Transport Canada Transports Canada

Advisory Circular

Subject:	**Remotely Piloted Aircraft Systems Operational Risk Assessment**		
Issuing Office:	Civil Aviation, Remotely Piloted Aircraft Systems Task Force	Document No.:	AC 903-001
File Classification No.:	Z 5000-34	Issue No.:	01
RDIMS No.:	15147375 v12	Effective Date:	2021-06-09

Table of contents

List of Figures

List of Tables

1.0 Introduction

(1) This Advisory Circular (AC) is provided for information and guidance purposes. It describes an example of an acceptable means, but not the only means, of demonstrating compliance with regulations and standards. This AC on its own does not change, create, amend or permit deviations from regulatory requirements, nor does it establish minimum standards.

1.1 Purpose

(1) This AC provides information and guidance to manufacturers and operators intending to develop or operate a Remotely Piloted Aircraft System (RPAS) for operations in accordance with the requirements of Part IX, Subpart 3 of the Canadian Aviation Regulations (CARs).

1.2 Applicability

(1) This document applies to manufacturers and operators intending to develop or operate an RPAS for one or more of the operations listed under CAR 903.01 which are identified as requiring a risk assessment during the application process for a Special Flight Operations Certificate (SFOC) – RPAS.

(2) Exclusions. In particular, the guidance provided by this document is not intended to address:

- (a) passenger-carrying operations;
- (b) risks associated with carriage of dangerous or potentially dangerous payloads;
- (c) risks associated with air-to-air collisions between two RPAs;
- (d) security risks not confined by the airworthiness of the systems (e.g., C2 link protection from interference is addressed, but protection of the ground control station from external malicious interference is not);
- (e) aircraft subject to the aircraft type certification process.

  Note: Formal policy defining how RPAS will be accommodated in the type certification process is still under development and will be addressed in future guidance material.

1.3 Description of Changes

(1) Not applicable.

2.0 References and requirements

2.1 Reference Documents

(1) It is intended that the following reference materials be used in conjunction with this document:

- (a) Part IX of the Canadian Aviation Regulations (CARs) — Remotely Piloted Aircraft Systems;
- (b) CAR Standard 922 — Remotely Piloted Aircraft System Safety Assurance;
- (c) Joint Authorities for Rulemaking of Unmanned Systems (JARUS) JAR-DEL-WG6-D.04, 2019-30-01 — Guidelines on Specific Operations Risk Assessment (SORA).

2.2 Cancelled Documents

(1) Not applicable.

(2) By default, it is understood that the publication of a new issue of a document automatically renders any earlier issues of the same document null and void.

2.3 Definitions and Abbreviations

(1) The following **definitions** are used in this document:

Note: The definitions provided below are strictly for the purposes of conducting an RPAS ORA as described in the remainder of the document. In the case of any conflict between these definitions and definitions from other sources (e.g., the CARs), these definitions shall be used only in the context of the RPAS ORA.

(a) **Adjacent Area / Airspace**: Any ground area or airspace that reachable from the border of the operational volume in T_{ERP} at the maximum performance capability of the RPA (groundspeed, climb rate). Performance capability shall include considerations of:

(i) Groundspeed created by the worst-case combination of wind allowed by the operation and airspeed capabilities of the RPA.

(ii) Maximum Climb Rate capabilities of the RPA.

(b) **Airport / Heliport Environment**: Airport / Heliport Environment is defined as within 5 nautical miles (9.3 km) from the centre of an airport, heliport, or aerodrome published in the Canada Flight Supplement or Water Aerodrome Supplement.

(c) **Atypical Airspace**: Atypical Airspace is defined as any of the following:

(i) Restricted Airspace, with permission from the coordinating authority;

(ii) Northern Domestic Airspace as defined in the Designated Airspace Handbook, outside an Airport Environment, at or below 400 ft (122 m) AGL.

(iii) Within 100 feet (30 m) or less above and 200 feet (61 m) or less horizontally from any building or structure located in uncontrolled airspace outside of an Airport Environment.

(d) **Beyond Visual Line of Sight (BVLOS)**: BVLOS flight of an RPAS is defined as an operation in which no crew member maintains unaided visual contact with the aircraft sufficient to be able to maintain control of the aircraft and know its location.

(e) **Concept of Operations (CONOPS)**: The clearly defined and detailed purpose of the system/operation intended for the RPAS. This includes a description of the operational aspects of the crew, RPAS system, Processes and Procedures, and the expected Environment.

(f) **Contingency Procedures**: Contingency Procedures describe the planned actions to address undesirable states that, if not addressed, could lead to unsafe situations. While conducting these procedures, the operation is generally still considered to be under control (provided that the RPAS is responding to the contingency procedure such that it is expected to remain inside the contingency volume). These may include procedures such as automatic landing, manual control takeover, or return-to-home.

(g) **Contingency Volume**: The Contingency Volume is the buffer area beyond the Flight Geography in which contingency procedures (e.g., return-to-home, auto-land, manual control) will be used to return the aircraft to the Flight Geography or safely terminate the flight. The Contingency Volume must be defined such that any contingency procedures to be used can be initiated when the RPA leaves the Flight Geography and completed without the RPA leaving the Contingency Volume.

(h) **Controlled Ground Area**: The ground below the intended RPAS Operational Volume (see 2.3(1)(o)), within which persons not involved in the operation are excluded. (Note: exclusion can be accomplished by geographical features, fencing, signage, etc).

(i) **Detection Volume**: The detection volume is the volume of airspace (temporal and/or spatial measurement) within which traditional aircraft must be detected in order to avoid a near mid-air collision, and remain well clear (if required). It can be thought of as the last point at which an aircraft must be detected, so that the Detect and Avoid (DAA) system can perform all the DAA functions. The detection volume is not tied to the sensor(s) Field of View/Field of Regard. The size of the detection volume depends on the aggravated closing speed of traffic that may reasonably be encountered, the time required by the remote pilot to command the avoidance manoeuvre, the time required by the system to respond and the manoeuvrability and performance of the aircraft.

(j) **Emergency Procedures**: Emergency procedures (or Emergency Response Plans) describe the planned actions to limit the escalating effects of an operation that is no longer in control (e.g., uncontrolled flyaway or impact with terrain). These procedures should include contacting relevant external organizations (e.g., Nav Canada, local law enforcement, environmental agencies).

(k) **Flight Geography**: The Flight Geography is the area within which the RPA is intended to fly for a specific operation. To determine the Flight Geography the applicant must consider the position keeping capabilities of the RPAS in 4D space (latitude, longitude, height and time). In particular, the accuracy of the navigation solution, the flight technical error of the RPAS and the path definition error (e.g. map error) and latencies must be considered and addressed in this determination.

(l) **Gathering of People**: An operation is defined as occurring over a gathering of people if the intent of the RPAS operation is to operate continuously over an outdoor area where:

  (i) an event advertised to the general public is being hosted, including a concert, festival, market or sporting event; or

  (ii) the public can reasonably be expected to gather (e.g., beaches, campgrounds, sports fields, etc).

(m) **Manufacturer**: A person, group of persons, or organization which builds, maintains, and/or operates facilities that produce, assemble, and/or sell a physical RPAS and the associated technical products (e.g. manuals) holding the intellectual property to substantiate its design and performance.

(n) **Near Mid-Air Collision**: A Near Mid-Air Collision (NMAC) is defined as two aircraft coming within 500 ft (152 m) horizontal and ± 100 ft (30 m) vertical of each other while in flight.

(o) **Operational Volume**: The Operational Volume is composed of the Flight Geography and the Contingency Volume, with an added ground risk buffer of at least 1 to 1 (i.e., if the RPA will be operated at 400 ft (122 m) AGL, the Operational Volume is extended an additional 400 ft (122 m) beyond the Contingency Volume).

(p) **Operator**: A person, group of persons, or organization seeking approval to operate an RPAS under the CAR, Part IX.

(q) **Population Centre**: An area with a population of at least 1,000 and a density of 400 or more people per square kilometer, based on the latest available census data. Refer to the Statistics Canada Geography tool (https://www150.statcan.gc.ca/n1/en/geo).

(r) **T_{ERP}**: the time required to complete the operational Emergency Response Procedures related to an aircraft fly-away. This shall include the time required to recognize a flyaway, complete any related checklists, contact appropriate airspace/ground users, and allow appropriate time for mitigations

(2) The following **abbreviations** are used in this document:

(a) **AC**: Advisory Circular;

(b) **AGL**: Above Ground Level;

(c) **ARC**: Air Risk Class;

(d) **BVLOS**: Beyond Visual Line of Sight;

(e) **C2 Link**: Command and Control Data Link;

(f) **CAR**: Canadian Aviation Regulation;

(g) **CE**: Conformité européene;

(h) **CFR**: Code of Federal Regulations;

(i) **CONOPS**: Concept of Operations;

(j) **DAA**: Detect and Avoid;

(k) **DND**: Department of National Defence;

(l) **GCS**: Ground Control Station;

(m) **GRC**: Ground Risk Class;

(n) **EM**: Electromagnetic;

(o) **EMI**: Electromagnetic Interference;

(p) **EU**: European Union;

(q) **ERP**: Emergency Response Plan;

(r) **FAA**: Federal Aviation Administration;

(s) **GNSS**: Global Navigation Satellite System;

(t) **HMI**: Human Machine Interface;

(u) **ISED**: Innovation, Science, and Economic Development Canada;

(v) **JARUS**: Joint Authorities for Rulemaking of Unmanned Systems;

(w) **MTOW**: Maximum Take-off Weight;

(x) **NMAC**: Near Mid-Air Collision;

(y) **ORA**: Operational Risk Assessment;

(z) **OSO**: Operational Safety Objective;

(aa) **PIC**: Pilot-In-Command.

(bb) **RF**: Radio Frequency;

(cc) **RPA**: Remotely Piloted Aircraft;

(dd) **RPAS**: Remotely Piloted Aircraft System;

(ee) **RTH**: Return-To-Home.

(ff) **SAIL**: Specific Assurance and Integrity Level;

(gg) **SFOC**: Special Flight Operations Certificate;

(hh) **SORA**: Specific Operational Risk Assessment;

(ii) **sRPA**: small Remotely Piloted Aircraft;

(jj) **TMPR**: Tactical Mitigation Performance Requirements;

(kk) **TCCA**: Transport Canada Civil Aviation;

(ll) **TSO**: Technical Standard Order;

(mm) **VLOS**: Visual Line of Sight.

3.0 Background

(1) The first set of regulations governing the operation of RPAS in Canada were published in 2019 in CAR Part IX, initially covering Visual Line of Sight (VLOS) operations with RPA having a Maximum Take-off Weight (MTOW) of 25 kg or less (under Subpart 1). Other types of operations may be authorized through an SFOC – RPAS issued by the Minister under CAR 903.03. These Special Flight Operations are listed in CAR 903.01, which states:

"No person shall conduct any of the following operations using a remotely piloted aircraft system that includes a remotely piloted aircraft having a maximum take-off weight of 250 g (0.55 pounds) or more unless the person complies with the provisions of a special flight operations certificate — RPAS issued by the Minister under section 903.03:

(a) the operation of a system that includes a remotely piloted aircraft having a maximum take-off weight of more than 25 kg (55 pounds);

(b) the operation of a system beyond visual line-of sight, as referred to in subsection 901.11(2);

(c) the operation of a system by a foreign operator or pilot who has been authorized to operate remotely piloted aircraft systems by the foreign state;

(d) the operation of a remotely piloted aircraft at an altitude greater than those referred to in subsection 901.25(1), unless the operation at a greater altitude is authorized under subsection 901.71(2);

(e) the operation of more than five remotely piloted aircraft at a time from a single control station, as referred to in subsection 901.40(2);

(f) the operation of a system at a special aviation event or at an advertised event, as referred to in section 901.41;

(g) the operation of a system when the aircraft is transporting any of the payloads referred to in subsection 901.43(1);

(h) the operation of a remotely piloted aircraft within three nautical miles of an aerodrome operated under the authority of the Minister of National Defence, as referred to in subsection 901.47(3); and

(i) any other operation of a system for which the Minister determines that a special flight operations certificate — RPAS is necessary to ensure aviation safety or the safety of any person.

(2) In order to be issued an SFOC – RPAS, an operator must submit an application to the Minister as detailed in CAR 903.02. In particular, CAR 903.02 (p) indicates that in addition to the specific

information required by 903.02 (a) through (o), the operator must submit "any other information requested by the Minister pertinent to the safe conduct of the operation". For certain complex operations, as determined during the application process, an Operational Risk Assessment (ORA), acceptable to the Minister, is one of the items of "other information" required in support of an application for an SFOC – RPAS.

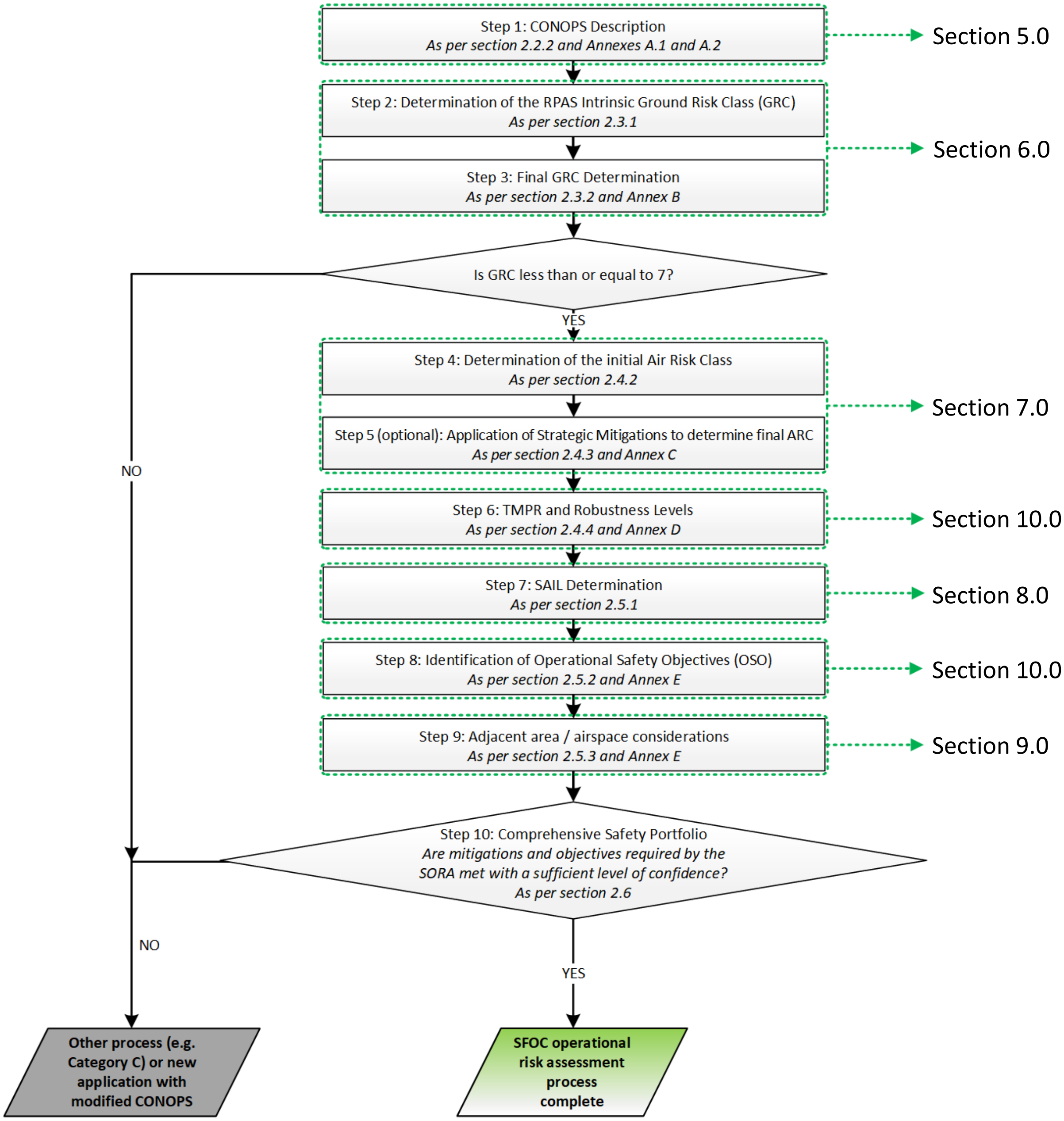
(3) This document described an ORA methodology based on the JARUS SORA guidelines, adapted for use in the Canadian aviation environment. As indicated in Section 1.0 of this document, this methodology is one means, but not the only means, of meeting the requirement for an ORA under the authority of CAR 903.02 (p).

4.0 RPAS ORA Overview

(1) This document describes an ORA based on the JARUS SORA process, which is explained in detail in documents published by JARUS working group 6 – see Reference (d). The remainder of this document describes how the JARUS SORA has been adjusted to accommodate the specificities of the Canadian environment and operational context.

(2) Figure 1, below, illustrates the JARUS SORA process and highlights the areas in which adjustments are necessary. Each of these adjustments are described in detail in the indicated sections of this AC. In general, the RPAS ORA endorses the overall JARUS SORA process steps shown in Figure 1, with adjustments as described in the remainder of this AC.

Figure 1 – JARUS SORA Process



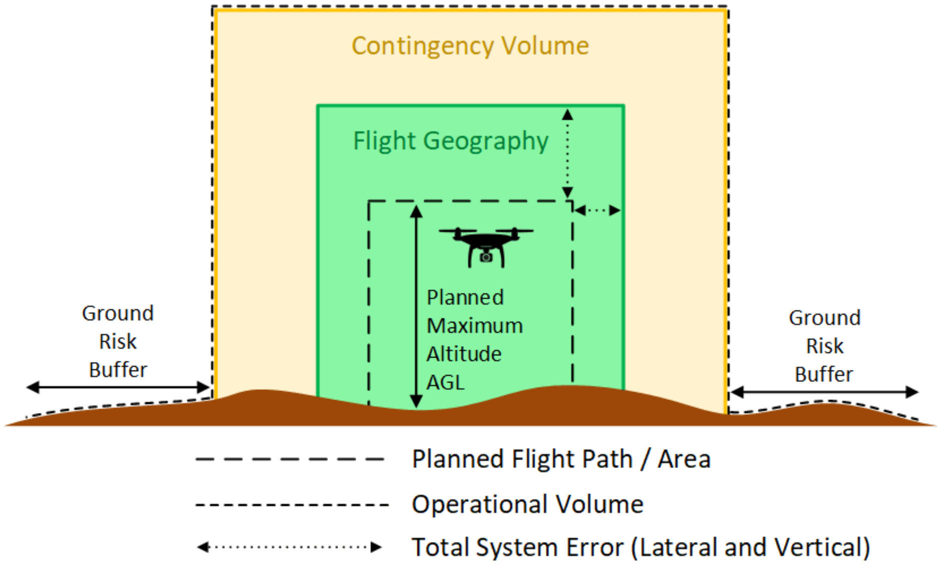
5.0 Concept of Operations and Definition of Operational Volume

(1) Step 1 of the JARUS SORA process involves defining the Concept of Operations (CONOPS) for the intended flight(s). Further explanation of the expected content of a CONOPS description is contained in JARUS SORA Section 2.2.2 and SORA Annex A. However, one of the key concepts that merits further explanation for the purposes of the RPAS ORA is the Operational Volume.

(2) The defined Operational Volume is used for the purposes of Ground Risk Determination (Section 6.0), Air Risk Determination (Section 7.0), and for assessment of Adjacent Area / Airspace Considerations (Section 8.0). As a result, correct definition of this volume is critical for the appropriate application of the RPAS ORA process. As defined in Section 2.3 above, the

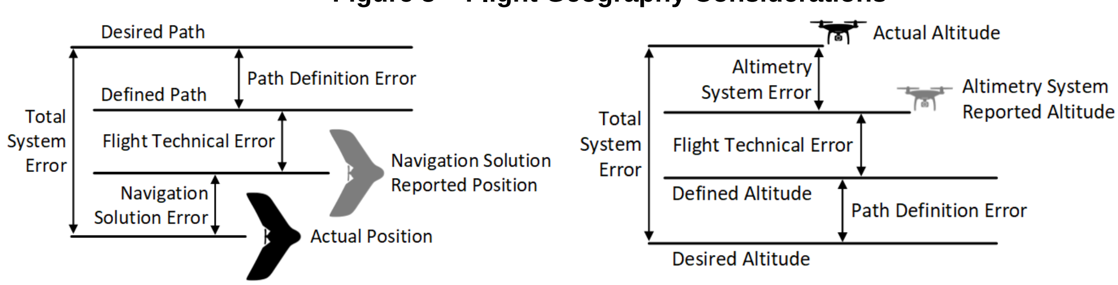
Operational Volume includes the Flight Geography, the Contingency Volume, and a 1-to-1 ground risk buffer. Refer to Figure 2, below, for an illustration of this concept.

Figure 2 – Operational Volume



(3) **Flight Geography**. As defined in Section 2.3 above, the starting point for the definition of the flight geography is the area or path where the RPA is intended to be flown for the specific operation. However, the definition of this area or path alone is not sufficient to address the intended flight area, as RPA positioning errors must also be considered. The relevant contributors to error are illustrated in Figure 3 and explained in further detail below.

Figure 3 – Flight Geography Considerations



(a) Path Definition Error. Path definition error refers to the difference between the intended path through the environment (laterally and vertically) and the defined path (i.e., what the pilot or autopilot is actually trying to follow). Path definition errors may result from:

(i) Map projection differences. Depending on the type of map or mapping software used to generate the flight plan, distortion resulting from the map projection may result in the actual path over ground being somewhat offset from the intended path plotted over the map features. (Note: A map projection is a systematic transformation of the latitudes and longitudes of locations from the surface of a sphere or an ellipsoid into locations on a plane (2D map), which necessarily results in some distortion of the surface).

(ii) Earth reference model differences. The aviation (and GPS) standard earth reference model is the WGS-84 system. Planned paths that are created using a different reference model may be subject to error upon conversion into WGS-84 referenced data.

(iii) Altitude considerations. As illustrated in Section 7.0 and Figures 4 and 5, some areas of the RPAS ORA air risk model have a step change in risk level at 400 ft AGL. As a result, the validity of the ORA for operations planned to occur at or below 400 ft AGL in these areas depends on ensuring that the defined path is created to ensure that the aircraft will remain below this altitude ceiling. For example, if the operation is planned to occur in an area with rolling terrain, the 3D path either needs to adjust altitude to follow the terrain, or set a consistent altitude such that the aircraft remains below 400 ft AGL at the lowest terrain elevation that will be overflown.

(iv) Terrain data errors. For areas or paths where the intended altitude is defined in AGL following the terrain, errors in the terrain data used to generate a 3D path will result in altitude deviations relative to the actual terrain.

(b) Flight Technical Error. Flight technical error refers to the accuracy with which the reported aircraft position and altitude are controlled relative to the defined path. This error is dependent on:

(i) The means of control and its associated performance (e.g., manual control vs. autopilot). For example, flight technical error for an autopilot following a 3D path within the performance capabilities of the aircraft is typically quite low. A pilot manually controlling to follow the same 3D path is generally not able to provide the same level of accuracy, leading to a greater flight technical error.

(ii) The means of determining the difference between the reported position and the defined path. Particularly in cases of manual control by a pilot, ability to follow a 3D path is highly dependent on the way the path and path deviation data is displayed (e.g., following a flight director command is much more accurate than trying to maintain path using graphical altitude and course deviation indications, which is again more accurate than trying to maintain path using digital readouts of path deviation).

(c) Navigation Solution and Altimetry System Accuracy. The accuracy of the navigation solution (laterally) and the altimetry system (vertically) must be considered to determine the potential difference between the reported position and the actual position of the aircraft.

(d) Latencies. Any latencies in the C2 link(s), navigation solution computation, or altimetry system may add to the total system error depending on the system architecture. For example, if the system position determination function is on-board the aircraft and the path control function is part of the Ground Control Station (GCS), any C2 link latency will result in flight technical error as the system tries to correct its path based on an out-of-date reported position. (Note that this would be the case in a system where the RPA is being manually controlled by a pilot at the ground control station – i.e., where the pilot is performing the path control function).

(4) **Contingency Volume**. As defined in Section 2.3 above, the contingency volume is intended to provide a buffer area beyond the Flight Geography to allow time and space for contingency procedures to be enacted.

(a) Contingency Procedures. In general, contingency procedures are put in place to support recovery from undesirable states that, if not addressed, could lead to unsafe situations. For example, operation outside of the planned flight path / area is an undesirable state that could be a precursor to a flyaway, and loss of C2 link is an undesirable state that may lead to additional operational risks as a result of a dynamic environment. Samples of typical contingency procedures and related considerations for calculation of the contingency volume are listed below. Note that the procedures listed below are not mandatory, nor is the list intended to be exhaustive; it simply provides examples of the types of considerations to be addressed in defining the contingency volume.

(b) Automatic Return-To-Home (RTH). If an automatic RTH function is used as part of any contingency procedures (e.g. for loss of C2 link), the design of this function should be considered in the definition of the contingency volume. For example, a common RTH function implementation involves the aircraft climbing to a specified altitude and then following a direct path from its current location to the home point. Using this type of RTH function, any planned operation that does not follow a direct linear route will need to include any area between the planned flight path and the home point as part of the contingency volume. The altitude used, if higher than the planned flight path altitude, will also need to be included in the contingency volume.

(c) Automatic Landing. If automatic landing at present position or a specified alternate location is included as part of any contingency procedures, the area surrounding the landing location should be addressed as part of the contingency volume if it may be outside of the flight geography. For example, automatic landing at present position is a common contingency procedure for loss of GPS navigation; however, loss of GPS navigation may also result in a loss of position-holding capability. In such cases, the potential position drift resulting from wind during the descent from operating altitude to landing needs to be included in the contingency volume.

(d) Pilot-In-Command (PIC) Manual Control Takeover. If a manual control takeover by the PIC (or a secondary pilot) is included as a contingency procedure to address departures from the planned flight path / area, the contingency volume needs to provide sufficient time and space to allow the pilot to:

(i) recognize the deviation from the planned path;

(ii) execute the manual control takeover procedure; and

(iii) maneuver the aircraft back to the planned flight path / area.

(5) **Ground Risk Buffer**. The ground risk buffer is added based on the expectation that some mechanism of flight termination may be included as part of the emergency procedure if the aircraft exceeds the contingency volume. Thus, some ground area outside of the contingency volume needs to be considered as part of the ground risk determination. The “1-to-1” concept means that the buffer is defined, at minimum, as a horizontal distance equal to the aircraft’s planned maximum altitude (AGL). Note that:

(a) The planned maximum altitude (and the resulting required buffer distance) may change across flight segments, and the appropriate buffer distance may be applied to the individual segments. For example, if a survey operation is to be flown at 2000 ft AGL, but the transit to the survey area is to be flown at 1000 ft AGL, it is not necessary to apply the 2000 ft buffer to the cruise segments of the flight (1000 ft is sufficient).

(b) The total system error (vertical) is assumed to be small compared to the planned maximum altitude (AGL). If the total system error (vertical) for the proposed operation is a significant percentage of the planned maximum altitude (greater than approx. 10%), the Flight Geography maximum height should be used to define the ground risk buffer.

(6) For an example of the definition of an operational volume, refer to Appendix A.

6.0 Ground Risk Determination

(1) Steps 2 and 3 of the JARUS SORA process involve determining the intrinsic ground risk associated with the operation, and applying any strategic mitigations to reduce this risk.

(2) **Intrinsic Ground Risk**. As described in JARUS SORA Section 2.3.1, the intrinsic ground risk class (GRC) is determined from the size / kinetic energy of the RPA and the generalized Operational Scenarios listed in Table 1, below. For the purposes of the RPAS ORA, the interpretation of these Operational Scenarios has been clarified based on the definitions contained in Section 2.3 (specifically, 2.3(1)(h), 2.3(1)(l), and 2.3(1)(q)).

Table 1 – RPAS ORA Intrinsic Ground Risk

Max RPA Characteristic Dimension	1 m / approx. 3 ft	3 m / approx 10 ft	8 m / approx. 25 ft	>8 m / approx. 25 ft
Typical Kinetic Energy Expected (ref. JARUS SORA Section 2.3.1 (k))	< 700 J	< 34 kJ	< 1084 kJ	> 1084 kJ
Operational Scenarios	Intrinsic GRC			
VLOS/BVLOS over controlled ground area	1	2	3	4
VLOS outside of a population centre	2	3	4	5
BVLOS outside of a population centre	3	4	5	6
VLOS within a population centre	4	5	6	8
BVLOS within a population centre	5	6	8	10
VLOS over gathering of people	7			
BVLOS over gathering of people	8			

(3) **Application of Operational Volume**. When determining the intrinsic ground risk based on Table 1, all ground within the operational volume as defined in Section 5.0 must be considered. Also note that it is acceptable to break the operation into segments based on changes in risk level, allowing different risk mitigations to be used for different segments of the operation (as illustrated in the example contained in Appendix A).

(4) **Strategic Mitigations for Ground Risk**. As described in JARUS SORA Section 2.3.2 and Annex B, there are a variety of strategic measures that may be put in place in order to reduce the ground risk of an operation. Applicants are encouraged to assess and make use of these strategic mitigations; however, there is currently no Canadian-specific guidance available regarding their use. As such, these mitigations will be considered on a case-by-case basis and may not result in credit being given in the form of GRC reductions.

Note: Strategic Mitigations will be assessed on an ongoing basis with the intent of setting performance and robustness requirements for GRC reductions in a future revision of this AC.

7.0 Air Risk Determination

(1) Steps 4, 5, and 6 of the JARUS SORA process involve determining the intrinsic air risk associated with the operation, and applying any strategic mitigations to reduce this risk. Tactical Mitigation Performance Requirements (TMPR) are also assigned based on the final Air Risk Class (ARC).

(2) **Intrinsic Air Risk**. As described in JARUS SORA Section 2.4.2, the intrinsic ARC is determined from the intended operational environment, by following the provided flow chart / decision tree. For the purposes of the RPAS ORA, the interpretation of the air risk classes has been adjusted based on the definitions contained in Section 2.3. Figure 4, below shows the air risk class decision tree as updated based on these definitions and Figure 5 provides a graphical depiction.

Figure 4 – Air Risk Class Decision Tree

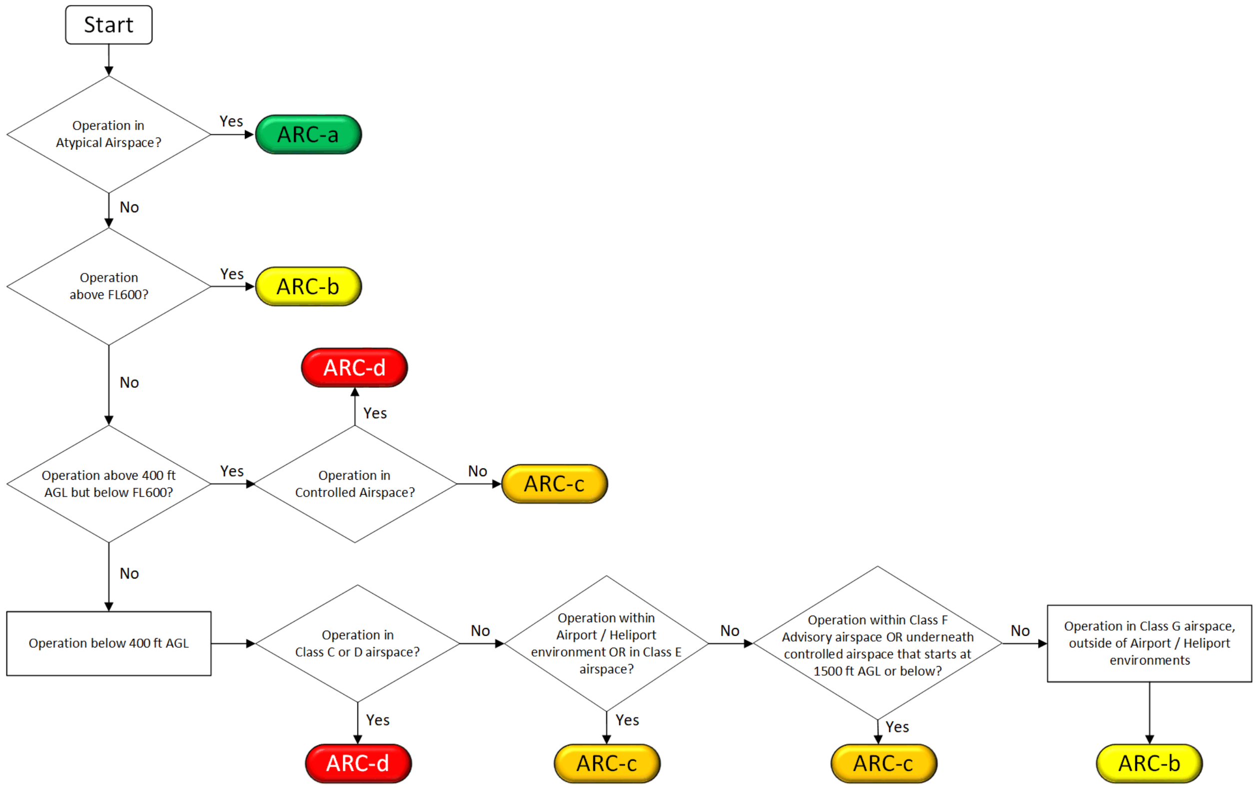
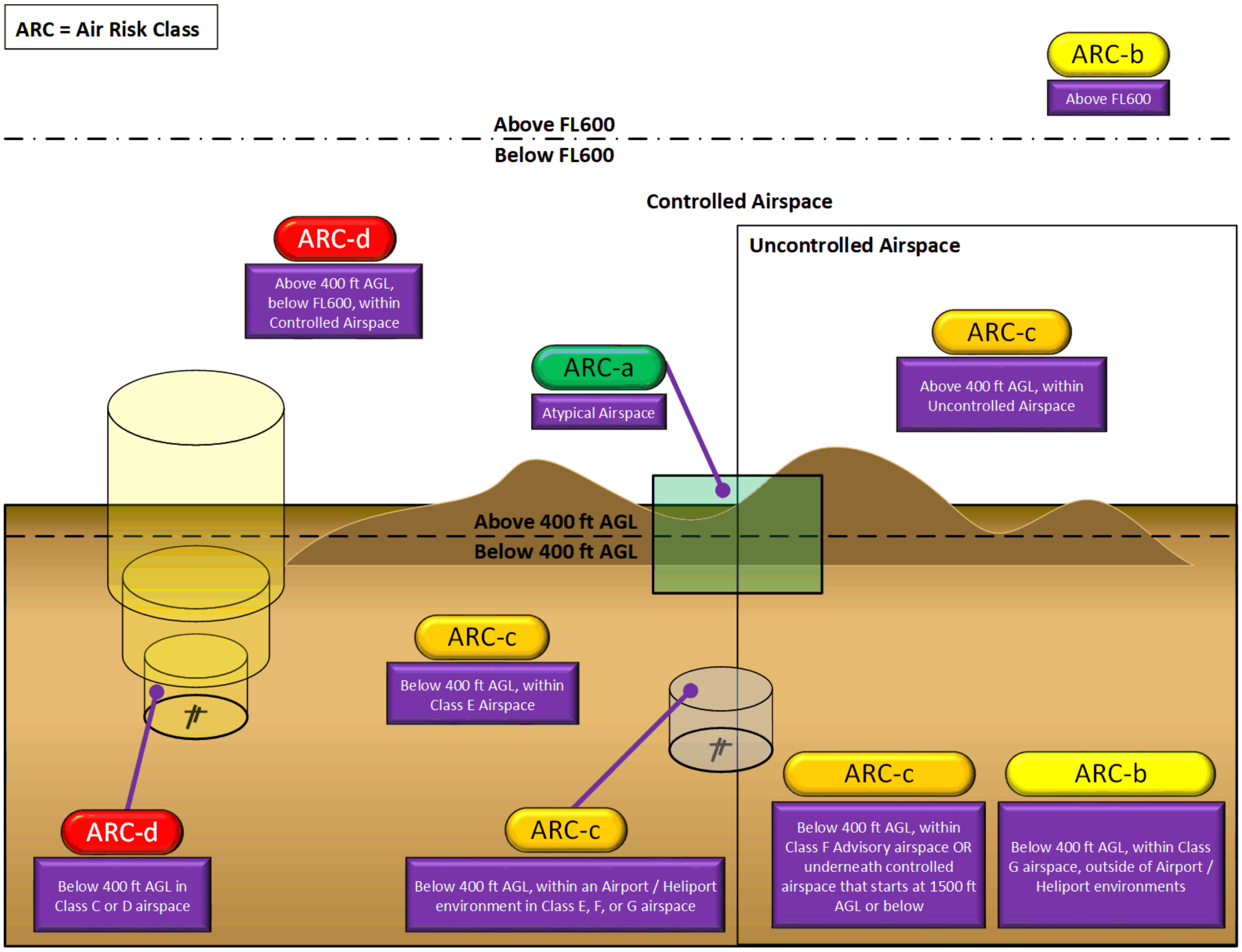


Figure 5 – Graphical Depiction of Air Risk Classes



(3) **Application of Operational Volume**. When determining the ARC based on Figure 4 or Figure 5, all airspace within the operational volume as defined in Section 5.0 must be considered. Also note that it is acceptable to break the operation into segments based on changes in risk level, allowing different risk mitigations to be used for different segments of the operation (as illustrated in the example contained in Appendix A).

(4) **Strategic Mitigations for Air Risk**. As described in JARUS SORA Section 2.4.3 and Annex C, there are a variety of strategic measures that may be put in place in order to reduce the air risk of an operation. Applicants are encouraged to assess and make use of these strategic mitigations; however, there is currently no Canadian-specific guidance available regarding their use. As such, these mitigations will be considered on a case-by-case basis and may not result in credit being given in the form of ARC reductions.

Note: Strategic Mitigations will be assessed on an ongoing basis with the intent of setting performance and robustness requirements for ARC reductions in a future revision of this AC.

(5) **Tactical Mitigation Performance Requirements**. The JARUS SORA TMPR provide the Detect and Avoid (DAA) requirements for the proposed operation, and their performance levels and required robustness levels are assigned based on the final ARC as per JARUS SORA Section 2.4.4. Further detail of the specific performance and robustness requirements for the RPAS ORA are contained in Section 10.1 of this AC.

8.0 SAIL Determination

(1) The determination of the overall risk score of the operation in the form of the Specific Assurance and Integrity Level (SAIL) is carried out as described in JARUS SORA Section 2.5.1 and illustrated in Table 2, below.

Table 2 – RPAS ORA Specific Assurance and Integrity Levels

	Final ARC			
Final GRC	a	b	c	d
1	I	II	IV	VI
2	I	II	IV	VI
3	II	II	IV	VI
4	III	III	IV	VI
5	IV	IV	IV	VI
6	V	V	V	VI
7	VI	VI	VI	VI
>7	RPAS ORA N/A at this time (e.g., may require certified operations / aircraft)			

9.0 Adjacent Area / Airspace Considerations

9.1 Determination of Adjacent Areas and Airspace

(1) The JARUS SORA includes requirements for an assessment of adjacent areas and airspace to determine what hazards may exist in the event of a loss of control of the operation resulting in a fly away. The risk level of these adjacent areas and airspaces are then used to determine an appropriate level of containment objective(s) to be applied to the operation. These containment objectives are expressed in terms of system reliability and design assurance against failure conditions resulting in the aircraft leaving the Operational Volume. However, the document leaves it up to the judgment of the operator and the certifying authority to determine what constitutes adjacent areas and adjacent airspace.

(2) A conservative approach to identifying adjacent areas/airspace would be to consider the maximum performance of the RPA and identify any locations attainable by the RPA under worst-case flyaway conditions. For instance, an RPA with a maximum ceiling of 20,000ft could theoretically reach Class A controlled airspace above FL180. A fixed wing RPA with a range of 200nm could theoretically reach any ground location that is within 200nm of the launch site. Defining the Operational Volume such that it includes adjacent areas and airspace calculated in this manner is acceptable and encouraged, and it will in many cases result in an increase to the resulting SAIL for the operation. However, it is acknowledged for some operations, this strategy may be overly conservative and result in overly restrictive operational limitations.

(3) The definition of Adjacent Areas and Airspace listed in Section 2.3 involves determining the time required to perform the Emergency Procedures related to an aircraft flyaway and using this time to establish practical limits on what locations the aircraft could reach before risk mitigations can be applied. The intent is to provide a reasonable safety buffer around the operational volume that gives the operator time to implement emergency procedures before the RPA reaches higher risk locations. The emergency procedures could include contacting other users to warn them of the

approaching RPA, as well as flight termination assuming that it is shown to have sufficient independence from the primary C2 link.

(4) Alternatively, for some specific operations it may be desirable to calculate the time required to reach the nearest high risk airspace, and use this time as a maximum limit when developing Emergency Procedures.

(5) Refer to Appendix A for a demonstration of the application of Adjacent Areas / Airspaces and Containment concepts based on a notional operation.

9.2 Operations not Requiring Containment Objectives

(1) The following operations are specifically excluded from the containment objectives detailed in this section:

(a) Operations performed wholly within the regulations of Part IX, Subpart 1. (VLOS, <25kgs, Basic or Advanced Operations, etc.). The requirements existing in Part IX, Subpart 1 are considered adequate to ensure safety.

(b) Operations at approved Test Ranges. It is assumed that the test range has been designed with adjacent areas/airspace in mind, and that operation there includes procedures required in the event of a fly-away.

(c) Operations for which the Operational Volume is defined such that it covers the maximum possible performance of the RPA, as described in Section 9.1(1) above. Operations defined in this way will be required to meet the SAIL safety objectives for the highest risk area within reach of the RPA, and therefore are not subject to containment requirements.

9.3 High Robustness Containment Objectives

(1) High Robustness Containment objectives must be satisfied when:

(a) an operation is conducted over a controlled ground area within a population centre; or

(b) areas and airspace adjacent to the operation include any of the following:

(i) Gatherings of people, unless the operation is already considering gatherings of people as part of the GRC estimation.

(ii) ARC-d unless the operational ARC is already ARC-d.

(2) The High Robustness Containment Objectives are:

(a) No single failure of the RPAS or any external system supporting the operation shall lead to operation outside of the operational volume.

(b) Any combination of failures of the RPAS and/or any external system supporting the operation that may lead to operation outside of the operational volume shall be shown to be remote.

Note: Quantitative probability values associated with “remote” failure conditions referenced here are intended to be scaled with the kinetic energy of the RPAS as described in Appendix E.

(c) Software (SW) and Airborne Electronic Hardware (AEH) whose development error(s) could directly lead to operations outside of the operational volume shall be developed to an industry standard or methodology recognized by TCCA (ref. AC 922-001 Appendix A).

(3) Compliance with the requirements above shall be demonstrated by a manufacturer declaration that the RPAS meets the reliability target.

9.4 Low Robustness Containment Objectives

(1) All operations that are not excluded operations (Section 9.2) and do not require High Robustness Containment Objectives (Section 9.3) are required to meet Low Robustness Containment Objectives.

(2) The Low Robustness Containment Objectives are:

(a) Any single failure of the RPAS or any external system supporting the operation that may lead to operation outside of the operational volume shall be shown to be remote.

Note: Quantitative probability values associated with “remote” failure conditions referenced here are intended to be scaled with the kinetic energy of the RPAS as described in Appendix E

(3) Compliance with the requirement above shall be demonstrated by an operator or manufacturer declaration that the RPAS meets the reliability target.

10.0 Performance Objectives

(1) The overall intent of the RPAS ORA process is to set performance objectives for approval of an operation that are commensurate with the risk involved in conducting the operation. The performance requirements applied through the RPAS ORA process can be divided into two categories:

(a) Tactical Mitigation Performance Requirements (TMPR), which are driven purely by the air risk in the form of the ARC, and describe the performance requirements for the Detect and Avoid (DAA) function; and

(b) Operational Safety Objectives (OSOs), which are driven by the overall risk as represented by the SAIL, and describe the performance requirements across a variety of elements that contribute to ensuring the overall safety of the operation.

10.1 DAA Performance Objectives

(1) As described above, the DAA performance objectives are driven by the final ARC of the proposed operation. The overall performance level and related robustness level are listed in Table 3, below, along with the System Risk Ratio that was used to guide the setting of the lower level performance requirements.

Note: System Risk Ratio refers to the ability of the complete, ‘end-to-end’ DAA system to mitigate potential collisions with conflicting traffic. A lower risk ratio means more potential collisions will be mitigated, e.g., a risk ratio of 0.1 indicates that out of 100 potential collisions, the DAA system would mitigate 90.

Table 3 – RPAS ORA Detect and Avoid Objectives

Air Risk Class	DAA Performance Level	DAA Robustness	DAA Risk Ratio
ARC-d	High Performance	High Robustness	≤ 0.1
ARC-c	Medium Performance	Medium Robustness	≤ 0.3
ARC-b	Low Performance	Low Robustness	≤ 0.5
ARC-a	Minimal Performance	Minimal Robustness Requirement	N/A

Note: The risk ratios listed in the above table are applied equally to cooperative and non-cooperative traffic (i.e., a DAA solution that only uses a cooperative sensor such as ADS-B

In will not meet the DAA Objectives in any airspace where the corresponding equipment is not mandatory for all aircraft).

(2) To clarify and ease understanding of the high-level DAA performance objectives listed in Table 3, they are broken down into five DAA functions, each of which is further described below.

(3) **Detect**. The detect function deals with the need to determine the location and/or speed of any traditional aircraft operating in the area near the RPAS operation ("intruders"). Note that the calculation of the required detection volume is a key driver of all DAA function objectives; refer to Appendix B for an example detection volume calculation.

Table 4 – DAA Detect Function Objectives

Air Risk Class	Functional Objectives
ARC-d	A system meeting RTCA SC-228 or EUROCAE WG-105 MOPS/MASPS (or similar) and installed in accordance with applicable Requirements.
ARC-c	As per ARC-b, except the detection threshold is 90% of all aircraft in the detection volume. In addition to technologies described in ARC-b, this could also include: • Use of ATC Separation Services • Active communication with ATC and other airspace users. The applicant provides an assessment of the effectiveness of the detection tools/methods chosen.
ARC-b	Everything in ARC-a, plus: The applicant provides an appropriate calculation of the required detection volume. The applicant provides a DAA Plan demonstrating means to detect approximately 70% of all aircraft in the detection volume (in absence of any failures or malfunctions). This could rely on one or more of the following: • Active or passive sensors (RADAR, EO, IR, acoustic, etc) • Use of Low Cost ADS-B In /UAT/FLARM/Pilot Aware aircraft trackers • Use of (web-based) real time aircraft tracking services • Monitoring aeronautical radio communication (i.e. use of a scanner)
ARC-a	The applicant provides a plan including: • use of visual observer(s) for the launch / recovery area, • monitoring of local radio frequency or frequencies, • advisory radio transmissions before takeoff, at regular intervals during flight operations, and after landing, and • means of increasing conspicuity of the RPA.

Note: The detection thresholds for ARC-b and ARC-c are increased from the minimum amount that would be required to meet the identified risk ratios to account for less than perfect performance of the remaining DAA functions (described below).

(4) **Decide**. The decide function describes the criteria used to determine whether any detected intruder aircraft constitute a threat or potential threat to the RPAS operation (i.e., whether any avoidance action needs to be taken).

Table 5 – DAA Decide Function Objectives

Air Risk Class	Functional Objectives
ARC-d	A system meeting RTCA SC-228 or EUROCAE WG-105 MOPS/MASPS (or similar) and installed in accordance with applicable Requirements.
ARC-c	All requirements of ARC-b and in addition: The operator provides an assessment of the human/machine interface factors that may affect the remote pilot’s ability to make a timely and appropriate decision. The operator provides an assessment of the effectiveness of the tools and methods utilized for the timely detection and avoidance of traffic. In this context timely is defined as enabling the remote pilot to decide within 5 seconds after the indication of incoming traffic is provided. The operator provides an assessment of the failure rate or availability of any tool or service the operator intends to use.
ARC-b	The operator must have a documented de-confliction scheme, in which the operator explains which tools or methods will be used for detection and what the criteria are that will be applied for the decision to avoid incoming traffic. In case the remote pilot relies on detection by someone else, the use of phraseology will have to be described as well. Examples: • The operator will initiate a rapid descent if traffic is crossing an alert boundary and operating at less than 1000ft. • The observer monitoring traffic uses the phrase: ‘DESCEND! DESCEND! DESCEND!’
ARC-a	The operator must have a documented de-confliction scheme, in which the operator explains what actions will be taken if local traffic is detected via radio monitoring.

(5) **Command**. The command function addresses the time required to communicate with the RPA when necessary to initiate an avoidance maneuver.

Table 6 – DAA Command Function Objectives

Air Risk Class	Functional Objectives
ARC-d	A system meeting RTCA SC-228 or EUROCAE WG-105 MOPS/MASPS (or similar) and installed in accordance with applicable Requirements.
ARC-c	The latency of the whole Command and Control (C2) data link, i.e. the time between the moment that the remote pilot gives the command and the airplane executes the comment shall not exceed the time allocated to it in the calculation of the detection volume. Recommendation: the latency of the whole C2 link should not exceed 3 seconds.
ARC-b	The latency of the whole C2 link shall not exceed the time allocated to it in the calculation of the detection volume. Recommendation: the latency of the whole C2 link should not exceed 5 seconds.
ARC-a	No minimum level of requirement. Recommendation: the latency of the whole C2 link should not exceed 8 seconds.

(6) **Execute.** The execute function includes the details of the avoidance maneuvers to be performed, accounting for the performance of the RPA.

Table 7 – DAA Execute Function Objectives

Air Risk Class	Functional Objectives
ARC-d	A system meeting RTCA SC-228 or EUROCAE WG-105 MOPS/MASPS (or similar) and installed in accordance with applicable Requirements.
ARC-c	The operator's documented de-confliction scheme must explain the avoidance maneuver(s) to be used, and the time required for the aircraft to execute the maneuver(s) shall be accounted for in the calculation of the detection volume. Avoidance may rely on vertical and horizontal avoidance maneuvering. Where horizontal maneuvering is applied, the aircraft shall be demonstrated to have adequate performance, such as airspeed, acceleration rates, climb/descend rates and turn rates. The following are suggested minimum performance criteria: • Airspeed: ≥ 50 knots • Rate of climb/descend: ≥ 500 ft/min • Turn rate: ≥ 3 degrees per second.
ARC-b	The operator's documented de-confliction scheme must explain the avoidance maneuver(s) to be used, and the time required for the aircraft to execute the maneuver(s) shall be accounted for in the calculation of the detection volume. RPAS descending to an altitude not higher than the nearest trees, buildings or infrastructure or ≤ 60 feet AGL is considered sufficient. The aircraft should be able to descend from its operating altitude to the 'safe altitude' in less than a minute.
ARC-a	The operator's documented de-confliction scheme must explain the avoidance maneuver(s) to be used.

(7) **Feedback**. The feedback function addresses the fact that the DAA function is a continuously operating system in which data needs to be sufficiently up-to-date to make appropriate decisions with respect to avoidance.

Table 8 – DAA Feedback Function Objectives

Air Risk Class	Functional Objectives
ARC-d	A system meeting RTCA SC-228 or EUROCAE WG-105 MOPS/MASPS (or similar) and installed in accordance with applicable Requirements.
ARC-c	The information is provided to the remote pilot with a latency and update rate that support the decision criteria. The following are suggested minimum criteria: • Intruder and RPA vector data update rates: ≤ 3 seconds.
ARC-b	Where electronic means assist the remote pilot in detecting traffic, the information is provided with a latency and update rate for intruder and RPA data (e.g. position, speed, altitude, track) that support the decision criteria.
ARC-a	Feedback is anticipated to be provided by a combination of visual observer(s) and radio frequency monitoring.

(8) **Integrity and Assurance**. Integrity and assurance describe the required reliability of the DAA system and the level of evidence required to demonstrate compliance with this reliability objective as well as the performance objectives of Tables 4 through 8 above.

Table 9 – DAA System Integrity and Assurance Objectives

Air Risk Class	Integrity	Assurance
ARC-d	Probability of failure: < 1 per 100,000 Flight Hours (10^{-5} loss / FH) Note: A quantitative analysis is required.	The evidence that the DAA System and procedures will reduce the risk of collisions with manned aircraft to an acceptable level is verified by an independent third party.
ARC-c	Probability of failure: < 1 per 1,000 Flight Hours (10^{-3} loss / FH) Note: This rate is commensurate with a probable failure condition. These failure conditions are anticipated to occur one or more times during the operational life of each RPAS. No quantitative analysis is required.	The operator provides evidence that the DAA System and procedures will reduce the risk of collisions with manned aircraft to an acceptable level.
ARC-b	Probability of failure: < 1 per 100 Flight Hours (10^{-2} loss / FH) Note: The requirement is considered to be met by commercially available products. No quantitative analysis is required.	The operator provides evidence that the DAA System and procedures will reduce the risk of collisions with manned aircraft to an acceptable level.
ARC-a	Probability of failure: < 1 per 100 Flight Hours (10^{-2} loss / FH) Note: The requirement is considered to be met by commercially available products. No quantitative analysis is required.	The operator's plan as described in the ARC-a DAA requirements is provided as part of their application for operational approval.

10.2 Operational Safety Objectives

(1) While the JARUS SORA suggests Operational Safety Objectives (OSO) and provides suggested robustness levels required for each SAIL level. The list of OSO and robustness levels is provided here. The reader's attention is drawn to OSO 4, 5, 10 and 12 where the robustness levels required have been changed from what is listed in the published JARUS SORA document.

(2) Refer to Appendix C for additional guidance on each OSO and the means of compliance for each robustness level expected.

(3) For each OSO, it is expected that the applicant demonstrate how the OSO is met to the required level of robustness within their RPAS ORA document. For some OSO and low robustness levels, the demonstration may be completely contained within the RPAS ORA document. For others, an external document reference (e.g., referring to an approved operational procedures document) may be required.

(4) Applicants are encouraged to document their compliance with Optional OSO requirements as a means to demonstrate the overall robustness level of the operation.

Table 10 – Operational Safety Objectives

OSO Number	OSO Description	SAIL					
		I	II	III	IV	V	VI
1	Ensure the Operator is Competent and/or proven	O	L	M	H	H	H

Table 10 – Operational Safety Objectives

OSO Number	OSO Description	SAIL					
		I	II	III	IV	V	VI
2	RPAS is manufactured by competent and/or proven entity	O	O	L	M	H	H
3	RPAS is maintained by competent and/or proven entity	L	L	M	M	H	H
4	RPAS is developed to authority recognized design standards	O	O	L[1]	L	M	H
5	RPAS is designed considering system safety and reliability	O	O	M[2]	M	H	H
6	C2 link performance is appropriate for the operation	O	L	L	M	H	H
7	Inspection of the RPAS (product inspection) to ensure consistency to the ConOps	L	L	M	M	H	H
8, 11, 14, 21[3]	Operational Procedures are defined, validated and adhered to	L	M	H	H	H	H
9, 15, 22[4]	Remote crew is trained and current and able to control the situation	L	L	M	M	H	H
10	Safe recovery from technical issue	O[5]	O[5]	L[5]	M	M[5]	H
12	The RPAS is designed to manage the deterioration of external systems supporting the RPAS operation.	O[6]	O[6]	M[6]	M	H	H
13	External Systems supporting the RPAS operations are adequate to the operation	L	L	M	H	H	H

[1] JARUS SORA V2 sets the Robustness requirement for OSO #4 at the SAIL III level as Optional (O). For Canadian Operations, this has been increased to Low robustness. Refer to Appendix C for additional information.
[2] JARUS SORA V2 sets the Robustness requirement for OSO #5 at the SAIL III level as Low (L). For Canadian Operations, this has been increased to Medium robustness. Refer to Appendix C for additional information.
[3] Operational Safety Objectives related to procedures have been grouped together for clarity. Refer to Appendix C for additional information.
[4] Operational Safety Objectives related to training have been grouped together for clarity. Refer to Appendix C for additional information.
[5] Robustness Requirements for OSO #10 were adjusted to match those of OSO #19. Refer to Appendix C for additional information.
[6] Robustness Requirements for OSO #12 were adjusted to match those of OSO #5. Refer to Appendix C for additional information.

Table 10 – Operational Safety Objectives

OSO Number	OSO Description	SAIL					
		I	II	III	IV	V	VI
16	Multi-crew coordination	L	L	M	M	H	H
17	Remote crew is fit to operate	L	L	M	M	H	H
18	Automatic protection of the flight envelope from Human Error	O	O	L	M	H	H
19	Safe recovery from human error	O	O	L	M	M	H
20	A Human Factors evaluation has been performed and the HMI found appropriate for the operation	O	L	L	M	M	H
23	Environmental conditions for safe operations defined, measurable and adhered to	L	L	M	M	H	H
24	RPAS designed and qualified for adverse environmental conditions	O	O	M	H	H	H

11.0 Information management

(1) Not applicable.

12.0 Document history

(1) Not applicable.

13.0 Contact office

For more information, please contact:

Transport Canada RPAS Task Force, Engineering (AARV)
4th Floor, Place de Ville, Tower C
330 Sparks Street, Ottawa, ON, K1A 0N8

E-mail: TC.RPASInfo-InfoSATP.TC@tc.gc.ca

Suggestions for amendment to this document are invited, and should be submitted via the contact information above.

Document approved by

X

Ryan Coates
Director Remotely Piloted Aircraft Systems T...

Ryan Coates
Director, Remotely Piloted Aircraft Systems Task Force
Civil Aviation
Transport Canada

APPENDIX A — RPAS ORA Example

(1) **General**. The following example uses notional data for a mission using a fixed-wing RPA in an operational environment selected specifically to demonstrate certain concepts of the RPAS ORA. The data used is not intended to be representative of any specific RPA, operator, or operational environment and should not be interpreted as such. Note that a full CONOPS has not been prepared; only the minimum set of information needed for the purposes of the example is provided below.

(a) **RPA Information**. The notional RPA has the following characteristics:

(i) wingspan of 2.8 m (9.2 ft),

(ii) Maximum Take-off Weight (MTOW) of 22 kg,

(iii) Cruise speed of 90 km/h (48.6 kts),

(iv) Maximum speed in level flight 110 km/h (59 kts),

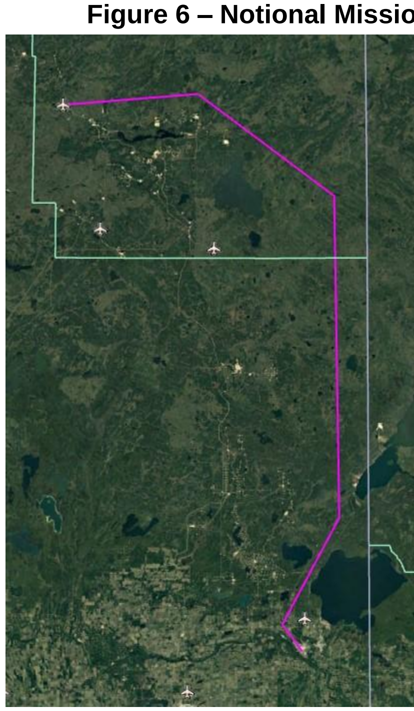
(v) Maximum operating altitude of 19,500 ft MSL, and

(vi) Maximum climb rate of 1500 ft/min.

(b) **Mission Information**. The notional mission is a point-to-point transit from Cold Lake Airport (CYOD) to Conklin (Leismer) (CET2). Planned cruising altitude is 300 ft AGL. Visual observers will be stationed at CYOD and CET2 such that takeoff and landing (and flight within approx. 1.5 km of takeoff and landing) will be conducted VLOS, with the remainder of the flight BVLOS. Refer to Figure 6, below for the planned course.

Note: For the purposes of this example, it is assumed that the operator has obtained permission from the Department of National Defence (DND) to operate from CYOD and within the Cold Lake Air Weapons Range (CYR204).

Figure 6 – Notional Mission



(2) **Definition of Operational Volume**. As described in Section 5.0, the Operational Volume needs to address Flight Geography considerations as well as Contingency Procedures. See below for examples.

(a) **Flight Geography**. The expected total system errors for the RPAS in the horizontal and vertical directions are ± 10 m and ± 30 m (100 ft) respectively. The contributors to this total system error are described below. For a conservative assessment, the flight geography is defined as ± 100 m horizontally and ± 30 m (100 ft) vertically from the planned path, illustrated as a green buffer in Figure 7.

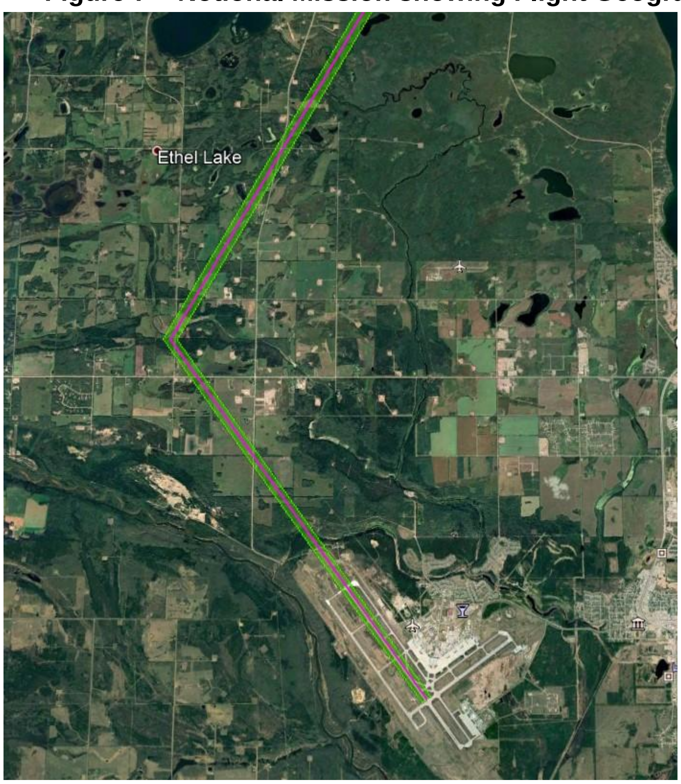
(i) **Path Definition Error**. Horizontal path definition error is expected to be negligible as the flight planning application uses a 3-dimensional projection based on the WGS-84 datum. Vertical path definition error is expected to be within ± 50 ft (15 m) as the flight planning software uses the latest available DTED data to set a vertical profile following the terrain along the planned route.

(ii) **Flight Technical Error**. Flight technical error is expected to be negligible as all path-following is performed by an autopilot and flight control system coupled to the navigation system, all located on board the aircraft. In addition, the flight planning software ensures that the planned path is within the center 50% of the performance envelope of the aircraft.

(iii) **Navigation Solution Accuracy**. The RPA navigation solution has maximum accuracies of ± 8 m horizontal and ± 10 m (33 ft) vertical.

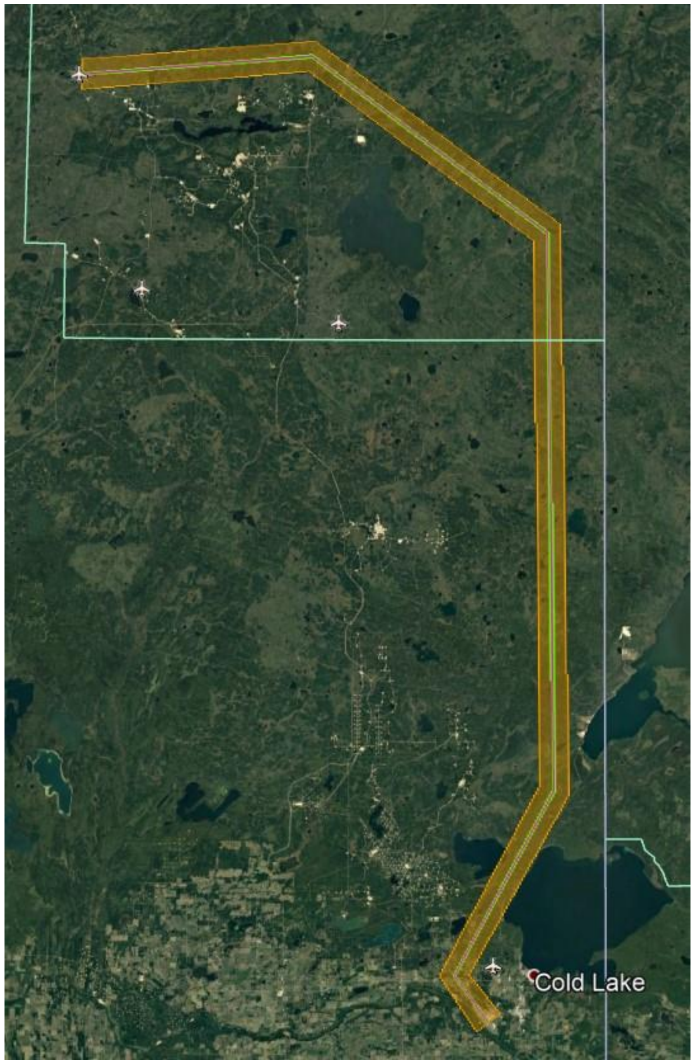
(iv) **Latencies**. Since all path-following is performed on board the aircraft, C2 link latency has no impact on the potential error sources. Latency within the navigation system, autopilot, and flight control system is negligible as these systems operate at 10 Hz or faster.

Figure 7 – Notional Mission showing Flight Geography



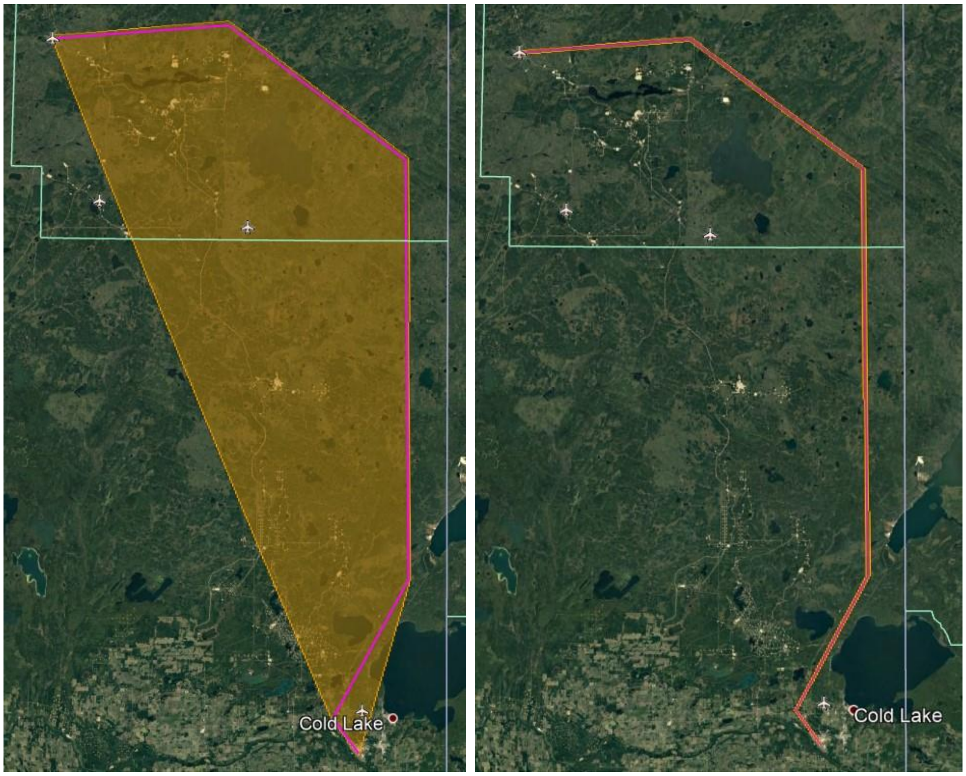
(a) **Contingency Volume.** Contingency procedures addressed in defining the Contingency Volume for this example are Loss of C2, Loss of GPS, and IMU or Engine Failure. The final contingency volume is illustrated in Figure 8, below.

Figure 8 – Notional Mission showing Contingency Volume



(i) **Loss of C2**. Typical RPAS provide an automatic RTH functionality upon loss of C2 link. These can vary between a simple, direct return to takeoff location up to full automatic route-following to multiple conditional "home" points. To illustrate the potential effects of these implementations on the contingency volume, Figure 9, below, shows a contingency volume based on a direct return to takeoff location (left) and a contingency volume based on automatic route-following along the flight plan to either the takeoff location or the intended destination (right). For the purposes of this example, the route-following implementation will be assumed.

Figure 9 – Notional Mission showing Loss of C2 Contingencies



(ii) **Loss of GPS**. Loss of GPS can be addressed in a variety of ways, depending on the design of the navigation system and the capabilities of the platform. For example, a navigation system that does not rely only on GPS for position may be able to continue as planned during such a loss, or a VTOL platform that relies fully on GPS may be able to conduct a safe landing at or near its present position in the event of GPS problems. For a fixed-wing platform that relies on GPS for navigation, as assumed in this example, a likely contingency procedure is to maintain course for a short period of time (based on IMU or air data) to attempt to regain GPS, followed by a controlled descent at minimum speed to ground impact. In such a case, the size of the contingency volume is driven by the worst-case potential horizontal drift for the time of flight following GPS failure, worst-case crosswind, and worst-case IMU/air data positional drift. As an example, consider maintaining course for 2 minutes to attempt regaining GPS, followed by a 500 ft/min descent (additional 36 seconds), with a worst-case crosswind of 25 kts and a worst-case IMU drift of 2 nm/hr. This results in a 1.17 nm horizontal contingency buffer around the flight geography (156 s = 0.0433 hr * 27 nm/hr = 1.17 nm).

(iii) **IMU or Engine Failure**. In the case of an IMU or engine failure, the flight control system automatically sets full vertical elevator and full left rudder to set the aircraft in a spin down to a low-energy controlled crash. This results in a 1000 ft/min descent, contained within a 200 m circle that drifts horizontally based on the wind conditions. With a worst-case crosswind drift of 25 kts, and a descent time of 18 seconds (300 ft at 1000 ft/min), the resulting horizontal contingency buffer is 0.25 nm. Since this value is smaller than the value calculated for the Loss of GPS scenario above, the final Contingency Volume shown in Figure 8 is based on the Loss of GPS scenario.

(3) **Application of Ground Risk**. The notional RPA with a 2.8m wingspan, 22kg MTOW, and 90km/h cruise speed (kinetic energy ~7kJ) falls into the 3 m / < 34 kJ category of RPA. As shown in Figure 10, below, the only population centres in proximity to the operation are Cold Lake and Grand Centre, AB (shown in green and blue, respectively). The cyan circles represent the location and VLOS coverage of the Visual Observers (large circles) and the GCS (small circle). Note that a second visual observer was added to cover the contingency volume over additional portion of Grand Centre (otherwise there would be a significant increase in GRC for the operation). Thus, the aircraft will remain within VLOS when transiting out of the Grand Centre area and is not planned to pass over Cold Lake itself. The Ground Risk Classes across the flight can therefore be determined as shown in Table 11, below.

Figure 10 – Notional Mission showing Population Centres

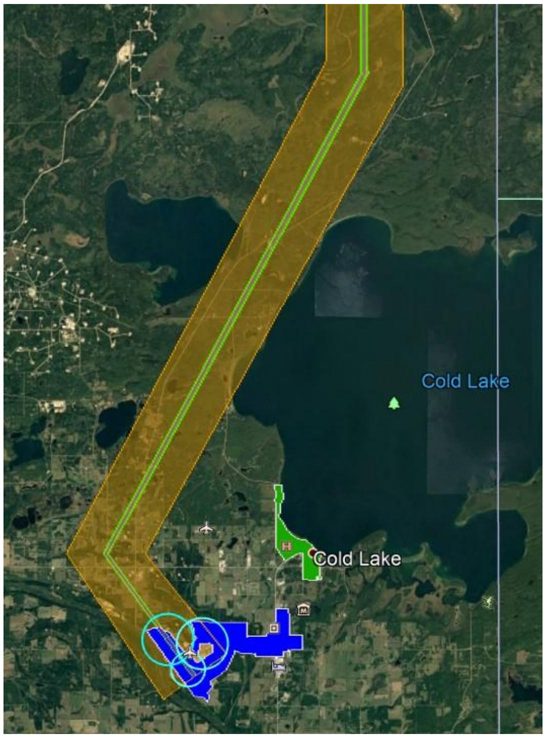


Table 11 – Example Application of Ground Risk

Flight Phase	Ground Risk Scenario	GRC
Takeoff & Initial Climb	VLOS within a population centre	5
Climb & Initial Cruise	VLOS outside of a population centre	3
Cruise & Initial Descent	BVLOS outside of a population centre	4
Approach & Landing	VLOS outside of a population centre	3

(4) **Application of Air Risk**. As illustrated in the flow chart in Figure 4, identifying the ARC of any given portion of the operation requires 5 pieces of information about that segment – whether the segment is in Atypical Airspace, the planned maximum altitude, whether the segment is in an Airport or Heliport environment, the class of airspace, and, if the segment is below 400 ft AGL, whether there is controlled airspace above starting at 1500 ft AGL or below. The segments of the proposed mission are illustrated in Table 12, below, and are based on creating a new segment whenever any one of the six factors changes. Also see Figure 11, below, for an illustration of the notional mission including overlay of the relevant airspaces (orange circles are Class E airspace, red circle is Class D airspace, green box is CYR204).

Table 12 – Example Application of Air Risk

Flight Segment	Atypical Airspace?	Altitude	Airspace Class	In Airport Environment?	Controlled airspace above?	ARC
Takeoff, Climb, & Transit out of Cold Lake Class D	No	< 400 ft AGL	D	Yes	N/A	d
From Cold Lake Class D to CYR204	No	< 400 ft AGL	G	No	Yes	c
Transit of CYR204	Yes	< 400 ft AGL	F	No	N/A	a
From CYR204 to passing Christina Lake	No	< 400 ft AGL	G	No	No	b
Passing Christina Lake	No	< 400 ft AGL	E	Yes	N/A	c
From Christina Lake to Conklin Class E	No	< 400 ft AGL	G	No	No	b
Approach & Landing	No	< 400 ft AGL	E	Yes	N/A	c

Figure 11 – Notional Mission showing Airspaces

(5) **SAIL Determination**. Based on Tables 11 and 12, the SAIL for the various mission segments can be determined as shown in Table 13, below.

Table 13 – Example SAIL Determination

<table>
<tr><th>Flight Phase (GRC)</th><th>Flight Segment (ARC)</th><th>GRC</th><th>ARC</th><th>SAIL</th></tr>
<tr><td>Takeoff & Initial Climb</td><td rowspan="3">Takeoff, Climb, & Transit out of Cold Lake Class D</td><td>5</td><td rowspan="3">d</td><td>VI</td></tr>
<tr><td>Climb & Initial Cruise</td><td>3</td><td>VI</td></tr>
<tr><td rowspan="7">Cruise & Initial Descent</td><td rowspan="7">4</td><td>VI</td></tr>
<tr><td>From Cold Lake Class D to CYR204</td><td>c</td><td>IV</td></tr>
<tr><td>Transit of CYR204</td><td>a</td><td>III</td></tr>
<tr><td>From CYR204 to passing Christina Lake</td><td>b</td><td>III</td></tr>
<tr><td>Passing Christina Lake</td><td>c</td><td>IV</td></tr>
<tr><td>From Christina Lake to Conklin Class E</td><td>b</td><td>III</td></tr>
<tr><td rowspan="2">Approach & Landing</td><td rowspan="2">c</td><td>IV</td></tr>
<tr><td>Approach & Landing</td><td>3</td><td>IV</td></tr>
</table>

(6) **Discussion**. The above example was selected intentionally to show a wide variation of GRC, ARC, and SAIL levels across a single mission. In such a case, the operator has a number of choices about how to address the resulting requirements.

(a) **SAIL**. As shown in Table 13, the SAIL for the notional mission varies from III in some segments to VI for the departure segment out of CYOD. One way of obtaining approval for such an operation would be to demonstrate performance at the required level to satisfy the requirements described in Section 10.0. Since the requirements for a SAIL VI operation are significantly more stringent than those of a SAIL III or IV, the operator of this mission may want to find a way to reduce the SAIL of the initial segments of the flight so that the complete operation may be conducted at SAIL IV.

(b) **ARC**. In this case, an examination of the GRC and ARC of the initial segments would show that the ARC-d airspace determination was the driver of this segment being SAIL VI, and the ARC-d determination was the result of operating in the Class D control zone of a DND aerodrome (as defined in Section 7.0). To lower this SAIL, the operator could choose to relocate the launch point of the operation to Bonnyville airport (CYBF), which is located outside of the Cold Lake Class D airspace and as a result would be ARC-c and SAIL IV.

(c) **GRC**. An additional benefit of relocating the launch point of the operation to CYBF is that this airport is not located within a population centre, so the associated GRC of this segment of the operation would be reduced from 5 to 3. This would also allow the operation to be conducted with one fewer visual observer since the added observer to cover the portion of population centre within the contingency volume would no longer be required to maintain the lower GRC.

(d) **DAA**. As the ARC of the notional mission varies across segments, so do the DAA requirements as described in Section 10.1. In this case, the most stringent requirement is for ARC-d as a result of the departure segment out of CYOD (due to the Class D CYOD control zone). Once the RPA is outside the CYOD control zone, the ARC reduces to ARC-c. To satisfy the DAA requirements for this segment, the operator could equip the aircraft with a DAA system meeting ARC-d minimum performance standards, or use additional visual observers to maintain VLOS until beyond the ARC-d airspace. If an ARC-d DAA system is used, then the performance standards for the remaining segments of the flight are also met; if visual observers are used for the ARC-d segment, then the operator will need to propose a DAA solution meeting ARC-c requirements. Alternatively, as described above, the operator could choose to relocate the departure point of the mission to CYBF, which would only require an ARC-c DAA solution. The remaining segments of the mission vary between ARC-c and ARC-a, allowing some flexibility in the proposed DAA solution (e.g., a system meeting ARC-c requirements is only necessary for the segments in ARC-c airspace).

(7) **Adjacent Area / Airspace Considerations**. As described in Section 8.0, the areas and airspaces adjacent to the proposed operation must also be considered as part of the RPAS ORA process. The notional mission above is operating primarily in remote locations and is not proposing to use a controlled ground area, so the primary item of concern for adjacent area / airspace risk is ARC-d airspace. Assuming the launch location of the mission was relocated to CYBF, the nearest ARC-d airspace is the Cold Lake Class E Terminal Control Area. The floor of this class E airspace is 700 ft AGL, which is 400 ft above the ceiling of the intended operation. At maximum climb rate, the aircraft used climbs at 1500 ft/min. Therefore it will take 16 seconds for the aircraft to reach ARC-d airspace in a worst case flyaway situation. At this point the operator has several choices for how to proceed:

(a) Increase the robustness of their operation to meet the ARC-d safety objectives. This would require a high robustness DAA system as well as increase the SAIL of the whole operation to VI.

(b) Prepare an emergency procedure for dealing with fly-away situations that takes less than 16 seconds to complete. The plan should include the time required to warn aircraft in the Class E airspace as well as provide time for them to react to the warning. Given the short time frame available, this is extremely unlikely, but would theoretically eliminate the Class E airspace from qualifying as adjacent airspace. In this case the operator would only need to meet the “Low Robustness” Containment Objectives as described in Section 9.4(2).

(c) Meet the “High Robustness” Containment Objectives as described in Section 9.3(2).

(8) **Sample Format for OSO Substantiation**. In order to simplify the process of substantiating and reviewing content related to each OSO, the following format is provided as a sample means of organizing such data. Note that the full details of the OSO substantiation can be provided in the table, or the substantiation can take the form of a reference to the specific content in another document (e.g., an operations manual or flight manual).

Note: For the purposes of this example, it is assumed that operational changes would be made such that the operation could be conducted at SAIL IV. Therefore, the below sample table provides the SAIL IV robustness levels. The appropriate robustness levels for the specific operation should be substituted in when using the sample format.

Table 14 – Sample Format for OSO Substantiation

OSO Number	OSO Description	SAIL	Substantiation of Robustness
		IV	
1	Ensure the Operator is Competent and/or proven	H	Substantiating data or reference to be provided.
2	RPAS is manufactured by competent and/or proven entity	M	Substantiating data or reference to be provided.
3	RPAS is maintained by competent and/or proven entity	M	Substantiating data or reference to be provided.
4	RPAS is developed to authority recognized design standards	L	Substantiating data or reference to be provided.

Table 14 – Sample Format for OSO Substantiation

OSO Number	OSO Description	SAIL	Substantiation of Robustness
		IV	
5	RPAS is designed considering system safety and reliability	M	Substantiating data or reference to be provided.
6	C2 link performance is appropriate for the operation	M	Substantiating data or reference to be provided.
7	Inspection of the RPAS (product inspection) to ensure consistency to the ConOps	M	Substantiating data or reference to be provided.
8, 11, 14, 21	Operational Procedures are defined, validated and adhered to	H	Substantiating data or reference to be provided.
9, 15, 22	Remote crew is trained and current and able to control the situation	M	Substantiating data or reference to be provided.
10	Safe recovery from technical issue	M	Substantiating data or reference to be provided.
12	The RPAS is designed to manage the deterioration of external systems supporting the RPAS operation.	M	Substantiating data or reference to be provided.
13	External Systems supporting the RPAS operations are adequate to the operation	H	Substantiating data or reference to be provided.
16	Multi-crew coordination	M	Substantiating data or reference to be provided.
17	Remote crew is fit to operate	M	Substantiating data or reference to be provided.
18	Automatic protection of the flight envelope from Human Error	M	Substantiating data or reference to be provided.
19	Safe recovery from human error	M	Substantiating data or reference to be provided.
20	A Human Factors evaluation has been performed and the HMI found appropriate for the operation	M	Substantiating data or reference to be provided.
23	Environmental conditions for safe operations defined, measurable and adhered to	M	Substantiating data or reference to be provided.

Table 14 – Sample Format for OSO Substantiation

OSO Number	OSO Description	SAIL	Substantiation of Robustness
		IV	
24	RPAS designed and qualified for adverse environmental conditions	H	Substantiating data or reference to be provided.

APPENDIX B — Detect and Avoid Considerations

1.0 DAA Detection Volume Calculation

(1) **General**. As described in Section 2.3, the detection volume describes the 3D volume within which traditional aircraft must be detected in order for the RPAS to avoid near mid-air collisions and, if possible, remain well clear. At any given point in time, the detection volume can be thought of as a “bubble” around the position of the RPA; however, applying this “bubble” during a mission in which the RPA is not stationary generates a 3D volume representing a buffer around the flight path of the RPA (see illustration in Figure 12, below). The DAA system is not necessarily required to maintain surveillance of the entire mission volume throughout the mission, but the “bubble” around the RPA must be under surveillance at all times. The detection volume “bubble” can be defined based on:

(a) the NMAC boundary dimensions,

(b) the expected maximum closing speed of traffic (horizontal and vertical),

(c) the expected time required for the sensor to establish a track,

(d) the expected accuracy of the sensor track,

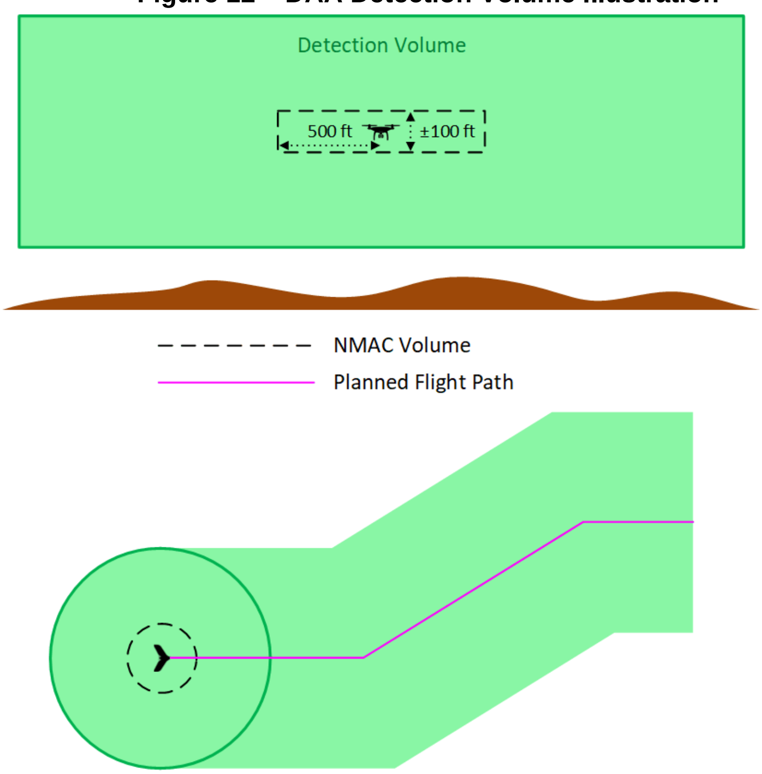
(e) the expected accuracy of the RPA position,

(f) the expected time required for the sensor operator or DAA system to detect and announce a conflict,

(g) the expected time required for the pilot or DAA system to initiate the avoidance maneuver, and

(h) the time required for the aircraft to complete the maneuver after the command is sent.

Figure 12 – DAA Detection Volume Illustration



(2) **Example**. The following example calculation uses notional values to represent RPA, DAA system, and intruder aircraft performance, based on a theoretical fixed-wing RPA, a ground-based radar sensor with a human operator, and a low-level class G operational environment. These values are not intended to be representative of any specific RPA or DAA sensor / system, and should be replaced with values appropriate for the RPA, DAA sensor / system, and operational environment under consideration when calculating the detection volume.

(a) **Horizontal Closing Rate**. The cruise speed of the notional RPA is 100 km/h, and the expected maximum closing speed of intruder aircraft is 340 km/h (based on a Cirrus SR22), for a worst-case closing rate of 440 km/h (122 m/s).

(b) **Vertical Closing Rate**. The notional RPA mission is assumed to be flown at a steady altitude, so only the maximum climb/descent rates of intruder aircraft is considered. Based on a Cirrus SR22, the worst-case climb rate is 1300 ft/min, and for the purposes of this example, the worst-case descent rate is also assumed to be 1300 ft/min.

(c) **Time-to-Track**. The maximum expected time required for the notional radar to establish a track once the intruder aircraft is within range is 6.25 seconds (the radar sweeps at 48 rpm and requires a maximum of 5 sweeps to establish a track). The track is updated once every 1.25 seconds thereafter.

(d) **Track Accuracy**. The accuracy of the notional radar is ±1° of bearing and 1% of the range scale in use. For a notional operation, range scales proposed for use are 6 nm, 12 nm, and 24 nm, leading to maximum possible errors of 776 m (1° of bearing error at 24 nm) and 445 m (1% of range error at 24 nm). These are perpendicular components, so the maximum total error in the worst-case direction is 895 m. The notional radar does not provide altitude data, so there is no consideration of vertical track accuracy.

(e) **RPA Position Accuracy**. Refer to Section 5.0(3) for discussion of RPA positioning accuracy; for the purposes of this example, it is assumed that the worst-case RPA position accuracy is ± 10 m laterally and ± 16 m (53 ft) vertically.

(f) **Conflict Assessment**. The maximum expected time required for the radar operator to detect an intruder and announce a conflict once a track is established on the display is 15 seconds.

(g) **Avoidance Initiation**. The maximum expected time required for the pilot to initiate an avoidance maneuver after notification from the radar operator is 10 seconds.

(h) **Maneuver Time**. The maximum expected time required for the aircraft to complete the avoidance maneuver is 24 seconds, consisting of up to 3 seconds for C2 link latency once the command is sent and 21 seconds for the aircraft to descend 350 ft (i.e., to 50 ft AGL) at the notional RPA's maximum descent rate of 1000 ft/min.

(i) **Detection Volume**. Based on the above assumptions, the detection volume must maintain a minimum buffer of 4.21 nm and ± 1353 ft from the current position of the RPA. See below for calculations.

(i) Horizontal Buffer:
Time Components: 6.25 s + 15 s + 10 s + 24 s = 55.25 s
Buffer based on closing rate: 55.25 s at 122 m/s closing rate = 6740 m
Worst-case intruder and RPA positional errors = 895 m + 10 m
NMAC buffer: 152 m (500 ft)
Final buffer: 7797 m = 4.21 nm

(ii) Vertical Buffer.
Time Components: 6.25 s + 15 s + 10 s + 24 s = 55.25 s
Buffer based on closing rate: 55.25 s at 1300 ft/min closing rate = 1200 ft
Worst-case RPA positional error = 16 m = 53 ft

NMAC buffer: 100 ft
Final buffer: 1353 ft

(3) **Discussion**. From the above example, there are several considerations with respect to the choice of RPA and DAA system that merit further discussion.

(a) Buffer size. It is apparent from the calculations that the time-based buffer driven by closing rate is the dominant contributor to the overall size of the “bubble” (approx. 88% of the horizontal buffer and 96% of the vertical). Since the intruder closing rates are not under the control of the RPA operator, the primary means for reducing the buffer required by the closing rate calculation is to reduce the time components in this calculation. This could be done by:

(i) selecting a sensor with a smaller time-to-track,

(ii) reducing the conflict assessment and/or avoidance initiation times through training and/or automation, and/or

(iii) reducing the maneuver time by selecting an RPA with lower C2 link latency and/or higher maneuvering performance.

(b) Ground vs. Airborne sensor. The example above was based on a ground-based sensor, which means that the full mission detection volume would ultimately extend 4.21 nm and ± 1353 ft from the RPA position at its furthest distance from the ground-based sensor. For example, if the ground-based sensor was located at the launch/recovery area, and the RPA was intended to fly up to 15 nm from the launch location, the ground based sensor would need to be capable of detecting intruder targets 19.21 nm from its location at altitudes 1353 ft above and below the RPA. An airborne sensor mounted on the RPA itself would only need to detect intruder aircraft at a distance of 4.21 nm; however, if nothing else in the example setup was adjusted, this would introduce further considerations in the detection volume calculation (e.g., latency of data transmission from the airborne sensor to the ground-based sensor operator).

2.0 DAA Detect Means of Compliance

(1) **Background.** This Section is intended to clarify the tests and validation activities that would be required when demonstrating the performance of a DAA sensor or sensors in support of a BVLOS operation using a technology-based DAA system. They are intended as a proposal of several means, but not necessarily the only means of showing that a DAA system can meet the DAA Detect performance objectives listed in Table 4.

(2) **General.** For both ARC-b and ARC-c airspace, the Detect function performance objective requires a calculation of the required detection volume and a substantiation of a detection rate within that volume. Refer to Appendix B Section 1.0 for an example of a DAA detection volume calculation. Note that, as for the top-level risk ratios, the detection rate requirement is applied equally to cooperative (transponder equipped) and non-cooperative (not transponder equipped) traffic (i.e., if the operational airspace may include non-cooperative traffic, the detection rate must be satisfied for non-cooperative traffic).
Each of the three MoCs below can be applied towards either a validation of Detect performance within a specific detection volume (e.g. demonstration of a detection volume for a specific operation), or a more generalized measurement of detect performance which can be used to identify the full spectrum of detection volumes that could be supported. For example, to validate a ground-based sensor for a linear inspection operation, it may not be necessary to collect data throughout the field of regard of the sensor; a central portion covering the detection volume required for the linear inspection may be sufficient. While a validation within a specific, operationally-driven detection volume may require less effort, it is expected that a generalized

validation approach would provide greater utility for any DAA solution that is intended to be used to support detection in more than one shape of detection volume.

The following considerations are applicable to each of the three MoCs described below:

(a) Source and accuracy of truth data: It should be self-evident that in order to quantify the performance of a system intended to detect aircraft, data recording the true intruder aircraft position and/or kinematics is required. This truth data should be obtained from a source or sources with known and verifiable accuracy (e.g., a TSO-certified GPS or other independently calibrated and validated data source), and should be recorded at a rate sufficient for comparison to the test sensor data and compatible with the overall DAA problem space (i.e., a truth data source that provides one data point per minute is not appropriate). The truth data source(s) should also provide all appropriate data for comparison to the data from the sensor(s) being tested. For example, if the sensor being tested provides position, altitude, and velocity for intruder aircraft then a truth data source that provides position only is not sufficient for a full characterization of the sensor.

(b) System operational limitations: If any operational limitations are being imposed on the use of the sensor system (e.g., only permitting daytime operations or operations in areas free of precipitation), the performance of the system need not be validated in conditions outside of this defined operational envelope.

(3) **MoC 1: Analysis with Flight Test Validation.** This MoC is a generalized version of the type used to develop and certify traffic collision avoidance systems (TCAS) and other similar systems. It requires significant engineering capability and effort but generates the most robust and transferable dataset. A Detect performance substantiation using this MoC is expected to include, at minimum:

(a) Sensor characterization analysis / modelling: The expected performance of the sensor is analyzed and modeled computationally. This analysis / modeling can be based on first principles (e.g., RF physics for RADAR) or based on developmental test data.

(b) Detect performance simulation: The computational model of the sensor system is exercised through extensive simulation of conflicting traffic orientations & maneuvers (e.g., through use of Monte Carlo simulation with validated encounter models - note that most available encounter models were developed in support of TCAS system development and validation and may not be representative of the intended operational airspace).

(c) Detect performance validation through flight test: The real-world sensor performance is validated through flight test of a specific set of test cases. These test cases should be selected based on the modeling and simulation results to generate data in the center and at the edges of the expected performance envelope. The test data is then used to compare against and validate the simulation data.

(d) If required, the validated computational model of the sensor system is then re-analyzed / simulated for the specific operational environment, including potential effects from terrain, obstructions, weather, etc.

(e) If any effects of significance are observed in the simulation of environmental effects, additional flight tests are conducted in a representative operational environment to validate the extent of these effects.

(4) **MoC 2: Large Dataset Sensor Validation.** This MoC is expected to require somewhat less engineering capability but potentially more time and/or cost than MoC 1 (depending on the sensor type). Essentially, this MoC replaces the simulation methodology of MoC 1 with an extensive data collection effort. A Detect performance substantiation using this MoC is expected to include, at minimum:

(a) Sensor characterization study: The performance envelope of the sensor is established through the collection of a statistically significant test data set, including sufficient variety of traffic types, orientations, and maneuvers as well as any environmental effects that need to be considered (time of day, weather, terrain, etc.). Depending on the sensor type, this will likely require collection of data from multiple locations across multiple days.

(b) If required, an analysis is developed showing the expected performance of the sensor system in the specific operational environment, including potential effects from terrain, obstructions, weather, etc. This analysis is created based on the data collected in step (a).

(c) A minimum set of flight tests is conducted to validate the expected boundaries of the sensor detection performance in the actual operational environment.

(5) **MoC 3: Operationally-Specific Testing.** This MoC is expected to require the least engineering effort of the three MoCs described here; however, the results are only applicable to a single operational environment (i.e., a single location). A Detect performance substantiation using this MoC is expected to include, at minimum:

(a) In-situ sensor characterization study: The performance envelope of the sensor is established through the collection of a representative, statistically significant test data set in the actual operational environment. This test data set covers the expected variety of traffic types, orientations, and maneuvers specific to the operational environment, as well as any local effects from terrain, obstructions, weather, etc. This MoC may require less data than MoC 2 since the variety of traffic and potential environmental effects that need to be considered are reduced; however, the results may not be generalizable to another operational environment without significant additional data collection.

3.0 Visual Observer DAA

(1) **Background.** In addition to the use of a technology-based DAA system, research shows that in low-risk airspace it is possible to safely perform BVLOS operation through the use of one or more Visual Observer(s) who are not required to have direct visual contact with the RPA but must know its location and be able to scan the surrounding airspace for conflicting traffic. When conducted in accordance with the operational restrictions and performance objectives described below, BVLOS operations of this type may be considered to address the DAA performance objectives described in Section 10.1.

(2) **Operation with Visual Observer DAA.** The use of visual observers as a DAA solution for low-risk airspace is subject to a set of requirements and limitations that have been determined to provide an acceptable level of safety. These requirements and limitations are derived from research conducted by regulatory authorities, with margins of safety added in some cases to accommodate the Canadian operational environment and risk tolerance. The requirements and limitations are described in the following four categories.

(3) **Operating Environment.** The operating environment for visual observer DAA operations must meet the following criteria:

(a) Airspace: ARC-b or ARC-c airspace as defined in Section 7.0.

(b) RPA operated at or below 400’ AGL.

(c) Distance from RPA to remote pilot and control station no greater than 4 nm.

(d) Distance from RPA to nearest visual observer no greater than 2 nm.

(e) Distance from RPA to C2 link ground antenna no greater than 50% of the maximum previously demonstrated distance using the same aircraft and C2 link configuration.

(f) Meteorological conditions:

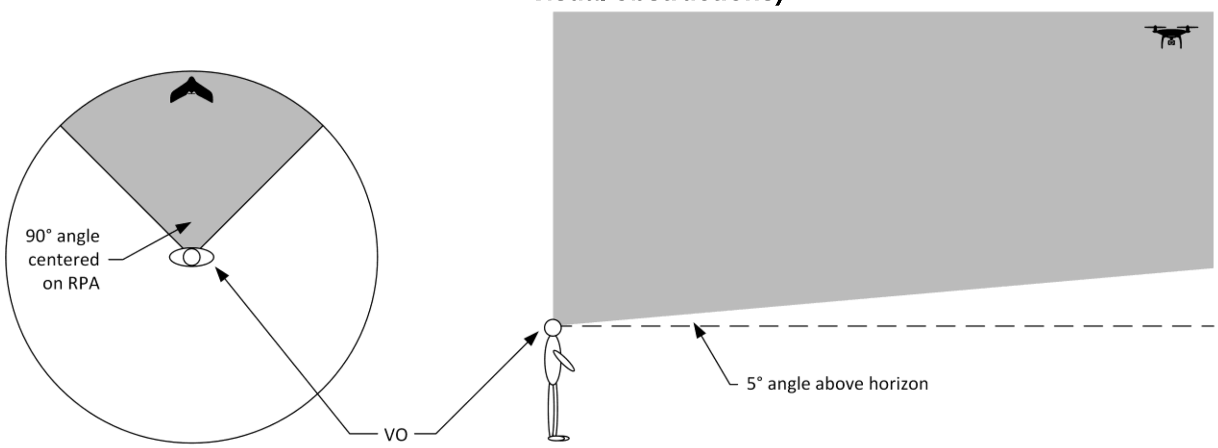
(i) visibility is not less than three miles at all visual observer location(s);

(ii) the cloud ceiling is not less than 1000 feet AGL.

(g) No visual obstructions more than 5 degrees of visual angle upwards from the horizon in the quadrant (90° of azimuth) centered on the RPA location.

Note: A simplified 'on-site' means to evaluate this requirement is for the visual observer to stretch out their arm, wrist flexed, palm facing forwards (i.e., looking at the backs of their fingers). The index finger is then placed along the horizon. If any obstructions are visible above the pinky finger then they are considered to be greater than 5 degrees above the horizon.

Figure 13 – Visual Observer must have a clear line of sight throughout the shaded area (no visual obstructions)



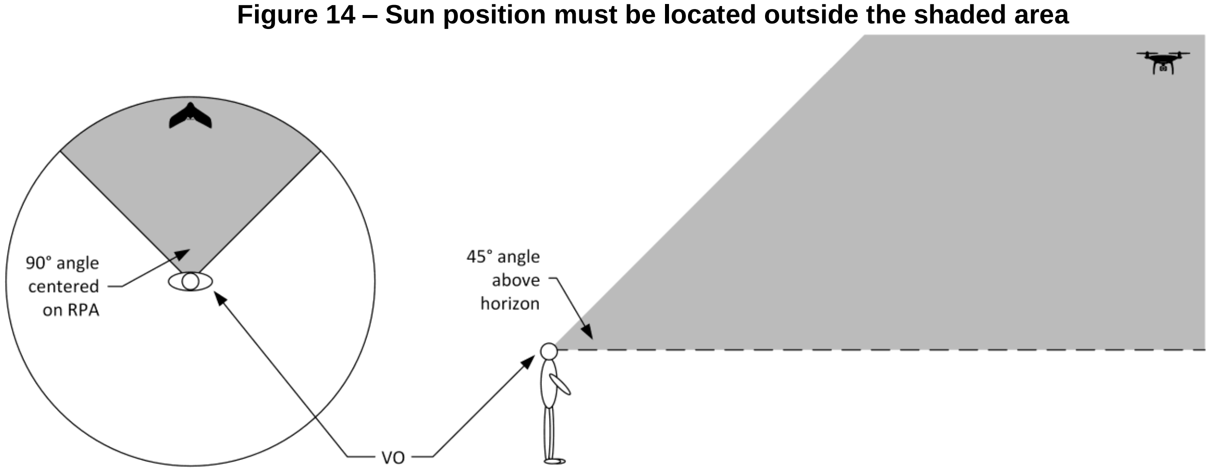
(h) Sun position is:

(i) Outside of the quadrant (90° of azimuth) centered on the RPA location; or

(ii) 45° or greater of elevation above the horizon; or

(iii) Below the horizon (i.e., night operations). Note: for night operations, the moon position must also meet conditions (a) and (b).

Figure 14 – Sun position must be located outside the shaded area



(i) Location of airspace observer(s) must be free of significant noise pollution (e.g., generators, farm equipment, trucks, etc).

(4) Equipment Requirements. The equipment used for a visual observer DAA operation must meet the following requirements:

(a) RPAS requirements:

(i) Compliant with CAR Standard 922.04.

(ii) Equipped with high intensity flashing anti-collision lighting that:

(A) is white in colour;

(B) for night operations, is visible through NVGs;

(C) flashes at a rate of not less than 40, nor more than 100, cycles per minute;

(D) is visible in all directions within 75° above and below the horizontal plane of the aircraft, except that there may be solid angles of obstructed visibility totalling not more than 0.5 steradians[7];

(E) has a minimum intensity sufficient to be visible to a minimum of 1 nm under operational conditions.

Note: A simplified 'on-site' means to evaluate this requirement is for the aircraft to be flown to a distance of 1 nm at the beginning of the mission and the visibility of the lighting confirmed. If the lighting is not visible at 1 nm under operational conditions of the day, the mission cannot be completed.

(iii) C2 link latency (from issuance of command to start of execution by the aircraft) no greater than 2 seconds.

(iv) C2 link must incorporate link strength / link quality monitoring and the link strength/quality must be maintained at or above 50% of maximum throughout the mission.

(b) Other equipment requirements:

(i) The operation must have access to an Aviation-band VHF radio with transmit functionality.

(ii) The remote pilot and the visual observer(s) must have a continuously active and reliable means of communication.

(5) Crew Qualifications. The crew conducting a visual observer DAA operation must have the following qualifications:

(a) General qualifications (applies to both PIC and visual observers):

(i) Advanced RPA Pilot Certificate.

(ii) ROC-A.

(iii) Completion of instructor-led TP15263 ground school.

(b) Additional PIC Qualifications:

(i) Minimum of 20 hrs of VLOS operation as an RPA pilot.

[7] The steradian is the SI unit of solid angle. One steradian is the solid angle subtended at the center of a unit sphere by a unit area on its surface. For a general sphere of radius r, any portion of its surface with area $A = r^2$ subtends one steradian at its center.

(ii) Minimum of 2 hrs “simulated” BVLOS operation where the RPA is not within sight of the pilot but is within sight of one or more visual observers.

(iii) Has completed the training specific to the make and model of the RPAS being used for the operation, and has been determined to be competent.

(c) Additional Visual Observer Qualifications:

(i) Minimum of 20 hrs of VLOS operation as a visual observer, including a minimum of 2 hrs where the visual observer communicates with a remotely-located pilot.

(ii) Has completed training on the means used to identify the location of the RPA, and has been determined to be competent using this means.

(6) Operational Procedures. Operational procedures for use in a visual observer DAA operation must meet the following:

(a) An airspace deconfliction procedure must be in place, including, at minimum:

(i) advisory position reporting to local air traffic (ongoing during operation, i.e. at regular intervals);

(ii) decision criteria for when an avoidance maneuver is required;

(iii) standardized avoidance maneuvers that allow the operation to give way to manned traffic, up to and including safely ditching the RPA if required;

(iv) standardized phraseology to be used in the communication between the remote pilot and the visual observer(s) – including, at minimum, phraseology for communicating:

(A) the position and orientation of RPA,

(B) the position and orientation of conflicting or potentially conflicting aircraft,

(C) the requirement to conduct an avoidance maneuver,

(D) the selection of the avoidance maneuver to be used (if more than one option is described under (iii) above),

(E) an ‘all clear’ state when the operational area is clear of conflicting traffic and the RPA may continue with the mission.

(b) SOPs must also address (note the below list is not exhaustive):

(i) Safe recovery of the RPA in case of:

(ii) C2 link loss / failure;

(iii) Pilot or visual observer incapacitation;

(iv) Loss of communication between the pilot and any visual observer; or

(v) Change of operational environment conditions that place the operation outside any of the conditions listed in Appendix B Section 3.0 Paragraph (3).

APPENDIX C — Operational Safety Objectives

(1) Robustness

As discussed in JARUS SORA Section 1.4.2, Robustness is achieved through a combination of integrity and assurance.

Integrity is a measure of the safety gain that is provided by a risk mitigation. When evaluating Integrity, the question to be asked is “How much will the proposed mitigation improve safety?”

Assurance is an assessment of the confidence that the risk mitigation will supply the claimed integrity. Assurance comes from an assessment of the proof that the safety gain has been achieved. When evaluating assurance, the question to be asked is, “What proof is available that the proposed mitigation will deliver the expected integrity?”

(2) OSO Categories

OSOs can be divided into seven categories. Within each category the OSOs assess specific aspects of the operation. Below is a description of the OSO categories, as well as generalized questions that an applicant should ask themselves when assessing the robustness of risk mitigations.

(c) Technical Issues with the RPAS (OSO #1, 2, 3, 4, 5, 6, 7)

How robust is the operation from a technical standpoint? Think about the technical ability of the crew, the technical quality of the RPAS, and the robustness of the C2 link.

(d) Operational Procedures (OSO # 8, 11, 14, 21)

What operational procedures does the applicant have in place? Assess the quality and completeness of the procedures. Have the procedures been practiced and been shown to work?

Highlight the fact that operational procedures are so important, they’re the only OSOs that require high robustness at SAIL III.

The following procedures must exist as a minimum:

- Flight planning,
- Pre and post-flight inspections,
- Procedures to evaluate environmental conditions before and during the mission (i.e. real-time evaluation),
- Procedures to cope with adverse operating conditions (e.g. what to do in case icing is encountered during the operation, when -the operation is not approved for icing conditions)
- Normal procedures,
- Contingency procedures (to cope with abnormal situations),
- Emergency procedures (to cope with emergency situations), and-
- Occurrence reporting procedures.

(e) Crew Training (OSO #9,15, 22)

What is the quality and completeness of crew training? Is it appropriate to the operation? How does the applicant verify training and ensure currency? Does the training include the entire crew (not just the PIC).

(f) Safe Design (OSO #10, 12)

Intended to complement the technical containment safety requirements (i.e. confidence that RPA will not exit the operational volume). Question to be asked is “If my RPAS does exit my operational volume, what is the risk of a fatality?”. The applicant should demonstrate how their system design minimizes this risk.

(g) Deterioration of External Systems (OSO #13)

If the applicant is relying on an external system for part of their operation, how has the applicant prepared for a deterioration of that system? Examples would be loss of GPS signal, loss of cell-phone network for C2 link, loss of NAV Canada coordination, etc.

(h) Human Error (OSO #16, 17, 18, 19, 20)

How has the applicant designed their operation to be tolerant to human error? Is the crew trained and do procedures include cross checks of critical items? Can the system recover from human errors? Does the applicant have procedures in place to control crew fatigue?

(i) Adverse Operating Conditions (OSO #23, 24)

Does the applicant have operational limits that respect the manufacturer declared operational limits of the RPAS? Does the RPAS have environmental qualifications that are appropriate for the intended operation?

(3) OSO Detailed Requirements

(a) Technical Issues with the RPAS

(i) OSO 1 – Ensure the operator is competent and/or proven.

(A) General Description and Comments:

The applicant is expected to demonstrate that the crew deployed to perform the operation has the knowledge, and skill required to perform the operation safely. Integrity for this OSO comes from the crew skill and accreditations and these much be consistent with the nature and level of risk for the intended operation. Assurance for this OSO comes from the method by which the applicant demonstrates crew proficiency ranging from an operator self-declaration to external operational proficiency checks (OPC) and recurrent training.

(B) SAIL Categories:

SAIL	I	II	III	IV	V	VI
Robustness	O	L	M	H	H	H

(ii) Integrity:

OSO 1 – Ensure the operator is competent and/or proven.		
Low	Medium	High
VLOS – Per Part IX Regs BVLOS – Advanced Pilot Certificate.	VLOS – Advanced Pilot Certificate BVLOS – Advanced Pilot Certificate plus evidence of BVLOS knowledge and training.	Advanced Pilot Certificate plus manned aviation knowledge and training requirements applicable to the operation.

(iii) Assurance:

OSO 1 – Ensure the operator is competent and/or proven.		
Low	Medium	High
Operator self declares competency and re-currency procedures.	Third Party (TC->Range or other party) reviews operator competency and re-currency procedures.	In addition to medium requirements, schedule and execute recurrent training supervised by a third party.

(ii) OSO 2 – RPAS Manufactured by competent and/or Proven Entity

(A) General Description and Comments:

This OSO is intended to evaluate the qualifications and competency of the RPAS manufacturer rather than the design of the RPAS itself. Robustness relates to the confidence that RPAS produced by the manufacturer will be of consistent quality, meet their technical specifications claimed by the manufacturer. Integrity is arrived by deliverables supplied by the manufacturer. Assurance is modulated by the conformity evidence supplied by the manufacturer, as well as the level of involvement by Transport Canada (or other third party) when evaluating the manufacturer.

(B) SAIL Categories:

SAIL	I	II	III	IV	V	VI
Robustness	O	O	L	M	H	H

(C) Integrity:

OSO 2 – RPAS Manufactured by competent and/or Proven Entity		
Low	Medium	High
Manufacturer with limited history but quality assurance program and standards in place.	Known manufacturer or modifier. Service history available. Industry certifications (ISO 9000, Safety Declarations, etc.)	Known manufacturer, extensive service history with good safety record. Industry certifications.

(D) Assurance:

OSO 2 – RPAS Manufactured by competent and/or Proven Entity		
Low	Medium	High
Manufacturer uses internal standards and procedures to control RPAS production and conformity.	Evidence of conformity is available from the manufacturer.	Evidence of conformity is reviewed by a third party. Conformity checked and maintained during operation.

(iii) OSO 3 - RPAS maintained by competent and/or proven entity

(A) General Description and Comments:

This OSO is intended to evaluate the means by which the RPAS is maintained in an airworthy state. Integrity is arrived at by examining the source of the maintenance procedures, the skills and qualifications of the maintenance crew and the quality of the maintenance program. Assurance is arrived at by examining the level of maintenance documentation available, and the training and re-currency required of the maintainers.

(B) SAIL Categories:

SAIL	I	II	III	IV	V	VI
Robustness	L	L	M	M	H	H

(C) Integrity:

OSO 3 - RPAS maintained by competent and/or proven entity		
Low	Medium	High
Operator has an internal maintenance program in place. Little or no contact with aircraft manufacturer.	Operator has an established maintenance program and maintenance procedures sourced from manufacturer recommendations.	Medium + external verification/review of maintenance program.

(D) Assurance:

OSO 3 - RPAS maintained by competent and/or proven entity		
Low	Medium	High
Minimal maintenance procedure documentation. Maintenance team training self-declarations.	Maintenance procedures validated, Maintenance Personnel undergoes initial training from manufacturer.	Maintenance team subject to recurrent training. Third party review of maintenance training syllabus.

(iv) OSO 4 - RPAS developed to authority recognized design standards.

(A) General Description and Comments:

This OSO is intended to evaluate that the RPAS is designed using standards that are appropriate for the operation, and that the means of compliance against those standards are adequate for the level of risk inherent to the operation. At all robustness levels, the applicant should evaluate that the design standards for the RPAS are appropriate for their intended CONOPS to determine integrity. Assurance is derived from the amount and type of evidence provided.

Note that the required robustness for this OSO at SAIL III has been increased from Optional to Low. This is to reflect the fact that at SAIL III, it is felt that the level of risk requires a minimum level of design rigour that is not Optional.

(B) SAIL Categories:

SAIL	I	II	III	IV	V	VI
Robustness	O	O	L	L	M	H

(C) Integrity:

OSO 4 - RPAS developed to authority recognized design standards		
Low	Medium	High
The RPAS is designed to standards that are appropriate for planned CONOPS.		

(D) Assurance:

OSO 4 - RPAS developed to authority recognized design standards		
Low	Medium	High
Manufacturer Self Declaration to appropriate design standards (i.e. Standard 922).	Manufacturer has selected appropriate industry standards and declares the RPAS compliant. There is evidence that the standards selected are appropriate for the CONOPS.	Medium plus compliance evidence has been reviewed by a competent third party.

(v) OSO 5 - RPAS is designed considering system safety and reliability

(A) General Description and Comments:

This OSO is intended to ensure that the RPAS has been designed with a level of system safety and reliability that is appropriate for the level of risk of the operation. When assessing Integrity, for all robustness levels, the safety objectives should be selected based on the kinetic energy of the aircraft (refer to Appendix E).

(B) SAIL Categories:

SAIL	I	II	III	IV	V	VI
Robustness	O	O	M	M	H	H

(C) Integrity:

<table>
<tr><th colspan="3">OSO 5 - RPAS is designed considering system safety and reliability</th></tr>
<tr><th>Low</th><th>Medium</th><th>High</th></tr>
<tr><td>N/A</td><td colspan="2">System Safety Assessment demonstrating compliance with the system safety objectives identified in Appendix E.

Note: Operational Limitations may be used to constrain the worst case criticality of failures that must be considered by the system safety assessment.</td></tr>
</table>

(D) Assurance:

OSO 5 - RPAS is designed considering system safety and reliability		
Low	Medium	High
N/A	Manufacturer declaration against the system safety objectives.	Accredited Manufacturer declaration or Third-Party validated declaration against the system safety objectives.

(vi) OSO 6 – C2 link performance is appropriate for the operation

(A) General Description and Comments:

This OSO is intended to examine the Command and Control (C2) link and verify that it is appropriate for the level of risk associated with the operation. Integrity is derived by the extent to which the link performance is monitored during the operation and on the type of band used (unlicensed vs licensed). Assurance is derived from who is declaring link appropriateness and on amount of evidence/experience with this link in this type of operation.

(B) SAIL Categories:

SAIL	I	II	III	IV	V	VI
Robustness	O	L	L	M	H	H

(C) Integrity:

OSO 6 - C3 link performance is appropriate for the operation		
Low	Medium	High
Unlicensed Band. RSSI can be monitored. System includes alerting functionality of low signal strength condition.	Low integrity criteria plus C2 link has been demonstrated to be appropriate (latency, error recovery, redundancy, availability, etc.) for the CONOPS. Evidence of demonstration available.	Medium integrity criteria plus C2 link uses a licensed Band and/or Quality of Service Agreements are place where appropriate.

(D) Assurance:

OSO 6 - C3 link performance is appropriate for the operation		
Low	Medium	High
Applicant self-declaration that the C2 link will perform adequately based on technical specifications from the manufacturer and an analysis performed that is specific to the operation. The analysis shall include link budget and site survey elements(EME/EMI etc.).	Low assurance criteria plus third party review of the link budget analysis specific to the operation.	Medium assurance criteria plus there has been a demonstration that C2 link operates appropriately and includes additional safety buffer to compensate for degradation that may be experienced during operation.

(vii) OSO 7 - Inspection of RPAS (product inspection) to ensure consistency to the CONOPS

(A) General Description and Comments:

This OSO is examining the pre-flight inspections of the RPAS prior to operation. Robustness for this safety objective is arrived at entirely through Assurance. All SAIL levels require some form of pre-flight inspection to determine that the RPAS is airworthy. Increasing assurance is arrived at by investigating the source of the pre-flight procedures as well as the crew training in the use of the pre-flight procedures.

(B) SAIL Categories:

SAIL	I	II	III	IV	V	VI
Robustness	L	L	M	M	H	H

(C) Integrity:

OSO 7 - Inspection of RPAS (product inspection) to ensure consistency to the CONOPS		
Low	Medium	High
Integrity level is achieved through assurance level.		

(D) Assurance:

OSO 7 - Inspection of RPAS (product inspection) to ensure consistency to the CONOPS		
Low	Medium	High
Pre-flight procedure is documented. Quality of the procedure and operational implementation is self-declared by the applicant.	Pre-flight procedure uses Manufacturer recommendation as a basis. A crew training syllabus is defined.	Pre-flight procedure and training syllabus as well as crew competency has been validated by a third party.

(viii) OSO 8, 11, 14, 21 – Operational Procedures

(A) General Description and Comments:

The Operational Procedures OSOs are each intended to examine a different aspect of the procedures associated with an operation. These are:

- OSO 8 – Ability to resolve technical issues
- OSO 14 – Ability to resolve Human Errors
- OSO 11 – Ability to manage the deterioration of external systems
- OSO 21 – Ability to manage Adverse Operating Conditions

It is expected that an operation will have the following procedures as a minimum:

- Flight planning (see note below),
- Pre and post-flight inspections,
- Procedures to evaluate environmental conditions before and during the mission (i.e. real-time evaluation),
- Procedures to cope with adverse operating conditions (e.g. what to do in case icing is encountered during the operation, when - the operation is not approved for icing conditions)
- Normal procedures,
- Contingency procedures (to cope with abnormal situations),
- Emergency procedures (to cope with emergency situations), and-
- Occurrence reporting procedures.

***Note**:* It is expected that the site survey process included in the flight planning procedure will address identifying and planning for locally-relevant features, including but not limited to:

- Local routes / features where VFR traffic would be expected (e.g., roads, rivers, railways, etc);
- Local areas commonly used for specific purposes that may not be marked on VFR Sectional charts (e.g., Flight Training Areas, Gliding Areas);
- Other airspace users that may affect the intended RPAS operation (e.g., Crop Dusting, Model Aircraft/Rocketry Clubs); and
- Aerodromes not registered in the CFS/WAS (e.g., “flying farmer” fields or water features typically used by floatplane traffic).

(B) SAIL Categories:

SAIL	I	II	III	IV	V	VI
Robustness	L	M	H	H	H	H

(C) Integrity:

OSO – 8, 11, 14, 21 Operational Procedures		
Low	Medium	High

Procedures are present.	Procedures are present, have been developed based on an adequate standard.	Procedures are present, simple, and easy to use by the operator. Ease of use is a judgement call made during Operational Proficiency Check or similar evaluation.

(D) Assurance:

OSO – 8, 11, 14, 21 Operational Procedures		
Low	Medium	High
Procedures have been written by the applicant. Emergency procedures have been tested.	Procedures have been reviewed, practiced and updated where required.	Procedures have been tested (third party validation) in throughout the flight envelope and found to function appropriately.

(ix) OSO 9, 15, 22 – Remote Crew Training

(A) General Description and Comments:

For all levels, the crew shall be trained in the following topics:

- Application of operational procedures (normal, contingency and emergency procedures, flight planning, pre-flight and post-flight inspections…)
- Communication
- RPA flight path management, automation
- Leadership, teamwork and self-management
- Problem solving and decision-making
- Situational awareness
- Workload management
- Coordination and handover
- CRM

The three OSOs related to Training are intended to each focus on a different aspect of crew training:

- OSO 9 – Technical Issues
- OSO 15 – Human Error
- OSO 22 – Environmental Conditions

Robustness is attained by reviewing the quality of the training syllabus, and the crew competency.

(B) SAIL Categories:

SAIL	I	II	III	IV	V	VI
Robustness	L	L	M	M	H	H

(C) Integrity:

OSO 9, 15, 22 – Remote Crew Training		
Low	Medium	High
Training shall cover everything listed above and be appropriate to the intended mission. Low medium or high rating comes from the assessed quality of the training.		

(D) Assurance:

OSO 9, 15, 22 – Remote Crew Training		
Low	Medium	High
Operator Self Declaration	Syllabus available and evidence that training is being performed.	Medium + Third party validation of syllabus and validation of crew competency.

(x) OSO 10 - Safe Recovery from Technical Issues

(A) General Description and Comments:

OSO 10 examines the ability of the RPAS to recover from a technical issue. The applicant should examine their system in search of probable failures, single points of failure, and any other technical issues that are expected to arise at least once during the operational life of the RPAS. Note that this failure assessment could be linked to the system safety assessment process conducted under OSO #5. Examples of technical issues would be engine/motor failure, C2 link failure, electrical generation failure, failure of "wear-out" items, etc. When considering probable failures, information from the manufacturer should be consulted as well as any technical issues that are induced by the specific operation planned by the applicant. The consequences of each technical issue should be assessed and either procedural or technical mitigations implemented where required to maintain safety.

For this OSO, Integrity is derived from the level of standards and practices used to develop the technical or procedural mitigations. Assurance is derived from how the mitigation has been demonstrated to be effective. This OSO is not intended to require the applicant to perform their own destructive testing, however, depending on the nature of the mitigation, it may be required for the applicant to conduct their own testing to reach Medium and High Robustness levels. This would be the case if it cannot be demonstrated that the manufacturer has performed representative testing. For example if a flight termination system has been installed to mitigate technical issues resulting in a fly-away, the applicant may be required to demonstrate the operation of this system if it cannot be shown that the manufacturer has not already conducted representative tests.

(B) SAIL Categories:

SAIL	I	II	III	IV	V	VI
Robustness	O	O	L	M	M	H

(C) Integrity:

<table>
<tr><th colspan="3">OSO 10 – Safe Recovery from Technical Issues</th></tr>
<tr><th>Low</th><th>Medium</th><th>High</th></tr>
<tr><td>Systems and procedures implemented to detect and recover from technical issues are developed to industry best practices.</td><td colspan="2">Systems and procedures implemented to detect and recover from technical issues are developed industry recognized standards.</td></tr>
</table>

(D) Assurance:

<table>
<tr><th colspan="3">OSO 10 – Safe Recovery from Technical Issues</th></tr>
<tr><th>Low</th><th>Medium</th><th>High</th></tr>
<tr><td>Operator declaration for procedural mitigations, Manufacturer/modifier declaration for technical solutions.</td><td>Demonstration of recovery using operational procedures.</td><td>Third party validation of the procedures and technical mitigations.</td></tr>
</table>

(xi) OSO 12 – The RPAS is designed to manage the deterioration of external systems supporting RPAS operation.

(A) General Description and Comments:

OSO 12 examines the ability of the RPAS to manage and recover from the deterioration of systems supporting the RPAS operation, but that are not directly under the control of the RPAS operator. Some examples of these systems are:

- satellite navigation systems (GNSS),
- C2 links that are operated by third parties (cell phone, internet, satellite, etc.),
- system power sources (GCS powered by the commercial power grid)
- DAA as a service

The applicant should assess their RPAS for its reliance on external systems and then assess how their RPAS would be affected by degradation and failures of those external systems. Integrity is arrived at by examining the reliability targets of the RPAS. Assurance comes from the manufacturer declaration that the reliability targets have been met. The reliability targets specified in Appendix E may be used to set the reliability level requirements for external systems.

(B) SAIL Categories:

SAIL	I	II	III	IV	V	VI
Robustness	O	O	M	M	H	H

(C) Integrity:

OSO 12 - The RPAS is designed to manage the deterioration of external systems supporting RPAS operation		
Low	Medium	High
N/A	System Safety Assessment demonstrating compliance with the system safety objectives identified in Appendix E. **Note:** Operational Limitations may be used to constrain the worst case criticality of failures that must be considered by the system safety assessment.	

(D) Assurance:

OSO 12 - The RPAS is designed to manage the deterioration of external systems supporting RPAS operation		
Low	Medium	High
N/A	Manufacturer declaration against the reliability targets.	Accredited Manufacturer declaration or Third-Party validated declaration against the reliability targets.

(xii) OSO 13 - External services supporting RPAS operations are adequate to the operation

(A) General Description and Comments:

OSO 13 examines that any external services used by the operation meet the reliability, integrity, and availability requirements of the operation. Some examples of external systems are:

- satellite navigation systems (GNSS),
- C2 links that are operated by third parties (cell phone, internet, satellite, etc.),
- system power sources (GCS powered by the commercial power grid)
- DAA as a service

The applicant should asses the effect of a failure of each external service on their operation and consider if the level of service provided is commensurate with the hazard created by such a failure. Integrity is arrived at by plans in place to deal with external service providers and the deterioration of their services. Assurance is arrived at by service level agreements with the providers and evidence showing that the service level provided is adequate for the operation.

(B) SAIL Categories:

SAIL	I	II	III	IV	V	VI
Robustness	L	L	M	H	H	H

(C) Integrity:

OSO 13 - External services supporting RPAS operations are adequate to the operation		
Low	Medium	High
No interaction with external service providers	Plan in place for dealing with external service providers.	Plan in place and procedures to mitigate deterioration of external services.

(D) Assurance:

OSO 13 - External services supporting RPAS operations are adequate to the operation		
Low	Medium	High
Self-declaration from the operator stating that the external services are adequate for the operation. No interfacing procedures developed. No service level agreements in place.	The operator has evidence to support that the service is adequate for the operation (i.e. Service-Level Agreement in place).	Third party review indicates that the operator’s evidence and the service level agreement are adequate for the operation.

(xiii) OSO 16 – Multi-Crew Coordination

(A) General Description and Comments:

OSO 16 is intended to examine the procedures and training that the RPAS crew uses to ensure a safe operation. Integrity is assessed by examining the procedures that are in place as well as the communication channels used by the crew. Increasing integrity is also arrived at by providing Crew Resource Management (CRM) training to the operational crew as well as redundant communication links as required. Assurance is arrived at by examining the level to which the procedures have been validated and any standards used in their development. Higher levels of assurance require that the crew procedures have been operationally tested and reviewed by third parties.

(B) SAIL Categories:

SAIL	I	II	III	IV	V	VI
Robustness	L	L	M	M	H	H

(C) Integrity:

OSO 16 – Multi-Crew Coordination		
Low	Medium	High
Procedures in place, but minimal review, and training.	Procedures have been reviewed, and practiced. Operators have minimal training in things like CRM.	Procedures in place, have been extensively practiced. Communication links include redundancy and failures are practiced.

(D) Assurance:

OSO 16 – Multi-Crew Coordination		
Low	Medium	High
Procedures developed by operator and not related to a recognized standard. Operator self declares checklists are adequate.	Procedures validated against recognized standards. Flight tests have shown procedures to be adequate.	Procedures/flight tests/simulations have been validated by competent third party. Flight Tests and simulations have shown that the procedures are conservative.

(xiv) OSO 17 – Remote Crew is Fit to Operate

(A) General Description and Comments:

This OSO is intended to evaluate how the operator certifies that the RPAS crew is fit to operate. Evaluation should include the effects of Illness, Stress, Fatigue, Alcohol and other substances, and Emotional well-being. Integrity is arrived at by the level of procedures in place to ensure crew fitness. Assurance is arrived at by the level to which the operator documents aspects of crew fitness, such as policies to enforce rest times and duty-day length.

(B) SAIL Categories:

SAIL	I	II	III	IV	V	VI
Robustness	L	L	M	M	H	H

(C) Integrity:

OSO 17 – Remote Crew is Fit to Operate		
Low	Medium	High
Applicant has self-declared policies on crew declaring themselves fit (including rules related to drugs and alcohol).	Rest times are declared and adequate for the operation.	Fatigue Risk Management program is in place.

(D) Assurance:

OSO 17 – Remote Crew is Fit to Operate		
Low	Medium	High
Self-Declaration of remote crew.	Rest times documented and enforced. Crew operation is logged.	Third party reviews crew logs and fitness, validates fatigue management program.

(xv) OSO 18 – Automatic Protection of the flight envelope from Human Error

(A) General Description and Comments:

This OSO is intended to be investigated only if the RPAS in use includes a flight envelope protection system. It is not intended to mandate the installation of an Automatic Flight Envelop protection system. Flight Envelope Protection is defined as any system that limits or interrupts a pilot command in order to maintain operation of the RPAS within its flight envelope. When available the flight protection system should be evaluated as to its capabilities to correct pilot error (Integrity) and the standards uses to develop the system (Assurance).

(B) SAIL Categories:

SAIL	I	II	III	IV	V	VI
Robustness	O	O	L	M	H	H

(C) Integrity:

OSO 18 – Automatic Protection of the flight envelope from Human Error		
Low	Medium	High
The RPAS flight control system incorporates automatic protection of the flight envelope to prevent the remote pilot from making any single input under normal operating conditions that would cause the UA to exceed its flight envelope or prevent it from recovering in a timely fashion.	The RPAS flight control system incorporates automatic protection of the flight envelope to ensure the UA remains within the flight envelope or ensures a timely recovery to the designed operational flight envelope following remote pilot error(s).	

(D) Assurance:

OSO 18 – Automatic Protection of the flight envelope from Human Error		
Low	Medium	High
Flight envelope protection system is COTS, or developed without following specific standards.	Flight Envelope protection has been developed following recognized industry standards and means of compliance that are acceptable to TC.	Medium plus compliance evidence is validated by a third party.

(xvi) OSO 19 – Safe Recovery from Human Error,

(A) General Description and Comments:

Applicants should show both procedural protection (normal checklist) and recovery (emergency checklist) from human error as well as technical solutions (warnings/alerts) to prevent human error where applicable. Integrity is arrived at by review of the procedures and checklists in place to determine if they use industry best practices or standards in their development. Assurance is arrived at by examining the validation of the means to recover from human error.

(B) SAIL Categories:

SAIL	I	II	III	IV	V	VI
Robustness	O	O	L	M	M	H

(C) Integrity:

OSO 19 – Safe Recovery from Human Error		
Low	Medium	High
Systems to detect/recover from human errors are developed to industry best practices.	Developed to industry recognized standards.	

(D) Assurance:

OSO 19 – Safe Recovery from Human Error		
Low	Medium	High
Procedures and Checklist have not been validated and technical solutions are developed to industry best practices.	Procedures and checklists are validated and technical solutions are developed to recognized industry standard.	Procedures and checklists are validated to industry standard and tested to ensure adequacy (Operational Proficiency Check from independent reviewer)

(xvii) OSO 20 – A Human Factors evaluation has been performed and the HMI found appropriate for the mission

(A) General Description and Comments:

This OSO is intended to evaluate the level to which the operation has been designed with Human Factors in mind. As SAIL increases, the criticality of the Human Machine Interface to the safety of the operation also increases. For all robustness levels, integrity is attained by a review of the RPAS control interfaces to ensure that they follow human factors best practices. Assurance is attained by the level to which the review has been documented and the supporting evidence provided.

(B) SAIL Categories:

SAIL	I	II	III	IV	V	VI
Robustness	O	L	L	M	M	H

(C) Integrity:

OSO 20 – A Human Factors evaluation has been performed and the HMI found appropriate for the mission		
Low	Medium	High
The RPAS information and control interfaces are clearly and succinctly presented and do not confuse, cause unreasonable fatigue, or contribute to remote crew error that could adversely affect the safety of the operation.		

(D) Assurance:

OSO 20 – A Human Factors evaluation has been performed and the HMI found appropriate for the mission		
Low	Medium	High
Applicant self-evaluation of system HFE.	The HMI has been validated in an environment that is representative of the real-world and the user interface has been shown to be adequate.	Medium + Third party validation of the HFE that is incorporated into the RPA control system.

(xviii) OSO 23 – Environmental conditions for safe operations defined, measurable and adhered to.

(A) General Description and Comments:

This OSO is intended to evaluate the how the operator plans to ensure that the operation remains within the environmental limitations of the RPAS system. Environmental limitations need to be tailored to the operation and the systems proposed for use (i.e. a visual DAA system may require VFR visibility limits). It is expected that the inputs to this OSO are the outputs from OSO 24. Integrity for this OSO is achieved through assurance. Assurance is derived from the examination of the means to which the operation is limited to appropriate environmental conditions.

(B) SAIL Categories:

SAIL	I	II	III	IV	V	VI
Robustness	L	L	M	M	H	H

(C) Integrity:

OSO 23 – Environmental conditions for safe operations defined, measurable and adhered to.		
Low	Medium	High
Integrity is achieved through assurance.		

(D) Assurance:

OSO 23 – Environmental conditions for safe operations defined, measurable and adhered to.		
Low	Medium	High
Operating Procedures with respect to environmental conditions are written by the operator and a self-declaration is made that they are adequate.	Procedures are written by operator using a recognized standard. Validation that the limits are less than or equal to the manufacturer limits has been done. Evidence that procedures are adequate is available. Training Syllabus is available	Medium + flight testing has been performed to show that the system can perform when operated within the environmental limitations. Procedures have been validated by a third party.

(xix) OSO 24 – RPAS Designed and qualified for Adverse Operating Conditions

(A) General Description and Comments:

This OSO is intended to examine the RPAS specifically to determine its qualification for adverse operating conditions. It is expected that the RPAS environmental qualifications will be supplied by the RPAS Manufacturer. It is the responsibility of the operator to show that their specific operation is within the qualification of the RPAS.

(B) SAIL Categories:

SAIL	I	II	III	IV	V	VI
Robustness	O	O	M	H	H	H

(C) Integrity:

OSO 24 – RPAS Designed and qualified for Adverse Operating Conditions		
Low	Medium	High
N/A	Manufacturer self-declaration that environmental qualification has been done with minimal supporting evidence (DDP).	Manufacturer declaration with complete supporting evidence (test reports, TSO, etc.).

(D) Assurance:

OSO 24 – RPAS Designed and qualified for Adverse Operating Conditions		
Low	Medium	High
N/A	Applicant provides all supporting evidence.	Applicant provides some sort of evidence that a third party has approved their claims (Delegate, Cert Authority, equivalent).

APPENDIX D — Reserved

Reserved.

APPENDIX E – RPAS Safety and Reliability Targets

(1) **General**. This appendix sets out the quantitative, probability-based reliability targets for RPAS that must be met when required by an Operational Safety Objective or other performance objective. The reliability targets are scaled based on the kinetic energy of the RPAS as illustrated in Table 15, below.

(2) **Guidance Regarding System Safety Assessment**. For additional guidance on System Safety Assessment processes and practices, refer to Transport Canada AC 922-001, JARUS AMC.RPAS 1309, FAA AC 23-1309E, and SAE ARP 4754A and ARP 4761.

(3) **Guidance Regarding Fatalities and Injuries**. The definitions of the failure categories below use the terms fatality and severe injury when considering catastrophic and hazardous failure cases. Clearly, given that the RPAS addressed by this ORA do not include human occupants, the fatalities and injuries referenced here refer to either people on the ground or aboard other aircraft. When assigning a criticality level to a specific failure, the manufacturer of the RPAS will have to refer to their notional CONOPS for the aircraft. For instance, a failure resulting in an immediate uncontrolled crash may be considered catastrophic for an RPAS operating over a gathering of people, but might only be considered Major or Hazardous for an RPAS operating over a controlled ground area. These decisions regarding failure classification made by the manufacturer during the design stage are expected to result in operational limitations that will be passed onto the operator.

Table 15 – RPAS Reliability Targets

Criticality Classification	Definition applied to RPAS	Safety Objective	Reliability Target by Kinetic Energy, Probability of Failure per Flight Hour		
			< 700 J	< 34 kJ	< 1084 kJ
Catastrophic	Failure conditions that could result in one or more fatalities.	Extremely Improbable	$P(x) < 10^{-4}$	$P(x) < 10^{-5}$	$P(x) < 10^{-6}$
Hazardous	Failure conditions that would reduce the capability of the RPAS or the ability of the pilot to cope with adverse operating conditions to the extent that there would be the following: i. Loss of the RPA where it can be reasonably expected that a fatality will not occur, though people on the ground will sustain severe injuries, or ii. A large reduction in safety margins or functional capabilities, or iii. High workload such that the pilot cannot be relied upon to perform their tasks accurately or completely.	Extremely Remote	$P(x) < 10^{-3}$	$P(x) < 10^{-4}$	$P(x) < 10^{-5}$
Major	Failure conditions that would reduce the capability of the RPAS or the ability of the pilot to cope with adverse operating conditions to the extent that there would be a significant reduction in safety margins, functional capabilities or separation assurance. People on the ground may not sustain severe injuries. In addition, the failure condition has a significant increase in pilot workload or impairs remote pilot efficiency.	Remote	$P(x) < 10^{-2}$	$P(x) < 10^{-3}$	$P(x) < 10^{-4}$
Minor	Failure conditions that would not significantly reduce RPAS safety and that involve crew actions that are within their capabilities. Minor failure conditions may include a slight reduction in safety margins or functional capabilities, a slight increase in pilot workload, such as flight plan changes.	Probable	$P(x) < 10^{-2}$	$P(x) < 10^{-2}$	$P(x) < 10^{-3}$
No Effect in safety	Failure conditions that would have no effect on safety. For example, failure conditions that would not affect the operational capability of the RPAS or increase the pilot workload.	N/A	N/A	N/A	N/A