Transport Canada Transports Canada

# Advisory Circular

**Subject:** **Remotely Piloted Aircraft Systems Safety Assurance**

| | | | |
|---|---|---|---|
| Issuing Office: | Civil Aviation, Remotely Piloted Aircraft Systems Task Force | Document No.: | AC 922-001 |
| File Classification No.: | Z 5000-32 | Issue No.: | 02 |
| RDIMS No.: | 13518324-V26 | Effective Date: | 2025-04-01 |

## Table of contents


**1.0 Introduction ..... 3**
1.1 Purpose ..... 3
1.2 Applicability ..... 3
1.2 Description of changes ..... 4
**2.0 References and requirements ..... 5**
2.1 Reference documents ..... 5
2.2 Cancelled documents ..... 5
2.3 Definitions and abbreviations ..... 5
**3.0 Background ..... 7**
**4.0 Methods for demonstrating compliance ..... 9**
4.1 General ..... 9
4.2 922.04 Operations in controlled airspace ..... 10
4.3 922.05 Operations near people ..... 11
4.4 922.06 Operations over people ..... 14
4.5 922.07 Safety and Reliability ..... 16
4.6 922.08 Containment ..... 18
4.7 922.09 Command and Control Link Reliability and Lost Link Behaviour ..... 20
4.8 922.10 Detect, Alert and Avoid Systems ..... 21
4.9 922.11 Control Station Design ..... 23
4.10 922.12 Demonstrated Environmental Envelope ..... 25
4.11 Classification of injury severity ..... 27
**5.0 RPAS design considerations ..... 28**
5.1 General ..... 28
5.2 System design and description ..... 28
5.3 Safety assurance requirements ..... 28
5.4 RPAS design characteristics ..... 29
5.5 Human Factors and Usability ..... 39
5.6 Configuration Management and Reliability Tracking ..... 40
5.7 Manufacturing ..... 41
5.8 Aircraft serviceability ..... 41


Canada

5.9 Payloads ..... 41
5.10 Command and control data link ..... 42
5.11 Operating limitations ..... 44
5.12 RPAS Integration ..... 45
**6.0 Modifications ..... 46**
**7.0 Operating Instructions and Limitations ..... 47**
**8.0 RPAS Configuration Management ..... 47**
**9.0 RPAS Declarant Obligations ..... 48**
**10.0 Information management ..... 51**
**11.0 Document history ..... 51**
**12.0 Contact office ..... 51**
**Appendix A – Recognized industry consensus standards ..... 52**
**Appendix B – System safety assessment ..... 54**
**1.0 Scope ..... 54**
**2.0 Acceptable methods ..... 54**
**3.0 Classification of failure conditions (severity) ..... 54**
**4.0 Safety objectives ..... 55**
**5.0 Development process ..... 56**
**Appendix C – Severe injury test methodology ..... 58**
**1.0 Discussion ..... 58**
1.1 Intent of tests ..... 58
1.2 Operating environment ..... 58
1.3 Standardized test procedures—Reason and practicalities ..... 58
1.4 Acknowledgement ..... 58
**2.0 References ..... 59**
**3.0 Standardized test procedures—Relationship to design ..... 60**
**4.0 Probable impact scenario development ..... 61**
**5.0 Test conditions ..... 61**
5.1 General ..... 61
5.2 Determination of critical orientation ..... 61
5.3 Impact to ATD ..... 62
**6.0 Test articles ..... 65**
**7.0 Test setup and test preparation ..... 65**
7.2 Test facilities ..... 66
7.3 Anthropomorphic test devices ..... 67
7.4 Instrumentation ..... 67
**8.0 Hazards ..... 69**
**9.0 Test failures vs. retest. ..... 69**

**10.0 Test reporting ..... 70**
**11.0 Data requirements ..... 70**
**12.0 Data analysis ..... 70**
**13.0 Test documentation ..... 73**
**14.0 Conclusions ..... 74**
**Appendix D – Considerations for the RPAS operating manual ..... 76**
**1.0 RPAS Operating Manual ..... 76**
1.1 General ..... 76
1.2 Use of Industry Standards ..... 76

**List of figures**

Figure 1 – Operations near people safety assessment compliance flowchart ..... 14
Figure 2– Operations over people safety assessment compliance flowchart ..... 16
Figure 3 – Bedford pilot workload rating scale ..... 26
Figure C-1 – Vertical drop test configuration ..... 64
Figure C-2 – Frontal head test configuration ..... 64
Figure C-3 – Head critical impact direction test configuration ..... 64
Figure C-4 – Head side impact test configuration ..... 65
Figure C-5 – ATD test seat setup ..... 67

# 1.0 Introduction

(1) This Advisory Circular (AC) provides information and guidance describing considerations relevant to assisting the public in complying with the regulations and standards. This AC 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 making Declarations and Pre-Validated Declarations (PVD) to the Minister for remotely piloted aircraft systems (RPAS) intended for Advanced Operations (ref CAR Part IX Div V) and Level 1 Complex Operations (ref CAR Part IX Div VI) in accordance with the requirements of Part IX of the *Canadian Aviation Regulations* (CARs). Furthermore, this AC provides guidance to manufacturers on how to comply with the documentation requirements in Part IX of the CARs associated with making a declaration, including the expected content of applicable operating manuals and maintenance programs.

(2) RPAS manufacturers are accountable to perform the necessary tests, evaluations, and/or assessments and record the results in a form that can be inspected by the Minister on demand. This AC outlines the safety assurance process to guide RPAS manufacturers with developing the necessary evidence to substantiate their declaration. A declaration is therefore the statement by

the manufacturer that their system meets the applicable safety assurance requirements and is fit for the intended Advanced or Complex Operations when operated and maintained in accordance with the manufacturer's instructions.

(3) This AC focuses on the contents of CAR Standard 922 and acceptable Means of Compliance (MoC) to that standard. It does not go into the details of the Declaration process, or the documentation needed to support a PVD application. For details about the Declaration and PVD processes, refer to AC 901-001 - RPAS Safety Assurance Declaration and PVD Processes.

### 1.2 Applicability

(1) This document applies to manufacturers of RPAS intended for Advanced Operations as described by CAR 901.62 and Level 1 Complex Operations described by CAR 901.97 as described in for which a declaration is required by Division V – Advanced Operations – in Part IX of the CARs.

(2) This AC provides guidance on the technical aspects and recommended means of compliance to CAR Standard 922. For guidance on the Declaration and Pre-Validated Declaration processes refer to AC 901-001.

(3) Table 1 provides a cross-reference between the regulatory requirements and this advisory material.

**Table 1 - Requirement/Guidance Cross-Reference**

| CAR Provision | AC Section |
|---|---|
| 901.194(1) | 4.0 |
| 901.194(2) | 4.0(5) |
| 901.194(4) | 4.0(7) |
| 901.195 | 4.0(8) |
| 901.197 | 4.0(10) |
| 901.200 | 5.0 |
| 901.200(c)(v) | 5.4(5)(a) |
| 901.200(c)(vi) | 5.4(5)(b) |
| 901.200(c)(vii) | 5.4(6) |
| 901.201 | 4.0(9) |
| Standard 922.04 | 7.1 |
| Standard 922.05 | 7.2 |
| Standard 922.06 | 7.3 |
| Standard 922.07 | 7.4 |

| | |
|---|---|
| Standard 922.08 | 7.5 |
| Standard 922.09 | 7.6 |
| Standard 922.10 | 7.7 |
| Standard 922.11 | 7.8 |
| Standard 922.12 | 7.9 |

### 1.2 Description of changes

(1) This document, formerly AC922-001 with an effective date of 2021-11-02 has been updated to cover the changes to Standard 922 that support VLOS operation of Medium Remotely Piloted Aircraft Systems (mRPAS), as well as BVLOS operation of Small Remotely Piloted Aircraft Systems (sRPAS) and mRPAS.

## 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 Systems Safety Assurance; and

(c) AC901-001 – Advisory Circular on the Declaration and Pre-Validated Declaration processes.

### 2.2 Cancelled documents

(2) Not applicable.

### 2.3 Definitions and abbreviations

**Note:** The definitions provided below are strictly for the purposes related to RPAS Safety Assurance 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 RPAS Safety Assurance.

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

(a) **Abbreviated Injury Scale (AIS)**: an anatomically-based, consensus-derived, global severity scoring system that classifies each injury by body region according to its relative importance on a 6 point ordinal scale. AIS is the basis for the Injury Severity Score (ISS) calculation of the multiply injured patient.

(b) **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.

(c) **Operator**: A person, group of persons, or organization which has possession of the RPAS as owner(s), lessee or otherwise and conducts operations of an RPAS under the CAR, Part IX.

(d) **Operational Volume:** means the area composed of the flight geography, contingency volume, and ground risk buffer.

(e) **Flight Geography:** means the area within which a remotely piloted aircraft is intended to fly for a specific operation.

(f) **Contingency Volume:** means the area immediately surrounding the flight geography within which contingency procedures are intended to be used to return a remotely piloted aircraft to the flight geography or safely terminate the flight.

(g) **Ground Risk Buffer:** means the area immediately surrounding the contingency volume that, when measured horizontally from the perimeter of the contingency volume, is at least equal to the planned maximum altitude of the remotely piloted aircraft for the flight.

(h) **Owner:** the person or entity who holds a valid RPAS Certification of Registration and has legal custody and control of the RPAS.

(i) **RPAS 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 (herein referred to as “manufacturer”).

(j) **Applicant:** The person or entity who is seeking to make a Declaration or apply for a Pre-Validated Declaration for a given section of CAR Standard 922. In this document Applicant is generally used to refer to individuals or entities before they submit a safety assurance declaration to Transport Canada. Once a safety assurance declaration is made, the Applicant is referred to as the RPAS Declarant.

(k) **RPAS Declarant**: The person or entity that is taking responsibility for, and making a declaration that, a specified RPAS meets a given section of CAR Standard 922.

(l) **Mandatory Action:** The inspection, repair or modification of a remotely piloted aircraft system that is necessary to prevent an unsafe or potentially unsafe condition. Mandatory actions are generally specified by the RPAS Declarant in response to a Service Difficulty Report. Refer to AC 9XX-TBD on PVD and Declarations for more information on Mandatory Actions.

(m) **Small Remotely Piloted Aircraft (sRPA, sRPAS):** is a remotely piloted aircraft that has an operating weight of at least 250g but not more than 25kg.

(n) **Medium Remotely Piloted Aircraft (mRPA, mRPAS):** is a remotely piloted aircraft that has an operating weight of more than 25kg, but not more than 150kg.

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

(a) **AAAM**: Association for the Advancement of Automotive Medicine;

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

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

(d) **AIS**: Abbreviated Injury Scale;

(e) **ASSURE**: Alliance for System Safety of UAS Through Research Excellence;

(f) **ATD**: Anthropomorphic Test Device;

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

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

(i) **C2SP**: C2 Link Service Providers

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

(k) **CE**: Conformité européene;

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

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

(n) **CS**: Control Station;

(o) **EM**: Electromagnetic;

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

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

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

(s) **FDAL**: Functional Design Assurance Level

(t) **FMEA**: Failure Mode and Effect Analysis

(u) **FMVSS**: Federal Motor Vehicle Safety Standards;

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

(w) **HIC**: Head Injury Criteria;

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

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

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

(aa) **PVD**: Pre-Validated Declaration

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

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

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

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

(ff) **mRPA**: medium Remotely Piloted Aircraft

(gg) **SSA**: System Safety Assessment

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

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

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

## 3.0 Background

(1) The goal of Canadian Aviation Regulation (CAR) Standard 922 *RPAS Safety Assurance* is to encourage the spirit of innovation while striking a balance between the safe use of RPAS in the national airspace, design requirements, and oversight of the industry. To this end, operational categories have been defined with specific requirements associated with the RPAS design, construction, and reliability.

(2) Standard 922 contains performance-based requirements that are intended to support the safe operation of RPAS in operations ranging from short range VLOS with sRPAS to BVLOS operations using mRPAS. Depending on the intended CONOPS of the RPAS various sections of

standard 922 may be applicable. When required, a declaration, or a pre-validated declaration will have to be received prior to the RPAS being permitted to operate (See AC 9XX-### for guidance on these processes). The sections of Standard 922 are as follows:

(a) 922.04: Operations in Controlled Airspace

(b) 922.05: Operations Near People

(c) 922.06: Operations Over People

(d) 922.07: Safety and Reliability

(e) 922.08: Containment

(f) 922.09: Command and Control Link Reliability and Lost Link Behaviour

(g) 922.10: Detect, Alert, and Avoid Systems

(h) 922.11: Control Station Design

(i) 922.12: Demonstrated Environmental Envelope

(3) Compliance with any part of Standard 922 is through a declaration made by an organization or individual who is taking responsibility for compliance of the RPAS with CAR Standard 922. To support the various levels of risk associated with RPAS operations, the Declaration system has two levels of robustness. For lower risk operations (i.e., sRPAS VLOS operation, and some BVLOS operations) an applicant is only required to submit a Declaration to TCCA that they comply with a particular standard. For higher risk operations a higher level of robustness is achieved by requiring the applicant seek a Pre-Validated Declaration.

(4) Pre-Validated Declarations require that the applicant submit additional documentation for review by TCCA prior to being permitted to Declare compliance with a part of Standard 922. The details of this application process are described in AC901-001 Declaration and Pre-Validated Declaration processes.

(5) VLOS operations using small RPAS, have three defined operational risk categories for which safety assurance of the RPAS is deemed necessary. They are listed in the table below.

| **CAR Reference** | **RPAS Size** | **Operation** | **Applicable section of Standard 922.** | **Type of Declaration Required** | **Section Reference** |
|---|---|---|---|---|---|
| 901.69(a) | Small | Controlled Airspace | 922.04 | Declaration | 4.2 |
| 901.69(b) | Small | Operations Near People | 922.05 | Declaration | 4.3 |
| 901.69(c) | Small | Operations Over People | 922.06 | Declaration | 4.4 |

(6) When considering VLOS operations using medium RPAS, the increased mass and complexity of the RPAS necessitates that safety assurance declarations are required for all operations. The operational categories, and the required declarations are summarized in the following table:

| CAR Reference | RPAS Size | Operation | Applicable section of Standard 922. | Type of Declaration Required | Section Reference |
|---|---|---|---|---|---|
| 901.69(e) | Medium | Operations Away from People | 922.08 | Declaration | 4.6 |
| 901.69(f) | Medium | Operations Near People | 922.07 | Pre-Validated Declaration | 4.5 |
| 901.69(g) | Medium | Operations Over People | 922.07 | Pre-Validated Declaration | 4.5 |
| 901.69(h) | Medium | Controlled Airspace | 922.04 | Declaration | 4.2 |

(7) BVLOS operations are divided by the proximity to populated areas as well as the size of the RPAS. The following operational classifications exist:

| CAR Reference | RPAS Size | Operation | Applicable section of Standard 922. | Type of Declaration Required | Section Reference |
|---|---|---|---|---|---|
| 901.87(a) | Small | Operations more than 1km from populated areas | 922.08 (1,2)<br>922.09<br>922.10<br>922.11 | Declaration | 4.6<br>4.7<br>4.8<br>4.9 |
| 901.87(a) | Medium | Operations more than 1km from populated areas | 922.08 (3,4,5,6)<br>922.09<br>922.10<br>922.11 | Declaration | 4.6<br>4.7<br>4.8<br>4.9 |

| | | | | | |
|---|---|---|---|---|---|
| 901.87(a) | Small | Operations less than 1km from populated areas, or over sparsely populated areas. | 922.07<br>922.09<br>922.10<br>922.11<br>922.12 | Pre-Validated Declaration | 4.5<br>4.7<br>4.8<br>4.9 |

(8) In addition to the design standards identified in CAR Standard 922, RPAS Declarants have a regulatory obligation to make available to each owner the information prescribed by CAR 901.200. This information may be contained within the operating manual published for each RPAS model.

## 4.0 Methods for demonstrating compliance

### 4.1 General

(1) RPAS Manufacturers are required to declare the compliance of their system against the safety assurance requirements of Standard 922. This section focusses on methods for demonstrating compliance with the each of the specific safety assurance requirements. These safety assurance requirements are based on the risk these operations pose to the public, and the expectations the public has regarding the reliability of aeronautical products.

(2) The following sub-sections provide information on each part of CAR Standard 922 and are intended to provide guidance to declarants on how to develop a high level of confidence that an RPA meets the standard.

Means of Compliance to various CAR Standard 922 sections. Refer to Appendix A for a list of industry standards that have been acknowledged by TC.

(3) Verification Methods. There are four main verification methods used in the design of safety critical products. These are:

(a) Inspection or Review

(b) Analysis

(c) Test or Demonstration

(d) Service Experience

(4) Inspection or Review. This consists of a systematic Inspection or Review of Drawings, Designs, Hardware, Software. Generally, this is used to verify requirements that can be easily observed and understood such as workmanship, dimensions (size, weight, etc.), and physical implementation.

(5) Analysis. Analysis involves a detailed examination of specific aspects of the design and may include things such as calculations, simulation or modelling, or traceability of requirements to design implementation.

(6) Test or Demonstration. Test or Demonstration is typically used to verify performance and behavioural requirements of the designed system. Tests verify both that the system correctly

implements all desired functionality and that there are no unintended or undesired behaviours of the system.

(7) Service Experience. Similarity and Service Experience can be used when a feature of a design is sufficiently similar to those on existing designs, and these existing designs exhibit adequate reliability. This method used documented service experience as well as engineering judgement to verify that the system will behave as expected with sufficient reliability.

### 4.2 922.04 Operations in controlled airspace

(1) General. For RPAS operating in controlled airspace CAR Standard 922.04 requires that design requirements are met to allow for communication of position and altitude to air traffic controllers and other participant aircraft with the specified level of accuracy.

While it is acknowledged that accuracy requirements alone do not provide any additional robustness or system reliability objectives, the intent is to provide a minimum required accuracy for position and altitude such that other users of the airspace are accurately made aware of any potential hazard the RPA may pose.

(2) Position Accuracy. A system position accuracy of +/-10m has been identified as the minimum accuracy for position within controlled airspace. Most modern Global Navigation Satellite System (GNSS) technologies can easily achieve this accuracy nearly 100% of the time. Considerations should be taken to ensure that this accuracy can be maintained while in degraded modes of operation, and in all portions of the proposed operational space (e.g., considerations for buildings, trees, valleys etc.). The accuracy should be clearly identified in the limitations portions of the operating manual.

(3) Altitude Accuracy. A system altitude accuracy of +/- 16m has been identified as the minimum accuracy for altitude within controlled airspace. Most modern GNSS technology can achieve this accuracy using the WGS-84 geodetic datum. Consideration should be taken when designing altitude measurement systems that differences between ground level, sea level, and various geodetic datum are taken into account.

(4) Errors. Accuracy is a probabilistic measurement based on assumptions related to the quality and integrity in a constantly changing environment. It is important to understand the errors that may contribute to degradation of accuracy and take these into account as part of the overall design error budget. Examples of sources of errors adversely affecting accuracy are identified below.

(a) Terrain Errors. GNSS signals are also subject to errors caused by the terrain. Terrain masking of the signal, for example by a building or mountain, blocks the antenna on the RPAS from receiving the satellite signal. A GNSS signal reflected by the landscape such that the receiver now receives “additional” signals which can create confusion and may need to be processed out to avoid creating position errors.

(b) Atmospheric Errors. Atmospheric errors are caused by the ionosphere and the troposphere, which are both capable of refracting GNSS radio signals. Ionospheric density is diurnally dependent, which means that it varies with time of day (or night). The density is affected by, among other factors, humidity, temperature and pressure. These variations adversely affect the “signal speed x time” equation built into GNSS position calculations. To correct for these errors, a number of steps are taken. Troposphere errors can be caused by moisture absorbing/refracting signal and cause errors up to 6m. Ionosphere errors can be caused by the atmospheric refraction of the GNSS signals and may be up to 40-60 m by day and 6-12 m at night. These errors can be mitigated by the use of multi-frequency receivers, selection of masking angle, and/or the use of augmentation systems (either ground-based, such as Local Area Augmentation System [LAAS], or space-based, such as European Geostationary Navigation Overlay Service [EGNOS]).

(c) Satellite Errors. These are errors resulting from poor or unexpected geometries related to the positions of the GNSS satellites in reference to an RPAS. Gravitational effects of the Sun and Moon may pull the SV from planned orbital path. Solar Radiation creates EMI prior to the signal hitting the atmosphere.

(d) Geometric Dilution of Precision (DOP). DOP occurs when there is no adequate cross cut in the "fix" (i.e. all satellites are all too closely located to each other). The consequence is that all of the signals are vulnerable to same errors from the atmosphere. Errors can occur in the horizontal (H), the vertical (V) and in time (T).

### 4.3 922.05 Operations near people

(1) General. CAR 901.62(b) allows operations of an RPA at a distance of 30m (100ft) but not less than 5m (15ft) of a person, except for crew member or person involved in the operation. This permission is only granted to RPAS for which a declaration was submitted by the manufacturer having confirmed that it is fit for operations near people. CAR Standard 922.05 identifies two technical requirements which are to be verified before a declaration is made. The manufacturer must also publish all associated limitations for operations near people (e.g. speed limits, allowed operational modes) in the operating manual.

(2) Protection Against Injury to Persons on the Ground

(a) General. The RPAS design must be assessed to show that the probability of occurrence of any single failure which may result in a severe injury to a person on the ground within 30m of the RPA while in operation is remote. This requirement is meant to protect people not associated with the operation of the RPAS from being severely injured or killed as a result of unreliable or unsafe system designs for this kind of operation.

(b) Single Failure. The principle of "no single failure" allows for the implementation of system architectures using redundancy to increase reliability of the overall RPAS. While it is acknowledged that certain single failures may occur without adversely affecting the capability to control and recover the RPA following the published non-normal or emergency procedures, the single failures referred to in this technical requirement are those in which no controlled recovery is possible. Some examples are identified below:

1. Flight control failure leading to a stall;
2. Antenna failure leading to a flyaway;
3. Motor winding failure leading to an engine failure; and
4. Electrical short leading to a fire.

(c) Safety Features. Safety features may be incorporated in the design to mitigate to risk of injury to people on the ground (see section 6.4 on injury severity). Possible safety features are identified below:

1. Stall warning;
2. Parachute;
3. Frangible design;
4. Soft materials;
5. Rotor shrouds;
6. A flight envelope protection system;
7. A battery/fuel gauge and a warning when the battery/fuel is low;
8. Commanding the aircraft to land when the battery/fuel is low;

9. A return to home function; and
10. A fast-acting rotor/propeller braking means.

(d) Remote. The term “remote” implies a probability prediction for a specific failure scenario. A safety assessment must be conducted for the elements on the RPAS in order to substantiate any probability prediction. Refer to Appendix B for further guidance; it should be clearly noted that this Appendix uses standard aviation terminologies and processes to perform a system safety assessment (i.e. refer to FAA AC 23-1309-1E or later published revision).

(e) Methods of Evaluation. Compliance with the safety assurance requirements entails the assessment of the injury sustained by persons on the ground as a result of each failure condition and the determination of the probability of their occurrence per flight-hour. The objective is for the RPAS manufacturer to demonstrate that the likelihood of the RPA inflicting severe injuries (AIS 4 to 6) to persons on the ground as a result of a failure condition is remote. A procedure for evaluating the injury severity is provided in Appendix C.

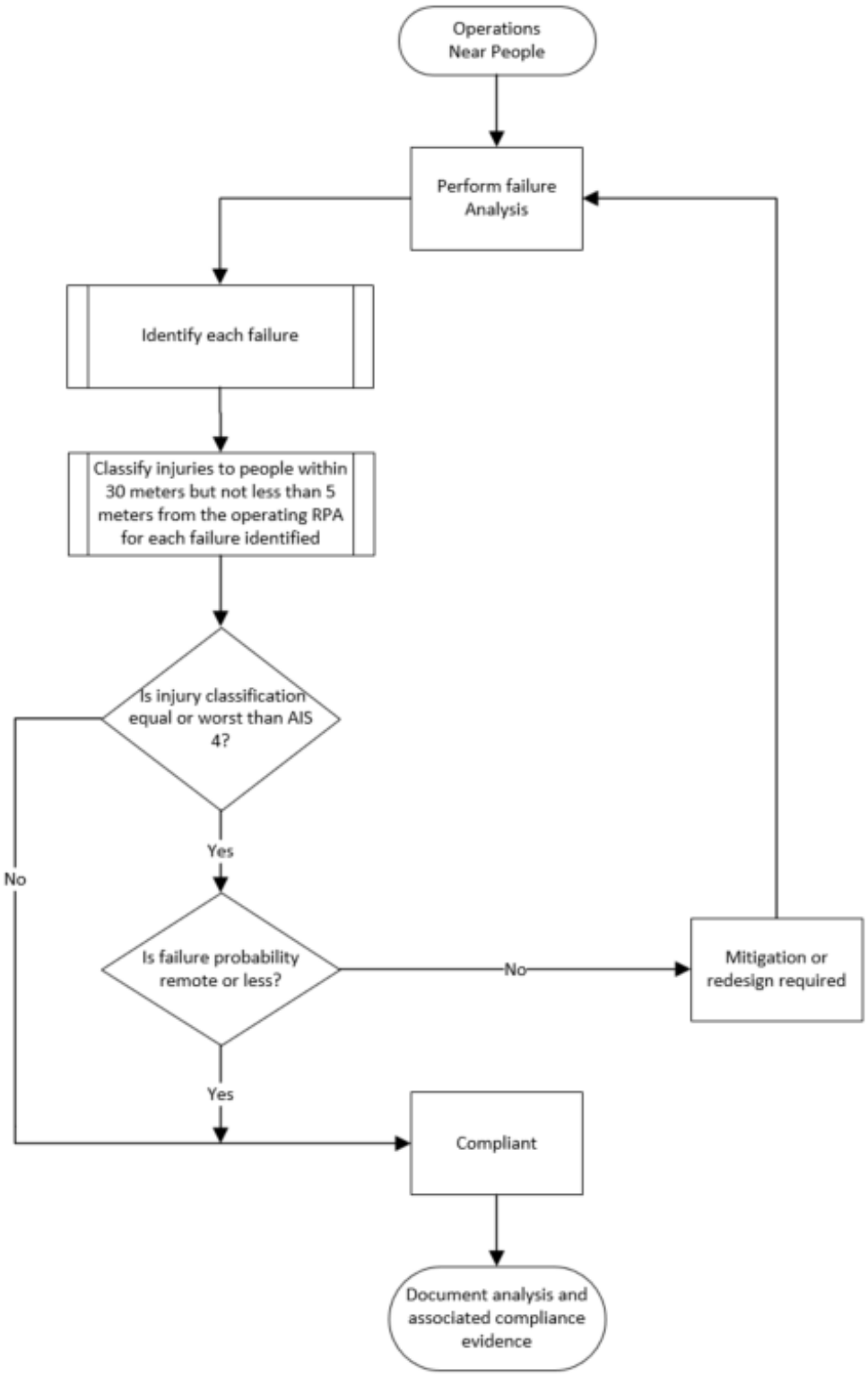



**Figure 1 – Operations near people safety assessment compliance flowchart**

(3) Warning and Alerts.

(a) General. Warnings and alerts on the CS are intended to inform the pilot when conditions exist which may impact RPAS safe flight operation. In the event that failures or unsafe conditions exist where an alert is presented to the pilot, the warning and alerting system must be designed to provide conspicuous indications minimizing the possibility of pilot errors which could exacerbate the situation. The safety objective is to design systems that support pilot duties by providing timely, accurate, and intuitive information for safe RPA operation.

There is a great deal of overlap between the Warning and Alerting aspects of 922.05, 922.06, and the 922.11 Control Station Design Standard. The means of compliance recommended in Section 7.8 below for CAR Standard 922.11 are equally appropriate to the demonstration that the system controls, monitoring and warnings are appropriate for operations Near and Over People. Refer to Section 7.8 for further discussion on human-system integration.

### 4.4 922.06 Operations over people

(1) General. CAR 901.62(a)(iii) allows operations of a small RPA at a distance of less 5m (16.4ft) from a person on the ground. This permission is only granted to RPAS for which a declaration was submitted by the manufacturer having confirmed that it is fit for operations over people. Standard 922.06 identifies the three key technical requirements that must be verified before a declaration is made. A description of means incorporated in the design to prevent exceeding operating limits when flying over people along with associated limitations for operations over people should be published in the operating manual.

(2) Protection Against Injury to Persons on the Ground

(a) General. The RPAS must be assessed to show that the design precludes the occurrence of any single failure which may result in a severe injury to a person on the ground within 5m of the RPA while in operation. In addition, any failure combinations which may result in a severe injury must be remote. These requirements are meant to protect people not associated with the operation of the RPAS from being severely injured or killed as a result of unreliable or unsafe system designs for this kind of operation.

(b) Single Failure. Consideration for the evaluation of single failures is similar to the considerations made for operations near people; see section 6.2(3)(b). The RPAS design should therefore provide for additional reliability which may be provided through architectural means such as redundancy, independence, and high development assurance levels. Any safety assessment must consider common modes and common cause failures.

(c) Failure Combinations. The safety assurance requirements specify that any failure combinations which may result in severe injury be evaluated to show that their combined probability of occurrence is remote.

(d) Remote. Refer to section 6.2(3)(c) for guidance on the use of the term “remote”.

(e) Methods of Evaluation. The methods of evaluating compliance are identical to those for operations near people in section 6.2(3)(d). Operations over people require a demonstration that severe injuries will not result from a single failure condition irrespective of its probability of occurrence. A procedure for evaluating the injury severity is provided in Appendix C.

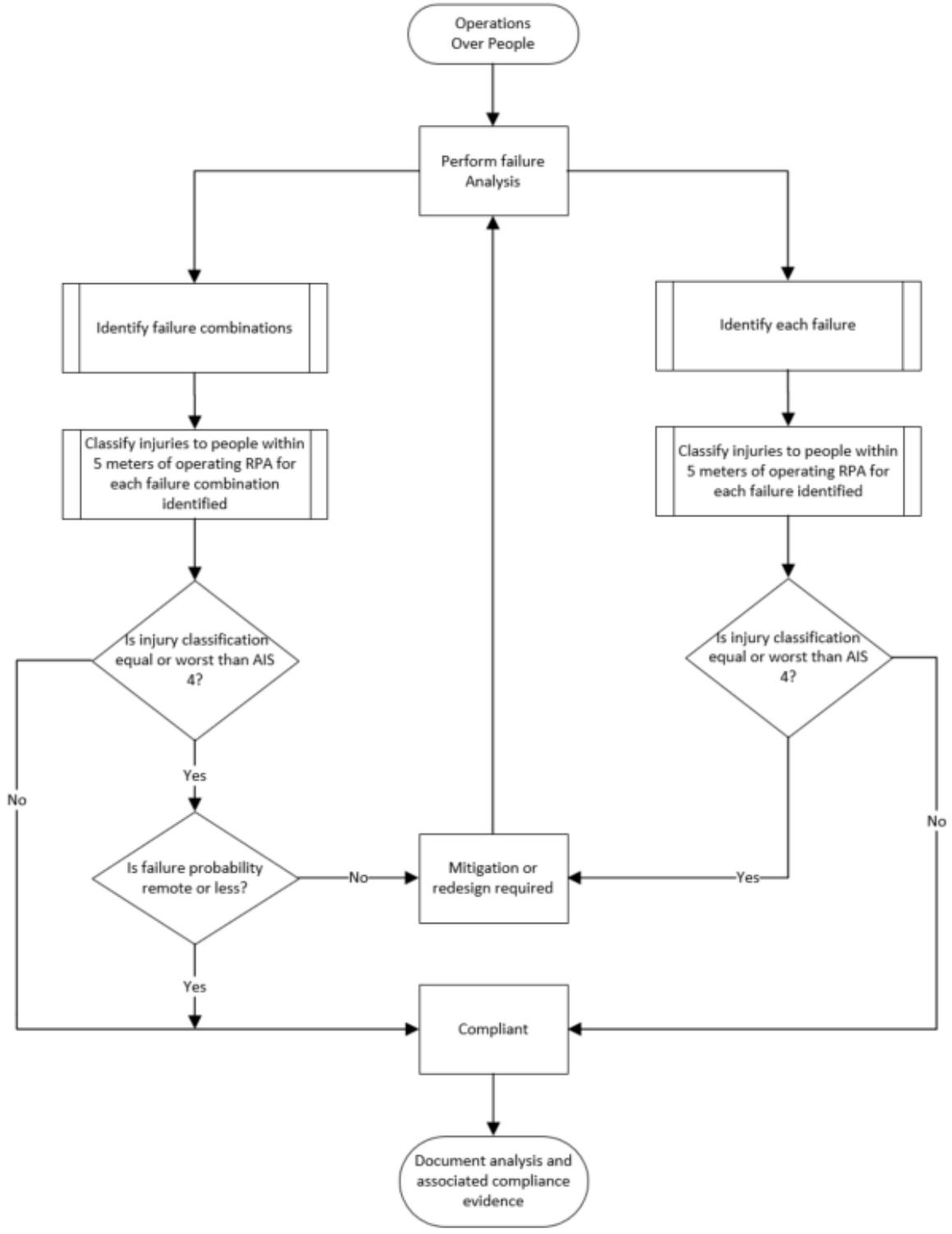



**Figure 2– Operations over people safety assessment compliance flowchart**

(3) Warning and Alerts

(a) As discussed above, analysis of Warnings and Alerting systems for RPAS operating over people follows the same processes appropriate for CAR Standard 922.12 described in Section 7.8 below.

### 4.5 922.07 Safety and Reliability

(1) General. This standard is applied to VLOS operations with medium RPAS that occur near and over people, as well as BVLOS operations that are over sparsely populated areas (i.e. between 5 and 25 people per square kilometer). At a high level, this standard requires the declarant to perform a formal system safety assessment on their RPAS. Medium RPAS will generally be more complex and this standard ensures that attention is given to how the various systems behave during failures and how sub-systems might interact during failures. In general, one can assume that if a >25kg comes in contact with a person or manned aircraft there will be a serious injury or death. Therefore, VLOS operations that don't have the luxury of an adequate standoff distance from people not involved with the operation are required to perform a System Safety Assessment on their RPAS to demonstrate that the probability that their RPAS will create a hazard to those people is sufficiently low.

The 922.07 standard is applied to all BVLOS operations that are not "Isolated" because it is important to understand how reliable the RPAS is and what failures can be expected. By being closer to people, RPAS failures during these operations can create more hazardous situations then the same failure might create in an Isolated area. Understanding the probability and criticality of these failures will often drive operational limitations as well as strategic and tactical mitigations required to keep the operation safe.

It should be noted that 922.08 (Containment) is not specifically called out for operations that require compliance with 922.07. This does not imply that containment considerations are not applicable to these operations. It is expected that analysis of an RPAS containment capability and fly-away mitigations will be performed as part of the 922.07 safety and reliability assessment process. As discussed in the 922.08 section below, Containment plays a significant role in the safety assurance of Isolated Operations. Declarants to 922.07 still need to assess their Notional CONOPS for the hazards associated with fly-aways and ensure that these hazards are sufficiently mitigated.

(2) Notional CONOPS. The first step in showing compliance to this standard will require the development of a Notional Concept of Operations. This will determine the expected "average operation", and to inform the criticality classifications of the system. The notional CONOPS will be used to assist in the failure effects analysis. If specific assumptions from the CONOPS are used to lower the hazard classification used, then these assumptions must be included as operational limitations in the RPAS operating manual. For example, if the notional CONOPS assumes that for certain types of operations, a flight termination system, parachute system, or an independent battery is available, then a limitation would be required for these operations requiring that these systems be installed and operational when the RPAS is operated.

The Notional CONOPS is critical enough to the RPAS development process that a copy of the Notional CONOPS is required as part of the data package when an applicant applies for a pre-validated declaration. Refer to AC <TBD on PVD> for more information. As discussed above, the notional CONOPS should be the superset of all permitted operations with the RPAS, and any limitations or assumptions that could result in limitations must be passed on to the operator.

(3) Use of Kinetic Energy to Specify Reliability Requirements. The specific safety objectives of 922.07 are based on the RPA maximum kinetic energy. Applicants are required to determine the maximum kinetic energy that their system is likely to attain following a worst-case failure condition. In general, this will require a creation of an Aircraft Level Functional Hazard Assessment (refer to SAE ARP4761) to determine which failure, or combination of failures could result in the highest RPA velocity. This assessment is intended to be the kinetic energy derived

from the maximum linear velocity of the aircraft at maximum operating mass. This measure can exclude rotational kinetic energy contained in rotating parts, as well as chemical potential energy contained in fuel tanks and batteries.

It's acknowledged that certain drone configurations can have considerable rotational kinetic energy in the form of spinning rotors, or chemical potential energy in the form of fuel or batteries, However, it is much harder to quantify the injury potential from these sources because they are highly dependent on the exact crash conditions. Furthermore, following a crash, rotating parts (which are typically light weight rotors and propellers) tend to dissipate kinetic energy over a short distance, and chemical sources (fuel/batteries) tend to dissipate energy slowly (burning) rather than explosively. As mentioned above, the hazard created by these energy sources depends greatly on the specific conditions of the crash. For these reasons, linear kinetic energy alone is used as it provides a standardized measurement of the damage potential present in a particular RPAS, and the intent is that the safety criteria (failure rates, design assurance, required standoff distances) are sufficient to provide adequate mitigation for the other sources of energy contained in the RPAS. However, there may be cases where unconventional aircraft designs make these assumptions invalid. In these cases, the safety case needs to be reviewed to determine if the use of linear kinetic energy alone is still applicable. Examples could include RPAS with heavier than normal rotating parts, pressurized tanks of fuel (i.e. Hydrogen, significant amounts of fuel, etc.), or carriage of dangerous goods. Refer to AC901-001 - RPAS Safety Assurance Declaration and Pre-Validated Declaration Processes for more information on declarations involving unconventional designs.

The Kinetic Energy categories used for 922.07 have an upper limit at 1084kJ. Applicants are encouraged to contact Transport Canada if they feel that the kinetic energy of their RPAS is more than 1084kJ, or if there are special considerations with respect to other energy sources (rotational or chemical energy as discussed above). At the lower end of the energy spectrum, when considering if small RPA can cause severe injury, a procedure for evaluating injury severity is provided in Appendix C.

(4) Failure Probability. Once the worst-case Kinetic energy is determined, Table 1 in CAR Standard 922.07 can be used to determine reliability targets for various failure criticality categories. An RPAS-level functional hazard assessment is performed to identify the specific hazard and failure classification associated with failures of various aircraft systems. Once the failure classifications are determined a System Safety Assessment is performed to demonstrate that the RPAS as designed meets or exceeds the CAR Standard 922.07 Table 1 reliability requirements. Depending on the complexity of the RPAS this demonstration can involve in-service experience, accelerated life testing, engineering analysis, fault tree analysis or other quantitative and qualitative reliability assessment tools. Refer to Appendix B of this document for further guidance.

(5) Development Assurance. Development assurance is the collection of processes through which a product design is evaluated and reviewed to ensure it functions as expected under safety-critical conditions. It is expected that a structured approach to Development Assurance will be used when designing an RPAS that complies with the reliability requirements of Standard 922.07. Assuming that traditional aviation Design Assurance Level definitions are applied, the recommended Design Assurance Levels are as follows:

*1. Table 2- DAL Assignment*

| **Classification** | **Reliability Objective** | **Functional Development Assurance Level (FDAL)** | | |
|---|---|---|---|---|
| | | <700 J | <34 kJ | <1084 kJ |
| Catastrophic | Extremely Improbable | FDAL D/Tier 3 | FDAL D/Tier 3 | FDAL C |
| Hazardous | Extremely Remote | FDAL D/Tier 3 | FDAL D/Tier 3 | FDAL D |
| Major | Remote | FDAL D/Tier 2 | FDAL D/Tier 2 | FDAL D |
| Minor | Probable | FDAL D/Tier 1 | FDAL D/Tier 1 | FDAL D |

| | | | | |
|---|---|---|---|---|
| No safety affect | No requirements | No requirements | No requirements | No requirements |

Development Assurance Levels (DAL) are intended to be used to provide a specified level of rigor the manufacturer/designer is required to put into the design and development of the hardware and software components of their systems. The assigned DAL determines the extent of assurance activities to be performed on the systems.

The specific levels assigned to each category of RPAS in Table 2 are selected as a balance between the more stringent requirements for certified Part 23 aircraft while ensuring that the applicant has a means to show that their design is 'correct'. The chosen levels are also consistent with what was proposed by JARUS in RPAS 1309, which also considers RPAS much larger than what is proposed in this standard (<6000 lb/2721 kg). Where specific DAL assignments are required, the recommended verification and validation requirements shall follow what is listed in SAE ARP 4754A. Where Tier levels are assigned, verification and validation is to follow requirements as per ASTM F3201 (where applicable for software development) or an equivalent process.

Where secondary systems are required in the design to meet the safety objectives, the secondary system is required to be assigned the same DAL as the primary. The DAL also dictates the type and amount of validation and verifications made by the applicant and described in their compliance plan. The development plan for these DAL artifacts, and methods used by the applicant should be included in the application stage for Pre-Validated Declaration RPAS, and may be subject to oversight under general RPAS surveillance procedures.

### 4.6 922.08 Containment

(1) General. This standard is applied to all operations where a majority of the risk mitigation comes from the fact that the operation is far from people (either on the ground or in the air). For these operations, a key element of safety is the assurance that the RPA can be kept inside the operational volume. In other words, having a fly away during these operations would result in a loss of most of the safety margin built into the operation. The containment standard is applied to provide confidence that the operation will keep the RPA inside the operational volume.

The 922.08 Containment Standard is applied to VLOS operations with mRPAS, more than 500ft away from people not involved in the operations. It's expected that many of these operations will be design and development flights of prototype RPAS. Prior to the first flight of an mRPAS, a Declaration needs to be made that the RPAS meets the Low Robustness Containment standard of 922.08(1) and 922.08(2).

In addition to Basic VLOS, and Isolated BVLOS, the Low Robustness Containment standard is also applied to VLOS in controlled airspace with RPA between 25kg and 150kg. Currently Part IX VLOS operations in controlled airspace requires the RPA be declared to the 922.04 standard, and that the operation has permission and coordination from the airspace controlling authority (ref 901.71). These VLOS operations will continue to be limited in altitude to whatever the controlling authority approves, and the operator will need to maintain VLOS (901.11), give right of way to all traditional aircraft (901.17), and not create a hazard to other traditional aircraft (901.18). These strategic mitigations keep the risks associated with a VLOS operation low regardless of the RPAS size. The application of low robustness containment is considered to provide enough confidence that this type of operation will not have a fly away in controlled airspace, and therefore mitigates the key additional risk of operation with an RPAS larger than 25kg.

It should be noted that this standard is not applied when an operation requires the 922.07 (Safety and Reliability) standard. Application of the containment standard can be thought of as a subset of the full system safety analysis process. It's expected that means of compliance to the Containment Standard will include the same types of safety assessments and design and

development assurance as means of compliance to 922.07, but that the focus of these processes will be the specific failure of a fly-away.

(2) Expected Means of Compliance. The following paragraphs are intended to provide guidance and some simple examples of how an applicant might choose to comply with the Containment Standard. The examples here are not intended to describe the only possible means of compliance.

(3) Single Failure Considerations. Both the low and high robustness containment standard require that no single failure result in a fly-away of the RPA. Therefore, the containment means needs to be independent from any systems on the RPAS that could result in a fly-away. For example, a flight termination system that relies on the RPAS C2 link for activation would not meet the single failure requirement, because presumably, a failure of the C2 link would result in an inability to both control and flight-terminate the RPA. The result would be that the operator no longer has the means to ensure containment. On the other hand, and flight termination system that safely ends the flight following a C2 link failure could be acceptable depending on the details of the system architecture. The system safety analysis would need to show that there are no common cause failures that could result in a failure of both the C2 link and the flight termination system (i.e., both the RF transceiver and the flight termination system should not be powered by the same power source).

Consideration also needs to be given to errors in Software and Electronic Hardware that could lead to a fly-away condition. System analysis needs to show that systems used to prevent flyaway are isolated from errors that could occur other software or electronic hardware components. In general, this will drive applicants to containment systems that are developed and implemented independently from other systems used in the RPAS.

(4) Low Robustness Containment. At the most basic level, and applicant could show compliance to this standard by limiting the fuel/electrical energy of the drone such that it does not have the endurance required to leave the operational volume. For example, an RPAS with 10 minutes of endurance inside an operational volume such that it is more than 10 minutes at max speed from any edge of the operational volume will be unable to exit that operational volume in the event of a failure.

More realistically, an applicant wishing to show that they meet the low robustness containment requirements will need to perform a system safety analysis on their RPAS with a focus on system failures that could result in the RPA leaving the operational volume without the operator being able to stop it. One example of a failure that could cause this would be C2 link loss while the RPAS programmed to maintain heading and altitude. Another example would be a failure in the navigation sensor leading the RPAS incorrectly flying outside of the operational volume. For failures such as these it is predicted that the manufacturer would add independent redundancy to their RPAS that will either take-over and perform the necessary function or terminate the flight safely.

As an example, a manufacturer of an RPAS performs a design review of their RPAS design and finds that the system autopilot uses open-source software that has no pedigree of design or developmental assurance. The review would then need to determine whether an autopilot software fault could lead to an aircraft flyaway. For a system like this, if the manufacturer wanted to show low robustness containment on this RPAS, their options are:

(a) Replace, Redesign and Validate the Autopilot in order to show that no single failure of that autopilot would lead leading to a flyaway. Since software items are typically assumed to contain software errors, this redesign would require independent redundancy to be designed into the autopilot.

(b) Add an independent flight termination system that can be activated by the operator in the event that a failure of the autopilot results in a fly-away. The applicant would need to show that the system allows the operator to be alerted if there is a failure of the flight

termination system. The applicant would also need to ensure that the operator is alerted to conditions that could indicate that a flyaway is imminent and have procedures established for activation of the flight termination system.

(5) High Robustness Containment. High robustness containment requirements are that no single failure can cause a flyaway and that any combination of failures that lead to a fly away is remote. Complying with high robustness containment would require an FMEA and SSA to analyze the RPAS and determine which failures could lead to a breach of containment. It would then require demonstration (likely through analysis) that these failures are sufficiently improbable.

In addition to the failure analysis, High Robustness containment also includes a requirement for design assurance on hardware and software where a fault could lead to a loss of containment. Applicants are expected to establish a system design process that is based on an industry standard such as DO-178/254 or ASTM F3201-16. The intent of this is to minimize the probability that the RPAS will suffer a loss of containment due to a software error.

### 4.7 922.09 Command and Control Link Reliability and Lost Link Behaviour

(1) General. When operating BVLOS, the C2 link is the only connection between the operator and the RPA. The operator needs to have enough information about the C2 link to make informed strategic decisions while designing an operation, as well as tactical decisions while executing an operation.

This standard is not required for VLOS operations because when operating VLOS, the C2 link is not the only means of maintaining situational awareness of the RPA and its environment. While it is true that C2 link loss in a VLOS operation can result in a loss of control of the RPAS, these operations will mitigate this hazard in other means. Basic Operations mitigate this hazard by the standoff distance from people as well as compliance with the 922.08 containment requirement. Other VLOS operations (such as VLOS operations near and over people with mRPAS) are expected to analyze a C2 link failure within the 922.07 standard process and mitigate hazards related to the C2 link accordingly.

(2) Operational Risks. This standard aims to mitigate two major operational risks:

First, it is intended to quantify the probability of a Loss of C2 Link, which will in general result in a Loss of Pilot Situational Awareness. Loss of C2 Link creates a scenario where an operator is “blind” to the state of the RPAS. Therefore, the intent of the standard is to ensure that C2 Link Service Providers (C2SP) and RPAS developers have assessed their designs and implementations to accurately describe the limitations of the C2 Link in supporting the pilot’s ability to aviate, navigate, communicate, and integrate seamlessly into the airspace. C2 Link performance information is required to be passed on to the operator (ref CAR 901.200) so that the operator can make informed decisions when designing operations and when making tactical decisions during an operation.

Second, it mitigates risks associated with loss of RPA control. In some RPAS a loss of C2 Link can result in a state with the RPAS is no longer controllable (e.g. Fly away, crash) and may present a hazard to aviation safety. The intent of the standard is to ensure that RPAS used for BVLOS operation exhibit behaviour which is predictable and understood by the operator such that safe operations can be planned. In the future it is expected that this will lead to standard operating behaviors when the aircraft loses connection with the pilots.

This standard includes safety requirements to allow robustness to be applied to the C2 link in environments that might not merit a full safety and reliability analysis. For these situations it is expected the applicant examines the architecture and reliability of the C2 link system when showing compliance to this standard. For other types of BVLOS operations, it is expected the analysis of the C2 Link system would be done as part of the required 922.07 Safety and Reliability standard. In these cases, it is expected the applicant would refer to their safety and

reliability analysis when showing compliance with the reliability component of the C2-Link standard.

(3) Expected Means of Compliance. C2 Service Providers (C2SP) are 3rd party organizations that provide a C2 link capability for RPAS use. For C2SP, compliance to the standard can be shown through a derivation of the performance criteria using a standardized method to evaluate the parameters (e.g. DO-377A methodology). It is expected that individuals making Declarations against this standard will possess expertise in radio engineering and produce and support radio operations in Canada.

For RPAS designers, compliance the lost link portion of the standard can be shown through a functional hazard analysis, system safety assessment, and component failure evaluation (e.g. ARP-4761 methodology). Redundancies in key C2 Link systems will provide for a method of ensuring robustness in design, while detailed analysis of key components (e.g. sourcing, reliability analysis) allows for single point failures if the robustness of the components can be adequately demonstrated. To sufficiently make Declarations against this standard the RPAS designer will need to have experience in reliability analysis and system design methodologies.

To address the requirement for predictable and safe behaviour, it's expected that the RPA will have some sort of automated behaviour in the event that C2 link is lost. The exact behaviour to minimize the creation of a hazard will depend on the exact CONOPS being considered. In some cases, a "return-to-home", or "land-at-designated-location" behaviour might be desirable. In other cases, an RPAS designer might decide that the safest course of action is for the RPA to increase altitude in an effort to regain C2 link. Regardless of the lost-link behaviour selected, the RPAS designer needs to document the behaviour and any pre-flight procedures required to ensure the correct behaviour in the event of a C2 link loss. This information must be present in the operating instructions of the RPAS to ensure that operators configure the aircraft correctly before flight. RPAS designers are also strongly encouraged to design operator interfaces in a manner that minimizes the possibility of error when programming C2 lost link behaviour. If the RPAS includes flexibility in the programmed lost link behaviour, operators should be able to easily and clearly verify that the planned behaviour for lost-link occurrences is as intended. For operations where CAR Standard 922.11 (Control Station Design) is applicable, it's assumed that these usability assessments will be performed as part of compliance with that standard.

### 4.8 922.10 Detect, Alert and Avoid Systems

(1) General. The DAA standard is required for all BVLOS operations. In the BVLOS domain, operators cannot rely on human vision to mitigate the risk of collision with another aircraft. Operators in this regime are required to have a technological solution for detecting and avoiding manned aircraft that may be found in their operational area.

The only exceptions to this requirement are operations that use Visual Observer DAA (VODAA – Ref Standard 923). These operations have specific procedural and operational restrictions on them and allow visual observers to monitor for incoming traditional aircraft while not being able to see the RPA itself. The regulatory framework has been designed so that Visual Observer DAA is a means to comply with Standard 922.10. Effectively, the visual observer becomes the Detect and Avoid System for the operation. The specific procedural and operational limitations on Visual Observer DAA can be found in Standard 923 Vision-Based DAA.

In general, however, it's expected that most operations will eventually rely on technological means for Detection and Avoidance of traditional aviation. These means could be radar, ADS-B, Electro-Optical/Infra-Red (EO/IR) sensors, or a combination of several technologies.

(2) Airspace Classification. From the standpoint of DAA, airspace is classified into several Air Risk Class (ARC) classifications. These represent the relative probability of encountering an aircraft in

a certain airspace. Refer to Advisory Circular AC903-001 for more details on how ARC classifications are assigned.

The information required to determine the ARC classification of any particular operational volume is:

(a) The “ATC” Airspace classification (Class A/B/C/D/E/F/G)

(b) The proximity to the nearest aerodrome.

(c) Presence of any advisory areas (CYA) near the ground.

Using this information, operators will determine the ARC classification for their operation and therefore determine the robustness of the DAA system required.

(3) Expected Means of Compliance. The simplest MoC for 922.10, but also the one with the most operational restrictions is the use of CAR Standard 923 for “Vision Based DAA”. As the name suggests, this means of DAA uses visual observers placed along the route of the RPA, and in communication with the PIC to provide detect, alert and avoid functionality to the operation.

To avoid the operational limitations that come with Standard 923, operations will require a technological solution for detecting and avoiding other aircraft that may enter their operational area. It’s expected that these technologies may include things such as radars, transponders, EO/IR sensors. These sensors would have to be integrated into the operations such that, the crew operating the RPA can be alerted to the presence of intruder aircraft, and can take steps to avoid a collision with intruder aircraft. Standards bodies such as ASTM are currently developing industry standards that are intended to target the types of operations supported by this regulatory package (Low Altitude, outside controlled airspace, <150kg RPAS). The use of this standard is expected to be an acceptable means of compliance to the 922.10 DAA standard.

If a specific industry standard is not used (or is not available), it is expected that one of three general strategies for showing compliance to the 922.10 DAA standard would be used. At a high level, these are:

(a) MoC 1: Analysis with Flight Test Validation

This MoC involves building an analytical model of the DAA system that can be used to simulate the performance of the DAA system. It also involves real-world flight testing of the DAA system to validate the results provide by the simulation. This MoC is the most work/time/cost intensive of the three, but if done properly will result in the most permissive operational limitations placed on the system.

(b) MoC 2: Large Dataset Sensor Validation

This MoC involves real world testing of the DAA system over a long period of time. Enough data needs to be collected to characterize the performance of the sensor throughout its operational envelope. This MoC is most appropriate for a ground-based system that can be “left running” long enough to track targets of opportunity throughout the surveillance volume. Once the surveillance volume is characterized, an applicant be expected to do simulations or analysis to show that the required risk ratio can be met given the operational and performance restrictions of the RPAS and the operation.

(c) MoC 3: Operationally Specific Testing

This MoC is intended to be used by operations that plan to remain in a specific operational area and never venture elsewhere. An operation that performs a periodic inspection of the same infrastructure could place their sensor permanently nearby and then perform testing to characterize the surveillance volume of that sensor. Once the sensor has been shown to have an adequate surveillance volume to support the CONOPS, the DAA System could be used for that operation only. Changes to the CONOPS may require that the sensor characterization be repeated.

A key aspect of these proposed MoCs is that the testing or simulation is done for airspace representative of the intended operation. This should include a validation that the simulated intruder composition (types of aircraft/speed/maneuverability and equipage) matches the intruders that the DAA system expects to encounter operationally.

Where the MoC involves a combination of simulation and real-world validation of the simulation, it's expected that applicants will demonstrate the acceptable correlation of their simulation with the real-world behaviour of their system. Reference is made to industry standards (ref ASTM DAA Test Methods Standards) for acceptable ways to show correlation between simulations and real operational scenarios.

### 4.9 922.11 Control Station Design

(1) General. Compliance with 922.11 is required for any RPAS that is to be used for a BVLOS operation. During BVLOS operations the remote pilot station is the only means an operator has of getting situational awareness of the operation and the state of the aircraft. The designer of the GCS needs to be mindful of the tasks performed by the operator and the information required by the operator during an operation. This standard is applied to all BVLOS operations to ensure that these considerations have been taken into account during the design of the GCS user interface.

The primary risks that this standard seeks to mitigate are those associated with "human error". These can be simple errors, such as typos when entering data into a system, or more complex interface-driven issues, such as instances where the crew misunderstands what an automated system is doing or should be expected to do. The consequences of these risks/errors can range from insignificant to catastrophic depending on the system design and other operational factors.

This type of standard can never completely mitigate all potential error mechanisms, as increasingly complex systems and new interface designs provide new opportunities for confusion and human error. However, this standard generates a requirement for system designers to follow a process that will minimize the number and consequence of errors.

This standard is also intended to ensure that the operator has all of the information and controls at his ground station required to accomplish the mission and deal with any failures or emergencies that may arise. In this respect, the standard is intended to include flight crew alerting aspects that might be traditionally covered under a Part 25.1322 Flight Crew Alerting analysis. In effect, a key task of all RPAS crew is the avoidance of hazardous operating conditions, and mitigation if those conditions are experienced. The designer of an RPAS station needs to ensure that their RPS provides the information required by the crew to accomplish these tasks. This information may take the form of warnings and alerts to the crew. RPAS designers are strongly encourage applicants to develop a flight crew alerting strategy similar to that described in Part 25.1322 and AC25.1322-1. However, applicants may elect alternate means of flight crew alerting depending on the specifics of their remote pilot station design.

In addition to "human error" and avoiding hazardous operating conditions, this standard seeks to ensure that the operator is provided with any other information and controls required to safely operate the RPAS. If an RPAS has specific environmental limitations that might need to be respected, analysis might show that sensors to detect hazardous conditions might be required and alerts be provided to the pilot. If there are regions of the flight envelope that are specifically hazardous for some reason, the design of the remote pilot station should include alerts to allow the pilot to avoid these conditions.

(2) Expected Means of Compliance. To be most effective, the human factors aspects of the RPAS design should be considered as early as possible in the design process. In consultation with the notional CONOPs, applicants need to consider tasks that the flight crew will be expected to complete, and the information and controls required to complete those tasks.

At minimum, the evaluations to show compliance to this standard should include the following:

(a) Identification of the system / component intended functions.

(b) Some form of work analysis to identify the RPAS crew tasks associated with each intended function.

(c) Some evidence that the design follows human factors principles/heuristics (e.g., information & controls are labeled, feedback is provided in a timely fashion when controls are used, etc.)

(d) Some evidence of evaluation with representative users in a sufficiently representative operational environment.

(3) Minimization of Pilot Errors. Failures and errors are an inevitability in any operation, the goal of warning and alerting systems is to minimize their occurrence commensurate with their impact on the safe flight and operation of the RPAS. The design should therefore be subjected to reviews, assessments, and testing to assure critical information for safe operation is presented to the pilot in an intuitive form while minimizing the occurrences of erroneous or misleading information.

(4) Methods of Evaluation. Evaluation of the warning and alerting systems should be done in conjunction with flight tests evaluating the handling qualities of the aircraft in order to evaluate the human machine interface and handling qualities during the RPAS development. The guidance in FAA AC 25.1322-1 – Flight Crew Alerting is appropriate for the design of warning and alerting system.

(5) Human Machine Interface. In order to evaluate the various capabilities of the aircraft and their impact on the pilots, the manufacturer should split the operation into discrete tasks (e.g. perform pre-flight check, perform a take-off, recover from lost link). These tasks should have procedure definitions with acceptable performance criteria identified. These tasks should be broken down to a level in which the targeted user class (e.g. experienced RPAS pilot, beginner RPAS pilot) can understand the steps to accomplish the task. In order to evaluate the pilot workload associated with the task, the Bedford Pilot Workload Rating Scale (Figure 1 – Bedford Pilot Workload Rating Scale) is recommended to guide test pilots evaluation of the suitability of the design to perform the task. While it is acknowledged that Human Machine Interfaces (HMI) continue to evolve in layout and symbology, in the absence of standardized user interfaces MIL-STD-1472 (current version) – Design Criteria Human Engineering – is a good guide for the design and evaluation of human responses. In general, due to the nature of HMI being primarily software based, the interface should continue to evolve to meet the needs identified by the user base over the development lifecycle.

(6) Handling Qualities. While it's expected that many RPAS designs will be highly automated, there may be aspects of the RPAS, or modes of operation where the pilot is directly involved with the control of the aircraft. In such cases, handling qualities of the system should be assessed to ensure that they do not place unreasonably high skill, workload, or concentration requirements on the crew. The current aviation standard for evaluating the handling qualities of aircraft is the Cooper-Harper rating system. While performing flight envelope maneuvers and piloting tasks (as recommended above), it is recommended the test pilot evaluate the ease of use of the system using the Cooper-Harper, Cranfield Aircraft Handling Qualities Rating Scale, or other equivalent evaluation methodology. The results of these tests are to be evaluated and additional design or implementation refinement should be made to resolve identified issues. It is expected all piloting tasks fall within the range of 1 to 6 on the Cooper-Harper scale for the system to be considered acceptable. When tasks have an evaluated value between 4-6, it is recommended that operational limitations, guidance, or procedures be provided in the operator's manual to help prepare pilots to manage workload around those tasks.

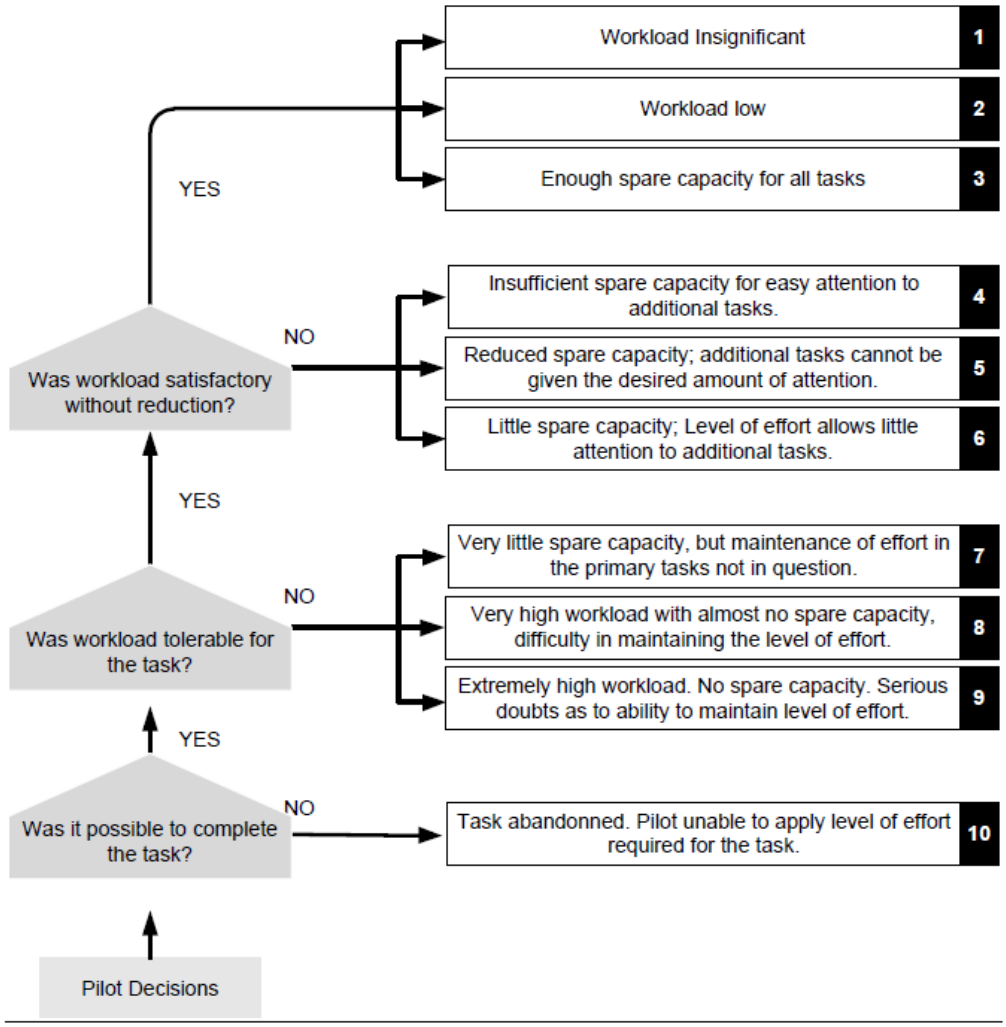



**Figure 3 – Bedford pilot workload rating scale**

### 4.10 922.12 Demonstrated Environmental Envelope

(1) General. Compliance with 922.12 is required for all BVLOS operations that are within 1km of populated areas, or over sparsely populated areas. CAR standard 922.12 is intended to ensure that RPAS used for specific BVLOS operations has a well-defined flight envelope, that has been demonstrated through flight test. It is not required for VLOS operations, as the visual nature of the operation makes it easier to determine when the RPAS is being negatively affected by environmental conditions than a similar operation performed BVLOS. A key aspect of the definition of VLOS is that visual contact is maintained with the RPA sufficient to maintain control of the aircraft. This requirement forces the RPAS to be close enough to the nearest observer that the environmental conditions at the observer would be the same as those at the RPA location, and the observer would clearly be able to see when the RPA is being adversely affected by environmental conditions to the extent that safety is affected. Therefore, for VLOS operations, it is assumed that the operator will have sufficient situational awareness of the operation to ensure that the RPAS is operated in environments in a safe manner. Furthermore, Part IX rules for VLOS operation of <25kg RPAS require that manufacturers define the effects of foreseeable weather conditions on the RPAS (ref CAR 901.200(c)(iv)).

In Isolated-BVLOS operations, any hazard that might be created by environmental factors (rain/wind/ice/EMI/etc.) is limited because the operation is away from people not involved in the operation. A crash caused by high winds, icing, or other environmental factors is not likely to harm anyone due to the isolated nature of the operation. Environmental factors leading to a crash are also unlikely to result in a flyaway that sends the RPA outside the operational volume because of the Isolated Operation standoff distance of 1km from sparsely populated areas. If an RPA design is such that exceedance of an environmental condition could lead to a flyaway further than 1km (icing of the control surfaces causing lockup, wind greater than RPA capabilities, etc.) it is assumed that these conditions would be mitigated in the design (i.e. flight termination system).

For non-Isolated BVLOS operations, there may be people not involved in the operation close enough that they could be injured in the event of a crash. Furthermore, for BVLOS operations, the operator might be planning the mission based on weather reporting at locations that can't be observed from the GCS. The Demonstrated Environmental Envelope standard is required because it is more likely that the RPAS is operated closer to its environmental limits due to the remote location of the operating crew. The operator needs to know the environmental limitations of their RPAS and have confidence that the RPAS can handle the expected environmental conditions. The proposed 922.12 Demonstrated Environmental Envelope standard is applied to these operations for this reason.

(2) Expected Means of Compliance. To show compliance to CAR Standard 922.12 applicants should first refer to the Notional CONOPS for their particular RPAS. Using the Concept of Operations for their RPAS, applicants will derive the expected RPAS performance and environmental envelope that they expect their RPAS to encounter. Applicants should carefully consider any situations that their RPAS could conceivably encounter during their expected operations and derive required operational capabilities from those situations.

As mentioned, the first step to any 922.12 Compliance demonstration is to refer to the Notional Concept of Operations for the RPAS. This CONOPS should generally contain the set of all different operations that the RPAS is intended to perform. For an RPAS with a very targeted set of intended operations, this concept of operations may be very limited. On the other hand, for RPAS that are intended to operate as utility vehicles accomplishing many different missions, the CONOPS may be complicated and multi-faceted. Applicants should take care that any mission they want to allow their operators to accomplish is represented in the Notional CONOPS.

Once these required operational capabilities are derived, these operational capabilities will form the basis for a test campaign that demonstrates that the RPAS can be used safely for the intended notional CONOPS. The test campaign should be carefully designed so that all significant points in the flight envelope are evaluated. As the technical expert on the RPAS, it is up to the declarant to identify specific worst-case operating configurations and environments to be demonstrated.

It is also important to ensure that the RPAS being tested conforms with the RPAS that will be identified in the declaration. If there are any differences (i.e. tests are performed on a prototype test article that differs from the production standard), these can influence the results of the test campaign. Any differences must be documented and demonstrated to have no effect on the RPAS performance during the test campaign.

At the conclusion of the test campaign, the test results should demonstrate that the RPAS can safely accomplish the missions described by the Notional CONOPS.

(3) Expected Number of Flight or Ground Test Hours. There is no specific minimum number of required hours of flight test or ground test hours associated with CAR Standard 922.12, however applicants must take a systematic approach to the development of their test effort to ensure that there is adequate coverage of the RPAS flight envelope. Declarants are encouraged to use standards such as ASTM F3478-20 (or later revision) as a standard for developing their flight test program. Declarants should be able to show traceability between system and performance

requirements assigned to flight/ground test and the flight/ground test procedures themselves. Therefore, the extent of requirements to be tested, combined with the breadth of the environmental envelope to be verified will set the number of ground and flight test hours needed.

### 4.11 Classification of injury severity

(1) General. CAR Standards 922.05 922.06 and 922.07, as well as CAR 901.200(c)(v) & (vi) apply a scale to classify the injury that may be inflicted to a person on the ground as a result of a malfunctioning RPA. The classification of "severe injury" is selected for evaluating the maximum acceptable injury that may be sustained and establishes the objectives required to meet the RPAS safety assurance requirements for operations near and over people. The Abbreviated Injury Scale is the primary industry standard with respect to evaluation of injury, though this may not be the only standard for determining injury severity.

(2) Abbreviated Injury Scale (AIS). The AIS was introduced in 1969 to help physicians and medical professionals classify various types of injuries, and this scale has been used around the world for decades as the de facto standard in evaluating injuries. The current version recognized in Canada is AIS 2005 Update 2008, which classifies a Severe Injury (AIS-4) having a probability of death from the injury up to approximately 50%. The AIS is developed and maintained by the Association for the Advancement of Automotive Medicine (AAAM).

(3) Determining a Severe Injury. There are many methods by which an AIS-4 injury may be evaluated. For trauma injuries related to the impact of an RPAS, these have generally been considered with respect to the kinetic energy transferred from an RPAS to a person during an impact. There have been various levels of kinetic energy proposed related to when an impact may result in a severe injury, some of this is backed by laboratory research and field experience. This circular considers energy transferred to the head, neck, or chest of a person as the worst case that may result in a severe injury. Initial rule making activities in Canada (CARAC UAV Systems Program Design Working Group - Phase 1) and the United States (Micro-UAS Advisory Rulemaking Committee) identified 12J/cm$^2$ as being the maximum allowable during an impact to avoid a serious (AIS-3) injury. This value was notionally validated by the work done in the FAA ASSURE impact to persons on the ground research.

(4) Operations Near and Over People. CAR Standard 922.05 and 922.06 both identify the need to constrain the probability of a severe injury to "remote" for various failure modes. Development of an RPAS for these types of operations necessitates an evaluation of the capacity of the RPA to inflict sever injuries. It is acknowledged there are many design approaches may be used to minimize the injury severity in the case of failures. These include but are not limited to:

(a) Structural design features such as:

Soft materials; and/or

Frangible materials.

(b) Additional protective equipment such as:

Parachutes; and/or

Inflatable capsules (e.g., "airbag").

(5) Methods of Evaluation. The RPAS manufacturer must evaluate the probability the RPAS will cause severe or worse injuries. There are many types of tests, analyses, and/or evaluations which may serve this purpose. For RPAS which have significant service history and failure tracking there may be sufficient evidence to support compliance with the standards defined in CAR Standards 922. For designs which service history may not be available, or which operate over people, Appendix C provides guidance on a test procedure to evaluate the RPAS capacity for injury severity. Where tests have determined the inherent design characteristics of the RPA

will not result in a severe injury (e.g., test criteria falls within those defined in Appendix C) there is no need to evaluate the probability of failures (Appendix B).

# 5.0 RPAS design considerations

## 5.1 General

(1) The following guidance applies to the design and development of RPAS, and the definition of associated operating envelope and limitations. It provides guidance on the technical information that must be provided to operators. This technical information is instrumental in elaborating the Concept of Operations (CONOPS) intended for the RPAS, and the CONOPS is necessary for performing an operational risk assessment which may dictate safety features needed by the RPAS design and/or specific procedures or instructions for operation to mitigate identified safety risks. It is expected that manufacturers conduct their due diligence in designing, testing, and constructing RPAS to ensure their products are safe for use in their intended environment. As such, the guidance provided in this circular is intended to be scaled to the risks of the intended operations with the RPAS.

## 5.2 System design and description

(1) CAR 901.200(c) specifies the information that must be made available to each owner of a system subject to a declaration that is intended for Advanced or Level 1 Complex Operations. The purpose of providing this information is to ensure that operators of the RPAS have all the information needed to ensure that they operate the RPAS safely, and that the RPAS, as operated, continues to comply with the declared standards. Declarants need to ensure that any assumptions made during the verification of the RPAS are clearly communicated to the operator.

(2) Occasionally, the RPAS verification process may uncover new operating limitations or best practices to ensure that the RPAS accomplishes the CONOPS safely and complies with the declared CAR Standard. Declarants are expected to review and update their maintenance programs and operating manuals at the end of their verification activities to ensure that they are complete and correct.

(3) Declarants should ensure that maintenance and operating instructions address not only flight operations, but all parts of the RPAS service life. If there are specific storage or transportations requirements, these need to be identified and communicated. Examples of this could include:

- (a) Environmental (temperature, humidity, vibration) limits for storage.
- (b) Care and maintenance required if the RPAS is not operated for long periods (i.e. battery maintenance, parachute repacking, etc.)
- (c) Overhaul or replacement times that depend on operating environment (i.e. filter changes in sandy/dusty environments). If certain operations decrease overhaul times.

(4) This material may be provided in electronic format (e.g. operating manual and/or maintenance manual available on the manufacturer’s website) or in a physical format (e.g. paper manual), but the information must be provided to each owner in a form that is easily accessible. In addition, the operating manual should be written in a way which allows it to be understood by the target consumers (e.g. the general public, vs. specially trained pilots).

## 5.3 Safety assurance requirements

(1) It should be noted that for the lowest risk operations, namely small RPAS operated VLOS, the safety assurance requirements effectively map directly to the type of operation. Small RPAS VLOS operations in controlled airspace need a declaration for CAR Standard 922.04 “Controlled

Airspace". VLOS Operations using sRPAS near people need a declaration for CAR Standard 922.05 "Operations Near People", and VLOS Operations using sRPAS over people need a declaration for CAR Standard 922.06 "Operations Over People".

(2) As the risk increases, the complexity of the operation also tends to increase, and a single performance-based standard is inadequate to address various aspects of the hazards related to the operation. For these higher risk operations, it should be noted that often there are several sections of CAR Standard 922 called out as requiring a declaration. The exact MoC for each standard will often depend on the exact details of the RPAS and any limitations of the operation – these details should be described in the CONOPS associated with the declaration.

(3) Applicants are encouraged to use industry standards when applicable as means of compliance to sections of CAR Standard 922. A list of recognized industry standards can be found in Appendix A of this document. For Declarations (not pre-validated) it is the responsibility of the declaring entity to determine that the standard used is applicable and adequate to the CONOPS, and the CAR Standard being declared against. For pre-validated Declarations, the applicant is required to propose the standards they intend to use, and the applicability of the proposed standard to the RPAS and CONOPS under consideration is subject to acceptance by Transport Canada before a declaration can be made.

(4) For small RPAS operating VLOS, the following sections of Standard 922 are applicable.

(a) 922.04 for operations in controlled airspace

(b) 922.05 for operations near people

(c) 922.06 for operations over people

(5) As the type of operation increases in complexity and risk, the relevant sections of CAR Standard 922 become more performance-based, and the specific applicable sections depend on the exact CONOPs (refer to the tables in Section 3.0 above). Depending on the operation, one or more of the following sections of CAR Standard 922 may be applicable:

(a) 922.07 for Safety and Reliability

(b) 922.08 for Containment

(c) 922.09 for Command and Control Link Reliability and Lost Link Behaviour

(d) 922.10 for Detect, Alert and Avoid Systems

(e) 922.11 for Control Station Design

(f) 922.12 for Demonstrated Flight Envelope

(6) Compliance with these technical requirements must be demonstrated by the RPAS manufacturer using adequate means and methods. For all declarations, per CAR 901.201, the means and methods of compliance must be documented and provided on request to the minister for review.

### 5.4 RPAS design characteristics

(1) General. The design process requires a well-defined CONOPS. The CONOPS includes a description of intended operation of the RPAS, the operational environment, notable hazards associated with the operation, and procedural and tactical risk mitigations. This should be the manufacturer's first step to collect and provide sufficient technical information regarding the operation. Information in the CONOPS will define the flight envelope.

A flight envelope is the set of operational limitations that determine the ideal flight characteristics of the aircraft as well as those which will exceed the aircrafts design limitations and result in a loss of the aircraft, or a loss of controllability. The extent of envelope is constrained by both the physical design of the RPA as well as the operational environment in which the system is

designed to fly. The following sections are intended to guide the evaluation of the design of an RPAS such that a safe flight envelope can be developed and the operational limitations can be communicated to pilots. The information required by CAR 901.200(c) forms what is, in essence, the RPAS flight envelope as it should be communicated to pilots as limits of the system which should not be exceeded. This section provides additional guidance on the requirements in CAR 901.200(c) as well as acceptable methods of compliance to these documentation requirements.

(2) Process. This section discusses the process to determine the physical design of the RPA and define the controllability and performance limitations identified in CAR 901.200(c)(ii) and (iii). The process to develop the limitations of the airframe should follow a standard engineering development approach. While there are many industry standards which outline a general process for system development (e.g. SAE ARP-4754) for the development of an airframe the process to follow can be generally outlined in the following iterative steps:

(a) Define the expected performance. Performance is generally refined from a high level concept of operations the system is attempting to satisfy, and the performance requirements can typically be clearly defined (e.g. “RPAS must fly 3km round-trip within 15 minutes, 250ft above the ground, and stay on-site for at least 15 minutes”). The general requirements of system operation then lead to the selection of a general design concept (e.g. fixed-wing vs rotary-wing vs hybrid vs lighter-than-air), and identification of the manufacturing needs which typically lead to material selections. Flight dynamics can then be assessed once these general performance requirements have been identified.

(b) Define the expected loads. With the performance criteria and general design selected, the next step is to clearly define the aerodynamic loading on the airframe. Aerodynamic loading is derived from the maximum operational velocities and altitudes needed to achieve the operational performance requirements. For example, limit height and speed need to be defined, including hover, under which a forced landing cannot be made under the applicable power failure condition. Thus, the maximum operational loads the airframe can withstand in flight, at each critical combination of altitude, speed, weight, centre of gravity, and payload configuration are identified.

(c) Model/Prototype the system. The loading and system design features (e.g. C2) are then applied to a model or prototype of the system to determine the reactions of the system and whether any design changes should be made. There are many ways of modeling or prototyping. Generally, computer models are used when creating new designs to avoid having to create multiple prototypes which can become costly. If a design is being incrementally updated it may be easier to build a prototype of an existing, earlier model to evaluate the changes.

(d) Identify a sufficient number of points within the design envelope to ensure that the maximum load for each part of the RPAS structure is achieved.

(e) Identify Critical Parts (CP) and Primary Structural Elements (PSE) – For operations near and over people, the models and/or prototypes are used to determine which parts of the RPAS design lead to catastrophic failures (refer to Appendix B), as well as which portions of the airframe are critical to the continued safe flight of the RPA. These are termed Critical Parts and Primary Structural Elements respectively.

(f) Validation of the model/prototype. Once the model/prototype has been produced and the design confirmed (at least mathematically) the results of the simulations and/or construction are to be validated. Validation of the model/prototype is key in the design process as it allows a manufacturer to confirm their calculations and provide a clear path to support design changes as the design is iterated. At least the loading on the CPs and PSEs are measured during the validation to ensure elements related to safety of the aircraft are well defined. There are multiple ways of validating a model; three of these methods are identified below:

Ground Testing – a ground test can provide useful information on early stages of the development such as behaviour of the subcomponents, a Building Block Approach (BBA) is a good system to understand how the airframe may meet the requirements.

Wind Tunnel – a wind tunnel test with either a prototype or scaled version of the RPA allows for dynamic loading to be evaluated in a controlled and well measured environment. A wind tunnel allows a manufacturer to very carefully control the aspects of flight in order to validate well defined test points in a model; and

Flight Test – a flight test protocol with a functional representative prototype allows for a combination of systems testing as well as aerodynamic model validation. While the conditions cannot be as well controlled as in a wind tunnel, a well-designed flight test protocol, along with sufficient test instrumentation, allows for the manufacturer to validate some model test points as well as validate broader RPAS functionality.

(g) Evaluate against Safety Assurance Requirements. The results of the validation of the model and the results of the simulation and/or flight testing are then evaluated against the safety assurance requirements and other safety objectives derived from a system safety assessment process to ensure the failures have been clearly identified and the hazards are well controlled and understood.

(h) Iterative Reviews. While this is identified at the end of the process, as mentioned above, iterative reviews may occur at any point during the design process. As issues are identified design changes or model updates may be required which would require additional execution of simulations, and/or additional validation.

(i) Definition of Operating Limitations. With the modeling complete on the design, the limitations (as identified in CAR 901.200(c)) must be documented and provided with the operating manual. The physical operational limitations identified as part of this process are one section of operational limitations, and for RPAS being declared for operations near and over people additional steps are taken to fully define the limitations. See section 6.0 for additional discussion on design requirements which will inform further operational limitations.

(j) Human Factors Evaluations. Systems are ideally developed to be controllable without undue piloting skill or training. This can be interpreted, for example, as the RPA controls are manageable, the system status is clearly discernible, and operational information is readily available. The pilot-system interface is designed and evaluated using methods collectively referred to as “human factors”. In determining the flight envelope, in addition to the technical capabilities of the aircraft, the ability of pilots (or supporting systems) to keep the aircraft within this flight envelope/be recoverable when reaching the edges of the flight envelope is developed and evaluated. Guidance on developing systems to account for human factors performance can be found within ISO 9241-210 and/or MIL-STD-46855A. For additional information related to warning and alerting see section 5.4.6 of this circular.

**Note:** There are many industry standards which outline a general process for system development (e.g. SAE ARP-4754 is well recognized for manned aircraft).

(3) Modes of Operation

(a) General. RPAS are typically capable of multiple modes of operation (e.g. remote controlled flight, assisted manual flight, automated waypoint tracking). All unique modes of operation should be included in the operator manuals including their limitations and expectations (e.g. user experience requirements, default modes). Operation of flight

controls and safety devices (e.g. parachutes, flight termination technologies) should be clearly identified within the operating manual as well as limitations of these systems imposed by different operational modes. As part of defining the operational modes the operating manual should clearly identify the minimum number of engines required to remain airborne.

(b) Human-on-the-Loop (HOTL) operational modes are defined as those types of operational modes in which the RPAS is the primary decision-making platform and the operator is actively monitoring the operation of the platform ready to take control in the event the operator determines the system operation requires intervention. In most cases the human plans the operation using flight planning software and uploads the flight plan to the RPAS which follows the plan to the best of its ability given the active environmental conditions. These operations differ from Human-in-the-Loop (HITL) operations in which the operator has direct positive control of the system and is directing the flight whether through controller inputs or through waypoint identification. For HOTL operations the operating manual should clearly define the necessary steps to plan, upload, and monitor the flight plan along with procedures to identify when issues arise throughout the process.

(c) Night Flight. If the aircraft is capable of safely operating at night the operating manual should clearly identify the configuration and limitations associated with night operations. For night operations CAR 901.39(1) requires that the RPA is equipped with position lights sufficient to allow the aircraft to be visible to the pilot and to any visual observer. There are no specific standards defined for the colour, positioning, or number of position lights, however the intent is to have lighting sufficient for it to be clear to the pilot which way the system is oriented while in flight. The position lighting needs to be sufficient for the pilot to exercise their 901.11 VLOS responsibilities (i.e. be able to maintain control of the aircraft, know its location, and be able to scan the airspace in which it is operating in order to perform the detect and avoid functions in respect of other aircraft or objects).

It's acknowledged that for some specific operations (i.e. drone light shows), the night lighting might not be primary means of fulfilling the pilot 901.11 VLOS responsibilities. In these cases, it's important that the operating manual clearly indicates any specific processes or procedures required to ensure safety during periods when the aircraft is operated with the lights off.

For CONOPS where the position and night lighting might be observed/interpreted by traditional aircraft pilots, applicants are encouraged to model their lighting systems after traditional aviation standards (red on port, green on starboard, white light pointing aft).

For an aircraft to safely operate at night, the lights should be bright enough to see from a distance and the lights cannot blind the pilot during landing. One way to meet these criteria by dimming the lights before landing.

(d) BVLOS Anti-Collision Lights. CAR 901.38.1 requires that all RPAS conducting BVLOS operation be equipped with anti-collision lights and that these lights be turned on during the BVLOS operation. CAR 901.38.1(2) provides operational performance requirements for these lights. Anti-Collision lights used for compliance with this CAR must be:

1. White
2. Be visible in night vision goggles (if BVLOS operations are expected to occur at night).
3. Flash at a rate between 40 and 100 flashes per minute.
4. Be visible in all directions within ±75° of the horizontal plane of the aircraft with no more than 0.5 steradians obscured in any direction.
5. Be visible at distances up to one statue mile.

Depending on the configuration of the RPA, designers have the option of meeting the 901.38.1 requirements using more than one light source (i.e. using a top and bottom anti-collision light). Designers also have flexibility on the Means of Compliance to meet these standards. It's expected that these performance requirements will be verified using a mix of analyses, product specifications, and ground and flight demonstrations.

(4) Environmental Effects

(a) General. CAR 901.200(c)(iv) identifies that the effects of foreseeable environmental conditions on the performance of the aircraft and the pilot-in-command must be established. These requirements identify the responsibility of the manufacturer to define how the RPAS is affected by the world around it, and communicate that information effectively to the operator through associated documentation (i.e. operating manuals). This supports CAR 901.31 which requires that the operation be conducted in accordance with the operating limitations and instructions established by the manufacturer.

(b) CAR Standard 922.12. For operations where CAR Standard 922.12 – Demonstrated Environmental Envelope is applicable, the consideration of environmental effects must go further. For declarations to 922.12, the declarant must consider the intended environmental envelope of the RPAS and demonstrate through ground and flight testing that the RPAS is capable of safe operations in those conditions. Even when CAR Standard 922.12 is not a requirement, declarants are encouraged to refer to that standard and associated guidance for best-practices when validating that their RPAS is capable of safe operation in conditions expected to be encountered.

(c) Meteorological Conditions

(i) General. The part of the environment which has the largest impact on the operational characteristics of the RPAS is undoubtedly the effect of weather (both macro and micro weather environments). While it is noted most RPA which weigh less than 25 kg will have a limited ability to operate in inclement weather it is incumbent on the manufacturer to clearly identify the specific limitations associated with a given model of RPAS in their operating manual.

(ii) Wind. Effects of wind on the safe operation of the RPAS should be clearly identified. Specifically, the strongest wind the aircraft can safely operate in without losing control of the platform. In addition, the maximum gust loading the RPA can withstand before losing structural integrity should be identified if it is less than the winds affecting the controllability of the RPA. Any limitations on controllability in turbulence and environments such as wind in urban canyons should be considered. Finally, effects of the wind conditions on the flight time of the aircraft may be identified. It is expected that operators have a clear understanding of the effect of wind on aviation, and that flying in wind will have operational effects, additional information on specific performance degradation as a result of winds may prove helpful to operators when conducting flight planning activities.

(iii) Temperature. Effects of ambient temperature on the safe operation of the RPAS should be clearly identified. Ideally this would simply be an operational temperature range specifying the ranges in which the aircraft can be safely operated. This range would be based on the rated temperature ranges of each of the components and a technical evaluation of how these components function together within the larger system. In most cases the temperature effects on the control surfaces of the aircraft (e.g. ailerons, rotor blades), the motors, and the fuel systems (e.g. batteries, fuel lines) would be the limiting factors, though effects on the transceivers for the C2 link and navigation systems would need to be considered as well. While the intention is to provide operators with limits of the

aircraft that impact safe operation, other limitations such as safe storage temperatures should be provided when applicable. Other configurable elements of the RPAS may also have temperature limitations that need to be described to the operator (i.e, minimum storage temperatures for parachutes, payloads or ground support equipment).

(iv) Air Density. Effects of the air density on the safe operation of the RPAS should be clearly identified. In general air density is related to the altitude of the operation as well as the ambient temperature and humidity of the air. Air density is an important factor in fixed wing, rotary-wing, and lighter-than-air aircraft operations as it directly impacts the generation of lift in heavier-than-air aircraft and on the relative lift generated by lighter-than-air aircraft. While the intention is to provide operators with the limits of the aircraft that impact safe operation (i.e., densities where not enough lift may be generated or sustained), additional performance limitations that occur as a result of air density may be identified such as higher take-off velocities, changes in stall characteristics, or limits on operational range.

(v) Precipitation. Effects of precipitation on the safe operation of the RPAS should be clearly identified. Precipitation (drizzle, rain, fog, snow, freeing rain, etc.) can affect an RPAS in a number of ways including, but not limited to, limiting the actuation of control surfaces, degrading the C2 link capability, reducing the lift experienced by the aircraft, and shorting electrical systems. Each RPAS design will have different capabilities, and different protections against, specific types of precipitation. The types of precipitation to consider when designing protective system include:

1. Drizzle;
2. Rain;
3. Fog condensation;
4. Freezing drizzle;
5. Freezing rain;
6. Rain and snow mixed;
7. Snow;
8. Snow grains;
9. Ice pellets/Sleet;
10. Hail;
11. Snow pellets/graupel; and
12. Ice crystals.

While the impacts of specific types of precipitation on a specific RPAS design will vary, the expectation is for manufacturers to communicate which types of precipitation their systems are capable of operating safely, and in which their capability is degraded to such an extent that safe operation is no longer possible. Precipitation would need to be taken into account along with other operating limitations (e.g. wind, altitude) in order to fully describe the precipitate environments in which the RPAS may safely be controlled. While the intention is to provide operators with the limits of the aircraft that effect safe operations, additional performance limitations may be identified such as reductions in operational range/altitude.

**Information Note**: If the RPAS is designed for operations where it may reasonably be exposed to saltwater (e.g. littoral operations) the precipitation conditions above, especially fog, should be evaluated with respect to a saltwater environment. It is recognized that salt spray and salt fog constitute special consideration on the reliability and function of an RPAS.

(vi) Vibration. The effects of vibration on the RPA shall be evaluated and mitigated to ensure safe operations throughout the flight envelope. Vibrations generally result from the operation of the RPA itself. Vibration has two primary impacts on the operation of the RPA: structural fatigue failure and controllability.

(A) As sources of vibration and of dynamic loading of materials have increased, fatigue failures have become increasingly important in engineering. Technological developments continually bring out new materials, new fabrication processes, improved design concepts, and additional information about service requirements. Effects of vibration on structural integrity shall be addressed as part of the RPA structural design. Trends in design and in operations indicate new complexities are certain to arise. Some of these trends are: higher design stresses, requirements for increased performance, and demands for increased operational flexibility. Moreover, special flight vehicles, such as rotary-wing aircraft, VTOL and STOL aircraft, present special problems.

(B) Changes in takeoff and landing speeds result in more severe taxiing loads, maneuvering loads, and landing dynamic loadings (catapult takeoffs and arrested landings are particularly severe).

(vii) Icing. CAR 901.35 identifies that no RPAS shall be operated where icing conditions exist or may reasonably exist without associated detection or protection equipment. Icing detection means allow for the identification of the accretion of precipitate on the control surfaces or other critical flight surfaces of an aircraft. Icing protection equipment is equipment which prevents the accretion of precipitate or reduces the rate of precipitate accretion on control surfaces or other critical flight surfaces. At the moment there are no recognized industry standards or technologies for the detection or prevention of icing on small RPAS, though it is expected that solutions will become available as the market expands and is further refined. As research and development related to icing progresses this circular will be updated to reflect the results to aid in the design and implementation of icing detection and prevention systems on small RPAS.

(d) Electromagnetic Environment

(i) General. RPAS inevitably operate within an electromagnetic (EM) environment. The airspace in which RPAS operates is bombarded by electromagnetic radiation from both cosmic (e.g. solar radiation) and terrestrial sources (e.g. cellphone towers). While the operator is expected to have some knowledge of EM interference and system susceptibility, most will rely on limitations and recommendations identified in material provided by manufacturers. As a result, impacts from the EM environment on the operation of the RPAS are to be communicated via the operating manual.

(ii) Electromagnetic Interference (EMI). Electromagnetic radiation interacts with all electronic circuits, unshielded current conducting materials, and other electromagnetic fields. This interaction may result in a number of unintended effects in RPAS functions and should be accounted for in both design and operation if protections (e.g. shielded conductors) are not in place. Some common sources of EMI which may affect RPAS are listed below:

1. Wi-Fi transmitters;
2. Microwave radio relays.
3. Cellphone radio towers;
4. Industrial, commercial, or private Supervisory Control and Data Acquisition (SCADA) systems;
5. Lightning (see below);
6. On-board devices (e.g. Bluetooth payload and C2 link).

During design of an RPAS, designers must consider EMI when choosing the layout and configuration of sources and receivers of EMI. Antennas generally need a clear light of sight to the sink and source of their transmitted and received signals respectively.

Evaluation of the impacts of EMI on RPAS functions should be identified based on the components of the system which may be affected: the C2 link, the RPA, and/or the Control Station. It is important to evaluate the effects on all these systems as each may be susceptible to interactions from different frequencies in the EM spectrum, and the impacts may result in different limitations to the RPAS operation.

With respect to effects of EMI on the RPA the evaluation should be focused on safety critical systems (e.g. flight control electronics/actuators, navigation electronics, C2 transceiver) as defined in the system safety assessment (refer to Appendix B). One common area of interference is when swapping payloads; it is recommended manufacturers provide clear descriptions of the types of payloads and the impacts their operations may have on the RPAS.

With respect to effects of EMI on the Control Station the evaluation should be focused on the risk of interference caused by positioning of the Control Station antenna in relation to potential sources of interference including radio-frequency (RF) reflectors (i.e. ground planes). Specific limitations would depend on the frequencies and designs chosen for C2 link.

With respect to the C2 link interference the evaluation should be focused on specific frequencies chosen for C2 link operation and associated sources of interference. The impacts (e.g. reduced operational range, degraded payload performance) should be clearly communicated as a risk to the operation to assist operators in planning their flights. It has been noted during operations EMI can be a significant source of unexpected link interruptions, which can lead to a loss of positive control (e.g. lost link) and invoking automated return-to-home or link recovery procedures in situations where these procedures may be undesirable.

(iii) Lightning. In general it is not recommended to operate RPAS in conditions where lightning may be present. If manufacturers design systems to operate in thunderstorms, lightning storms, or other conditions where lightning may be present, it is recommended the impact of lightning on the RPAS systems be clearly explained in the operating manual. While most RPAS will not be designed to survive a direct lightning strike, there may be system architectures which allow for a safe recovery of the system. If an RPAS is being designed for operation in an environment where lightning effects are expected, then the impact of transients induced by lightning on the RPAS functions should be evaluated.

(e) Methods of Evaluation. In order to communicate the limitations noted above, the manufacturer is expected to undertake appropriate testing and evaluation to show that these limitations have been established for each intended configuration of RPAS. It is

acknowledged there are many forms of testing and evaluation that the manufacturer/designer/verifier may choose in establishing limitations. For aeronautical products RTCA DO-160 (current revision) is the de facto standard for environmental testing (outside of flight testing). In the case of RPAS, DO-160 may provide a significant cost especially when considering operations that may not necessarily be safety critical. With this said, the standard provides a good starting point for developing and evaluating RPAS specific methodologies.

With respect to evaluating the impacts of environmental limitations, especially as they are related to EMI, it is recommended that RPAS manufacturers conduct a system safety assessment to identify safety critical functions of the system from which equipment qualification requirements could be derived. As part of a system safety assessment, a functional hazard assessment contributes to identifying specific functional hazards related to operation of the system.

Finally, for those RPAS that require declarations or pre-validated declarations to CAR Standard 922.12, it is required that the environmental limitations be demonstrated through ground and flight testing of the RPAS. The specific ground and flight tests required will depend on the details of the declared environmental envelope.

(5) Hazards Identification

(a) Hazards to RPAS Crew. CAR 901.200(c)(v) requires that the characteristics of the system which may result in a severe injury (see section 6.4 of this circular for the definition of severe injury) to the RPAS crew members during normal or abnormal operations must be identified. There are a number of hazards which may result from operations of RPAS including but not limited to: electric shocks, lacerations, trauma injuries, and burns. In order to prevent injuries when operating and maintaining the RPAS, the characteristics of RPAS sub-systems (e.g. voltages) should be clearly identified to operators, and instructions for the safe handling, operation and maintenance of the systems and sub-systems should be provided.

With respect to abnormal operations, the intent is for manufacturers to provide information to safely handle an RPAS when it is in a mode of operation posing a safety risk to the RPAS crew or other people associated with the operation. While it is noted there is an assumption of risk when an individual is involved in the operation of an RPAS it is expected that manufacturers will perform due diligence to help ensure operators have the information required to effectively address emergency situations. To this end the manufacturer should provide the operator with checklists outlining emergency procedures related to situations resulting from technical issues in which the RPAS operation becomes unsafe. Some examples of emergency situations include: loss of C2 link, loss of one or more motors, loss of control in-flight (e.g. flight controls), loss of navigation (e.g. GPS).

**Information Note:** The manufacturer need not provide procedures to address hazards when features implemented in the design are intended to prevent their occurrence. For instance, a flight envelope protection function that prevents the aircraft from stalling would obviate the need of stall prevention procedures.

(b) Hazards to Persons on the Ground. CAR 901.200(c)(vi) requires that design features and their associated operations, which are intended to protect against injury to persons on the ground must be identified. In conjunction with the hazard identification above, failures of elements of the RPAS that may pose a hazard to people on the ground. These specific features intended to mitigate against the hazard to people on the ground implemented in the RPAS design (e.g. parachutes, rotor guards) are clearly identified in the operating manual. Procedures associated with the operation of these safety features and emergency procedures with respect to handling the RPAS in the case of abnormal

operations should be clearly communicated in the operating manual; emergency checklists and automated warnings/procedures displayed on Control Stations are acceptable methods of communicating this information to pilots. While the safety assurance standard only requires the assessment of hazards of injury to people within the identified operational environment, it is recommended to evaluate and communicate safety impacts to any potential people on the ground identified as a result of a comprehensive system safety assessment.

(c) Methods of Evaluation. To aid in the identification of system hazards it is recommended that manufacturers complete a functional hazard assessment. The functional hazard assessment relates the functional failures to hazard criticality classifications from which safety objectives are allocated to the design and operation of the RPAS. The design is further decomposed into the specific technologies to identify specific modes of failure which can cause or contribute to the functional failures. The safety objectives that must be demonstrated are outlined in Appendix B.

(6) Warnings and Alerts

(a) General. The remote nature of RPAS control stations result in the separation of the pilot from the physical environment of the aircraft. As a consequence of this physical decoupling, the pilot no longer has the acoustic, visual, or haptic feedback associated with the airframe and on-board equipment and so relies solely on the information presented on the Control Station (CS). The sources of this information are either systems on-board the aircraft transmitted over the C2 link or computations performed by the CS itself (e.g. controller battery power, analysis of data received from the aircraft). Safe operation is predicated on information presented by the CS to the pilot. CAR 901.200(c)(vii) requires manufacturers to identify applicable warning information provided to the pilot in the event of degraded system performance which results in unsafe operating conditions. For example: for electrical engine applications, a minimum voltage threshold that indicates low remaining capacity should be determined in the worst environmental conditions. A low battery warning is provided in the CS in order to alert the RPA operator that the battery has discharged to a level which requires immediate RPA recovery actions. The procedure to be followed in case of low battery warning is established and provided in the operating manual.

(b) Control Station Design: For systems that require a declaration against CAR Standard 922.11 Control Station Design, it is expected that a thorough analysis of the Warnings and Alerts will be conducted. Dealing with abnormal operating conditions, and the associated warnings and alerts can be time critical, and often leads to high workload situations where the crew requires a rapid understanding of the RPAS status. It is expected that the Control Station Warning and Alerting scheme be designed so that it can support the crew during these situations. For compliance to CAR Standard 922.11, a detailed task and human factors analysis is expected that shows that the warning and alerting strategy of the control station assists the crew in completing their duties. Even for systems not requiring compliance with CAR Standard 922.11, designers are encouraged to have a systematic process for demonstrating that the CS meets crew needs and presents information to the crew in a timely and clear manner.

(c) Alerting. Alerts are to inform the pilot of system malfunctions or unsafe conditions (e.g. low fuel, degraded C2 capability) thereby appropriate actions may be taken. In addition, the alerts should be conspicuous and intelligible to the pilot under all foreseeable operating conditions, including conditions where multiple alerts are provided. Alerts should be removed when the alerting conditions no longer exist. In order to support timely pilot decision making, alerts should provide timely attention-getting cues when taking into account normal piloting operations and workload. Alerts should also not be so frequent that the pilots are overloaded with information, or prone to ignoring nuisance alerts. Alert

prioritization and alert suppression may be employed when the conditions warrant. The suppression mechanism should not allow for inadvertent or reflexive suppression of the alerts as the goal is to present the information for pilot action. Finally, the operating manual should clearly define all the alerts that may be displayed including their impacts to the operation of the RPAS and the required pilot actions.

(d) Prioritization. Alerting schemes should have priorities related to the types of information they display in order to ensure that spurious, or nuisance alerts are minimized in order to assure timely pilot response to conditions when they occur. The following hierarchy of alerting prioritization is suggested as an aviation best practice:

(i) Warning Alert: For conditions that require immediate pilot awareness and immediate response;

(ii) Caution Alert: For conditions that require immediate pilot awareness and subsequent response; and

(iii) Advisory Alert: For conditions that require pilot awareness and may require subsequent response.

(e) Marginal Performance. Part of the purpose of the alerting system is to make the pilot aware of the status of the RPAS such that they can confidently make decisions regarding the continued safe operation. To that end it is recommended that alerting systems include alerts (advisories) which provide an indication that a flight critical system (e.g. Navigation, C2 Link, battery), as determined by the system safety assessment, is operating at marginal capacity. Some examples of degraded or marginal performance include:

GNSS errors including GNSS satellite errors such as gravitational effects (which pull the satellite from planned orbital path), and GNSS dilution of precision (DOP) when the geometries of available satellites do not provide sufficient coverage to meet navigation precision.

Navigation/Orientation errors such as pitot/static obstruction which can lead to invalid airspeed/altitude readings, and Inertial Measurement Unit sensor faults/drifts.

Errors caused by the terrain such as terrain masking, where the landscape (e.g. mountain) blocks the antenna on the RPAS from receiving the satellite signal, and “multi-pathing” where a signal is reflected by the landscape such that the receiver now receives “additional” signals which can create confusion and need to be processed out to avoid creating position errors.

Degradations in C2 link bandwidth and responsiveness cause by unknown or uncharacterized sources of interference (e.g. RADAR), or operating near the edge of range.

(f) Reserved

### 5.5 Human Factors and Usability

(1) The User Interface for the crew requires special consideration for RPAS that receiving a declaration to CAR Standard 922.11, however this aspect of the RPAS design is of high importance to all RPAS designs. It is considered best-practice for any RPAS design to perform a crew task analysis to ensure that the Control Station (CS) provides all information and controls to the crew in a manner provides the most clarity while minimizing crew fatigue and confusion.

(2) Declarants should refer to guidance related to CAR Standard 922.11 (refer to Section 4.9) and related standards to assist them in their design of the CS. A methodical approach to the human factors aspects of an RPAS design should be considered even for RPAS that do not require declarations to CAR Standard 922.11.

(3) Extra care should be taken with displays and the units being used on those displays. Traditional aviation does not use the SI units, so these units are may not be ideal if the RPAS crew is expected to interact with traditional aviation.

(4) Applicants should refer to standards and practices used in traditional aviation cockpit design when implementing controls and indications, especially when the crew is expected to make time-critical decisions during emergency situations. Traditional aviation has developed standard practices such as colour coding, using multiple senses to communicate and prioritize warnings and alerts, and control standardization in order to minimize the occurrence of crew errors. RPAS designers are strongly encouraged to consider these best practices when designing their control stations.

### 5.6 Configuration Management and Reliability Tracking

(1) A manufacturer should have configuration control over their specific RPAS designs or specific element designs to have sufficient traceability to track the life of the RPAS and its components. Thus, configuration management is crucial in the establishment of service history tracking systems, and to the declaration filed to the Minister. The manufacturer may follow FAA AC20-153B, SAE EIA-649, ASTM, ISO or other equivalent industry standards in order to establish a configuration management system appropriate the risks of their declarations.

(2) Operators and manufacturers are recommended to use maintenance systems (e.g. traceability software) to track the configuration of in-service RPAS to track life-cycle data associated with the components. These types of systems are generally used in conjunction with aircraft health monitoring systems (AHMS) on-board the aircraft which allow for health and usage data to be connected directly to operational databases to support the lifecycle management of RPAS in service. The maintenance systems (either computer based or otherwise) should contain the configuration of the various operational RPAS in order to build a history of the actual life-cycle of the components, and systems in different operating environments. When the entirety of an RPAS fleet (either a specific operator, or as part of a manufacturer/designer sourced maintenance system) is tracked the reliability data will have the right level of sensitivity and accuracy needed for broad system life-cycle analysis. In traditional aviation, service difficulty reporting (SDR) is used to track issues experienced by operators and designers/manufacturers use this data to help determine root causes of issues and to understand the reliability of systems and system components. Information from SDR can be used to perform trend analyses of issues, defects, and failures to substantiate claims of reliability for operations near or over people.

(3) When an RPAS Declarant is not the manufacturer of the complete RPAS, it may be more difficult to have complete configuration control over all parts of the RPAS. This might be the situation for declarants who are declaring for a modification (i.e. an after-market parachute system), or provision of a service (i.e. DAA or C2 as a service). Ideally, the RPAS Declarant will have a relationship with the original equipment manufacturer to support their declaration. This could take the form of Application Programming Interface (API) documentation when developing add-on systems for the RPAS, or detailed specifications and tolerances that allow the applicant to understand any variations that might be present in the original RPAS. In these cases, the declarant should carefully consider what aspects of the RPAS need to be configured to support their declaration. For example, if the declaration relies on certain firmware versions, or certain operational limitations of the RPAS, then these need to be communicated clearly to the operator. In cases where a relationship with the original equipment manufacturer is not possible, it is the responsibility of the RPAS Declarant to perform any tests and analyses required to ensure that the final RPAS as declared (i.e. including their service or modification) meets the declared 922 standards.

### 5.7 Manufacturing

(1) When the declaring entity is the manufacturer of the RPAS, it is assumed that they are responsible for a product that complies with accepted manufacturing industry standards at the time of delivery is demonstrated as fit and safe for flight, and conforms with the design receiving the declaration.

(2) When required, the manufacturer will identify the materials and manufacturing processes used in the construction of the RPA and the criteria implemented to control materials performance variability among specimens. Materials are to be compatible with the usage spectrum. Manufactured parts, assemblies, and the complete RPAS are produced in accordance with the manufacturer's Quality Management System.

(3) For further manufacturing requirements and a list of TC acknowledged manufacturing industry standards, refer to AC901-001 - RPAS Safety Assurance Declaration and Pre-Validated Declaration Processes.

### 5.8 Aircraft serviceability

(1) Maintenance Manual. The RPAS shall have a maintenance manual (which may be part of the operating manual) that defines actions to be taken to keep the RPAS serviceable. Appendix A provides some acceptable means of defining maintenance tasks.

(2) In particular, the manual provides instructions for maintaining the serviceability of the RPA structure, engine, propeller and any subsystem for which inspection, substitution (e.g. life limited parts), adjustment, and lubrication are required. Declarants should pay special attention to areas and items that have historically caused safety issues such as connector security, wire chafing, Software/Hardware Version control, powerplant maintenance and tuning. For these and other aspects of the RPAS, detailed maintenance procedures should be developed and provided to operators.

(3) The manufacturer must promulgate all necessary instructions for ensuring the safe operation of the aircraft including mandatory serviceability actions. The manufacturer should provide a method to track technical occurrences affecting safety throughout the life of the program and implement preventive and corrective actions as necessary.

(4) The maintenance manual should be clear what maintenance activities can be performed by untrained personnel, and which activities need special training considerations. If certain aspects of the RPAS require special skills or specially trained personnel to ensure proper maintenance, these details need to be communicated in the maintenance manual. Examples of this would be if an engine requires specially training to operate safely, or if an OEM training course is required for maintainers supporting the RPAS in operation.

### 5.9 Payloads

(1) General. Under CAR Part IX, payloads are defined as systems, objects, or a collection of objects including slung loads that are on board or otherwise attached to the aircraft and that are not necessary for flight. Payloads may include items such as sensor packages, containers, or additional radios. Payloads themselves are part of the RPA airframe as they are attached to the structural elements in some way. As such, where CAR 901.200(c)(ii) requires that controllability and centre-of-gravity be assessed, the effects of payloads must be considered.

(2) Payload Definition. It is important for manufacturers to define the limits of the various payload configurations a RPAS is designed to support. The payload limitations are generally defined in terms of mass, physical dimensions, and airframe integration. There are many different ways of incorporating payloads onto an RPAS, some designs include a specific payload "compartment" while other designs have "ports" where payloads may be affixed, still others require payloads to

be carried using external equipment affixed to the airframe. The operating manual should clearly define the payload carriage capabilities and their impact on the operational characteristics of the RPAS (e.g. reduction in range, susceptibility to winds). Payload configurations that invalidate the declared capabilities of the RPAS for Advanced Operations (e.g. if the failure of a payload system may cause a severe injury to a person on the ground) are to be clearly identified in the operating manual.

In lieu of dimensional, mass, and integration considerations (expanded on below), the operating manual may specify specific payloads which are deemed acceptable. This option may be especially attractive in cases where a declaration of the provided capability is made, and effects of unknown payloads may not be characterized.

(3) Mass Limitations. Mass limitations are to be defined within the scope of the weight and centre-of-gravity of the RPAS. The operating manual should clearly state the maximum weight capacity for payloads such as it will not adversely affect the controllability and airworthiness of the system. In addition, if specific mass distributions are not acceptable (e.g. payload mounted with majority of mass in the nose) the operating manual should clearly identify loading limitations with respect to the distribution of mass across the RPAS. If the payload mass has been considered when making a declaration relating to Advanced Operational capability the maximum payload mass (and distribution) must be established in the operating manual. In general, the operating manual should clearly define the acceptable ranges of payload mass and distribution for which the RPAS will remain operational.

(4) Dimension Limitations. Payload dimensions are to be defined within the scope of the centre-of-gravity of the RPAS. The operating manual should clearly state the limits on the dimensions of payloads which would adversely affect the controllability of the system in flight. If there are multiple configurations of payload dimensions (e.g. a cubic footprint and a spherical footprint) the operating manual should define the maximum limits of the payload. If the payload dimensions have been considered in making a declaration relating to advanced operational capability (e.g. sharp edges, payload contained within the airframe) the payload maximum dimensions should be established in the operating manual.

(5) Integration Limitations. Integration of the payload within the airframe should be defined within the scope of the aerodynamics of the aircraft. Payloads may be attached to the airframe in any orientation and may integrate with the electronic systems through various means (e.g. USB). The operating manual should clearly state how payloads may be integrated onto the airframe both physically and electrically to avoid hazards. Electrical hazards should be identified where appropriate especially when considering direct connections to the aircraft electrical systems. Effects on the controllable operation of the aircraft should be identified when providing information on airframe integration (e.g. if a payload is installed outside of a payload compartment). When integration of a payload has been considered as part of a declaration relating to advanced operational capabilities, limitations on changes to the specified integration methodologies must be clearly identified in the operating manual.

### 5.10 Command and control data link

(1) General. The importance of the command and control (C2) data link cannot be overstated. The C2 link is the only means of controlling the flight of an RPAS and is, in most cases, the most critical limiting factor in its operation. Industry has implemented various types of C2 links in order to meet specific consumer, or client needs while providing optimum reliability commensurate with the intended operation. Nevertheless, due to the complexities of the operational environments, “loss of link” events are expected to occur.

(2) Lost Link. A “loss of link” state has occurred when C2 Link is unavailable and the pilot is unable to intervene in the management of the flight. Lost C2 Links can be caused by equipment failure,

human error, electromagnetic interference, or many other factors. Lost link can also be caused by radio frequency (RF) propagation related conditions such as:

(a) Atmosphere/weather; and

(b) Reflection of signals from terrain, buildings and airframe causes received RF signal level to vary with time (fade).

**Note:** Fades may cause temporary, self-repairing, link outages and are more probable when conducting longer range operations.

It should be a design goal to minimize the probability of a loss link state such that uninterrupted operation of the RPAS can be maintained. It is considered a best practice that RPAS have features to detect a loss link state and initiate recovery procedures to either re-establish a nominal link state, or safely recover the vehicle. Furthermore, if a Declaration to 922.09 (C2 Link Reliability and Lost Link Behavior) is sought, then a lost link event should result in the RPAS behaving consistently and in a manner that minimizes any resulting hazard.

(3) Lost Link Behaviour. Regardless of how reliable the C2 Link is, designers should consider the RPA behaviour in the event that the C2 link is lost during flight. While there are different lost link behaviours that a designer can choose from, key aspects of acceptable lost link behaviour are consistency, and predictability. The operator should know exactly what they can expect the RPA to do in the event of a lost link, and where applicable be able to program key aspects of the behaviour (RTH altitude, Loiter, Auto Land, etc.) prior to flight.

(4) Radio Standards. In Canada, Innovation Science and Economic Development Canada (ISED) regulates the use of the frequency spectrum. The manufacturer may have to contact ISED with their specific requirements and conditions for frequency allocation to support the C2 link. ISED has published Radio Standards Specifications (RSS) which define the technical parameters for radios intended for specific operations:

https://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/h_sf06129.html

(5) Design and Performance Considerations. Design of the C2 link should be commensurate with the operations of the RPAS. Most operators are unfamiliar with the impacts of EMI on their radios, or the RF theory and situations that may adversely affect their operations. The C2 link should be designed with a maximum theoretical range defined for the intended operation based nominally on the frequency and transmission power of the radio.

(a) For a complete listing of frequency allocations and where operation is available refer to the ISED website on spectrum allocation:

https://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/h_sf01678.html

(2) Link Security. Current radio systems are not immune to the threats of radio jamming, signal spoofing, and/or signal interception and overriding. It is recognized at the moment there are no industry standards existing that allow for a completely secure C2 link, though different technologies offer different levels of vulnerability to these threats. Operators should be aware of the risk related to operating unsecure radio transmitters and be aware of anomalous situations related to their C2 operations. To this end, if the manufacturer has any supporting information to provide on how jamming, spoofing, or interception may present themselves in their systems this information should be made available to operators to assist in maintaining a safe and secure airspace.

(3) Use of Licensed Bands. For BVLOS operations specifically, considering the fundamental role the C2 link has on the safety of the operation, operators are strongly encouraged to make use of licensed frequency bands for C2 link operation. Coordination with ISED will be required to provide radio licenses for the use of these bands.

(4) Safety and Reliability. Analysis of the C2 link and associated failures will generally be performed in association with any CAR Standard 922.07 Safety and Reliability assessment. Given that the failures of the C2 link can have a cascading effect on other aspects of a BVLOS RPAS operation, the loss and degradation of the C2 link must be a specific failure mode that is assessed in detail.

(5) Link Characterization. Applicants should consider characterizing their C2 Link for at least the items of continuity, availability, integrity, Transaction Expiration Time and Geographic Coverage. Refer to Appendix A for industry standards for the characterization of C2 Links for RPAS operation.

(6) Service Level Agreements. For operations that are using service providers to provide C2 Links as a service (i.e. Cellular, Satellite, etc.) it is encouraged that service level agreements be put in place to ensure that any assumptions made when characterizing the C2 Link are maintained during RPAS BVLOS operation.

(7) Consideration of other Regulators. Prior to operation of a C2 link applicants should ensure that they consult with other regulators involved such as ISED and NAV Canada. For operation in some frequency bands, radio station licenses may be required from ISED.

### 5.11 Operating limitations

(1) General. The RPAS manufacturer must define operating limitations as defined in CAR 901.200(c) and make them available to each owner for the intended Advanced Operations. The manufacturer should publish those limitations on the use of their RPAS to support operators in selecting the system appropriate to their specific needs. Some examples of limitations which may need to be considered are:

(a) The maximum expected operational range for the C2 link;

(b) Latencies as a function of all relevant operating conditions (note: latencies should not lead to an unsafe condition in any Flight Control System (FCS) operating mode);

(c) C2 link channel availability when it has the capability to use multiple channels; and

(d) Environmental limitations such as temperature, wind, altitude, precipitation.

(e) Payload limitations.

(f) Operating modes that are incompatible with the safety assurance declaration (i.e. if the aircraft is limited to a low speed mode during operations over people).

(2) C2 Link. When evaluating technical options for C2 link radios the operational environment as well as the capabilities and limitations of specific frequencies should be kept in mind. In general, the following characteristics have been noted for the following common frequency allocations:

(a) 2.4 GHz occupies unlicensed radio bandwidth. Most radios operating on this frequency use the IEEE 802.11 standards (e.g. Wi-Fi) and the frequency is in very common use to the point of crowding the band. As a result, it is recommended that this frequency be used for systems aimed at operating away from a large number of radio transmitters (e.g. urban areas). Items which may interfere in this frequency range include Wi-Fi routers, Bluetooth devices, microwave ovens, wireless microphones and keyboards.

(b) 5.8GHz occupies unlicensed radio bandwidth. Most radios operating on this frequency use the Wi-Fi standard. 5.8 GHz Wi-Fi radios will typically have more bandwidth available than 2.4 GHz Wi-Fi radios, and while more resistant to interference, are not immune to losing bandwidth in the presence of other 5.8 GHz sources. As a result, it is recommended that this frequency be used for systems aimed at operating away from areas where other 5.8 GHz are present. Some items which may interfere in this frequency range include cordless phones, AC power supplies, and other RPAS.

(c) 5040-5050 MHz (C-Band) – C-Band occupies licensed radio bandwidth. As a result RPAS that use these radios require operators hold licenses issued by ISED. These frequencies have been identified as usable for high reliability systems. Design criteria for C-Band radios can be found in TSO-C213 and the supporting documents. These radios are recommended for more robust operations, and in areas approved by ISED. For more information on licenses refer to the ISED website:

https://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/h_sf10772.html

(d) L-Band, Satellite Communications and others – While it is noted there are dozens of other technologies that may be used to fulfill the C2 capability (including cellular radios) they primarily operate within licensed frequencies and as a result will have similar characteristics to the C-Band radios above (albeit with different sources of interference). Again, care should be used when selecting which radios should be used based on the operational environment of the RPAS.

(3) System Options for Limiting Operations. In addition to specific uses, there are a number of operating limitations that relevant aviation authorities may impose on the operation of RPAS (e.g. above 400 feet AGL, over correctional institutions, in restricted airspace). While it is the responsibility of the operator to ensure they are abiding by the aviation regulations and codes of the jurisdictions in which they are operating, a number of manufacturers include functions which assist operators in respecting jurisdictionally imposed operational limitations. Two examples of such technologies are “Geo-Fencing” and “Altitude Limiters.” These technologies allow restrictions to be set within the RPAS flight controller related to specific areas of operation. While these types of systems are not currently required by regulations, their incorporation is considered a best-practice aimed at minimizing the risk to aviation. The operator’s manual should provide clear instructions for enabling these features including override functions and their limitations.

(4) Specific Operating Limitations. While the regulatory framework has certain specific operational limitations (i.e. 25 or 150kg, 100ft from people, 25 people per $km^2$). Declarants should be aware that they should place additional limitations on their RPAS if they deem it required to meet the safety assurance standard. If it is determined that an RPAS is only safe for operation over people while operating at reduced speed, or reduced takeoff weight, then these limitations need to be communicated to the operator.

(5) Control of Multiple Systems. CAR 901.40(1) provides for the operation of multiple RPA from a single GCS provided that system and control station has been designed to perform these functions. RPAS manufacturers must provide instructions for operation of multiple RPAs from a single GCS and the limitations in the operating manual. These instructions should define how to manage, coordinate, and control the RPA under both normal and abnormal operations. It should consider:

(a) The maximum number of RPA to be controlled from a single control station at any given time; noting that the regulations require that the operator have an SFOC if they intend to control more than 5 RPA from a single control station.;

(b) Control each individual RPA;

(c) Pausing and/or cessation of control; and

(d) Control handover to another GCS if applicable.

These GCS and RPAS operations should be validated by flight testing to evaluate the user interface, the procedures and the pilot workload (human factors).

### 5.12 RPAS Integration

(1) General. System Integration broadly refers to the task of ensuring that all component systems operate together correctly and there are no undesired interactions between components. It is a

key step in any complex design process; however, it can be especially important when a declarant provides an add-on or supplementary system to an existing RPAS. Examples would be a parachute recovery system, or a detect and avoid system.

(2) Integration Testing. When integrating RPAS systems, declarants are expected to develop a test program to ensure that RPAS systems, including any supplementary systems operate together correctly. If there are any adverse effects noted, these need to be corrected during the development phase of the RPAS project. In some cases, adverse effects may become operational limitations that must be communicated to operators (i.e. a DAA system that interferes with a certain type of C2 link, or that is incompatible with a certain payload or mission).

## 6.0 Modifications

(1) General: The rules surrounding modifications of RPAS depend on whether the RPAS intended to be used for a CONOPS that requires a Declaration or a Pre-Validated Declaration. Third parties have more flexibility when modifying RPAS that have Declarations than those with Pre-Validated Declarations. Refer to Advisory Circular AC901-001 for further discussion of the considerations regarding modifications of RPAS with declared capabilities. A brief overview of the rules around declarations is presented below.

(2) RPAS with Declarations: When modifying an RPAS that possesses a Safety Assurance Declaration, it is left up to the modifier to determine whether or not the modification under consideration affects the declared capability of the RPAS. It's expected that modifiers will exercise technical judgment and consult RPAS manuals and technical data when required to determine if the modification has any effect on the declared capabilities. Depending on the extent of the modification, the modifier may also need to conduct ground and/or flight tests to verify that the RPAS continues to comply with the declared sections of CAR Standard 922.

(3) RPAS with Pre-Validated Declarations: Modifications to RPAS that possess Pre-Validated Declarations should only be done in accordance with manufacturer instructions. The modifier may need to contact the holder of the Pre-Validated Declaration if their desired modification is not supported by the existing Operating Instructions supplied by the PVD holder. If an operator decides to modify an RPAS in a way that is not specifically in accordance with the PVD holder instructions, the PVD against that RPAS will no longer be valid, and the aircraft will only be eligible for operations that don't require a PVD. (i.e. BVLOS away from Populated Areas, or VLOS away from people). RPAS with associated PVD are expected to be more complex and there may be safety considerations associated with the declaration that are not immediately obvious to the modifier. Since modifications not specifically approved by or consulted with the RPAS Declarant effectively invalidate any PVD associated with the RPAS, these modifications make the RPAS ineligible for any operations that require a PVD.

(4) Extent of Modifications. Modifications may fall into one of two categories: (1) modifications which affect the declared capabilities of the RPAS, and (2) modifications which do not affect the declared capabilities of the RPAS. As discussed above, for aircraft with an associated PVD, it is the PVD holder who decides what modifications can be made to the RPAS. For RPAS that only have a Declaration, it is the responsibility of the party making the modification to evaluate whether there is an effect on the declared capabilities, specifically as they apply to the technical and documentation requirements set out in CAR 901.200. Evaluation of the impact of modifications may require coordination with the RPAS manufacturer to obtain detailed technical information. There is no notification to the Minister is necessary for modifications that are judged to not alter the RPAS's declared capabilities (or continued satisfaction of CAR Standard 922 technical requirements). For modifications that are judged to affect the declared capabilities of the RPAS, it is the responsibility of the operator to ensure that no operations requiring those capabilities are conducted (i.e. if a modifications invalidates an 922.06 Operations Over People Declaration, then

it is the responsibility of the operator to ensure that the modified RPAS is not used to conduct operations over people).

(5) RPAS Modifier Obligations. Even for RPAS that don't have safety assurance declarations, anyone making a modification to an RPAS must consider the CAR 900.06 responsibilities that rest with the pilot that prohibit any operation that is reckless or negligent that could endanger aviation safety or the safety of any person. Therefore, modifiers should consider whether their modification increases the hazard presented by the RPAS in any way. This assessment may result in changes to the modification to make it safer, or it might result in additional operational procedures or limitations to reduce the hazard created by the modification. For example, an RPA that has been modified to trim branches from forest canopies might no longer be applicable for operations near or over people. This modification might be acceptable, provided that the pilot is alerted to the new operational limitations.

## 7.0 Operating Instructions and Limitations

(1) Most Declarations will rely on assumptions about the operator of the RPAS, and the operations that the RPAS will be conducting. Declarants must carefully consider if operators of the RPAS need special skills or training to operate the RPAS safely. They should also consider what knowledge the operator needs to ensure that the RPAS is operated within a safe envelope. Examples of these situations could be:

(a) Safe recovery of the RPAS in certain situations needs additional attentiveness or expertise.

(b) Safety systems (i.e. a Parachute) that have environmental limitations (i.e. maximum permissible wind).

(c) Any considerations required regarding integration of configurable elements or payloads (i.e. certain payloads are incompatible with certain missions or configurable elements).

(2) Declarants need to communicate all required information to operators of the declared RPAS. Usually, this information is contained in the RPAS operating instructions. Declarants may also decide that special training is required to ensure that operators have the skills and knowledge necessary to operate the declared RPAS. Declarants are free to mandate classroom/virtual instruction to their operators.

(3) Declarants might also determine that their declaration modifies the operational limitations of an existing RPAS. (ie. A parachute system that allows for operation over people, or a system change that allows for flight in windier conditions). Declarants are permitted to change operating limitations as desired provided their development process has demonstrated that these new limitations are safe, and the RPAS meets the declared CAR 922 standard. Where operational limitations change, the instructions to the operator need to be clear on what the operator needs to do to access these new operational privileges.

## 8.0 RPAS Configuration Management

(1) Configuration Management. Proper configuration management is an extremely important aspect of Safety Assurance Declarations. By making a safety assurance declaration, the declarant is asserting for the record that the declared make and model of RPAS complies with the CAR standard, and that all RPAS manufactured under that make and model also meet the CAR standard. If the declarant is unable to document all critical aspects of RPAS hardware, software, and architecture they won't be able to assert that future instances of the same RPAS make and model will continue to comply with the declared standard.

(2) Service Life Considerations. Once the RPAS enters service it is understood that there may be occasional modifications and upgrades made to the RPAS. Examples of this might be firmware upgrades, or replacement parts. It is the responsibility of the declarant to ensure that any changes they make to the RPAS do not affect the declared compliance with CAR Standard 922. If there are various configurations of an RPAS make and model that continue to meet the declared standard, it is the responsibility of the declarant to maintain this list of applicable configurations. It is also important to communicate to operators if there are any configurations that specifically do not comply with CAR Standard 922 so that operators can be aware of situations where certain types of operations might not be permitted.

## 9.0 RPAS Declarant Obligations

(1) General. Once the declaration is made Declarants have certain obligations under CAR Part IX. While these obligations are summarized below, additional guidance on these responsibilities can be found in AC 901-001 Declaration and Pre-Validated Declaration processes.

(2) Maintenance Instructions and Operating Manual. Applicants need to ensure that their operational documentation (User Manual, Maintenance Procedures, etc.) clearly state what operations have been analyzed and declared as safe. Any operational assumptions that are a basis of the declaration need to be translated into operational limitations that are communicated to the end user. The Declarant should not rely on the RPAS certificate of registration to list the operational limitations of the RPAS.

(3) RPAS Elements. CAR 101 defines a RPAS as a set of configurable elements consisting of a remotely piloted aircraft (RPA), a remote control station (CS), the command and control (C2) links and any other elements required for operation.

Each safety assurance declaration must identify each of the elements that are required to form an RPAS that complies with the declaration. In some cases, the applicant might not be the manufacturer or designer of all elements of the RPAS. Examples of this might include cases where the applicant makes a parachute for installation on third party RPA, or cases where the applicant provides C2 or DAA services to a drone operation consisting of specific models of RPA. When this is the case, the applicant needs to carefully consider and clearly indicate what collection of configurable elements are covered by their safety assurance declaration. Safety assurance declarations are made for a complete RPAS, not a subset of configurable elements. Therefore, the declaration must fully describe the RPAS and included configurable elements that is considered to comply with CAR Standard 922. It should also be noted that operators might make use of additional configurable elements in addition to the declared RPAS to complete their mission. Declarants need to carefully consider if there are any specific limitations that operators need to respect. For example, if a C2 link antenna needs unobstructed view of the sky, the operating limitations need to inform the operator not to modify the RPAS in such a way that the antenna is obstructed. Therefore, the operating manual should include warnings to prevent the installation of a parachute assembly, or other equipment in a location that might interfere with the C2 antenna performance. Another example might be a DAA system that is known to not be compatible with certain C2 link technologies, either because of EMI interference, or because the C2 is not capable of sending intruder data to the ground station. As before, in cases like this, the operating manual must outline all known limitations of the system that need to be understood by the end user.

(4) Content of a Declaration. As noted in CAR 901.194(2) the declaration form contains the following information:

(a) Make –Manufacturer’s Name;

(b) Model – Specific model designation which identifies the configuration of elements that make up the RPAS;

(i) As discussed above, for an applicant who manufacturers a ‘complete’ RPAS, this may be a simple as listing the model of aircraft.

(ii) For an applicant who does not manufacture the ‘complete’ RPAS, this item may consist of a list of configurable elements that when combined make an RPAS that meets the declared technical standard(s).

(iii) Applicants may choose to refer to their internal parts lists or configuration control drawings by document number when referring to the RPAS Model.

(c) Maximum Take-off Weight (MTOW) – The maximum designed operating weight of the RPA in kilograms;

(d) CAR Standard 922 sections – A multi-select checkbox to identify which technical requirements the RPAS has been verified against. Any combination of the checkboxes can be selected to reflect the capability of the aircraft;

(e) Signature of the Responsible Person – A box for the signature of the person making the declaration on behalf of the manufacturer;

(f) Title of Signatory – The business title/position of the person making the declaration;

(g) E-mail Address – The valid and active e-mail address that can be used to contact the person making the declaration; and

(h) Date – day, month, and year on which the declaration is signed.

(5) Persons Making a Declaration. A declaration may be made by any person who is knowledgeable enough to perform the necessary tests or analysis to show that a given RPAS meets the applicable part of CAR Standard 922. Often declarants are the designer or manufacturers of the RPAS, however this does not have to be the case. In some cases, a declarant could be a third-party who is able to demonstrate compliance of the RPAS with CAR Standard 922 (e.g., an RPAS modifier), or a service provider whose service allows an RPAS to meet a required section of CAR Standard 922 (e.g., C2 Link Service Provider, or DAA Service Provider). It is expected that a market for third party modifiers and service providers may emerge given the proliferation of systems. Regardless of the declarant type, the obligations required by Part IX of the CARs are identical. It is further envisioned that RPAS modifiers would generally need to enter into an agreement with the RPAS manufacturer or other entity having ownership of intellectual property required to substantiate a declaration that the modified RPAS meets the applicable safety objectives. To the extent practical, the RPAS modifiers may declare modifications applicable to multiple RPAS models of the same make on a single declaration form. Section 6.0 provides further guidance on modifications. More guidance on who can make declarations is provided in AC901-001.

(6) Retention of Declarations. The Minister retains declarations for the purposes of inspection, program oversight, administer compliance and designated provisions, and to derive demographic information. The Minister may inspect any element of the RPAS, the technical evidence supporting a declaration, and any related publications by the RPAS manufacturer. The Declarant has the responsibility to provide this documentation to the Minister when requested.

(7) Validity of Declarations. Declarations remain valid unless the RPAS manufacturer notifies the Minister otherwise, or the Minister determines that the RPAS does not meet the technical requirements set out by CAR Standard 922. In the case of Pre-Validated Declarations, declaration validity is also based on the applicant submitting a report to TC annually to renew the status of the Pre-Validated Declaration. For both Declarations and Pre-Validated Declarations, the declaring entity is required to notify the Minister as soon as practical upon discovery of an issue affecting safe operation. Once the declaration is found invalid, the RPAS will be restricted to operations that do not require the Declaration or Pre-Validated Declaration as appropriate.

While 901.194(4)(b) identifies that a declaration is invalid if the Minister is notified of an issue, the recommended actions from the RPAS manufacturer will be taken into account and the validity of the declaration evaluated within that context.

(8) Notice to the Minister. The objective for notification of issues related to declarations is to ensure Transport Canada is kept up to date of known issues leading to unsafe operations and to support the user community by disseminating procedures or additional limitations to registered owners. An RPAS manufacturer with a declared RPAS must notify Transport Canada by specifying the make and model, describing the nature of the issue and which technical requirement is no longer met, along with any recommended action, and the name and contact information of the responsible persons to:

E-mail: RPASDeclaration-DeclarationSATP@tc.gc.ca

The nature of the recommended actions will differ based on the specific issue identified. Transport Canada may review and ask for clarifications regarding recommended actions and/or may mandate limitations.

(9) Record Keeping by the Declaring Entity. To verify that a particular RPAS meets the technical requirements, and that the limitations communicated to the operator have been developed correctly, the declaring entity must complete the necessary tests, analysis, simulations to support a declaration. CAR 901.201 identifies the record-keeping obligations of the Declaring Entity. The Declaring Entity is required to produce on demand by the Minister current records corroborating a declaration. The records comprise:

(a) Reports containing the results of testing, analyses, assessments, and verifications undertaken to demonstrate compliance with the applicable safety assurance requirements of CAR Standard 922 for which the declaration applies.

(b) All mandatory actions in respect of the RPAS;

(c) The results of any service difficulty investigations that the person has undertaken.

The RPAS manufacturer shall retain these records for the greater of (1) two years following the date the manufacturing of the appertaining RPAS permanently ceases, and (2) or two years after the day on which the person provides a notification to the Minister that they declaration is no longer valid.

(10) Service Difficulty Reporting. While all declaration holders are encouraged to establish a Service Difficulty Reporting System, regulations require that declarations that have associated Letters of Acceptance (i.e. Pre-Validated Declarations), have a means by which operators can submit service difficulties. For further details on RPAS Service Difficulty Reporting refer to AC901-001. When a service difficulty report is received, the declaration holder is required to investigate the service difficulty to determine if the RPAS continues to comply with the applicable sections of CAR Standard 922. While it is strongly encouraged that all service difficulties be fully addressed by the declaration holder, the declaration holder is only required to develop mandatory actions to resolve the Service Difficulty when the RPAS is found to no longer comply with CAR Standard 922. Mandatory actions must be communicated to all operators of the RPAS who could be affected by similar service difficulties.

(11) Annual Reporting. Holders of Pre-Validated Declarations are required to provide annual reports to TCCA in accordance with CAR 901.199. This annual report includes the number of RPAS operating and a summary of any Service Difficulty Reports that may have been encountered in the previous year. Refer to AC901-001 - RPAS Safety Assurance Declaration and Pre-Validated Declaration Processes for more information on annual reporting requirements.

(12) Additional Guidance. Declarants are directed to Advisory Circular 901-001 for additional details on the Declaration and Pre-Validated Declaration processes, as well as the other responsibilities of Declaration holders.

## 10.0 Information management

(1) Not applicable

## 11.0 Document history

(1) Not applicable

## 12.0 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 address:** 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**

**Jeremy Fountain**
**Acting Director, RPAS Task Force**

# Appendix A – Recognized industry consensus standards

| **Documentation** |
|---|
| ASTM F2908 Standard Specification for Unmanned Aircraft Flight Manual (UFM) for an Unmanned Aircraft System (UAS) |
| ASTM F2909 Standard Practice for Maintenance and Continued Airworthiness of Small Unmanned Aircraft Systems (sUAS) |

| **Electrical Systems** |
|---|
| UL 3030 Standard for Unmanned Aircraft Systems |
| ASTM F2639 Standard Practice for Design, Alteration, and Certification of Aircraft Electrical Wiring Systems |
| ASTM F2490 Standard Guide for Aircraft Electrical Load and Power Source Capacity Analysis |
| SAE AS 4805-2007, Solid State Power Controller, General Standard For |
| SAE AS 50881F, Wiring Aerospace Vehicle |

| **Equipment** |
|---|
| ASTM F3322 - Parachutes |
| ASTM F3002 Standard Specification for Design of the Command and Control System for Small Unmanned Aircraft Systems (sUAS) |
| ASTM F3005 Standard Specification for Batteries for Use in Small Unmanned Aircraft Systems (UAS) |
| SAE AS 8033, Nickel Cadmium Vented Rechargeable Aircraft Batteries (Non-Sealed, Maintainable Type) |
| SAE J3042-2015, Measuring Properties of Li-Battery Electrolyte |
| SAE J3021-2014, Recommended Practice for Determining Material Properties of Li-Battery Cathode Active Materials |
| SAE ARP 5724, Aerospace - Testing of Electromechanical Actuators, General Guidelines For |
| TSO-C213-Unmanned Aircraft Systems Control and Non-Payload Communications Terrestrial Link System Radios |

| **Human Factors Evaluation** |
|---|
| ISO 9241-210 |
| MIL-STD-46855A |
| Aeronautical design standard performance specification handling qualities requirements for military rotorcraft ADS-33E-PRF |
| Display Guidance: AC23.1311-1C |

| **Software** |
|---|
| ASTM F3201 Standard Practice for Ensuring Dependability of Software Used in Unmanned Aircraft Systems (UAS) |
| ASTM F3269 Standard Practice for Methods to Safely Bound Flight Behavior of Unmanned Aircraft Systems Containing Complex Functions |
| RTCA DO-178C |

| **Safety Assessment** |
|---|
| FAA AC 23.1309-1E |
| JARUS AMC RPAS.1309, Safety Assessment of Remotely Piloted Aircraft Systems |
| SAE ARP 4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment |
| SAE ARP 4754B – Guidelines for Development of Civil Aircraft and Systems |
| ASTM F3309 - Standard Practice for Simplified Safety Assessment of Systems and Equipment in Small Aircraft |
| ASTM F3230 – Standard Practice for Safety Assessment of Systems and Equipment in Small |

| Aircraft |
| --- |
| Aircraft F3389/F3389M Standard Test Method for Assessing the Safety of Small Unmanned Aircraft Impacts |

| **Design Specifications** |
| --- |
| ASTM F3298 Standard Practice for Design, Construction, and Verification of Fixed-Wing Unmanned Aircraft Systems (UAS) |
| EU CE Designations, Appendices 2-5 |
| JARUS CS-LUAS, Recommendations for Certification Specification for Light Unmanned Aeroplane Systems |
| JARUS CS-LURS, Certification Specification for Light Unmanned Rotorcraft Systems |
| STANAG 4703 Light UAV System Airworthiness Requirement for NATO UAV Systems |
| TCCA SI 623-001 Issue 02 Appendix C |
| ICAO Doc 10019 - Manual on Remotely Piloted Aircraft Systems (RPAS) |

**Note:** Satisfying the standards that have been developed for large systems and/or traditionally piloted aircraft is one acceptable means of compliance but not mandatory for the operation of small RPAS.

# Appendix B – System safety assessment

## 1.0 Scope

(1) The appendix offers guidance to assist manufacturers in demonstrating compliance with sections of CAR Standard 922 that include performance requirements related to the probability of an event occurring. These include the following CAR Standards:

(a) 922.05,

(b) 922.06,

(c) 922.07,

(d) 922.08,

(e) 922.09, and

(f) 922.10.

(2) Where these standards require that a failure event must be shown to meet a certain probability requirement (i.e. Extremely Improbable, Extremely Remote, Remote, etc.), it is expected that applicants will follow a system safety assessment process to demonstrate that the RPAS meets the requirement. These processes generally involve a systematic review of the RPAS architecture to determine the effect of foreseeable failures of each subsystem and determination of the criticality of any hazards created by foreseeable failures. Once the criticality of each hazard is determined a required likelihood can be assigned. The final step in the process is to demonstrate that the various sub-systems of the RPAS meet or exceed the likelihood of failure requirements.

## 2.0 Acceptable methods

(1) A common industry standard developed for aeronautical products is SAE ARP 4761 – Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment. An RPAS manufacturer may choose to use other acceptable methods and processes for conducting a system safety assessment provided that they are documented such that they can be consistently adhered to and that artifacts and evidence generated from those processes are auditable. It is recommended that RPAS manufacturers endorse rigorous standards and practices suitable for the aviation industry to the maximum extent as possible.

(2) Advisory material published by TCCA, and that of other civil aviation authorities acceptable to TCCA, may be used in conjunction with acceptable methods for performing the system safety assessment process. Namely JARUS AMC RPAS.1309, FAA AC 23.1309-1E, AC 25.1309-1A, AC 27-1B and AC 29-2C may be used to complement the guidance of this AC.

## 3.0 Classification of failure conditions (severity)

(1) TCCA endorses the same failure criticality classification and associated safety objectives as those defined by airworthiness standards for type certification, FAA AC 23.1309 or the most recent version. The criticality classifications and safety objectives adapted to RPAS are outlined in Table B-1:

**Table B-1 – Criticality classification and safety objective**

| Criticality Classification | Definition applied to RPAS | Safety Objective |
|---|---|---|
| Catastrophic | Failure conditions that could result in one or more fatalities. | Extremely Improbable |
| 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:<br>(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<br>(ii) A large reduction in safety margins or functional capabilities, or<br>(iii) High workload such that the pilot cannot be relied upon to perform their tasks accurately or completely. | Extremely Remote |
| 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 |
| 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 |
| 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. | No probability requirements |

## 4.0 Safety objectives

(1) TCCA defines the following safety objectives prescribing quantitative probability targets commensurate with the maximum expected kinetic energy of the RPA.

(a) The quantitative safety objectives for each hazard category and each level of RPA kinetic energy are given in Table 1 associated with CAR Standard 922.07.

**Table B-2 – RPAS Reliability Targets**

| Classification | Reliability Objective | P(x) – Probability of Failure | | |
|---|---|---|---|---|
| | | RPA KE <700 J | RPA KE <34 kJ | RPA KE <1084 kJ |
| Catastrophic | Extremely Improbable | 10^-4 | 10^-5 | 10^-6 |
| Hazardous | Extremely Remote | 10^-3 | 10^-4 | 10^-5 |
| Major | Remote | 10^-2 | 10^-3 | 10^-4 |
| Minor | Probable | 10^-2 | 10^-2 | 10^-3 |
| No safety affect | No requirements | No requirements | No requirements | No requirements |

(b) The declarant is required to determine the amount of kinetic energy that the RPA can attain to determine which column of Table B-2 to use. This determination may be based

on worst-case assumptions, or the declarant may choose to consider specific situations that can reasonably be expected given the failure being analyzed (i.e. if a particular failure can only occur during low altitude, low speed operation). Declarants should document their assumptions and calculations and retain this evidence as part of their means of compliance.

(c) Traditional aviation has developed many methods for analysis of complex systems and determination of quantitative probabilities of failure. RPAS manufacturers are encouraged to seek out and implement existing methods of failure analysis such as those documented in SAE ARP 4761, and FAA AC23.1309-1E.

(d) In many cases, there are operational considerations and assumptions that serve as the basis for the failure analysis. These might be operational procedures (i.e. verify safety system availability prior to each flight), maintenance actions (i.e. parachute system must be inspected and repacked annually), or operational limitations (i.e. no flight over assemblies of people, no flight in precipitation, etc). When these assumptions are used to control the exposure to a failure or the hazard caused by a failure, the applicant needs to ensure that these limitations and procedures are communicated to the operator, usually via the operating manual and maintenance instructions that are supplied with the RPAS (ref CAR 901.200).

As RPAS complexity increases, it can be difficult to determine the hazard caused by various failure conditions. For this reason, a systematic method of analyzing each failure in the system (such as methods referred to above) is needed to ensure that possible failures and their associated hazards are not missed. Applicants should perform a full assessment of their RPAS to identify all the failure conditions that could result in various hazards. Once this assessment is complete, the failures leading to each hazardous condition (i.e. serious injury, fly-away, loss of DAA capability, etc.) can be grouped and overall reliability rates can be assessed. ~~gr~~

## 5.0 Development process

(1) The engineering system used for the development of the RPAS will significantly contribute to the degree of confidence in the RPAS performing as intended. The RPAS manufacturer should follow a suitable development process to provide an adequate level of confidence that design requirements are correctly implemented through successive validation and verification activities. The objective is to minimize the likelihood of errors which may adversely affect the performance of the RPAS and create hazards to people on ground or other aircraft.

(2) Though the preferred standard developed for aeronautical products is SAE ARP 4754 – Guidelines for Development of Civil Aircraft and Systems, RPAS manufacturers may follow other processes that provide an equivalent degree of confidence. The RPAS manufacturer's engineering system should be documented such that procedures and processes are consistently adhered to and that artifacts and evidence generated traceable and thereby auditable.

(3) A System Safety Assessment should be performed for the RPAS (including all contributions coming from the RPA, Control Station, Data Link, required services, and any other configurabl elements necessary to operate the RPAS). This assessment should include a Functional Hazard Analysis, a Failure Mode Effect and Criticality Analysis and a Fault Tree Analysis.

(4) Depending on the section of CAR Standard 922 that is applicable to the CONOPS, certain hazards will need to be specifically assessed and demonstrated to meet the reliability targets.

(a) <u>922.07 Safety and Reliability</u> This standard invokes is a complete assessment of all possible failures of the RPAS and the criticality of the associated hazards. In addition,

this standard places other considerations on some classes of failures (Catastrophic failures must not result from single failures).

(b) 922.08 Containment This standard requires that any failures leading to the hazard of a fly-away (i.e. operation outside of the operational volume) be assessed. Other failures that don't directly lead to a fly-away do not need to be specifically assessed. However, as discussed above, if there are any assumptions or limitations used when determining that a failure won't result in a fly-away (i.e. ground risk buffer, use of geo-fencing, lost-link behaviour programming), these limitations and assumptions must be communicated to the operator.

(c) 922.09 Command and Control Link Reliability and Lost Link Behaviour This standard requires that any failures leading to a loss of control of the RPA be assessed.

(d) 922.10 Detect, Avoid and Alert Systems This standard requires that any failures leading to a loss of detect and avoid capability be assessed. It further divides failures of the DAA system into annunciated and un-annunciated failures. It is assumed that an operator who is alerted to the failure of DAA capability will have contingency procedures in place to allow the RPA to safely exit the airspace, the exposure time for annunciated failures of the DAA system is expected to be minimal. Conversely, when an operator is not alerted to a failure of the DAA system or is provided with misleading guidance from the DAA system a serious hazard to the safety of the operation is created. For this reason, DAA system designers should implement fault-monitoring and built-in testing to their DAA products to minimize the likelihood of un-annunciated failures.

(5) A key aspect of the development process will be the documentation of system behaviour and corresponding verification that the final system as constructed meets the documented system behaviour. This verification will most often be through tests, analysis, inspection.

(6) Throughout the development process, artifacts documenting the process and results of verification activities must be created and retained by the declarant as they may be subject to surveillance activities in accordance with CAR 901.201. Declarants must be able to produce a record of all verification activities that are used to support the declaration.

# Appendix C – Severe injury test methodology

## 1.0 Discussion

### 1.1 Intent of tests

(1) The intent of the tests is to assess the safety of RPAS operations involving flight operations over people, and thus the potential for severe injury (see section 7.10 for definition of severe injury) to a person on the ground. This test evaluates the trauma to a person impacted by a head strike, or chest strike. By performing these tests, the manufacturer can correlate between reaction of dummy head impact G's (force of acceleration due to gravity) and RPAS kinetic energy, and set operational limits that correspond to injury thresholds established in this AC. The manufacturer should understand the correlation of the test with AIS scale. Also, this guidance allows for determination of existing RPAS designs' injury potential during a collision with a person on the ground, and encourages designers/manufacturers to modify the RPAS accordingly to reduce injury potential.

(2) Secondary Impacts. This procedure assumes that the majority of energy will be transferred from the RPA to the initial person struck. As such, the procedures do not specifically measure or evaluate the speed, acceleration, or orientation of the RPA after the impact. If the manufacturer expects the specific design may create hazards following an initial impact it is recommended that the effect of secondary impacts to persons be evaluated in a similar manner as prescribed in this appendix.

### 1.2 Operating environment

(1) The manufacturer should have an understanding of the actual operating environment in which the system is designed to function. For example, if the manufacturer intends for operations with 30km/h gusts when operating over people, the critical conditions defined should take into consideration the influence of the gust on the terminal velocity used for these tests.

### 1.3 Standardized test procedures—Reason and practicalities

(1) The tests described in this circular are standardized procedures generally regarded as the minimum necessary to develop the flight envelope of an RPAS in a way that provides for assurance of the safe use of the system in the advanced environment. Standardized procedures seek to obtain consistent results between different test facilities. These facilities may be of varying types; often they are not under the direct control of the designer or manufacturer of the article under test. To foster industry standardization, this circular describes many of the procedures and evaluations that are already accepted (or in the process of becoming accepted) as part of industry standards.

### 1.4 Acknowledgement

(1) These methodologies are based on methods researched by the FAA Center for Excellence for Unmanned Aerial Systems (UAS) supported by the Alliance for System Safety of UAS Through Research Excellence (ASSURE). These methods expand on extensive research and testing conducted by the automotive industry to support quantitative automotive passenger safety standards and testing and test data on RPAS collected by ASSURE. This appendix presents deltas on interpretation that will be resolved with further experience on real case scenarios, or further testing.

## 2.0 References

(1) ASTM F3322 – Parachutes

(2) Assessment of Head Injury Criteria Potential During Aircraft Longitudinal Impact. The Eight Triennial Aviation Fire and Research Conference Richard Deweese FAA Civil Aerospace Medical Institute, October 27 2016

(3) DOT/FAA/AM-17/9 Office of Aerospace Medicine Washington, DC 20591 Assessment of Head and Neck Injury Potential During Aircraft Longitudinal Impacts Civil Aerospace Medical Institute Federal Aviation Administration February 2017 Richard L. DeWeese, David M. Moorcroft, M.M.G.M. Philippens

(4) Development of Improved Injury Criteria for the Assessment of Advanced Automotive Restraint Systems – II November 1999

(5) European new car assessment Program (Euro NCAP) Pedestrian Testing Protocol Version 8.4 November 2017

(6) FAA UAS Center of Excellence Task A4: UAS Ground Collision Severity Evaluation Revision 2 Mr. David Arterburn, Principal Investigator – arterbd@uah.edu Director, Rotorcraft Systems Engineering and Simulation Center The University of Alabama in Huntsville, Dr. Mark Ewing – mewing@ku.edu Associate Professor and Director of the Flight Research Laboratory The University of Kansas 28 Apr 2017

(7) FAA AC 25.562-1B - Dynamic Evaluation of Seat Restraint Systems and Occupant Protection on Transport Airplanes / with Change 1 January 10, 2016

(8) Federal Motor Vehicle Safety Standards 208 (FMVSS 208)

(9) Final Report of Workshop on Criteria for Head Injury and Helmet Standards Scientific Editors: Harold Fenner, Jr., Daniel J. Thomas, Thomas Gennarelli, Frank A. Pintar, Edward B. Becker, James A. Newman, Narayan Yoganandan, Department of Neurosurgery, Medical College of Wisconsin December 16, 2005

(10) Moderate Overlap Frontal Crashworthiness Evaluation Guidelines for Rating Injury Measures September 2014

(11) National Highway Traffic Safety Administration Test Procedure TP208-14 Appendix A (Part 572E (50th Male) Dummy Performance Calibration Test Procedure

(12) Prasad P, Mertz HJ. The position of the United States Delegation to the ISO Working Group 6 on the use of HIC in the automotive environment. Warrendale, PA. Report No.: SAE 851246,1985.

viii. SAE J1727 Issued 1996-08 Revised 2015-02 Calculation Guidelines for Impact Testing

ix. SAE International. Sign Convention for Vehicle Crash Testing. Warrendale, PA: SAE International; Dec. 1994; SAE Surface Vehicle Information Report No: J1733.

x. SAE International. Instrumentation for Impact Test – Part 1- Electronic Instrumentation. Warrendale, PA: SAE International; 2014; Surface Vehicle Recommended Practice No: J211/1.

xi. SAE International. Instrumentation for Impact Test – Part 2- Photographic Instrumentation. Warrendale, PA: SAE International; 2014; SAE Surface Vehicle Recommended Practice No: J211/2.

xii. SAE J2570: Performance Specifications for Anthropomorphic Test Device Transducers

xiii. The Abbreviated Injury Scale 2005 - Update 2008, Barrington, Illinois, Association for the Advancement of Automotive Medicine, 2008.

xiv. Transport Canada UAV systems program design working group phase 1 final report march 2012

(13) United Nations [UN] Global Technical Regulation [GTR] n°9, Pedestrian Safety, November, 12, 2008.

(14) UN Regulation n°94 (R94), Uniform provisions concerning the approval of vehicles with regard to the protection of the occupants in the event of a frontal collision, August, 20, 2013.

(15) US Code of Federal Regulations, Title 14, Part 25.562. Airworthiness Standards: Transport Category Airplanes, Emergency Landing Conditions. Washington, DC: US Government Printing Office, 1988.

(16) US Code of Federal Regulations, Title 14, Part 23.562. Airworthiness Standards: Transport Category Airplanes, Emergency Landing Conditions. Washington, DC: US Government Printing Office, 1988.

(17) US Code of Federal Regulations, Title 49, Part 571.208. Occupant Crash Protection. Washington, DC: US Government Printing Office, 2011.

## 3.0 Standardized test procedures—Relationship to design

(1) As stated above, the tests are standardized by necessity, and are presented below.

(a) Third Party. The dynamic tests are performed with an anthropomorphic test device (ATD), Hybrid III—representing approximately the 50$^{th}$ percentile male.

Third Party Weight. A 50$^{th}$ percentile ATD provides for an assessment against the widest range of Third Parties.

(b) Test conditions. This circular describes six (6) basic types of dynamic test procedures (see Figures C-1 through C-6): a test where the predominant impact vector is vertical, three tests where the dominant impact vector is horizontal, and two tests using a worst case vector defined by flight testing showing different failure conditions. These procedures address the tests required to demonstrate a safe flight envelope for operating over people. Additional tests may be necessary to demonstrate safe operations for these variations if they cannot be adequately addressed by analysis.

(c) Speeds. The speed of the RPAS prior to the impact will vary depending on both the test as well as the type of RPAS used. Two speeds are defined:

Critical Speed: this is the speed at which the aircraft is capable of its maximum kinetic energy considering both powered flight as well as failure conditions. The Critical Speed for fixed wing aircraft is the maximum cruise speed. The Critical Speed for rotary-wing aircraft is the speed of the rotorcraft at terminal velocity.

Operational Speed: this is the maximum speed at which the aircraft can normally operate (considering the usage expectations and limitations within the operating manual).

**Information Note:** There may be several other aspects of the standardized test procedure that need to be considered when determining the test program required to demonstrate the safety assured flight envelope or interpret the test results. The extent of the test program will depend on the most critical case determination and its applicability to other configurations. Further discussion on this aspect of testing is provided in section 5.0..

## 4.0 Probable impact scenario development

(1) The manufacturer may determine the most probable impact orientations for the sRPA to hit a person's head based on engineering judgment, flight test, any parachute or recovery systems installed, simulation, and/or understanding of the operating characteristics of the sRPA. For each probable impact orientation, the manufacturer shall perform a series of drop tests to determine the worst case, that which produces the most severe injury, of these probable orientations. These drop tests shall consist of at least three drops in each orientation with a drop height as specified below.

## 5.0 Test conditions

### 5.1 General

(1) Testing is always a trade-off between that which is being monitored and the impact of additional monitors, as such tests should be structured and calibrated to achieve the highest precision and accuracy for the parameters being evaluated. The objectives of the tests are to evaluate the critical impact direction, and corresponding injury severity to support the analysis required in CAR standard 922 related to injuries. The manufacturer should have an understanding of the actual operating characteristics of their RPAS before starting the process outlined in this guidance. It is assumed that the manufacturer will be able to substantiate: the most probable critical case impacts, typical and maximum operating heights and speeds, and terminal velocity of their RPAS in order to compare the results of the impact analysis with the proposed vehicle concept of operations. Thus, the manufacturer should have a good understanding of the failure modes (e.g. engine failure, etc.), and the flight operating envelope shall consider different environmental conditions such as gust in order to define the critical conditions.

### 5.2 Determination of critical orientation

(1) The manufacturer shall determine the critical impact orientation, that which produces the highest risk of severe injury, for the RPAS to hit a person's body. This can be accomplished through flight testing or other methods (see section 4.0 of this Appendix), and test or simulation of the failure modes of the RPAS shall be accomplished to determine the impact on the critical cases.

(2) Simulation. Through use of simulation the manufacturer may determine no flight test is required, however, the manufacturer needs to provide an engineering rationale describing the differences between model simulation results (model validation methodology), as well as determine if the results produce minimal differences in flying attitudes as compared to operational test data. The use of computational fluid dynamics (CFD) analysis is recommended when the manufacturer has demonstrated it is able to replicate the RPAS behavior. The correlation between the CFD model and RPAS design can be extrapolated to similar RPAS configuration to support other analyses.

(3) A minimum of six (6) tests at the maximum flying speed with different failure conditions shall be done.

(4) In cases where a parachute or recovery system is installed, the manufacturer needs to understand the effect of the system on the most probable critical orientation of the RPA, and flight test the RPAS to determine if there are impacts to previously defined critical cases (if applicable). For RPAS employing parachute (or other recovery system) mitigations for uncontrolled flight, the drop height shall be chosen such that the impact speed is at least equal to the maximum descent speed with the parachute (or other recovery system) deployed (the goal of the test is to evaluate whether the recovery system successfully mitigates the impact as measured by the injury criteria in table C-1).

(5) The test vehicles shall be instrumented in order to define acceleration and speed at impact.

(6) The manufacturer shall record the following results of the test:

(a) RPAS configuration;

(b) RPAS impact orientation;

(c) RPAS speed at impact, the maximum magnitude of maximum resultant speed;

(d) Any relevant notes about the impact;

(e) Any damage to the sRPA or ATD shall be noted, and photography kept in the records; and

(f) Maximum accelerations for each impact orientation.

The designers/manufactures shall produce a test report with the information described above along with general conclusions from the test. Specifically, the manufacturer shall identify the critical impact orientation as the orientation that resulted in the greatest measured maximum acceleration over the three drops.

**Information Note**: This identified critical impact orientation is only valid for the specific configuration tested by the manufacturer.

(7) If a modifier does not have access to this critical impact orientation specified by the manufacturer, a modifier shall create a failure mode analysis, and follow the procedures described in section critical orientation (see section 7.0 of this appendix for information on modifications).

(a) If the manufacturer wishes to use simulation as a method of compliance with this procedure, or with the general injury prevention requirement, it is recommended that the manufacturer discuss the proposed methodology with TCCA. This will allow TCCA to both gain experience with the methodology used as well as support the dissemination and adoption of the latest industry safety standards. Also, a correlation should be done to validate the simulation with flight test data.

### 5.3 Impact to ATD

(1) The dynamic test methods identified below may be correlated to other standards, such as FMVSS 208, to determine the corresponding probability of an injury. A minimum of six (6) dynamic tests are required to define the operating limits of the RPAS flying over people.

**Information Note**: The following diagrams depict the RPAS as a multi-rotor rotorcraft, but it is meant to be representative of any RPAS whether fixed-wing, rotary-wing, hybrid, or lighter-than-air.

(2) Test 1 - Vertical Drop Test. The vertical drop test is to drop the RPA onto the head of the male ATD at the Critical Speed, and normal flight orientation. A minimum of two (2) drops shall be done in this orientation in order to reduce possible variability.

**Figure C-1 – Vertical drop test configuration**




(3) Test 2 - Frontal Head Test. The frontal head test is to impact the forehead of the male ATD with the RPA at the Operational Speed, and normal flight orientation. A minimum of two (2) tests shall be done in this orientation in order to reduce possible variability.

**Figure C-2 – Frontal head test configuration**



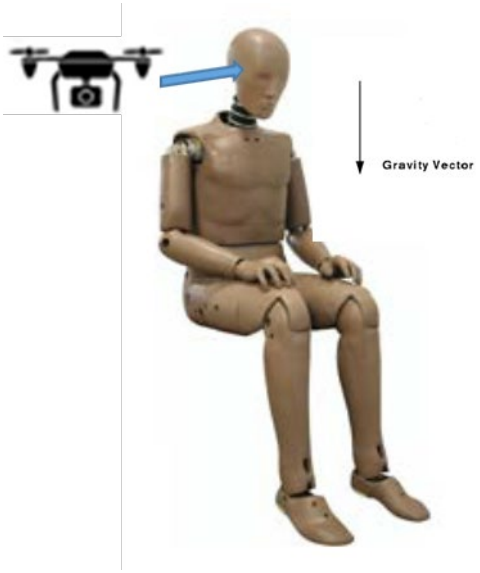

(4) Test 3 - Head Critical Impact Direction. The head critical impact direction test is to impact the head of the ATD at the Critical Orientation at the Critical Speed. A minimum of two (2) test shall be done in this orientation.

**Figure C-3 – Head critical impact direction test configuration**




(5) Test 4 - Head Side Impact. The head side impact test is to impact the head of the male ATD from the side at the Operating Speed, and normal flight orientation. A minimum of 2 tests shall be done in this orientation in order to reduce possible variability.

**Figure C-4 – Head side impact test configuration**




**Information Note**: It may be possible to evaluate the Head Injury Criteria (HIC) using alternative tests. It is recommended that if other methodologies are being used the manufacturer coordinate with TCCA to support a collaborative development process.

## 6.0 Test articles

(1) General. In all cases, the test article (i.e. RPAS) shall be representative of the final production article and shall include a structural frame, motors, propellers, electronics, batteries, and payload. It shall also include functioning servos, if any. The RPAS does not necessarily need to be powered. The configuration of each RPAS used in each impact test shall be documented, and this configuration should conform to the production specification of the RPAS for which a declaration will be provided. Specific modifications to the RPAS which are made to support or conduct the tests shall be clearly documented along with their potential impacts on the results of the tests. If the RPAS has several configurations (i.e. different batteries/props/gear/payload) that are to be tested, the declarant must either test each configuration, or document why a certain configuration represents the worst case scenario, and then test that configuration.

(2) Cameras. The payload may be replaced by a dummy-load made of representative shape, stiffness, and mass.

(3) Item of mass. Defined as any part of the RPA that can detach during impact (e.g. removable cameras, batteries) and may become a projectile with enough energy to cause a serious injury (see section 6.5) to a person. Detachment of these items are grounds for re-test and the means of restraint for these items should be improved by changes to design or implementation. Detachment of an item of mass should not leave any sharp or injurious edges. Once retention of an item of mass has been demonstrated using the standard RPAS configuration, subsequent tests may be conducted with the item secured by means other than those in the standard operational configuration for the purposes of the test (if required).

   (a) Batteries. Batteries that present a potential for fire during impact should be discharged as much as possible to minimize the fire risk. The batteries should be tested separately to demonstrate that there is no risk of fire at impact (many battery manufacturers perform such tests as part of their development process). The manufacturer should maintain a report of the battery impact test, with photographic or video evidence, to demonstrate the battery does not catch fire at impact.

   (b) Used Articles. Test units shall not be used for more than one test except if the test article is found to be mechanically equivalent to the original configuration. In this case, a report stating the method used to determine the equivalence shall be completed. For example, visual inspection of composite material may find the impacted materials to be mechanically equivalent to the original configuration, but micro-cracks may not be visually distinct.

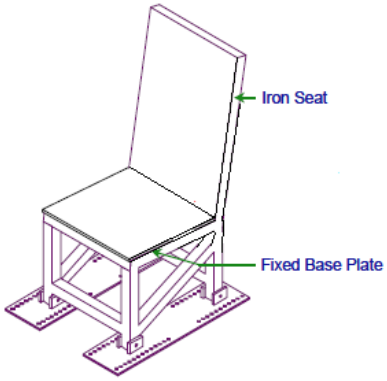
   (c) Critical Components. Design changes may influence other performance parameters such as HIC. The following summarizes critical elements relative to the assessment criteria.

(4) The frame is the basic layout upon which the rest of the structure is built. The frame supports the motors and various other devices in a way that they maintain stability during the flight and keep the vehicle levelled. There are several frame types that define the multi-rotor or fixed wing RPA. The modification of material may change the impact characteristics of the RPA. Thus, the HIC may need to be reassessed.

## 7.0 Test setup and test preparation

(1) General. The test setup dictates how the impact loads are introduced into the ATD and how the ATD reacts. Every effort should be made to introduce and react to loads as realistically as possible. To aid this, the ATD shall be seated in a rigid position in order to obtain conservative results, and used to control variability. The seat should be rigid in order to avoid any type of deformation that may alter the test results (Figure C-5).

**Figure C-5 – ATD test seat setup**




The ATD should be seated in a straight position, and a restraint system may be needed depending on the test facilities and ATD configuration. In addition, attention should be given to positioning the ATD against the seat back and to proper positioning of the ATD's arms and legs. Demonstration of compliance with the HIC should address critical cases (as noted above). From these cases, the flight envelope will be defined. The evaluation showing HIC of 700 or less shall be from an ATD head impact that is a solid strike and not a glancing blow. Dynamic tests are conducted with an ATD (or equivalent) that is representative of a 50th percentile male occupant.

Compliance with the HIC is dependent on the details of the RPAS design as well as the test Setup.

Preparation for tests involves positioning and securing the ATD, the RPAS, and the instrumentation. This is done for the specific critical condition being tested. Preparations that pertain to the normal operation of the test facility, such as safety provisions and the actual procedures for accomplishment of the tests, are specific to the test facility and are not addressed in this circular.

## 7.2 Test facilities

(1) General. There are a number of test facilities that can be used to accomplish dynamic testing scenarios identified in section 22.0 above. Any of the following test devices are acceptable to perform the testing, as well, other test devices, facilities, or mechanisms may be used provided they provide the same capabilities regarding the measurement of the impacts and the reproducibility of the tests.

(2) RPAS Launcher. In this case, the RPAS is launched towards the ATD as a projectile. This test facility may present difficulties in obtaining the right exit speed, and orientation due to influence of aerodynamic surfaces of the RPAS. In this case the impact angles can be obtained by changing the seat location and angle with respect to the launcher, or the launcher may change its location and position so different angles of impact may be tested.

Photometric film coverage of the RPAS at the exit of the launcher may be used to define the orientation of the RPAS. Also, the exit speed may be measured to make sure that the maximum speed is obtained, and the impact impulse is obtained at the speed required for that particular test case.

Side cameras should be used to provide film coverage of the test. Side cameras need to be at each side of the ATD, and on the top in order to provide a good indication of the RPAS orientation during impact. This will assist in determining if the worst case (as defined above) was achieved.

(3) Sled Tester. If a sled tester is used for this test the recommendations of FAA AC 25.562 for this type of test facility shall be followed, or equivalent.

(4) Drop Tower. Drop towers are one of the easiest facilities to build and operate; as a result, they are frequently used for these types of tests. In these facilities, the pull of earth's gravity is used to accelerate the RPA to impact velocity so the need for a complex mechanical accelerating system is eliminated. The seat angle can be changed in order to achieve the required test scenario geometries. Special care should be taken to ensure variations of sit orientation do not prevent the ATD from achieving the right posture for the test.

Side cameras should be used at each side of the dummy as well as above the ATD in order to provide a good indication of the RPAS orientation during impact. This will assist in determining if the worst case (as defined above) was achieved.

### 7.3 Anthropomorphic test devices

(1) General. The use of the 50th percentile male Hybrid III test dummy specified in 49 CFR part 572, subpart E, is required unless TCCA agrees with other type of ATD.

(2) Calibration. ATD load cells shall be calibrated on an "as needed" basis, or a minimum of once per year, whichever comes first. ATD accelerometers shall be calibrated on an "as needed" basis, or a minimum of once every six months whichever comes first. Need is determined by a pre- and post-test shunt calibration. If the bridge balance remained unchanged after the test, and if full-scale shunt calibration results in the same value as the pre-test value, then the transducer characteristics are within calibration. If loads become suspect, linearity of the load cell will be checked with a universal compression testing machine. Exact calibration procedure can be found in National Highway Traffic Safety Administration Test Procedure TP208-14 Appendix A (Part 572E (50th Male) Dummy Performance Calibration Test Procedure.

(3) Maintenance. Anthropomorphic dummies used in the tests shall be maintained to perform in accordance with the requirements described in their specification. Periodic teardown and inspection of the ATD should be accomplished to identify and correct any worn or damaged components, and appropriate ATD calibration tests (as described in their specification) should be completed if major components are replaced.

(4) Setup. The ATD shall be placed in the test fixture seat in a way to ensure repeatability of the tests, and to ensure the maximum transfer of energy between the RPAS and the ATD representing the worst-case impact on the ATD. As such the following ATD setup is recommended:

(a) The ATD should be placed in the center of the test fixture seat in as nearly a symmetrical position as possible. The ATD should be placed in the seat in a uniform manner so as to obtain reproducible test results.

(b) The ATD's back should be against the seatback without clearance. This condition can be achieved if the ATD's legs are lifted as it is lowered into the seat. Then the ATD is pushed back into the seatback as it is lowered the last few inches into the seat pan. Once all lifting devices have been removed from the ATD, the ATD should be "rocked" slightly to settle it in the seat.

(c) The ATD's knees should be separated about four inches.

(d) The ATD's hands should be placed on the top of its upper legs, just behind the knees.

### 7.4 Instrumentation

(1) General. Electronic and photographic instrumentation systems shall be used to record data for qualification of RPAS. Electronic instrumentation should measure the test environment and

measure and record data required for the comparison of performance to established pass/fail criteria. Photographic instrumentation should be used to document the overall results of tests.

(2) Electronic Instrumentation. Electronic instrumentation should be accomplished in accordance with the Society of Automotive Engineers Recommended Practice SAE J211, “Instrumentation for Impact Tests,” using the sign convention of SAE J1733 “Sign Convention for Vehicle Crash Testing.” In this practice, a data channel is considered to include all of the instrumentation components from the transducer through to the final data measurement, including connecting cables and any analytical procedures which may alter the magnitude or frequency content of the data. Each dynamic data channel is assigned a nominal channel class equivalent to the high frequency limit for that channel based on a constant output/input ratio versus frequency response plot, which begins at 0.1 Hz (+1/2 to -1/2 dB) and extends to the high frequency limit (+1/2 to -1 dB). Frequency response characteristics beyond this high frequency limit are also specified. When digitizing data, the sample rate should be at least five times the 3 dB cutoff frequency of the pre-sample analog filters. Since most facilities set all pre-sample analog filters for Channel Class 1000, and since the 3 dB cutoff frequency for channel class 1000 is 1650 Hz, the minimum digital sampling rate would be about 8000 samples per second. For the dynamic tests discussed in this in this appendix the dynamic data channels shall comply with the following channel class characteristics:

(a) Launcher or drop tower vehicle acceleration is measured in accordance with the requirements of Channel Class 60;

(b) ATD head accelerations used for calculating the Head Injury Criterion (HIC) are measured in accordance with the requirements of Channel Class 1000;

(c) The full-scale calibration range for each channel provides sufficient dynamic range for the data being measured; and

(d) Digital conversion of analog data provides sample resolution of not less than 1 percent of full-scale input.

**Note:** On the selection of data channel, SAE J 211, paragraph 5, states, "that selection of frequency response class is dependent upon many considerations, some of which may be unique to a particular test." Further, SAE J211 notes, "the channel class recommendations for a particular application should not be considered to imply that all the frequencies passed by that channel are significant for the application. Accordingly, the TCCA seeks comments on an appropriate CFC for evaluating data.

(3) Photographic Instrumentation. Photographic instrumentation is used for documenting the response of the ATDs and the test items to the dynamic test environment. Both high-speed video and static imaging cameras should be used. The following recommendations for the selection, installation, and calibration of the photographic instrumentation should be relied on as best practices:

(a) Photographic instrumentation should be selected in accordance with SAE J211, Part 2;

(b) Photo instrumentation methods should not be used for measurement of acceleration

(c) High-speed cameras that provide data used to calculate displacement or velocity should operate at a minimum nominal speed of 1000 frames per second;

(d) Cameras operating at a nominal rate of 1000 frames per second or greater may be used to document the response of ATDs and test items if measurements are not required.

(e) The locations of the camera and targets or targeted measuring points within the field of view should be measured and documented;

(f) Targets should be at least 1/100 of the field width covered by the camera, and should be of contrasting colors or should contrast with their background;

(g) The center of the target should be easily discernible;

(h) A description of photographic calibration boards, or scales, should be within the camera field of view;

(i) The following should be documented for each test:

Camera lens focal length;

Camera and lens make;

Camera and lens model; and

Camera and lens serial numbers.

(j) Appropriate digital or serial timing should be provided on the image media.

(k) Rectilinearity of the image is documented in accordance with SAE J211, Part 2.

If the image is not rectilinear, as indicated by an overall error in excess of 1 percent, appropriate correction factors should be used in the data analysis process.

(l) Still image cameras should be used to document the pre-test installation and the post-test response of the ATDs and the test items. At least four pictures should be obtained from different positions around the test items in pre-test and post-test conditions.

(m) A description of the timing signal(s), the offset of the timing signal to the image(s), and the means of correlating the time of the image(s) with the time of the electronic data shall be provided.

(n) A rigorous, verified analytical procedure should be used for data analysis. The accuracy of the procedure is considered adequate, if the difference between the measured and derived distance separating the Validation Target Pair, as defined in SAE J211, Part 2, is not greater than 1.0 cm (0.4 inches).

(4) Setup. Professional practice should be followed when installing instrumentation. Test Facility instrumentation shall follow SAE J211.

## 8.0 Hazards

(1) This test method involves impacts with significant kinetic energy and RPAS may have parts which (as discussed above) may come free and result in injuries to test participants if hazards are not appropriately identified and mitigated. The test apparatus should be set up to control the RPAS impact such that it remains within the test apparatus throughout the impact. The test apparatus should be designed to prevent flying debris from becoming a hazard. Participants should use appropriate personal protective equipment (PPE), or remain protected during the test. When testing an RPAS with power plants and/or lithium batteries, appropriate fire extinguishing equipment for each application should be easily accessible. Participants should be made aware of the hazards of lithium batteries and which fire extinguishers are appropriate for lithium-based fires. In case of a battery fire, it should be documented design changes to the battery may be required (depending on failure analysis). A retest of the battery at the same impact level shall be done until no fire hazards are presented.

## 9.0 Test failures vs. retest.

(1) A variety of failures can result in an unsuccessful test. Failures can range from not obtaining the adequate orientation. All such failures should be addressed and corrective action taken. However, the necessity of repeating tests following corrective action is the same decision process as that used to determine which tests are initially conducted.

(2) If a test exceeds the minimum test conditions and results in a failure, an assessment of the test conditions, and a rational basis for retest without a design change shall be presented to allow a retest without modification.

## 10.0 Test reporting

(1) General. As required by record keeping requirements, the results of verifications associated with the technical requirements of CAR Standard 922 shall be maintained by the manufacturer. To this end, test reports created from the raw and analyzed test data associated with the test procedures in this appendix shall be created and maintained to demonstrate the tests have been completed and that all requirements of this appendix have been met.

## 11.0 Data requirements

(1) General. The data generated as a result of tests and analysis should include charts, listings, and/or tabulated results, along with copies of any photo instrumentation used to support the results. The following should be recorded:

(a) Impact pulse shape;

(b) Head and Neck sensor impact response;

(c) Chest sensor impact response;

(d) Total velocity change in the RPAS;

(e) Maximum resultant acceleration recorded by dummy head form on each of three axes: $a_x$, $a_y$, $a_z$ with the magnitude of the acceleration $a_{mag}=(a_x^2+a_y^2+a_z^2)^{1/2}$;

(f) Maximum rotational acceleration recorded by the dummy head form on each of three axes ($\dot{\omega}$ x, $\dot{\omega}$ y, $\dot{\omega}$ z);

(g) Calculated kinetic energy experienced by the ATD;

(h) Retention of Cameras, batteries or other parts that can detach during impact;

(i) Angle of Impact and Mass of the RPAS;

(j) Recording of video impact of collision and vehicle and ATD response at no less than 1000 frames/sec; and

(k) Any notes about the details of the impact. Any damage to the RPAS shall be noted.

## 12.0 Data analysis

(1) General. All data obtained in the dynamic tests should be reviewed for errors. Baseline drift, masking, ringing, and other common electronic instrumentation problems should be detected and corrected before the tests executed. Loss of data during the test is readily observed in a plot of the data versus time and is typically indicated by sharp discontinuities in the data, often exceeding the amplitude limits of the data collection system. If these occur early in the test in essential data channels, the data should be rejected and the test repeated. If they occur late in the test after the peak data in each channel has been recorded, the validity of the data should be carefully evaluated, and the maximum values of the data may still be acceptable for the tests described above. The instrumentation, collection of data, and filtering of that data in these tests shall meet the requirements of SAE J211-1: Instrumentation for Impact Test. Refer to Table C-1 for injury parameter cutoff values associated acceptable values for injuries.

(2) Impact Pulse Shape. The pulse shall meet the requirements of SAE 1727 Calculation Guidelines for Impact Testing.

(3) Total Velocity Change. The speed of the RPAS just prior to the time of impact shall be measured for each test point. Video of the impact made perpendicular to the fall, with a way of measuring the distance travelled between frames (e.g. radar, ultrasonic distance measurements, or other sensors). The uncertainty of the measurement shall be documented. When making such a computation the possible errors of the time and displacement measurements are used to calculate a possible velocity measurement error, and the test impact velocity should exceed the terminal velocity calculated in the critical case analysis by at least the velocity measurement error.

(4) Head and Neck.

(a) Head injury mechanism. There are three major types of head injury by direct impact:

(b) Brain injury: Brain injury can be produced by high accelerations to the entire brain producing injuries often related to impacts with rigid flat or semi blunt objects, or it can be produced by a direct impact to a local area of the brain from minor contusions (bruising) to direct penetration of the brain often related to blunt or sharp object impacts. Brain injury is not covered in this AC.

(c) Skull fracture: Skull fracture can be produced by direct impact. Cranial fractures can be produced by two different impact-loading mechanisms.

Impact with a flat surface producing linear type fractures

Impact with a blunt object producing localized depressed fractures

(d) Facial lacerations: caused by sharp objects are likely to have discrete edges but may extend deeply and involve underlying structures, such as the muscles of facial expression, nerves, and arteries. Wounds caused by blunt forces burst the skin open, damage cells, and produce tissue edema, which slows the wound-healing process. Therefore, a mitigation needs to be used to reduce the risk of these type of injuries. For example, rotor guards, blade stoppage, detect and stop and others. These mitigations will need to be flight tested to show their effectiveness. The results of the test should be annexed to the test results report. The AC does not account for laceration's injury criteria, and it is shown on table C-1 as pass or fail criteria only.

(e) We consider a HIC value calculated with a time interval that maximizes the HIC value up to a 15 ms period, and not 36 ms, which is generally used for car occupants. The main reason is that head impact to an RPAS structure is very short, only a few milliseconds of contact. Thus while the time interval used in the calculation may be up to 15 ms, depending on the design of the RPA, a period of only a few milliseconds can be expected for this calculation.

(f) At this moment, this AC will evaluate head injury risk mainly on the basis of head injury criterion (HIC) with a time interval that maximizes the HIC value, up to a 15 ms limit, over which it is calculated. A HIC value of 1000 is equivalent to approximately a 15 per cent risk of AIS 4+ head injury whereas a HIC 700 to 5 percent risk of AIS 4+ head injury. A "severe" injury is one with a score of 4+ on the Abbreviated Injury Scale (AIS). The maximum calculated HIC-15 value shall not exceed 700, and the maximum peak acceleration shall not exceed 237g.

(g) Neck. The resulting neck injury criteria, called "$N_{ij}$", propose critical limits for all four possible modes of neck loading; tension or compression combined with either flexion (forward) or extension (rearward) bending moment. The $N_{ij}$ is defined as the sum of the normalized loads and moments. The calculation shall meet the requirements of SAE

1727 Calculation Guidelines for Impact Testing. The $N_{ij}$ should not exceed a value of 1.21, it was estimated to represent an 30 percent risk of AIS 3 injury.

(h) The shear force ($F_x$), axial force ($F_z$), and bending moment ($M_y$) shall be measured by the dummy upper neck load cell for the duration of the crash event as specified in FMVSS 208 S4.11. Shear force, axial force, and bending moment shall be filtered for $N_{ij}$ purposes at SAE Recommended Practice J211.

(i) During the event, the axial force ($F_z$) can be either in tension or compression while the occipital condyle bending moment ($M_{ocy}$) can be in either flexion or extension. This results in four possible loading conditions for $N_{ij}$: tension-extension ($N_{te}$), tension-flexion ($N_{tf}$), compression-extension ($N_{ce}$), or compression-flexion ($N_{cf}$).

(j) When calculating $N_{ij}$, the critical values, $F_{zc}$ and $M_{yc}$, are:

$F_{zc}$ = 6806 N (1530 lbf) when $F_z$ is in tension

$F_{zc}$ = 6160 N (1385 lbf) when $F_z$ is in compression

$M_{yc}$ = 310 Nm (229 lbf-ft) when a flexion moment exists at the occipital condyle

$M_{yc}$ = 135 Nm (100 lbf-ft) when an extension moment exists at the occipital condyle.

(k) At each point in time, only one of the four loading conditions occurs and the $N_{ij}$ value corresponding to that loading condition is computed and the three remaining loading modes shall be considered a value of zero. The expression for calculating each $N_{ij}$ loading condition is given by:

$N_{ij} = (F_z/F_{zc}) + (M_{ocy}/M_{yc})$

Each of the four Nij values shall not exceed 1.0 at any time during the event.

Peak tension. Tension force ($F_z$), measured at the upper neck load cell, shall not exceed 4170 N (937 lbf) at any time.

Peak compression. Compression force ($F_z$), measured at the upper neck load cell, shall not exceed 4000 N (899 lbf) at any time.

Unless otherwise indicated, instrumentation for data acquisition, data channel frequency class, and moment calculations are the same as given for the 49 CFR Part 572, Subpart E Hybrid III test dummy.

(5) Chest. Chest injury risk is evaluated on the basis of spine acceleration, and sternum deflection rate. A sternum deflection of 63 mm represents either a 45 or 70 percent risk of an AIS 3+ chest injury.

(a) The resultant acceleration calculated from the output of the thoracic instrumentation shown in drawing 78051.218, revision R incorporated by reference in 49 CFR part 572, subpart E of US Code of Federal Regulations, Title 49 shall not exceed 60 g's, except for intervals whose cumulative duration is not more than 3 milliseconds.

(b) Compressive deflection of the sternum relative to the spine shall not exceed 63 mm (2.5 in).

**Table C-1**

| Body Region | Parameter | Values not to exceed | Measurement | | | |
|---|---|---|---|---|---|---|
| | | | C-1 | C-2 | C-3 | C-4 |
| **Head** | HIC-15 | 700 | | | | |
| | Peak Acceleration (g) | 237 | | | | |
| **Neck** | $N_{ij}$ | 1.21 | | | | |
| | $F_z$ Tension (N) | 4170 | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | $F_z$ Compression (N) | 4297 | | | | |

(6) Note: These injury metrics have an associated risk of a specific level of injury, typically based on the Abbreviated Injury Scale (AIS). The AIS is an anatomical-based coding system developed by the Association for the Advancement of Automotive Medicine that classifies and ranks the severity of specific injuries. It represents the threat to life associated with the injury rather than the comprehensive assessment of the severity of the injury. An AIS value of two is denoted as moderate, a value of three is denoted as serious, and a value of four is denoted as severe.

(a) Based on the following technical requirements UN ECE R94, GTR No.9 Pedestrian Safety, FAA AC 25.562, and FMVSS 208.

(b) Table C-1 provides a summary of test pass criteria and provides the applicant guidance on how to present and collect information.

## 13.0 Test documentation

(1) General. The tests should be documented in reports that describe the procedures, limitations, results, and deviations to the tests discussed in this appendix.

(2) Facility data. In order to clearly document the facilities (see section C7.2) in which the tests took place the following facility information shall be documented in the test report:

(a) The name and address of the test facility performing the tests;

(b) The name and telephone number of the individual at the test facility responsible for conducting the tests;

(c) A brief description and/or photograph of each test fixture;

(d) Statements confirming:

All instrumentation and data collection equipment used in the test meet the facility's internal calibration requirements;

These calibration requirements are documented and available for inspection upon request;

All calibrations are traceable to a national standard; and

The records of current calibration of all instruments used in the test are maintained at the facility.

(e) A statement confirming the data collection was done in accordance with the recommendations in this appendix, or a detailed description of the actual procedure used and technical analysis showing equivalence to the procedures and expected outcomes of this circular;

(f) The manufacturer, governing specification, serial number, and test weight of the ATDs used in the tests, and a description of any modifications or repairs performed on the ATDs which may cause them to deviate from the specification; and

(g) A description of the photographic-instrumentation system used in the tests.

(3) RPAS Data. As the RPAS is the unit under test in this case, detailed information on test articles helps ensure the requirements were appropriately met. This data includes, but is not limited to:

(a) The manufacturer's name and identifying model numbers of the RPAS used in the tests with a brief description of the system, including identification and a functional description of all major components and photographs or drawings, as applicable;

(b) RPAS mass; and

(c) Critical impact direction, terminal velocity, acceleration, and environmental conditions report (as described in this appendix).

(4) Test Description. The description of the test should be documented in sufficient detail, such that the tests could be reproduced simply by following the guidance given in the report. The procedures outlined in this appendix can be referenced in the report, but should be supplemented by such details as are necessary to describe the unique conditions of the tests. For example:

(a) Pertinent dimensions and other details of the installation that are not included in the drawings of the test items should be provided;

(b) The placement and characteristics of electronic and photographic instrumentation chosen for the test beyond that information provided by the facility should be documented. This can include special targets, grids, or marking used for interpretation of photo documentation, transducers, restraint system loads, floor reaction forces, or other measurements beyond those discussed in this appendix;

(c) Any unusual or unique activity or event pertinent to conducting the test should be documented. This could include RPAS damage or support for the ATDs, test items or transducers, operational conditions or activities such as delayed or aborted test procedures, and failures of test fixtures, instrumentation system components, or ATDs; and

(d) The expected structural behavior that will result should be documented.

## 14.0 Conclusions

(1) General. The results of the tests conducted above are expected to inform the operating limitations of the RPAS when conducting operations over people. There are two effective ways of responding to the results of the tests:

(2) Modification of Design. If the results of the tests indicate the RPA will result in measurements which fall above the “acceptable marginal” values described in Table C-1, the RPA may be redesigned utilizing different materials, structural configurations, or equipment mitigations. If this option is chosen, the updated design should be retested against this appendix.

(3) Hard Operational Limits. If the results of the tests indicate there is a speed (or set of speeds) and altitude (or set of altitudes) at which the RPA will have a HIC-15 result which is below the maximum allowed, the manufacturer may provide hard operational limits within their design to restrict the speeds of the RPA to these lower speeds. It should be noted in the case of rotorcraft, the terminal speed is the Critical Speed and as such would most likely result in a redesign of the system if the tests are determined to fail. Mechanisms to restrict operations to ensure the safety of people on the ground must be included as part of the failure mode evaluation as required by the safety assurance process.

(4) In general, the results of these tests should provide the manufacturer enough information to determine the maximum allowable altitudes, speeds, flight configurations, and operational maneuvers of the RPA.

(5) The manufacturer may decide to create a fight mode that allows operating safely over people. Thus, reducing the workload to the Pilot in Command, and considering within this flight mode operational limits allowable altitudes, speeds, flight configurations, and operational maneuvers of the RPA. In this development, the manufacturer should consider the following:

(a) Human Factors

A qualitative evaluation of crew workload and degree of difficulty in all FCS operating modes including manual direct piloting (where applicable) and in all flight phases (e.g. launching strength) should be done in order to demonstrate that the probability of piloting errors is reduced to the minimum. This assessment must include workload evaluation while in emergency conditions.

(b) Transition

It should be possible to make a smooth transition from one flight phase and/or condition to another (including turns and slips) without danger of exceeding the limit load factor, under any probable operating condition, (including, for multi-engine RPA, those conditions normally encountered in the sudden failure of any engine). Where applicable, consideration should be given to the transition from launch phase to normal flight condition, as well as the transition from normal flight condition to recovery phase.

(c) Flight Envelope Protection

Flight envelope protection may be implemented in the flight control system.

Characteristics of each envelope protection feature should be smooth, appropriate to the phase of flight and type of maneuver.

Limit values of protected flight parameters must be compatible with:

RPA structural limits;

With acceptable values of table C-1; and

Required safe and controllable maneuvering of the RPA.

A safe margin to catastrophic failure conditions.

The RPA must respond to intentional dynamic maneuvering within a suitable range of control parameter limits.

Dynamic characteristics such as damping and overshoot must also be appropriate for the maneuver and limit parameter concerned.

Characteristics of the flight control system must not result in residual oscillations in commanded output due to combinations of flight envelope protection limits.

Rapidly engage automatic flight envelope protection in response to flight critical parameters.

Examples of mission maneuvers that may bring about the conditions cited above may include, but are not limited to, in case of rotary-wing RPAS roll reversals, pull-ups, push-overs, rapid sidesteps, and large amplitude heading changes. ADS-33, “Aeronautical Design Standard Performance Specification Handling Qualities Requirements for Military Aircraft” describe these and other maneuvers that may be part of the rotorcraft RPAS mission.

(6) The manufacturer may consider using parachutes in case of emergency conditions; ASTM provides standard in regards to parachutes refer to appendix A of this AC.

# Appendix D – Considerations for the RPAS operating manual

## 1.0 RPAS Operating Manual

### 1.1 General

(1) The example operating manual that was previously provided in this Appendix has been removed. Since the initial release of this advisory circular there have been industry efforts to produce standard and guidance specific to RPAS operating manuals that should be referenced by RPAS manufacturers and declarants. This appendix now contains guidance and special considerations that declarants should understand when preparing the documentation necessary to support their RPAS operationally and ensure continued compliance with the applicable sections of CAR Standard 922.

(2) RPAS Declarants are responsible for communicating to the operators of their RPAS all information needed to ensure safe operation. Declarants should place themselves in the mindset of an operator who might not be intimately familiar with all aspects of the RPAS design. Elements of the RPAS design that might be obvious to the designer might not be obvious to an operator. Consider the following questions when developing an RPAS user manual:

(a) What aspects of the RPAS system architecture does an operator need to understand to make decisions about the safety and serviceability of the RPAS?

(b) What configurable elements of the RPAS are required for continued compliance with the RPAS declaration? Are there configurable elements that are not required on each flight? Are there configurable elements that are only required for certain types of operation?

(c) Are there any operational limitations (procedural, environmental, maintenance, inspection, etc.) that must be met to ensure continued compliance with the declaration to CAR Standard 922?

(d) Are there any specific indications, built-in tests, or RPAS operational behaviours that an operator should be aware of that might indicate that the RPAS is no longer in compliance with the declaration? How does the RPAS react if the C2 link is degraded? What is the effect of extreme environmental conditions (temperature, moisture, precipitation, terrain, etc) on the system?

(e) Operating manuals should be written considering the minimum knowledge, skill and experience expected from the end-user. Are there any minimum qualifications, or specific experience necessary to safely operate the RPAS in accordance with the assumptions made in the declaration? If assumptions related to pilot ability were fundamental to the declaration, it may be necessary to mandate training, currency and proficiency requirements on operators of the RPAS.

### 1.2 Use of Industry Standards

(1) Applicants are encouraged to seek out more recent industry standards (i.e. ASTM F2908-23 or later approved revision) and guidance available from other industry associations (JARUS SORA Annex A)