Detect & Avoid
Design, Test & Evaluation Guideline

Appendix F
Hazard Analysis Data

Version 1.0

ID: REVAERO-1462090167-139328


RevAero UTM Demonstration 2023

RevAero Flight Trials 2022

RevAero; a Defence Jobs QLD delegate at Avalon Airshow 2022

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	Dr Terry Martin CEO and Co-founder Revolution Aerospace
Mr Angus McLaren Senior Systems Engineer Revolution Aerospace	Mr Kristian Cruickshank CTO 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 F,*" 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

1 Introduction 6
2 Hazard Severity Metrics 6
3 Operational Hazard Analysis Data 8
4 Functional Hazard Analysis Data 16
4.1 External Event Frequency of a MAC 21
4.2 Allowable Loss of Protection Probabilities Given the External Event Frequency 24
5 References 31

List of Figures

Figure 1 - Table C-1 Severity Conditions from 8040.6A [2] 6
Figure 2: External Event Effect on MAC Event 21

List of Tables

Table 1 - Hazard Severity Classification - Development Assurance for DAA Systems 7
Table 2: Operational Hazard Analysis Data 8
Table 3: Functional Hazard Analysis Table 16
Table 4: Maximum Well Clear Violation Rate 23
Table 5: Loss of Function (unannunciated or annunciated) and inadvertent operation outside of the intended operational environment 23
Table 6: Increased Risk of Collision 24
Table 7: FHA Outputs – Unmodified, and Modified by External Event Probabilities 25

1 Introduction

This document contains the full Operational Hazard Analysis (OHA) and Functional Hazard Analysis (FHA) conducted for a DAA System within the context of the OSED (at Appendix A to this Guideline). These analyses were essential in the determination of the most relevant hazards from operation of a DAA system, appropriate risk controls, and ultimately a set of core system requirements, per the Requirements Derivation document at Appendix E of the Guideline.

Note that the OHA was heavily informed by previous work undertaken by the Federal Aviation Administration (FAA) in their Safety Risk Management Document for UAS DAA System Safety Assessment [1] and previous international work.

The full contents of the OHA and FHA were omitted from Appendix E for brevity; however, they are contained in full below.

2 Hazard Severity Metrics

As a reminder, Appendix E to the Guideline derives hazard severity metrics for:

- Operational airspace risk, using the FAA Safety Risk Management (SRM) Policy, Order 8040.6A, replicated below:

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

Figure 1 - Table C-1 Severity Conditions from 8040.6A [2]

- For operational ground risk, using JARUS Scoping Paper to AMC RPAS.1309 [3], focusing specifically on fatalities to third parties on the ground, 1 fatality on the ground is considered a catastrophic event.
- The conversion between operational outcomes and engineering requirements using Table 1, generated from the above airspace hazard severity metrics and Figure 2 from FAA AC 23.1309-1E [4]:

Table 1 - Hazard Severity Classification - Development Assurance for DAA Systems

	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				

3 Operational Hazard Analysis Data

Table 2: Operational Hazard Analysis Data

<table>
<tr><td rowspan="4">OHAZ-1</td><td colspan="2">Hazard Title: Failed or Inadequate Manoeuvre when one is required</td></tr>
<tr><td>Description:
UAS and Intruder on a loss of well clear or collision course. During this time, the operational and technical mechanisms intended to mitigate or prevent a loss of well clear or collision are not effective, leading to a failed manoeuvre or an ineffective/inadequate manoeuvre</td><td>Causes:
UAS and intruder on a collision course, and:
The functions involved in avoiding other air traffic are not effective under nominal conditions.
The systems that enact the avoid air traffic function fail or partially fail.
Human error leads to the non-functioning or partial functioning of the avoid air traffic function.
Operations outside the intended operational environment lead to reduced or complete loss of the avoid air traffic function.
*Note: as the CONOPs is restricted to uncontrolled airspace, there is no ATC separation provided and is not included as a cause</td></tr>
<tr><td>Severity:
Major (Well Clear Violation)
Hazardous (NMAC)
Catastrophic (MAC and ground fatalities)</td><td>Effects:
Loss of Well Clear
Near Mid Air Collision
Mid Air Collision
in the case of a Mid Air Collision, there is potential for secondary casualties due to ground impact of debris</td></tr>
<tr><td colspan="2">Controls / Mitigations:
Design of DAA systems and algorithms for manoeuvre to meet the TLOS, based on the well clear rate and risk ratio performance of the DAA system.
System designed and demonstrated to meet functional performance requirements.</td></tr>
</table>

	• Verification and validation of system design using 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. • Systems are designed and demonstrated to operate within the intended operational environment. • 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. • DAA system manufactured in accordance with aerospace best practice manufacturing processes. • System configuration is controlled to prevent unapproved configurations from being released to service. • Maintenance schedules and maintenance instructions are available to ensure the DAA system is kept in an airworthy and safe to fly state. • UAS maintenance is certified by appropriately competent persons. • Operations are restricted to areas where the total allowable WCV rate meets the TLOS. • 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. • Remote Pilots are competent to operate the system across all states and modes. • Human Machine Interface design verification/validation • Logging system data to review system performance.

<table>
<tr><td rowspan="4">OHAZ-2</td><td colspan="2">Hazard Title: Increased Collision Risk from Manoeuvre</td></tr>
<tr><td>Hazard Description:
UAS and Intruder on a loss of well clear or collision course. During this time, the operational and technical mechanisms intended to mitigate or prevent a loss of well clear or collision result in an increased risk of more severe events (WCV/NMAC/MAC)</td><td>Causes:
UAS and intruder on a collision course, and:
Hazardously misleading malfunction of the avoid air traffic function, causing an increased risk of more hazardous events.
Human error (errors, lapses, or mistakes) that cause an increased risk of more hazardous events.
Operations outside of the intended operational environment, in conjunction with nominal system function, causing an increased risk of more hazardous events</td></tr>
<tr><td>Severity:
Catastrophic (WCVs, NMACs and MACs at a rate higher than intended)</td><td>Effects:
Loss of Well Clear at a rate higher than if there was no system implemented.
Near Mid Air Collision at a higher rate than if there was no system implemented
Mid Air Collision at a higher rate than if there was no system implemented.
(in the case of a Mid Air Collision, there is potential for secondary casualties due to ground impact of debris)</td></tr>
<tr><td colspan="2">Controls / Mitigations:
Design of DAA systems and algorithms for manoeuvre meet right of way requirements to prevent confusion or misinterpretation of Ownship manoeuvre by intruder.
System designed and demonstrated to meet functional performance requirements.
Verification and validation of system design using 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.
Systems are designed and demonstrated to operate within the intended operational environment.</td></tr>
</table>

	• 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. • DAA system manufactured in accordance with aerospace best practice manufacturing processes. • System configuration is controlled to prevent unapproved configurations from being released to service. • Maintenance schedules and maintenance instructions are available to ensure the DAA system is kept in an airworthy and safe to fly state. • UAS maintenance is certified by appropriately competent persons. • Operations are restricted to areas where the total allowable WCV rate meets the TLOS. • 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. • Remote Pilots are competent to operate the system across all states and modes. • Human Machine Interface design verification/validation • Logging of all detected encounters and system health to validate system operational performance

<table>
<tr><td rowspan="4">OHAZ-3</td><td colspan="2">Hazard Title: Secondary Effects on Manoeuvre</td></tr>
<tr><td>Hazard Description:
UAS manoeuvre to remain well clear results in a secondary hazard:
encounter with another aircraft in proximity to the UAS,
intrusion into adjacent airspace
ground hazard (manoeuvre causes impact with the ground or ground obstacle)
manoeuvre exceeds aircraft design characteristics</td><td>Causes:
UAS manoeuvres to a legitimate threat or false alert, and:
(Environmental condition) UAS in proximity to other aircraft
(Environmental condition) UAS in proximity to operational boundary
(Environmental condition) UAS manoeuvres in close proximity to ground or ground obstacles
(Operational/Design condition) UAS exceeds design loads</td></tr>
<tr><td>Severity:
Catastrophic
(ground fatalities or potential MACs)</td><td>Effects:
Induced encounter, potential for this to default to a natural encounter, also potential that the induced encounter geometry/dynamics results in differing conditional unmitigated probabilities.
Loss of aircraft- Ground fatalities, damage to critical infrastructure.</td></tr>
<tr><td colspan="2">Controls / Mitigations:
Design of DAA system and algorithms for manoeuvre minimises the necessary manoeuvre:
Time from initiation to return to intended flight path.
Stress on the airframe
Whilst still ensuring safety of the primary encounter
Operational procedures and planning to ensure that any manoeuvres taken as a result of DAA operation do not cause the UAS to leave the intended operational area.
Altitude limitations on the use of the DAA system to prevent operation at low altitude/operation outside of the intended operational volume.
Minimisation of false alerts through system design whilst still retaining DAA capability
System designed and demonstrated to meet functional performance requirements.</td></tr>
</table>

	• Verification and validation of system design using 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. • Systems are designed and demonstrated to operate within the intended operational environment. • 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. • DAA system manufactured in accordance with aerospace best practice manufacturing processes. • System configuration is controlled to prevent unapproved configurations from being released to service. • Maintenance schedules and maintenance instructions are available to ensure the DAA system is kept in an airworthy and safe to fly state. • UAS maintenance is certified by appropriately competent persons. • Operations are restricted to areas where the total allowable WCV rate meets the TLOS. • 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. • Remote Pilots are competent to operate the system across all states and modes. • Human Machine Interface design verification/validation • Logging of all detected encounters and system health to validate system operational performance

<table>
<tr><td rowspan="4">OHAZ-4</td><td colspan="2">Hazard Title: False Alarm/Alert</td></tr>
<tr><td>Hazard Description:
DAA equipment generates detection and/or track when there is no aircraft potentially resulting in a significant increase in RPIC workload or in conditions impairing RPIC efficiency and/or execution of invalid avoidance manoeuvres.</td><td>Causes:
• Nominal equipment operation
• System malfunction
• Environmental factors</td></tr>
<tr><td>Severity:
Minor
Note: False Alarms/Alerts that lead to another encounter or ground collision are captured in OHAZ-3.</td><td>Effects:
• Nuisance manoeuvres
• Increased crew/machine distraction
• Could lead to induced encounter (but this is captured in OHAZ-3)</td></tr>
<tr><td colspan="2">Controls / Mitigations:
• Minimisation of false alerts through system design whilst still retaining DAA capability
• System designed and demonstrated to meet functional performance requirements.
• Verification and validation of system design using 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.
• Systems are designed and demonstrated to operate within the intended operational environment.
• 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.
• DAA system manufactured in accordance with aerospace best practice manufacturing processes.
• System configuration is controlled to prevent unapproved configurations from being released to service.
• Maintenance schedules and maintenance instructions are available to ensure the DAA system is kept in an airworthy and safe to fly state.
• UAS maintenance is certified by appropriately competent persons.
• Operations are restricted to areas where the total allowable WCV rate meets the TLOS.</td></tr>
</table>

	• 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. • Remote Pilots are competent to operate the system across all states and modes. • Human Machine Interface design verification/validation • Logging of all detected encounters and system health to validate system operational performance

4 Functional Hazard Analysis Data

Table 3: Functional Hazard Analysis Table

<table>
<tr><td rowspan="3">FHA-001</td><td colspan="3">Failure Condition Hazard Description: Loss of Function (Detected)</td></tr>
<tr><td>Phase of Flight:
Under DAA Operational Conditions</td><td>Classification:
Major*</td><td>UAS Function:
Avoid Air Traffic</td></tr>
<tr><td colspan="3">Effect of Failure Condition:
RPIC or Ownship would be alerted of the failure (assuming that detection capability is available), contingency actions would be taken by the RPIC. The contingency actions are expected to include emergency radio broadcasting to alert proximate aircraft of the UA's position and heading, followed by an emergency landing at a predefined safe landing location. Safety margins would be significantly reduced.
During the period whereby contingency procedures are being undertaken, if an intruder is on a collision course with the Ownship and has not been made aware of the Ownship DAA failure, a MAC will occur.
Additionally, if another system that prevents the aircraft from completing the contingency procedure (i.e., climbing to an altitude where radio carriage is required, and then the C3 link fails), there exists the possibility that a MAC could occur during the time it takes to further mitigate this multiple failure condition. In this case, the debris from the Mid-Air Collision could lead to ground fatalities as well.</td></tr>
<tr><td colspan="3">Analysis Considerations:
External event "intruder present and on collision course" required to occur alongside this failure condition, during the time it takes to enact contingency procedures and the Ownship to move into a safe location.
If the loss of function is annunciated, the actions required to be taken by the RPIC is not onerous and this risk should be easily managed</td></tr>
</table>

<table>
<tr><td rowspan="4">FHA-002</td><td colspan="3">Failure Condition Hazard Description: Hazardously Misleading Malfunction (Unannunciated Loss of Function)</td></tr>
<tr><td>Phase of Flight:
Under DAA Operational Conditions</td><td>Classification:
Catastrophic*</td><td>UAS Function:
Avoid Air Traffic</td></tr>
<tr><td colspan="3">Effect of Failure Condition:

RPIC or OS would not be notified of the loss of function, and the aircraft would continue the mission with no protection against a collision with another aircraft (assuming that intruders would not be capable of detecting and avoiding the Ownship). If the OS and an intruder are on a collision course, the outcome would be a hull loss for both aircraft and multiple fatalities (crew and occupants of intruder). Additionally, the debris from the Mid-Air Collision could lead to ground fatalities as well.</td></tr>
<tr><td colspan="3">Analysis Considerations:

External event “intruder present and on collision course” required to occur alongside this failure condition.

In order for an annunciated failure to occur, both the detection system and the loss of function must occur.

Analysis should take into consideration any failure that results in the inability to remove the aircraft from integrated airspace in the event of a detected failure.</td></tr>
</table>

<table>
<tr><td rowspan="4">FHA-003</td><td colspan="3">Failure Condition Hazard Description: Increased Risk from Malfunction</td></tr>
<tr><td>Phase of Flight:
Under DAA Operational Conditions</td><td>Classification:
Catastrophic*</td><td>UAS Function:
Avoid Air Traffic</td></tr>
<tr><td colspan="3">Effect of Failure Condition:

RPIC or OS would not be notified of the malfunction, and the aircraft would continue the mission with an increased risk of a collision with another aircraft (assuming that intruders would not be capable of detecting and avoiding the Ownship). If the OS and an intruder are on a collision course, the outcome would be a hull loss for both aircraft and multiple fatalities (crew and occupants of intruder). Additionally, the debris from the Mid-Air Collision could lead to ground fatalities as well.</td></tr>
<tr><td colspan="3">Analysis Considerations:

External event “intruder present and on collision course” required to occur alongside this failure condition. However, the external event probabilities would not be equivalent to the “unannunciated loss of function” failure conditions, as this could result in more risk than a complete loss of function.

Assuming that it is not possible to detect a hazardously misleading malfunction during flight, an appropriate functional built in test must be undertaken before flight to reduce the probability of the event occurring during flight. In order for the hazard to be realised, either a hazardously misleading malfunction must occur during operation (after the functional test), or the hazardously misleading malfunction must occur before flight and the functional test must fail to detect this malfunction.

Analysis should take into consideration any failure that results in the inability to remove the aircraft from integrated airspace in the event of a detected failure.</td></tr>
</table>

<table>
<tr><td rowspan="4">FHA-004 (manual)</td><td colspan="3">Failure Condition Hazard Description: Inadvertent Operation Outside Intended Operational Environment</td></tr>
<tr><td>Phase of Flight:
Outside of DAA Operational Conditions</td><td>Classification:
During Taxi/Take-off: Minor*
During Operation: Major*</td><td>UAS Function:
Avoid Air Traffic</td></tr>
<tr><td colspan="3">Effect of Failure Condition:

During Taxi, Take-off and landing:

• Could cause UAS to crash during taxi, take-off or landing (within the “airport environment”, due to inappropriate commands being issued during these times. The RPIC would have control authority and should ignore any warnings during this time. Take-off and landing area assumed to be a controlled ground area, Increase in crew workloads, slight reduction in safety to other people and crew.

During Operation Outside of DAA Approved Operating Environment: Operational Area:

• Too low (causing crash) – potential serious injury or fatalities.

• In airspace that does not align with allowable encounter rates or airspace intruders/equipage etc. – potential to induce a MAC.

Similar to the Taxi, Take-off and landing situation, the RPIC would have control authority and should ignore any warnings during this time.</td></tr>
<tr><td colspan="3">Analysis Considerations:

It seems unlikely that a “loss of function” could result in this outcome (because this requires it to malfunction rather than stop functioning), it is much more likely that a hazardously misleading malfunction would cause this outcome.

Analysis should consider mitigations/controls to prevent the inadvertent operation of the DAA system outside the environment, taking into consideration that the pilot should have sufficient knowledge of the operation to know when the DAA system should be functioning</td></tr>
</table>

<table>
<tr><td rowspan="3">FHA-004 (automatic)</td><td colspan="3">Failure Condition Hazard Description: Inadvertent Operation Outside Intended Operational Environment</td></tr>
<tr><td>Phase of Flight: Outside of DAA Operational Conditions</td><td>Classification:
During Taxi/Take-off: Major*
During operation: Potentially Catastrophic*</td><td>UAS Function:
Avoid Air Traffic</td></tr>
<tr><td colspan="3">Effect of Failure Condition:

During Taxi, Take-off and landing:

• Could cause UAS to crash during taxi, take-off or landing (within the “airport environment”, due to inappropriate commands being issued during these times. Take-off and landing area assumed to be a controlled ground area, Increase in crew workloads, slight reduction in safety to other people and crew.

During Operation Outside of DAA Approved Operating Environment: Operational Area:

• Too low (causing crash) – potential serious injury or fatalities.
• In airspace that does not align with allowable encounter rates or airspace intruders/equipage etc. – potential to induce a MAC</td></tr>
<tr><td colspan="3">Analysis Considerations:

It seems unlikely that a “loss of function” could result in this outcome (because this requires it to malfunction rather than stop functioning), it is much more likely that a hazardously misleading malfunction would cause this outcome.

Analysis should consider mitigations/controls to prevent the inadvertent operation of the DAA system outside the environment, particularly in the case where the OS automatically issues command.</td></tr>
</table>

*All classifications assume that the external event occurs, and requires tailoring of requirements using external event probability

4.1 External Event Frequency of a MAC

Because the loss of the Avoid Air Traffic function in and of itself does not result in a MAC, but requires that an intruder aircraft be present and on a collision course to result in a MAC, two events can be represented under an AND gate (assuming of course that there is independence between these two events):

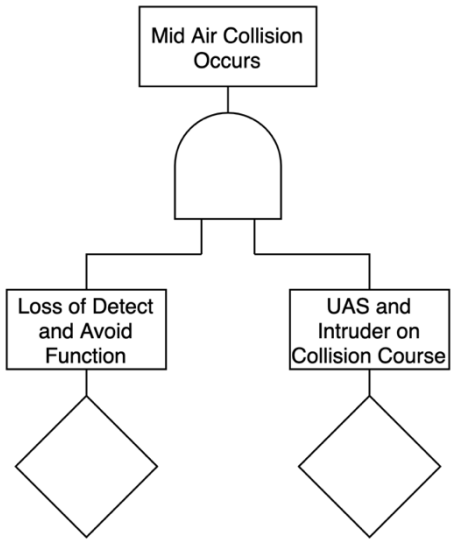

Figure 2: External Event Effect on MAC Event

The term on the left (loss of the avoid air traffic function), is the system-based failure that can occur, whilst the term on the right details the external event probability of a MAC occurring. Broadly speaking, this external event can be summarised as:

1. An intruder enters the declaration volume; and then
2. A well-clear violation occurs; and then
3. An NMAC occurs; and then
4. A MAC occurs.

The identified functional failure conditions in Table 2, can have different levels of effect on the conditional probabilities:

- Complete Loss of Function (LoF) – When this type of failure occurs, there is no ability to detect and avoid mid-air collisions. This effectively results in a situation equivalent to if there is no detect and avoid system at all (i.e., the unmitigated case).

$$P_{LoF}(WCV|DR) = P_{unmit}(WCV|DR)$$

$$P_{LoF}(NMAC|WCV) = P_{unmit}(NMAC|WCV)$$

$$P_{LoF}(MAC|NMAC) = P_{unmit}(MAC|NMAC)$$

- Partial Loss of Function (PLoF) – A partial loss of function results in DAA performance that is less effective than under nominal scenarios, but not

necessarily equivalent to the unmitigated case. In general, we will assume that a partial loss of function has the same outcome as a complete loss of function (regardless of annunciation).

$$P_{mit}(WCV|DR) \leq P_{PLoF}(WCV|DR) \leq P_{unmit}(WCV|DR)$$

$$P_{mit}(NMAC|WCV) \leq P_{PLoF}(NMAC|WCV) \leq P_{unmit}(NMAC|WCV)$$

$$P_{mit}(MAC|NMAC) \leq P_{PLoF}(MAC|NMAC) \leq P_{unmit}(MAC|NMAC)$$

- Hazardously Misleading Malfunction (HMM) – A hazardously misleading malfunction is one where incorrect information is provided to decision making functions without any indication that the information is incorrect. In the case of a DAA system, there are two "kinds" of hazardously misleading malfunctions:
    - An Undetected Loss of Function (ULoF) (i.e., the malfunction of a failure detection or monitor function) – In this case, the system has the same outcome as for a Loss of Function, however there is no detection of this failure.

$$P_{mit}(WCV|DR) \leq P_{ULoF}(WCV|DR) \leq P_{unmit}(WCV|DR)$$

$$P_{mit}(NMAC|WCV) \leq P_{ULoF}(NMAC|WCV) \leq P_{unmit}(NMAC|WCV)$$

$$P_{mit}(MAC|NMAC) \leq P_{ULoF}(MAC|NMAC) \leq P_{unmit}(MAC|NMAC)$$

    - Increased Risk from Malfunction (IRM)- safety is adversely affected by the malfunction compared to the unmitigated case. The effect of this malfunction can range from minor (being slightly worse than the unmitigated case), to severe (always resulting in an NMAC):

$$P_{unmit}(WCV|DR) \leq P_{IRM}(WCV|DR) \leq 1$$

$$P_{unmit}(NMAC|WCV) \leq P_{IRM}(NMAC|WCV) \leq 1$$

$$P_{unmit}(MAC|NMAC) \leq P_{IRM}(MAC|NMAC) \leq 1$$

- Inadvertent Operation Outside of the Intended Operational Environment (cont) – The final type of functional failure is classified as a malfunction, and may be detectable dependent on architecture (i.e., if there is a containment function, or if the remote pilot or UA issues commands to execute avoidance manoeuvres. For the purposes of this assessment (leading to airspace hazards) we can treat it the same as a hazardously misleading malfunction that has the same effect as an undetected loss of function.[1]

The following parameters will be used to determine the maximum allowable probability of occurrence for each failure condition described above:

[1] This is only valid for the purposes of assessing the airspace risk. Ground hazards will require a separate assessment to ensure safety objectives are met.

Table 4: Maximum Well Clear Violation Rate

Parameter	Value	Rationale
$\lambda_{WCV,max}$	0.01	For this guideline, it is assumed that the maximum allowable WCV rate cannot exceed 1 WCV per hundred hours of operation (0.01 encounters per hour). For a system that meets the logic NMAC risk ratio of 0.3 (with an assumed 0.1 MAC risk ratio associated with this), and given the other conditional probabilities derived and assumed in this guideline, this is the maximum WCV rate that results in the TLOS being met.

Table 5: Loss of Function[2] (unannunciated or annunciated) and inadvertent operation outside of the intended operational environment

Parameter	Value	Rationale
$P_{LoF}(WCV\|DR)$ $P_{ULoF}(WCV\|DR)$ $P_{cont}(WCV\|DR)$	1	This depends on the actual definition of the encounter volume. To be conservative, a value of 1 will be assumed. (this effectively sets the DR to the WCV).
$P_{LoF}(NMAC\|WCV)$ $P_{ULoF}(NMAC\|WCV)$ $P_{cont}(NMAC\|WCV)$	0.1	Internationally accepted value for the conditional probability of an NMAC occurring, given a WCV has occurred. Valid for WCV defined as 2000ft HMD and 250ft VMD.
$P_{LoF}(MAC\|NMAC)$ $P_{ULoF}(MAC\|NMAC)$ $P_{cont}(MAC\|NMAC)$	0.01	Based off Weinert study. Valid for combined intruder and Ownship wingspans of 100ft.
$P_{LoF}(MAC\|DR)$ $P_{ULoF}(MAC\|DR)$ $P_{cont}(MAC\|DR)$	0.001	Resultant value = $P(WCV\|DR) \times P(NMAC\|WCV) \times P(MAC\|NMAC)$

[2] Note that here although the probabilities are equivalent between the annunciated and unannunciated loss of function events, they are classified at different hazard severity levels, and hence the maximum allowable failure rate for either event will be different.

Table 6: Increased Risk of Collision

Parameter	Value	Rationale
$P_{HMM}(WCV\|DR)$	1	This depends on the actual definition of the encounter volume. To be conservative, a value of 1 will be assumed.
$P_{HMM}(NMAC\|WCV)$	0.5	Assuming a 500% increase in the probability of NMAC on condition of a WCV
$P_{HMM}(MAC\|NMAC)$	0.01	No change, it is assumed that inside the NMAC volume, only providence prevents an NMAC. Based off Weinert study. Valid for combined intruder and Ownship wingspans of 100ft.
$P_{HMM}(MAC, DR)$	0.005	Resultant value = $P(WCV\|DR) \times P(NMAC\|WCV) \times P(MAC\|NMAC)$

4.2 Allowable Loss of Protection Probabilities Given the External Event Frequency

The allowable probabilities of failure for protective functions can be derived by contrasting the outcome with the probability of the external event that must occur for the outcome to occur. In the case of a loss of function the following equation can be used:

$$P(Loss\ of\ Function) \leq \frac{QPF_{hazard\ severity}}{\lambda_{enc} \times P_{LoF}(WCV|DR) \times P_{LoF}(NMAC|WCV) \times P_{LoF}(MAC|NMAC)}$$

Recalculating and re-evaluating the quantitative probabilities of failure (QPF) and development assurance levels (DAL) for each aircraft level failure condition and scaling by the calculated $P(MAC|Enc)_{unmit}$ and $P(MAC|Enc)_{HMM}$ results in modified quantitative probabilities of failure and development assurance levels (changes are highlighted in red):

Table 7: FHA Outputs – Unmodified, and Modified by External Event Probabilities

FHA Ref.	Classification	DAL	QPF	Identified Mitigations/Controls to Reduce Likelihood/ Consequence of Hazard[3]	Verification Means
FHA-001 Annunciated loss of function	Unmodified: Major	Unmodified: Primary: DAL C Secondary: DAL D	Unmodified: <1×10^{-5} pfh	W/E/D – Pre-Flight Functional Built in Test, to prevent latent failure prevailing between flights and to minimize time an undetectable loss of function or hazardously misleading failure could exist during flight. W/P/E – In-flight monitoring of Avoid Air Traffic Function System(s) performance, Procedures to move aircraft to Atypical or Segregated Airspace in the case of detected failure, CNPC availability, AP/FCC logic to commence ditch if DAA failed and CNPC failed. E/D – Algorithms for Avoid Air Traffic appropriately defined, analysed and tested. E/D – Data transfer/receival Developed to Standard.	FHA with Design and Installation Appraisal per AC 23.1309-1E, sections 17(a) and (b) [4]. 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.
	Modified: Minor	Modified: Primary: DAL D Secondary: DAL E	Modified: <1×10^{-2} pfh (1 pfh actual calculation)[4]		

[3] D = Design change, E= Engineered Safety Feature, S = Safety Device, W = Warning Device, P = Procedures/Training
[4] Although the actual calculation results in a failure rate of 1 per hour, this is clearly unreasonable and a minimum reliability of 100 hours MTBF is instated. This aligns with the current expected failure rate for UAS operating under Part 107 Operations.

FHA Ref.	Classification	DAL	QPF	Identified Mitigations/Controls to Reduce Likelihood/ Consequence of Hazard[3]	Verification Means
FHA-002 Unannunciated loss of function	Unmodified: Catastrophic	Unmodified: Primary: DAL A Secondary: DAL B	Unmodified: $<1\times10^{-9}$ pfh	W/E/D – Pre-Flight Built in Test Prevent latent failure prevailing between flights. W/P/E – In-flight monitoring of Avoid Air Traffic Function System(s) performance, Procedures to move aircraft to Atypical or Segregated Airspace in the case of detected failure, CNPC availability, AP/FCC logic to commence ditch if DAA failed and CNPC failed. E/D – Algorithm for Avoid Air Traffic Developed to Standard E/D – Software Development Assurance to Standard E/D – Hardware developed to standard. E/D – Data transfer/receival Developed to Standard E/D – Software Development Assurance to Standard E/D – Correlate EO/IR with ADS-B Traffic (Only valid for ADS-B traffic) P – Adequate Maintenance practices to maintain DAA system E/P – Installation guidelines/functional tests to ensure appropriate installation of DAA system. S – system is design to prevent activation or function of DAA outside of intended operating environment	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) [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) [4])
	Modified: Major	Modified: Primary: DAL C Secondary: DAL C	Modified: $<1\times10^{-4}$ pfh		

FHA Ref.	Classification	DAL	QPF	Identified Mitigations/Controls to Reduce Likelihood/ Consequence of Hazard[3]	Verification Means
FHA-003 Increased Collision Risk from Malfunction	Unmodified: Catastrophic	Unmodified: Primary: DAL A Secondary: DAL B	Unmodified: $<1\times10^{-9}$ pfh	W/E/D – Pre-Flight Built in Test – Prevent latent failure prevailing between flights. E/D – Algorithm for Detection Developed to Standard E/D – Software Development Assurance to Standard E/D – Hardware developed to standard. E/D – Data transfer/receival Developed to Standard E/D – Software Development Assurance to Standard E/D – Correlate EO/IR with ADS-B Traffic (Only valid for ADS-B traffic) P – Adequate Maintenance practices to maintain DAA system E/P – Installation guidelines/functional tests to ensure appropriate installation of DAA system. S – system is design to prevent activation or function of DAA outside of intended operating environment	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.
	Modified: Major	Modified: Primary: DAL C Secondary: DAL D	Modified: $<1\times10^{-4}$ pfh (2×10^{-5} actual calculation)[5]		

[5] Given the assumption that every intruder that breaches the declaration range breaches the WCV, and that the increase in risk from this failure condition is 500% worse than the unmitigated case, it seemed reasonable to leave the QPF at the same level as FHA-002.

FHA Ref.	Classification	DAL	QPF	Identified Mitigations/Controls to Reduce Likelihood/ Consequence of Hazard[3]	Verification Means
FHA-004 (Manual) Inadvertent operation outside of intended	Unmodified: Major	Unmodified: Primary: DAL C Secondary: DAL D	Unmodified: $<1\times10^{-5}$ pfh	W/E/D – Pre-Flight Built in Test – Prevent latent failure prevailing between flights. W/P/E – In-flight monitoring of Avoid Air Traffic Function System(s) performance, Procedures to move aircraft to Atypical or Segregated Airspace in the case of detected failure, CNPC availability, AP/FCC logic to commence ditch if DAA failed and CNPC failed. S- system is design to prevent activation or avoid air traffic function outside of intended operating environment. E/D – System is designed to operate within all possible intended operational environments and is resilient to operational environments outside of intended operational environments	If RPIC issues command: FHA with Design and Installation Appraisal per AC 23.1309-1E, sections 17(a) and (b) [4]. 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.
	Modified: Minor	Modified: Primary: DAL D Secondary: DAL E	Modified: $<1\times10^{-2}$ pfh		

FHA Ref.	Classification	DAL	QPF	Identified Mitigations/Controls to Reduce Likelihood/ Consequence of Hazard[3]	Verification Means
FHA-004 (Automatic) Inadvertent operation outside of intended operational area	Unmodified: Catastrophic	Unmodified: Primary: DAL A Secondary: DAL B	Unmodified: <1×10^{-9} pfh	W/E/D – Pre-Flight Built in Test – Prevent latent failure prevailing between flights. W/P/E – In-flight monitoring of Avoid Air Traffic Function System(s) performance, Procedures to move aircraft to Atypical or Segregated Airspace in the case of detected failure, CNPC availability, AP/FCC logic to commence ditch if DAA failed and CNPC failed. S- system is design to prevent activation or avoid air traffic function outside of intended operating environment. E/D – System is designed to operate within all possible intended operational environments and is resilient to operational environments outside of intended operational environments. P – Operational procedures are in place and effective to "enable" or "disable" Avoid Air Traffic function if outside of intended operational environment P – Flight planning in place to determine appropriate locations for use of Avoid Air Traffic Function	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) [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) [4])
	Modified: Major	Modified: Primary: DAL C Secondary: DAL D	Modified: <1×10^{-4} pfh		

These adjusted quantitative probabilities of failure align with sections 5.5.2.2 and 5.5.3.3 for Class II DAA systems in ASTM F3442-20 [5] requirements for detect and avoid systems.

Note that the ASTM standard only deals with a loss of function or performance and does not delineate an annunciated loss of function (which can then be dealt with by the RPIC or flight computer) and an unannunciated loss of function (which cannot). This guideline has a requirement for annunciated loss of function (QPF <1E-2 pfh) and unannunciated loss of function (QPF <1E-4 pfh), which does align with the intent of the ASTM standard, despite not directly correlating with the loss of function requirement for Class II systems (QPF <1E-3 pfh).

5 References

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

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

[3] JARUS, "Scoping Paper to AMC RPAS.1309 Issue 2," JARUS, 2015.

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

[5] ASTM, "F3442/F3442M - 20, Detect and Avoid System Performance Requirements," 2020.