for equipage between different classes of intruder (IFR, VFR, UAS etc.) that will include the ability to coordinate with an appropriately equipped intruder.

The determination of appropriate avoidance manoeuvre is held between the Decide and the Command core functions.

4.1.3.3 To third parties on the ground

Alongside the requirement to protect the airworthiness of the Ownship, it is clear from core requirement 6 (CR-06) that an impact with the ground poses a potential hazard to third parties on the ground. In addition to the considerations for any avoidance algorithm to protect the Ownship, this should be further reinforced to ensure that persons on the ground are protected from a potential ground impact due to the AAT Function.

4.1.4 Minimise disruption to the National Airspace System

Achieving the ultimate objective outlined in Core Requirement 2 (CR-002), which involves minimising disruption to the National Airspace System (NAS), is viewed as a relatively minor requirement within the operational context of this Guideline. Nevertheless, the AAT Function is expected to factor in the impact of its manoeuvres on the NAS, always ensuring that such considerations do not compromise the fulfillment of higher-priority goals. Specific examples of this consideration includes:

- Minimising the overall deviation from the track during a manoeuvre, thereby reducing the likelihood of induced encounters during any avoidance manoeuvres.
- Recognising that adherence to the imperative of causing no harm to coordinating traffic, as described in 4.1.3.2, will inherently contribute to the mitigation of disruption to the NAS.

4.2 Requirements Derivation and Validation

As described in Section 2.4.3, a potential avenue for functional failures is through latent defects, which are errors occurring in the development of the function itself (depicted as one of the branches in Figure 6). Mitigating the risk of such latent defects is vital when designing a system in accordance with a set of requirements. The Verification and Validation process plays a crucial role in achieving this reduction in risk, encompassing:

- Verification to ensure the system complies with the requirements (often expressed as "Did we build the system right?").
- Validation of the requirements themselves (expressed as "Did we build the right system?").
- Verification of a system must be carried out during its development, and therefore, the DAA T&E Guideline is not equipped to perform verification but aims to provide guidance (Future Appendix G to this Guideline). The guideline strives to furnish a valid set of requirements within the operating context outlined in the OSED at Appendix A.

In assuring the design of an intended function, it is imperative to:

- Establish requirements traceability from high-level to low-level requirements (for non-derived requirements).
- Test, analyse, or model to validate that these requirements align with objectives[23].

This document section undertakes limited validation of the lower-level functional requirements within the Requirement Set. It achieves this by providing rationale for the inclusion of those requirements as they are derived and establishing traceability to higher-level requirements.

However, it's important to note that this Guideline does not offer traceability from aircraft-level functional requirements to subsystem-level and component-level requirements or implemented code. The responsibility falls on the applicant to present a comprehensive and defensible Safety Case argument. The hope is that the use of the Requirement Ret in designing the DAA System, combined with the rationale provided against the requirements in this and other sections of the document, can contribute significantly to forming a robust part of that safety argument.

4.2.1 AAT Function - General Requirements

The following section describes emergent properties of the AAT Function that do not specifically align with any of the core or supporting Functions or are common across them all.

4.2.1.1 States, Modes, and Overrides

It is critical that the interrelationships between the core and supporting AAT functions are managed, and functionality across all potential operating states and modes is retained. Due to the required architecture and behaviours of a DAA system, it is implicit that several different modes of operation are necessary. These include at least the following:

[23] As per ss. 5.4.6(b), (c), and (d) from [7]. As this section is about a novel avoid air traffic function, similarity is not considered a viable means of validating the functional requirements.

- A "**Nominal**" mode – This mode includes the full functionality of the avoid air traffic function.
- A "**Pre-Flight Test**" mode – As part of the pre-flight built-in-test function, the system is to be functionally examined for any faults. This necessitates a separate mode specific to the pre-flight test function.
- A "**Surveillance Only**" mode – Throughout flight, there will be situations where the remote pilot may not need or want DAA alerts due to the state of flight (take-off and landing) or other operational constraints. In these situations, a mode which only provides surveillance information to the remote pilot is appropriate.
- An "**Isolated**" mode – where the Containment Function (or the RPIC) locks out the DAA System from operating. This is used to prevent the system from operating in areas where it is not desired, or it is unsafe to do so.
- Various "**Degraded**" modes where one or more elements of the system have been identified as having failed, and the system adapts or disables its functionalities to prevent unsafe behaviour.

In order for the full behaviour of the system to be adequately understood, these states and modes, and any automated behaviours switching between them, must be defined and captured in the relevant documentation for the system. The RPIC must be able to determine the current state /mode of the system during operation and be alerted to any changes between modes. Any automated behaviour must also be accompanied by a manual override by the RPIC to ensure that the aircraft can be controlled as needed by the operator responsible for flight safety.

4.2.1.2 Ownship Performance Estimation

The AAT Function uses an estimate of the Ownship's behaviour as a point of reference for several key elements of Detect and Avoid. This includes calculation of trajectories and determination of the appropriate avoidance manoeuvres. Accurate and reliable estimates of the Ownship's performance and behaviour at ang point in an operation is critical to prevent either misleading guidance to operators, or to prevent the execution of unsafe manoeuvres.

4.2.1.3 Timing

Detect-and-Avoid is a time-sensitive, and time-critical capability. Furthermore, DAA System elements may be located at significant distances from each other and may experience significant latency in communication. The total time taken across the AAT function needs to be established, to ensure there is enough time for a Well-Clear Violation to be prevented.

Additionally, to ensure the correct calculation of intruder tracks, and appropriate manoeuvre guidance, it is critical that each critical piece of data is timestamped (i.e. a detection frame's actual time of creation, which will be different to the time of ingestion into the track function). This leads to the requirement that a suitable time

reference must be used for all elements of the system, and the accuracy of this time reference needs to be established.

4.2.1.4 Derived Requirements

Considering the above discussions, the following requirements related to high-level behaviour of the AAT Function have been derived and are included in the Requirement Set:

Table 28: Avoid Air Traffic Function – High-Level Derived Requirements

Req. ID	Requirement Text	Rationale
AAT-001	The functional performance of the avoid air traffic function shall be such that the Logic Risk Ratio requirements are satisfied.	This requirement is a traceability requirement, ensuring that we allocate the correct functional performance assurance that make up a portion of the system risk ratio

Req. ID	Requirement Text	Rationale
AAT-002	The operational states and modes of the AAT function shall be defined. The AAT Function shall be able to transition between modes safely. At a minimum, the AAT function shall have a: ○ **Nominal Mode** – used when the AAT Function is operating as intended within the intended operational environment. ○ **Surveillance Only Mode** – used during stages of flight where the AAT function is operating as intended, but alerting and/or guidance is not needed and may cause confusion (i.e. take-off and landing). ○ **Pre-Flight Test Mode** – used to undertake pre-flight testing of the AAT Function to identify any faults or failures before flight. ○ **Isolated Mode(s)** – used (automatically or manually) to isolate the entirety of AAT Function (Core and Supporting Functions) when an in-flight failure has occurred, or the AAT function operates outside of the intended operational environment. Additional modes shall be defined and established.	This is a derived requirement. Already from the above requirements It is required that the system can: • determine if there is a loss of function implies being able to turn off or not allow output of AAT. • prevent operation outside of the intended operational environment, implies being able to select whether to use system or not. • undertake a functional test on the ground (i.e., function is tested without actually implementing guidance). These are the minimum set of states and modes.
AAT-003	The remote pilot shall have the ability to switch between different states and modes under all operating circumstances.	Derived requirement. Ensures that under all circumstances, the remote pilot can control the state and mode that the DAA system is in. Prevents any unwanted logic preventing the safing of the system, or other unintended operation of the DAA system through lockout of the appropriate state or mode.

Req. ID	Requirement Text	Rationale
AAT-004	If there is any automated switching of modes, the remote pilot shall have the ability to disable automated mode switching, without affecting the ability of the pilot to manually switch modes.	The ability for the system to automatically change the mode of the AAT function requires that the person in charge of the safety of flight (RPIC) can override any decisions.
AAT-005	The criteria (manual and/or automated) for transitioning between states and modes shall be established across all phases of flight under all operating circumstances.	if there is any automated switching, the associated criteria need to be established for predictability of system performance.
AAT-006	For any state or mode changes that have a potential impact on safety of flight, all switching between these states and modes shall be accompanied by visual and/or aural alerts to the remote pilot.	If there is automated switching, the remote pilot must be informed to alter/adjust operation as required by the change of modes. If done manually, it is still beneficial to notify and ensure that the pilot is aware of the current mode of the DAA system.
AAT-007	For any automated decision-making capability, the prioritisation of automated decisions and RPIC input shall be defined to prevent unwanted interactions between inter-automated or automated/manual control disagreements.	Driven by the chance that defining any automated modes will need appropriate prioritisation to prevent disagreements between RPIC and DAA, RPIC and UA, UA and DAA.
AAT-008	There shall be a means to safely restart the AAT Function in-flight in the event that the AAT Function is not functioning as intended.	If there is any in-flight failure or poor performance of the AAT function, it is more beneficial that this function can be restarted in flight safely, than cease the mission.
AAT-009	the DAA System shall incorporate a means of estimating the flight performance of the Ownship when calculating manoeuvres.	To calculate avoidance manoeuvres for intruders, an estimate of the manoeuvrability of the system is required. This is an input to the Decide Function.
AAT-010	The estimations of aircraft performance shall be suitably accurate (or are conservative) to ensure that a commanded avoidance manoeuvre will not increase the risk of MAC, NMAC, or LoWC.	A poor estimation of aircraft performance may result in the recommendation and subsequent execution of manoeuvres that increase the risk of LoWC, NMAC or MAC.

Req. ID	Requirement Text	Rationale
AAT-011	The declaration range (and time) based on the expected intruders and Ownship characteristics shall be established across the range of possible encounter geometries.	Establishing this value for the declaration range allows this to be compared to the detection volume and time taken to complete the AAT function.
AAT-012	The AAT function shall refer to a global timing schema to ensure appropriate measurement of time across the entire functioning of the AAT function.	Time is a critical factor in ensuring timely alerts and guidance. To facilitate a harmonised picture of time across the functions, a global time variable being tracked is needed.
AAT-013	The global timing schema accuracy shall be suitable.	This is a requirement directly driven by AAT-008, if there is a global timing scheme, the accuracy of the timing should be established.
AAT-014	The time taken (average/ 95%) to complete a full cycle of the AAT function across all operating environments shall be established.	Driven by AAT-012 the measurement of timing is critical.
AAT-015	The avoid air traffic function shall consist of the: • Detect Function • Track Function • Decide Function • Command Function • Execute Function • Convey Function • In-Flight Monitor Function • Containment Function • Built-In Test Function	These functions are required to both; undertake the AAT function in the intended environment and provide functionality required by the FHA implemented functional architecture.

4.2.2 Detect Function

As described earlier, the Detect Function is responsible for assimilating sense data from the external environment, refining the data as necessary, and forwarding the information on any identified object of interest (i.e., an estimate of the detected object's position in space) to the Track Function through the Convey Function. To execute its intended function, the Detect Function must perform the following processes:

- Ingest sense data (at a single or across multiple time steps), including high-resolution image frames from the EO/IR sensor for VFR aircraft and ADS-B signals from IFR aircraft.

- Filter and clean the data for use in subsequent internal steps [21]. For example, it may be necessary to align two successive image frames for use in the detection algorithm to compensate for sensor movement.
- Execute the "detection" of objects using a detection algorithm, resolving parameters of interest (e.g., object position and position uncertainty in 3D space or range and bearing, time of detection, confidence in the detection being accurate).
- Output the detected objects and the relevant predicted parameters of input data through a detection algorithm to the relevant functions (i.e., track, decide, etc.) via the Convey function.

To accomplish these steps, several derived requirements must be established:

- Sense data is meaningful when compared to a reference time and location; hence, additional data must be ingested to ensure the correct localisation of sense data in time and space, accounting for potential movement or vibration effects.
- In the case of a camera system, obtaining frame alignment between previous and current frames is crucial to compensate for camera motion.
- Objects must be classified, distinguishing between intruders of interest and non-interest. The definition of what is considered an intruder of interest or non-interest needs clarification.
    - Intruders of non-interest may depend on the system's sensitivity, which may lead to more frequent detection of other objects (e.g., cars, trains) considered non-interest intruders.
    - Intruders of interest beyond crewed aircraft may include objects capable of causing a collision with the UA (e.g., another UA, large birds). However, the system's capability to detect and avoid these objects successfully is beyond this guideline's scope.
- Given the two types of intruders (cooperative and non-cooperative), the system must have a means to detect both.
- To verify the detector(s) capability, its characteristics (including key detection parameters) should be quantified for simulation replication, troubleshooting, and incident investigations. At a minimum, the following detection parameters should be defined and demonstrated (for both cooperative and non-cooperative intruders of interest)
    - The Field of Regard (including any effects that reduce this, such as masking by aircraft structures or ego-motion compensation)
    - The maximum detection range (across the Field of Regard). This is a key parameter that effectively limits the total time available to complete the DAA process.

- The minimum detection range (across the Field of Regard).
- The detectors classification performance across the field of regard within the maximum and minimum detection range (i.e., true positive, false positive, false negative rates),
- The detectors localisation uncertainty of objects in space and time (range error, bearing error, longitude/latitude/altitude error)
- The detectors false alarm rate when operating within the intended operational environment.

- Establishing the time required for the Detect Function to complete a detect cycle across the intended operational environment is crucial for ensuring safety.
- Detected objects should be uniquely identified for traceability throughout the DAA process.

An additional, optional functionality of the DAA System involves the ability to detect and avoid operating conditions not meeting VMC, such as cloud, and ensuring appropriate stand-off distances from clouds. Various means, including operating procedures, processes, or ground-based/3rd party weather tracking, can achieve this. However, embedding this functionality within a capable DAA system presents benefits and synergies, such as maximising operational flexibility and utilising existing Detect and Track capabilities. This has a number of benefits and synergies including:

- Maximising operational flexibility by directly measuring the position of cloud from nearby, and not relying on other means that require conservative estimates of cloud position.
- Utilising the existing Detect and Track capabilities in the DAA system.

4.2.2.1 Derived Requirements

From the above discussion, the following requirements for the Detect Function are derived:

Table 29: Detect Function – Derived Requirements

Req. ID	Requirement Text	Rationale
DET-001	The Detect Function shall have adequate functionality to ensure the AAT function meets the logic risk ratios and meets the DAA objectives (CR-002).	Top level requirement driven by AAT-011. Captures traceability of all sub requirements attached to the Detect Function.

Req. ID	Requirement Text	Rationale
DET-002	The Detect Function shall detect intruders of interest and non-interest.	This requirement is the first of the "classification" requirements. With any detection system that will detect a useful number of intruders of interest, there will be some detections that are not valid or useful for the purposes of the AAT function.
DET-003	The criteria for classifying intruders as "intruders of interest" or "intruders of non-interest" shall be defined.	This is a traceability requirement, driven from the requirement to meet the logic risk ratio (DET-001) and to detect intruders of interest/non-interest (DET-002). In order to meet the RR, it is critical that the classification of targets of non-interest/interest is done correctly. confidence criteria (i.e., an 80% confidence of an intruder = intruder) should be included
DET-004	The Detect Function may detect adverse environments for the purposes of meeting VMC criteria (i.e., standoff distances from cloud).	If the system is operating off a visual based system, stand-off from cloud is needed to ensure adequate time to detect and avoid an aircraft that breaks through the into a collision course with the aircraft. There may be non-technical means to achieve this too. Additionally, it might be argued that as the AAT function must also detect cooperative intruders, this requirement may not be necessary (aside from the rare case of an IFR aircraft with a non-transmitting ADS-B receiver, or a VFR aircraft that has entered IMC and happens to break through the cloud on a collision course with the UAS).
DET-005	The Detect Function shall be able to detect cooperative intruders through the cooperative means.	Standards relating to the AAT function will generally require a higher RR performance for cooperative aircraft. This is reflected in CR-003 RR for cooperative aircraft. To facilitate this, the Detect Function must be able to detect cooperative aircraft.
DET-006	The Detect Function shall have a means to detect non-cooperative intruders.	As part of the OSED, the AAT function will be operating in airspace with non-cooperative aircraft. To meet safety objectives, there must be a means to detect the non-cooperative intruders.

Req. ID	Requirement Text	Rationale
DET-007	The field of regard for the Detect Function shall be specified and include all masking effects. The field of regard shall be such that the required risk ratios are satisfied. The specification of the Field of Regard shall take into consideration any compensation undertaken by the Detect Function that reduces the effective FoR.	Key to a functioning detector is the ability to perceive a threat from the potential areas it may come from. In the case of an AAT function, bearing (angles from a cardinal direction) in 2 dimensions, as well as the range at which a detect occurs are critical parameters. The field of regard must be specified as part of characterising the performance of the detector.
DET-008	The Detect Function's performance shall be established across the intended operational environment (including true positive rate, true negative rate, false detection rate, miss rate).	These are required performance values for any classifier/detector. The intended operational environment should cover all expected combinations of: • intruder types and geometries (speeds/accelerations/paths) • background clutter (RF/cloud/sun/horizon etc.) These values, when determined across the entire operational environment can be used to infer risk ratios/induced encounter rates etc.
DET-009	the sensor(s) average false detection rate(s) shall be established.	This requirement ensures that an hourly rate (based off the intended operational environment) of false alarms is quantified.
DET-010	The Detect Function's uncertainty of detected objects position (bearing, elevation, range, or 3D position in the space and if available, velocity) shall be established across the intended operational environment.	DET-008 only deals with the correct classification of an intruder (from a binary classification perspective). Within a true detection, the detector's uncertainty of the intruder's position (range and bearing) and, in the case where data is available (i.e., ADS-B) velocity needs to be established to account for the uncertainty as part of the Decide Function.
DET-011	The scan rate (average, 95%) across the entire FOV shall be established.	The time taken to complete the Detect Function will likely be driven primarily by the scan rate (the time taken to ingest all pixels in a scene). This performance should be determined to correctly classify the latency of the Detect Function.

Req. ID	Requirement Text	Rationale
DET-012	The latency (average, 95%) of the Detect Function shall be established	as part of AAT-010 the Detect Function time forms part of determining the time taken to complete an AAT cycle. Classifying this can also assist in any detection of loss of function of the Detect Function.
DET-013	The maximum and minimum ranges at which a detection can occur for each type of intruder (cooperative and non-cooperative) across the Field of Regard shall be established.	This requirement is a key performance metric when calculating the capability of the system in any analysis of worst-case encounters.
DET-014	The maximum range at which adverse environments can be reliably detected (for the purposes of ensuring operation in VMC) may be established across the Field of Regard.	This requirement assists in the analysis of the performance of this system, to ensure it can meet standoff requirements from cloud.
DET-015	The functionality of the Detect Function in each operating mode shall be established.	Under each operating mode, the functionality of the Detect Function may be different, depending on the software implemented. These modal functionalities need to be defined. For example, if the Detect Function has a detectable failure, the DAA system may be placed into the **Isolated Mode**, and not be able to interact with other UAS functions.

4.2.3 Track Function

The Track Function's purpose is to create, update, and remove tracks and then provide tracked objects[24] data (i.e., position, velocity, heading, and associated uncertainty) to the Decide Function via the Convey Function.

In order to create, update or remove tracks, the following tasks need to be undertaken:

- Ingestion of relevant data via the Convey Function. This is comprised of several data elements and from several different sources within the DAA and aircraft systems. This includes:
    - Detection data, and detection data uncertainty. This data originates from the Detect Function

[24] As discussed in section 4.2.2, this may also include the tracking of cloud banks, for the purposes of ensuring suitable standoff from Instrument Meteorological Conditions, per the requirements of flight under VFR.

- The current UAS position, heading and velocity parameters (including any uncertainties), as well as the manoeuvrability of the ownship. This data is sourced from the UA.
- Existing track data (to correlate previous tracks with the new detect data) This data is retained in the Track Function from earlier timesteps.

- Create new tracks, update existing tracks with new intruder positions, and remove old/stale tracks.
- Analyse the results of the tracker against the object tracking metrics to assess the performance of the tracking function [22] [23].
- Output relevant track information via the Convey Function to other relevant functions in the DAA system (primarily the Decide Function).

The ability to create, update or remove tracks specifically implies that the Track Function has the following capabilities:

- The criteria for the creation, update, or removal of tracks are defined.
- The criteria for the prioritisation of the intruder tracks are defined.
- The ability to uniquely identify, and attach track data (i.e., position, velocity, source, uncertainty, range, and timestamp) for each track.
- The ability to accurately associate detection outputs from the detector with the correct track.
- The ability to retain or recall the information from previous Detect and Track Function outputs so that they may be appended with new information or removed from consideration due to a lack of further detections.
- The ability to fuse data from different sources representing the same intruder into a single track (e.g., ADS-B data and visual information, or multiple sensor overlap).
- In the cases where there is a limit to the number of tracks the function can handle at any one time, the implementation of a limitation feature within the Function and some prioritisation scheme when there is a need to remove lower-priority tracks.
- The completion of the track function should occur in a reasonably short amount of time such that the risk ratios in CR-002 can be met.
- As part of the verification process, it is necessary to be able to quantify the performance of the tracker. Key performance metrics for trackers include:
  - tracker correctness (rates of true / false positives, true / false negatives),
  - track matching errors,
  - track completeness,

- track uncertainty.
- false track rate

- As part of ensuring the continued functionality of the DAA system during flight, the closest point of approach for all encounters should be measured and recorded as part of REC-001.

4.2.3.1 Derived Requirements

From the above discussion, the following requirements for the Track Function are derived:

Table 30: Track Function – Derived Requirements

Req. ID	Requirement Text	Rationale
TRK-001	The Track Function shall have adequate functionality to ensure the AAT function meets the logic risk ratio and meets the DAA objectives (CR-002).	This is a traceability requirement to ensure the Track Function's performance is characterised and able to form part of the analysis for AAT-011.
TRK-002	The Track Function shall create, update, and remove tracks of intruders of interest and non-interest.	This requirement ensures the Track Function includes these key features (creation/update/removal of tracks).
TRK-003	The Track Function may track adverse environmental conditions.	If the DAA System is also used to ensure adequate standoff from IFR conditions, their detections will be tracked by the Track Function.
TRK-004	The Track Function shall prioritise intruder tracks.	There may be a point where the Track Function may become saturated with high numbers of tracks. In such a case, there should be some criteria for tracks not to be passed to the Decide Function. This is to prevent track saturation and avoid unintended function if the Track Function cannot pass all tracks to the Decide Function.
TRK-005	The criteria for the prioritisation of tracks shall be established.	Traceability requirement from TRK-004 to ensure the criteria for prioritisation is explicitly stated.
TRK-006	The Track Function shall be able to ingest information in different formats (cooperative and non-cooperative intruders).	It is likely that non-cooperative and cooperative data will utilise different formats and data which will need to be converted into a format needed for the Decide Function. This requirement ensures that data is provided in the format set by DEC-002.

Req. ID	Requirement Text	Rationale
TRK-007	The Track Function shall establish intruder unique ID, position, velocity, range, and timestamp.	This requirement, alongside TRK-006 ensures that the necessary data is provided to the Decide Function.
TRK-008	The Track Function shall receive Ownship position, velocity, and heading data, as well as the time at which the data was valid.	This requirement is derived. To ensure the Track Function can establish the requirements of TRK-007 The Ownship position, velocity, and heading data is required.
TRK-009	The accuracy of the Ownship's position, velocity and heading information shall be established.	Derived from TRK-008. The accuracy of the Ownship data is required to ensure correct function of the Decide Function.
TRK-010	The Track Function's correctness shall be established across the intended operational environment (true positive track rate, true negative track rate, false track rate, missed track rate).	key performance metric for trackers (i.e., classifier) to ensure correct characterisation of function. This data is used to calculate higher requirement performance objectives (i.e., induced encounter rates, risk ratio).
TRK-011	The average false track rate (per flight hour) of the Track Function shall be determined.	As part of the induced encounter rate, the average false track rate per hour needs to be calculated. This requirement ensures that value is derived.
TRK-012	The quality of the Track Function (track matching error, track completeness, track uncertainty) shall be established.	A derived requirement from TRK-010 capturing more detail of the tracker performance. Of note is the uncertainty of tracks, which is needed for the Decide Function to incorporate into calculations.
TRK-013	The criteria for establishing, updating, coasting, and removing a track shall be established.	Key criteria for a tracker to establish, update, and remove a track. This criterion drives the effectiveness of the tracker via requirements TRK-010 and TRK-012
TRK-014	The maximum number of simultaneous tracks that can be tracked without adversely affecting tracker performance shall be established.	This requirement is needed as part of design decisions for the track prioritisation and the dropping of non-prioritised tracks to prevent poor functioning of the tracker.
TRK-015	The latency of the Track Function to complete a cycle (initiating, updating, and removing tracks) across all tracks in the expected operational environment shall be established.	This is a traceability requirement that ensures the latency of the tracker is captured as part of AAT-010. Additionally, the known time it takes to complete a track cycle can inform fault detection.

Req. ID	Requirement Text	Rationale
TRK-016	The latency (average, 95%) taken to establish, update, or remove a track shall be established.	This requirement derives from TRK-015 applied to an individual track.
TRK-017	The expected performance of the Track Function to classify and filter out tracks of non-interest shall be established.	These metrics will be necessary to roll up into the overall effectiveness of the DAA System's ability to prevent LoWC, NMAC, and MAC, as measured by the Risk Ratios.
TRK-018	The Closest Point of Approach (vertical, horizontal) of intruders shall be estimated (where possible), and the data shall be recorded as part of the data logged per requirement REC-001.	The CPA is a key performance parameter for recording and logging actual encounter events. This data can be used to ensure the correct and continuing safe function of the DAA system.
TRK-019	The functionality of the Track Function whilst the AAT Function is in each operating mode shall be established.	Under each operating mode, the functionality of the Track Function may be different, depending on the software implemented. These modal functionalities need to be defined. For example, if the Track Function has a detectable failure, the DAA system may be placed into the **Isolated Mode**, and not be able to interact with other UAS functions.

4.2.3.2 Simultaneous Detect While Tracking

The previous discussion of the detect and track function assumes that the detect function does not ingest any data from the track function. However, it may be that to better the capability of the detector, tracking data is provided back to the detector to improve the overall DAA function performance. In these cases, additional requirements should be derived to cater for this additional data flow path and criteria to establish a detected and tracked object.

4.2.4 Decide Function

The decide function's purpose is to classify and prioritise tracked objects as threats (i.e., may pose a collision risk), and to then, if necessary, calculate the most appropriate alerting and manoeuvre and guidance to the Command Function.

To complete this process, the following tasks need to be completed:

- The decide function needs to ingest track data via the Convey Function from the Track Function and UAS position, velocity, heading, and UA manoeuvrability data from the UA.

- The decide function then needs to determine if a given track should be classified as:
    - A threat that warrants a manoeuvre,
    - a potential threat that doesn't warrant a manoeuvre, now, but may in the future.
    - a non-threat that does not warrant a manoeuvre.
- Given there may be multiple tracks, the prioritisation of tracks needs to be evaluated such that manoeuvre priority (if required) can be determined.
- The decide function then needs to determine the relevant manoeuvre guidance and alerting for the combination of intruder threats.
- The decide function should then provide the relevant manoeuvre guidance and alerts to the Command Function via the Convey Function.

In order to be able to complete these tasks, the following is required:

- The formatting and data schema used as part of the decide function should be defined. If ingested data is not in the correct format, it should be converted (i.e. relative coordinates to Earth Centred Earth Fixed coordinates).
- The decide function needs a classification scheme for intruders (whether they are considered a threat or a non-threat, or other classifications), such that the determination to undertake manoeuvres, or provide warnings to the remote pilot can be undertaken.
- The decide function needs to be able to undertake some algorithm to determine manoeuvre guidance for those intruders that were classified as ones that need to be avoided. This algorithm needs to consider:
    - The manoeuvrability of the Ownship. This could be a static value, or one that is dynamically updated based on the Ownship state.
    - Restrictions on manoeuvres due to the ground plane
- Algorithms to find paths to avoid a well clear violation or to regain well clear may provide multiple solutions to the problem. In these cases, prioritising the "most beneficial" manoeuvre needs to be undertaken.
- The decide function needs to have some method to convert the information generated into a format that can be understood by the remote pilot.
- The time taken to complete the Decide Function needs to be established.
- Flowing on from false detections and false tracks, the rate of false alerts to the command function (human pilot or automated) should also be captured, as this is the point where the false detection/false track is actually provided to a decision maker for command.

4.2.4.1 Derived Requirements

From the above discussion, the following requirements for the Decide Function are derived:

Table 31: Decide Function – Derived Requirements

Req. ID	Requirement Text	Rationale
DEC-001	The Decide Function shall have adequate functionality to ensure the AAT function meets the logic risk ratio and meets the DAA objectives (CR-002). This will include: • the classification and prioritisation of threats (intruders of interest). • the calculation of avoidance manoeuvres based on the prioritised threats. • the determination of alerts and guidance to the Command Function, based on those determined manoeuvres.	Traceability requirement from AAT-001 to ensure the Decide Function's performance affecting the risk ratio is captured. This is also the point where the purpose of the Decide Function is stipulated.
DEC-002	The required format and type of data utilised in the Decide Function shall be defined.	Derived requirement. In order to ensure correct calculation of avoidance manoeuvres, the data should all be specified to the Decide Function in the correct format and type.
DEC-003	The criteria for the classification and prioritisation of tracks as threats (i.e. alerting schema and their priority) shall be established across all expected encounter scenarios	Derived from DEC-001, this requirement ensures that the criteria for prioritisation are established.
DEC-004	The algorithm for the determination of manoeuvre guidance shall be established across all expected encounter scenarios	This is the foremost requirement of the Decide Function. This requirement allows for traceability down to the algorithmic and classification requirements of the Decide Function.

Req. ID	Requirement Text	Rationale
DEC-005	The Decide Function shall prioritise avoidance manoeuvres during an encounter with an intruder (or intruders).	In the case where there are multiple solutions for an avoidance, or in scenarios where there is a priority of manoeuvring that should be implemented, the Decide Function should take that into consideration (example, two aircraft on a direct collision course, but one is substantially further away than the other. The Ownship should prioritise the one closer than the one further, until that priority changes).
DEC-006	The Decide Function shall take into consideration the Ownship's manoeuvrability (at the time of function) and flight envelope in determining alerting and guidance	The manoeuvrability and flight envelope of the Ownship is a key variable in the determination of manoeuvres and must be considered as part of any avoidance manoeuvre calculation.
DEC-007	The Decide Function shall take into consideration any manoeuvrability restrictions based on ground hazards	Although there are different methods in which to take into consideration ground hazards (i.e., detecting ground obstacles, using a digital terrain model, have a hard floor below which manoeuvres are not permitted) the Decide Function should still take these into consideration when determining any alerting and guidance.
DEC-008	The Decide Function shall determine DAA alerting and guidance relating to avoidance manoeuvres during an encounter with an intruder.	The actual alerts and guidance required to inform the pilot will take a different form than the priority classification and prioritised manoeuvre path, and this alerting/guidance needs to be determined to then be passed to the Convey Function (and then to the remote pilot or decision-making system).
DEC-009	In the case where multiple manoeuvre guidance options are provided to the command function, the priority of each potential manoeuvre should be established	There are likely situations where multiple manoeuvre paths can be suggested (i.e. a right turn and left turn will lead to an avoidance of WCV. This requirement ensures that in addition to determining the multiple means to avoid the situation, a prioritisation of which manoeuvre is "more beneficial" should be established.

Req. ID	Requirement Text	Rationale
DEC-010	The criteria for prioritising multiple manoeuvres shall be established	This requirement follows from DEC-009, to ensure that the criteria for prioritisation are established.
DEC-011	The validity of the Decide Function's alerting and guidance shall be demonstrated	This is a verification requirement to ensure the algorithm for determining alerting and guidance is appropriate.
DEC-012	The average false alert rate of the Decide Function shall be determined, and shown to be acceptable to meet risk ratio requirements	This is a further derived requirement to capture the number of false alerts that are provided from the Decide Function to the Command Function. False alerting rate is used as part of requirements to prevent nuisance alerting, and to infer the induced encounter rate.
DEC-013	The average false alert rate shall not exceed a value where the rate has an adverse effect on the safety of operation, or causes a nuisance to the flight crew	This is a derived requirement, due to the known issue of humans ignoring overly sensitive false alarms.
DEC-014	The decision latency (average, 95%) of the Decide Function shall be established across all expected encounter scenarios	This requirement ensures traceability to the overarching timing requirement and can be used to infer fault detection in the Decide Function.
DEC-015	The functionality of the Decide Function whilst the AAT Function is in each operating mode shall be established.	Under each operating mode, the functionality of the Decide Function may be different, depending on the software implemented. These modal functionalities need to be defined. For example, if the system is in **surveillance only** mode, then the Decide Function may be "disabled", or its outputs suppressed, as only the track data would be provided to the RPIC.

4.2.5 Command Function

The Command Function's purpose is to issue a manoeuvre command to the execute function, based upon the received alerting and manoeuvre guidance from the Decide Function. To do this, the following tasks need to be completed:

- The Command Function needs to receive the alerting and manoeuvre guidance from the Decide Function.
- The Command Function needs to determine the appropriate command manoeuvre given the information from the Decide Function

- The Command Function then needs to provide the appropriate command to the Execute Function.

4.2.5.1 Derived Requirements

From the above discussion, the following requirements for the Command Function are derived:

Table 32: Command Function – Derived Requirements

Req. ID	Requirement Text	Rationale
CMD-001	The Command Function shall have adequate functionality to ensure the AAT function meets the logic risk ratio and meets the DAA objectives (CR-002). The Command Function may be automated or commanded by the remote pilot.	Initial traceability requirement to ensure that the Command Function provides all the functionality required by the risk ratios.
CMD-002	The Command Function shall determine the appropriate command manoeuvre when necessary to maintain safety.	High level requirement for the Command Function. For the case where the command is issued by a pilot, this is the pilot's responsibility to undertake.
CMD-003	The Command Function, where possible and without affecting the safety of the primary manoeuvre, should attempt to minimise disruption to other aviation traffic.	As per CR-002, there should be some criteria for minimising disruption to other aviation traffic. This requirement ensures the command function includes this determination and should include the return to the intended flight path.
CMD-004	The criteria for manoeuvre selection, including criteria for minimising disruption to other aviation traffic shall be established.	In the case where the command is automated, this requirement ensures there criteria for consideration for the reduction of disruption to aviation traffic.
CMD-005	If applicable, the criteria for enacting (and not enacting) automated manoeuvres shall be established.	This requirement is derived to ensure that there exists a stipulated criteria for the automated command based on the alerting and guidance provided.
CMD-006	If the command is issued automatically, then an alert that this has occurred shall be provided by the Command Function to the remote pilot via the Convey Function.	This requirement is necessary so in the case of an automated manoeuvre, the remote pilot is kept informed of the automated manoeuvre.

Req. ID	Requirement Text	Rationale
CMD-007	If the command is issued automatically, throughout the automated manoeuvre, the remote pilot shall be able to intervene and override any avoidance command.	As the pilot is ultimately responsible for the flight, there may be sufficient reason for the pilot to intervene in a manoeuvre even though an avoidance manoeuvre has been issued.
CMD-008	If the pilot intervenes in an avoidance manoeuvre, automated manoeuvres cannot be issued by the command function until the pilot positively enables this function again.	In a similar vein to CMD-007, the pilot is ultimately responsible for the safety of the flight and should have the capability to intervene (if necessary). To prevent a command tug-of-war, there should be logic within the functionality of command function that upon pilot intervention, the automated manoeuvre capability is disabled.
CMD-009	A latency (average, 95%) for the Command Function when initiating an avoidance command shall be established. For human commanded manoeuvres, a pilot response model shall be used.	This is a further decomposition of the timing requirement in AAT-010. Additionally, the knowledge of the average latency can be used as part of fault detection
CMD-010	The functionality of the Command Function whilst the AAT Function is in each operating mode shall be established.	Under each operating mode, the functionality of the Command Function may be different, depending on the software implemented. These modal functionalities need to be defined. For example, if the system is in **surveillance only** mode, then the Command Function may be “disabled”, or its outputs suppressed, as only the track data would be provided to the RPIC.

4.2.6 Execute Function

The Execute Function receives a command and executes the command to physically control the aircraft through the manoeuvre. It is expected that this function resides primarily external to the DAA system, through the normal flight control pathways.

From the purposes of verification and validation, the time taken to execute manoeuvres is a key performance parameter and should be determined.

4.2.6.1 Derived Requirements

From the above discussion, the following requirements for the Execute Function are derived:

Table 33: Execute Function – Derived Requirements

Req. ID	Requirement Text	Rationale
EXC-001	The Execute Function shall have adequate functionality to ensure the AAT function meets the logic risk ratio and meets the DAA objectives (CR-002). This should include: • receiving manoeuvre commands • executing manoeuvre commands	High level requirement for the Execute Function, ensuring there is traceability from AAT-001 and AAT-011.
EXC-002	The Execute Function shall execute all manoeuvres from the Command Function.	Basic requirement to ensure the execute function completes commanded manoeuvres.
EXC-003	The time taken (average, worst case reversal) to reestablish well clear shall be established. (Execute an alert to the operator and suggest an Avoidance manoeuvre)	This is a further decomposition of the timing requirement in AAT-010. Additionally, the knowledge of the average latency can be used as part of fault detection.

4.2.7 Convey Function (Inter-Function Requirements)

The inter-functional Convey Function's purpose is to provide the interface between all of the DAA functions and any other UAS function. This information passed between functions is discussed in the relevant function requirements.

4.2.7.1 Derived Requirements

From the above discussion and in other functions derived requirements, the following Inter-function requirements for the Convey Function are derived:

Table 34: Convey Function – Derived Inter-Function Requirements

Req. ID	Requirement Text	Rationale
CVY-001	The Convey Function shall have adequate functionality to ensure all relevant information is passed between UAS functions, and to the remote crew in a timely manner.	High level requirement for the Convey Function. Ensuring that the functionality required by AAT-001 and AAT-011 is traceable to the function itself.
CVY-002	The Convey Function shall convey information from the Detect Function (intruders of interest/non-interest, position, and velocity information) to relevant functions.	Each of these lower-level requirements provides a further breakdown of CVY-001 to address each Inter-Function interface individually
CVY-003	The Convey Function shall convey information from the Track Function (intruders of interest/non-interest) to relevant functions.	Each of these lower-level requirements provides a further breakdown of CVY-001 to address each Inter-Function interface individually

Req. ID	Requirement Text	Rationale
CVY-004	The Convey Function shall convey information from the Decide Function (alerts, manoeuvre guidance and options based upon prioritisation) to relevant functions.	Each of these lower-level requirements provides a further breakdown of CVY-001 to address each Inter-Function interface individually
CVY-005	The Convey Function shall convey DAA system health information (loss of function, manoeuvrability) to relevant functions and the remote pilot (or automated functions).	Each of these lower-level requirements provides a further breakdown of CVY-001 to address each Inter-Function interface individually
CVY-006	The Ownship's position and velocity estimate (including uncertainty), and the time at which the estimate was valid, shall be provided to relevant functions.	Each of these lower-level requirements provides a further breakdown of CVY-001 to address each Inter-Function interface individually
CVY-007	The information, formats, and timing of information between the detect, track, decide, command, execute, monitor, and contain functions shall be established to ensure appropriate interfacing between functions.	Data interfaces between functions must be assured to be interoperable, in order to prevent internal errors leading to unintended, and potentially unsafe behaviour of the system.
CVY-008	The time taken (average, 95%) to convey information between functions shall be established.	This is a further decomposition of the timing requirement in AAT-010. Additionally, the knowledge of the average latency can be used as part of fault detection.
CVY-009	The functionality of the Convey Function whilst the AAT Function is in each operating mode shall be established.	Under each operating mode, the functionality of the Convey Function may be different, depending on the software implemented. These modal functionalities need to be defined. For example, if the system is in **isolated mode**, then the Convey Function may be "disabled".

4.2.8 Convey Function (UI Requirements)

The Convey Function – User Interface is responsible for delivering the relevant information From the other AAT Functions to the remote crew. In order for the remote crew to undertake their relevant responsibilities, they need to be able to understand the current mode and capability of the AAT Function. From that point, they need to understand the information given to them to enable them to undertake their role within the intended AAT Function (i.e. issuing Commands if non automated), or manage the AAT Function given the health information provided to them (i.e. a validly passed pre-flight functional test required the remote crew to continue the

commencement of flight, or a loss of function indication will require the remote crew to isolate the AAT Function and begin continency procedures).

The UI plays a key role in this by providing:

- Clarity to the remote crew of the current operating mode of the AAT Function.
- Key information to the remote crew to undertake the Core AAT Function.
- Relevant AAT Function health information such that the remote crew can manage the AAT Function and flight safely.

This should be done in an unambiguous way and in a timely manner. This requires that there is:

- Clear symbology (visual, aural) defined and utilised such that the remote crew is able to unambiguously interpret UI information correctly.
- The average time to complete the UI function allows for the adequate interpretation of the current external state by the flight crew to make decisions and manage the safety of flight (with respect to both undertaking avoidance manoeuvres and managing contingencies).

4.2.8.1 Derived Requirements

From the above discussion, the following User Interface requirements for the Convey Function are derived:

Table 35: Convey Function – Derived UI Requirements

Req. ID	Requirement Text	Rationale
UI-001	The DAA User Interface (UI) shall display relevant information to the Remote Crew in a way that does not cause confusion or reduce the crew's situational awareness. This shall occur in a timely manner.	Initial functional requirement for the User Interface.
UI-002	The symbology used for all information presented to the remote crew shall be clear and unambiguous.	Across all possible sets of information provided to the remote crew, it should be clear what each piece of information is. This requires that there is some definition of the symbology used within the UI Function.
UI-003	The DAA UI shall provide the remote pilot with intruder tracks.	The purpose of a DAA system is to allow the remote crew to be informed of the airspace situation immediately around the Ownship such that they can make the best decision to ensure the safety of flight. A clear part of this information are the intruder tracks.

Req. ID	Requirement Text	Rationale
UI-004	The DAA UI shall provide visual indicators allowing intruders of interest to be clearly differentiated from intruders of non-interest.	Because of the inherent sensitivity requirements of the detector, intruders of non-interest will be detected. These should be clearly tagged to ensure the remote crew understand the relative importance of all intruders on the display.
UI-005	The DAA UI shall provide clear indication of the position and heading of the Ownship.	The positions and tracks of intruders only makes sense when placed in relation to the Ownship's position and heading. This information should be clearly available to the remote crew to orient their internal airspace picture.
UI-006	The DAA UI shall display intruders to an appropriate minimum range.	Requirement to ensure the intruders are continually displayed until they reach some minimum range.
UI-007	The DAA UI shall display intruders to an appropriate maximum range.	Requirement to ensure the intruders are continually displayed from some maximum range (i.e. the declaration range).
UI-008	The DAA UI shall display relevant alerts (and their priority). This may be a combination of visual and aural alerts.	Key aspect of the AAT function is to provide alerts to the remote crew. The type and priority of these alerts should also be clear to the remote crew. This requirement ensures this information is provided.
UI-009	The DAA UI shall display manoeuvre guidance instructions associated with relevant alerts (and their priority). This may be in the form of manoeuvre bands.	Alongside the provision of alerts as part of the AAT function is the provision of manoeuvre guidance for those alerts (if applicable). This requirement ensures that manoeuvre guidance is provided to the remote crew.
UI-010	The DAA UI may display the location of adverse environmental conditions.	As an optional detect and track functionality for adverse environmental conditions, this information can be provided to the remote pilot such that they can maintain VMC.
UI-011	The DAA UI shall clearly display relevant Ownship state information. This may include historical as well as current information.	Alongside the AAT Core Function requirements, it is critical that the remote crew has an understanding of the state of the Ownship.

Req. ID	Requirement Text	Rationale
UI-012	The Ownship information relevant to the AAT Function presented to the remote crew shall be established.	This requirement ensures that the information from the Ownship necessary to complete the AAT function successfully (including knowledge of failed states/functions) is defined.
UI-013	The DAA UI shall clearly provide information on the current operational mode of the DAA function.	The current operational mode of the AAT Function (aligned with the modes defined in AAT-002) at any point in time is critical information for the remote crew.
UI-014	The DAA UI shall clearly indicate the current health of the AAT Function. The health state as provided to the UI function by IFM-004, CON-004, and PFT-005 via the Convey Function.	A higher level requirement to capture the ability of the UI to provide AAT function health information as defined as part of the supporting AAT Function: • In flight failures detected by the in-flight monitor. • Pre-flight test failures from the pre-flight test system. • Loss of containment as detected by the CON function.
UI-015	The DAA UI shall show clear indication of loss of DAA function. This may include the loss of the detect, track, and/or alerting functions.	Derivative of UI-014, any loss of the AAT Function should be clearly articulated to the remote crew, as this will allow the remote pilot to transition the AAT Function to the correct operational mode (i.e. isolate mode) and begin the relevant contingency procedures.
UI-016	The DAA UI shall show clear indication of a loss of containment of the AAT Function (as per the CON Function).	Derivative of UI-014, any loss of containment of the AAT Function should be clearly articulated to the remote crew, as this will allow the remote pilot to transition the AAT Function to the correct operational mode (i.e. isolate mode) and begin the relevant contingency procedures.
UI-017	The DAA UI shall provide clear indication of the result of pre-flight functional tests to the remote pilot.	Derivative of UI-014, any failure of the AAT Function to pass the pre-flight test should be clearly articulated to the remote crew, as this will allow the remote pilot to prevent the commencement of flight.

Req. ID	Requirement Text	Rationale
UI-018	In the case of automated manoeuvres, the UI shall clearly inform the remote pilot aurally and visually that the AAT Function is undertaking an automated manoeuvre.	If automated manoeuvres are possible, it is paramount that any manoeuvre made is immediately indicated to the remote crew, in particular the remote pilot as the person responsible for the safety of the operation.
UI-019	In the case that an automated manoeuvre has been undertaken, the intended flight path under automated manoeuvre shall be clearly articulated to the remote pilot.	To give further situational awareness to the remote crew during an automated manoeuvre, it should be clear what the intended automated flight path is. This requirement ensures this information is provided to the remote crew.
UI-020	The DAA UI may display visual feed of the EO/IR sensor.	An optional requirement. It may be beneficial to provide the remote crew with a visual feed from the EO/IR sensor, particularly if detected tracks can be highlighted relative to the Ownship's heading.
UI-021	The DAA UI shall provide all relevant information to the pilot in a timely manner.	High level requirement to ensure there is some consideration of the timing of information provided to the remote crew such that they can make reasonable decisions in a reasonable amount of time.
UI-022	The time (average, 95%) taken for the UI to display information shall be established.	Derivative of AAT-012, ensuring that the latency to associated with the UI function is captured as part of the overall timing of the AAT Function.
UI-023	The functionality of the User Interface Function whilst the AAT Function is in each operating mode shall be established.	Under each operating mode, the functionality of the UI Function may be different, depending on the software implemented. These modal functionalities need to be defined. For example, if the system is in **isolated mode**, then the UI Function may be "disabled".

4.2.9 In-Flight Monitor Function

The purpose of this function is to monitor the core AAT functions **and the** AAT Containment Function during flight, and to detect any failures or faults in these functions. The In-Flight Monitor Function should provide health information to the remote pilot such that they can undertake the appropriate procedures in the event of a fault or failure. This function assumes that in the case of a detect loss of function, the pilot can undertake contingency procedures to:

- Isolate the AAT function to prevent any unwanted actions or information from being undertaken or received.
- Notify the pilot of the fault or failure.
- (if available) enact procedures to rectify the fault (i.e., a restart of the AAT software)

In the case where the AAT function is not recoverable, the pilot is assumed to undertake procedures to safely terminate the flight, minimising the time at which the AAT function is not able to provide detect and avoid functionality.

The following tasks are assumed to be needed to complete this function:

- The in-flight monitor needs to ingest data, both functional input/output data and other health information from the AAT function and DAA equipped UA systems respectively.
- The function then needs to determine if the ingested data suggests that the AAT function is functioning as intended or is faulty.
- Regardless of whether the In-Flight Monitor Function determines the AAT Function is functioning correctly or not, the RPIC should be provided the health status, such that they can make the appropriate
- In the case where the RPIC is notified of an issue, they can isolate the Core AAT Function or the AAT Containment Function
- There may be an option to automate the isolation of the AAT Function. In the cases where this is allowed/occurs, the RPIC must be immediately notified.

In order to complete these tasks, the following is assumed:

- Health is defined for the Core AAT Function and AAT Containment Function. The point at which the Core AAT Function and AAT Containment Function are considered to be non-functional also needs to be established.
- The combination of physical and software-based criteria to measure the health of the functions is defined.
- There is a means to ingest data (functional output or sensors) to measure health criteria.
- There is an **Isolated Mode** for the AAT Function which prevents the AAT Function from having an adverse effect on the safety of the operation.
- There is an ability to restart the AAT Function (i.e. restore to a functioning state) from an isolated mode. Undertaking this step should not cause any unwanted effects on the operation.

4.2.9.1 Derived Requirements

From the above discussion, the following requirements for the In-Flight Monitor Function are derived:

Table 36: In-Flight Monitor Function – Derived Requirements

Req. ID	Requirement Text	Rationale
IFM-001	The In-Flight Monitor Function shall be able to detect a loss of function (in flight) of the following Core AAT Functions: • Detect, • Track, • Decide, • Command, • Execute, • Convey, And the following supporting AAT functions: • AAT Containment. • In Flight Monitor. And notify the RPIC via the Convey Function such that contingency procedures can be initiated to safely return the flight to normal or to end flight.	Initial requirement to provide traceability from AAT-015.
IFM-002	For the following Core AAT Functions: • Detect, • Track, • Decide, • Command, • Execute, • Convey, And the following supporting AAT functions: • AAT Containment • In Flight Monitor The criteria to establish whether these functions are non-functional shall be established. If there are multiple degraded, non-functional states, these shall be uniquely identified.	Follows directly from IFM-001, in order to detect a loss of function, the criteria for a loss of function across the core AAT Functions, the AAT Containment Function, and the In Flight Monitor Function shall be defined. Note that the Pre-Flight Test Function is not included here as it does not operate in flight (and PFT-007 ensures the PFT Function can be interrupted if it does indeed come on in flight).

Req. ID	Requirement Text	Rationale
IFM-003	The means by which the In-Flight Test Function measures the health of the Core AAT Functions and AAT Containment Functions shall be established.	Alongside criteria for what is considered functional across the AAT Functions, the means by which this criterion is inferred needs to be defined. This may be through data directly from the functions (i.e. checksums), or by some external sensor that measures data that allows the inference of functionality.
IFM-004	The IFT Function shall provide the Convey Function with the relevant health information for the RPIC.	Critical piece to ensure the health status of the AAT Function is provided to the RPIC via the Convey Function.
IFM-005	The functionality of the IFT Function whilst the AAT Function is in each operating mode shall be established.	Under each operating mode, the functionality of the IFM Function may be different, depending on the software implemented. These modal functionalities need to be defined. For example, if the system is in nominal mode, then the IFM Function is active.

4.2.10 Containment Function

The AAT Containment Function is intended to ensure that the AAT only operates within the intended operational environment.

In order to complete this function, the following tasks need to be undertaken:

- The Containment Function needs to ingest relevant data to determine if the AAT function is operating within the intended operational environment.
- The Containment Function needs to determine if the AAT function is operating within the correct operational environment.
- In the case where the AAT Function is operating outside of the intended operational environment, the AAT Function either needs to:
    - In the case where the AAT function can only inform the RPIC, notify the pilot that the AAT Function is operating outside its intended operational environment, and that it needs to be isolated.
    - In the case where the Containment Function can isolate the AAT Function itself, the RPIC must be notified when this occurs.
- When the AAT Function returns to the correct operating environment, the AAT Function should notify the RPIC.
    - In this case, the RPIC can then re-activate the AAT Function (it is considered ill advised to have an automated re-activation).

- Alongside these tasks, there should be a means for the RPIC to disable the functioning of the Containment Function. There should be clear visual and/or aural indication that the Containment Function is disabled.

To do these tasks, the following is required:

- This intended operational environment needs to be defined. The specific criteria the Containment Function uses to determine if the AAT Function is within the operational environment should also be defined. The operational environment should consider:
    - States or modes that the pilot sets and the expected functionality of the AAT Function in those states,
    - Geographical or altitude restrictions implemented by the remote pilot,
    - Phases of flight within which the AAT function is not intended to operate (i.e., take-off/landing), and
    - Operation of the AAT function when the system is in a faulty or failed state.
- The states and modes associated with the disabling or enabling of the AAT function due to the Containment Function need to be defined and established.
- There are corner cases where the act of undertaking an avoidance manoeuvre would cause an aircraft to violate the operational environment. To prevent unwanted automated containment functionality (i.e. the aircraft beginning to avoid an aircraft by manoeuvring laterally outside a defined area, which causes the containment function to disable the manoeuvre), logic needs to be implemented that prioritises the appropriate action.
    - To do this, criteria stipulating priority (i.e. avoid WCV unless this causes a ground collision, but avoid MAC at all costs) needs to be defined.

Note: It is assumed that alongside any functioning of the Containment Function, there would be appropriate procedures and processes for the remote pilot to undertake to manage any contingency.

4.2.10.1 +Derived Requirements

From the above discussion, the following requirements for the Containment Function are derived:

Table 37: Containment Function – Derived Requirements

Req. ID	Requirement Text	Rationale
CON-001	The Containment Function shall ensure that the DAA system only functions within the intended operating environment.	Top level requirement for the Containment Function. Provides traceability to subsequent requirements.

Req. ID	Requirement Text	Rationale
CON-002	The operational environment for the Containment Function to ensure operation within the intended operating shall be established across all operating modes.	To be able to define the criteria by which the Containment Function makes a determination that the AAT Function is operating outside of the intended operating environment, this needs to be well defined.
CON-003	The criteria used to determine if the AAT Function is operating within the intended operating environment shall be defined.	This requirement differs from CON-002 by requiring the specific measurable criteria that will allow the inference of the operating environment an whether the Containment Function is required to take action.
CON-004	The Containment Function shall provide relevant information to the Convey Function to display to the RPIC.	This requirement ensures that there is some functionality to provide relevant information (in this case the current "operational environment" state of the operation), such that the RPIC can monitor and make the appropriate decision.
CON-005	Criteria for the enactment of the containment function in cases where the act of undertaking an avoidance manoeuvre would cause an automated containment functionality to prevent the use of the AAT function shall be defined.	To prevent unwanted functionality, the priority of manoeuvres and containment when in conflict must be defined and criteria established.
CON-006	The functionality of the AAT Containment Function whilst the AAT Function is in each operating mode shall be established.	Under each operating mode, the functionality of the AAT Containment Function may be different, depending on the software implemented. These modal functionalities need to be defined. For example, if the system is in nominal mode, then the AAT Containment Function is active.

4.2.11 Pre-Flight Test Function

The pre-flight built in test function serves as an additional fault detection mechanism, designed to functionally test of all other system functions before flight.

This should identify any latent failures or faults that may have occurred in the previous flight or during the time between flights. Its purpose is to identify latent failures or faults that may have occurred in the preceding flight or during the time between flights. This function is expected to be an integral part of all pre-flight procedures. To ensure its effectiveness in fault detection, the following tasks must be carried out:

- Upon start-up or initialisation of the DAA equipped UA, the flight crew initiates the pre-flight test.
- Upon completion of the pre-flight test (with positive results), a series of robust functional tests are conducted to ensure the AAT function is working as intended.
- Regardless of the test outcome (successful or not), the Remote Pilot in Command (RPIC) needs to be clearly informed of the results.
- It is assumed that if the test outcome is not successful, the flight cannot commence until the situation is rectified.

To fulfill these tasks, the following requirements are established:

- A "pre-flight test" mode must be included to safely test the functionality of the DAA system on the ground. This is particularly relevant as calibrated image data may be injected into the system for testing the AAT Function.
- There should be functionality to transition from the pre-flight test mode to any other mode if the pre-flight test mode becomes active during flight.
- The calibrated pre-flight test data, including input and success/failure outputs, needs to be defined.
- Criteria for determining the success or failure of the pre-flight test must be established. This includes any meta-criteria, such as considering 90% success across many tests as a successful pre-flight test.
- Upon completion of the test, a clear, positive, or negative result must be provided to the flight crew to ensure they understand the outcome.

It is assumed that a clear success or failure of the pre-flight test will result in the commencement or cancellation of the flight, respectively.

4.2.11.1 Derived Requirements

From the above discussion, the following requirements for the Pre-Flight Test Function are derived:

Table 38: Pre-Flight Test Function – Derived Requirements

Req. ID	Requirement Text	Rationale
PFT-001	The Pre-Flight Test function shall include functional pre-flight tests on DAA subsystems to ascertain the health of each subsystem (including the In-Flight Monitor and Containment Function) before flight.	Top level requirement to capture the pre-flight test requirements.
PFT-002	The functional tests undertaken, and the functions tested during the functional pre-flight test shall be established.	This requirement ensures that the pre-flight tests undertaken are well defined, and their effect on various functions (as well as what is not effected) is defined.

Req. ID	Requirement Text	Rationale
PFT-003	The calibrated test data used as part of the pre-flight test shall be established.	In order to have a pre-flight test, the actual simulated data injected into the system during the pre-flight test needs to be defined.
PFT-004	The pass/fail criteria for the functional pre-flight test shall be established.	In order to make sense of the pre-flight test function, pass/fail criteria against all relevant test data needs to be established, such that the system can provide this data to the RPIC upon completion of the test.
PFT-005	There shall be a clear and unambiguous indication to the flight crew that the pre-flight test has completed, and the system has passed or failed the test. This should include a partially complete test being considered not successful.	At the end of the functional test, there should be a clear go/no-go result for the flight crew to make the decision to commence flight or to cancel the flight. A non-complete test (even if all the test points up to the point of cancellation are successfully passed) should be considered a non-successful test.
PFT-006	The functionality of the Pre-Flight Test Function whilst the AAT Function is in each operating mode shall be established.	Under each operating mode, the functionality of the Pre-Flight Test Function may be different, depending on the software implemented. These modal functionalities need to be defined. For example, if the system is in nominal mode, then the Pre-Flight Test Function is “disabled”.
PFT-007	There shall be a means for the pilot to interrupt the pre-flight test function at any point and move the system to any other mode safely.	To prevent any unusual circumstances where the pre-flight test mode is engaged during flight (or on the ground), needs to be interrupted, but there is no interruption capability, the ability to the pilot to interrupt the test, **and** transition the system to another mode safely needs to be included.

5 References

[1] ICAO, “Annex 2: Rules of the Air,” 2005.

[2] FAA, “Sense and Avoid (SAA) for Unmanned Aircraft Systems (UAS) - Second Caucus Workshop Report,” 2013.

[3] MITRE, “Study on Airspace Across the US”.

[4] K. Hayhurst, “Preliminary Considerations for Classifying Hazards of Unmanned Aircraft Systems,” 2007.

[5] JARUS, “SORA Annex D, Tactical Mitigation Collision Risk Assessment”.

[6] ASTM, “F3442/F3442M - 20, Detect and Avoid System Performance Requirements,” 2020.

[7] SAE, “Aerospace Recommended Practice 4754A: Guidelines for Development of Civil Aircraft Systems,” 2010.

[8] FAA, “Safety Risk Management Document (SRMD) for Unmanned Aircraft Systems (UAS) Detect and Avoid (DAA) System Safety Assessment,” 2017.

[9] FAA, *Order 8040.6A - Unmanned Aircraft Systems (UAS) Safety Risk Management (SRM) Policy,* Washington DC, 2023.

[10] A. Weinert, S. Campbell, A. Vela, D. Schuldt and J. Kurucar, “Well-Clear Recommendation for Small Unmanned Aircraft Systems Base on Unmitigated Collision Risk,” Journal of Air Transportation, vol. 26, no. 3, pp. 113-112, 2018.

[11] JARUS, “Guideline for Annex G, Safety Risk Management (SRM) Working Group Draft,” 2019.

[12] A. De Abreu, G. Arboleda, G. Olivares, L. Gomez, D. Sing, T. Bruner, T. Haritos, K. Silas, R. J. Wallace and A. Weinert, “sUAS Mid Air Collision Likelihood - Final Report,” ASSURE, 2023.

[13] ICAO, “Outcome of the DAA Performance Expert Meeting DRAFT,” ICAO, Montreal, 2018.

[14] JARUS, *JARUS guidelines on Specific Operational Risk Assessment (SORA) - Main Body,* 2022.

[15] JARUS, “Scoping Paper to AMC RPAS.1309 Issue 2,” JARUS, 2015.

[16] “Range Safety Criteria for Unmanned Air Vehicles Rational and Methodology Supplement,” Range Commanders Council Range Safety Group, 2001.

[17] JARUS, *SORA Annex F (Draft) - Supporting data for the Ground Risk Model.*

[18] JARUS, "AMC RPAS.1309, Working Group 6, Safety and Risk Assessment: Safety Assessment of Remotely Piloted Aircraft Systems," 2015.

[19] FAA, "Advisory Circular (AC) 23.1309-1E, System Safety Analysis and Assessment for Part 23 Airplanes," 2011.

[20] J. M. Cluzeau, X. Henriquel, G. Rebender, G. Soudain, L. van Dijk, A. Gronskiy, D. Hader, C. Perret-Gentil and R. Polak, "Concepts of Design Assurance for Neural Networks (CoDANN)," European Aviation Safety Authority, 2020.

[21] S. Ghoush, J. Patrikar, B. Moon, M. M. Hamidi and S. Scherer, "Airtrack: onboard deep learning framework for long-range aircraft detection and tracking," in *IEEE International Conference on Robotics and Automation (ICRA)*, 2023.

[22] K. Bernardin and R. Stiefelhagen, "Evaluating multiple object tracking performance: the clear mot metrics," *EURASIP Journal on Image and Video Processing,* vol. 2008, pp. 1 - 10, 2008.

[23] D. Du, Y. Qi, H. Yu, Y. Yang, K. Duan, G. Li, W. Zhang, Q. Huang and Q. Tian, "The unmanned aerial vehicle benchmark: Object detection and tracking," in *Poceedings of European Conference on Computer Vision (ECCV)*, 2018.

[24] "SKYbrary," [Online]. Available: https://skybrary.aero/aircraft/f50. [Accessed 2023].

[25] "Airborne object tracking challenge, AIcrowd," 2021.

[26] W. Xing, Z. Cui and J. Qi, "HRCTNet: a hybrid network with high-resolution representation for object detection in UAV image," *Complex & Intelligent Systems,* pp. 1 - 21, 2023.

[27] K. Oksuz, B. Cam, C. Akbas and S. Kalkan, "Localization recall precision (LRP): A new performance metric for object detection," 2018.

[28] A. A. Micheal, K. Vani, S. Sanjeevi and C.-H. Lin, "Object detection and tracking with UAV data using deep learning," *Journal of the Indian Society of Remote Sensing,* vol. 49, pp. 463-469, 2021.