Australian Government
Department of Defence

ADVISORY CIRCULAR

AC 001/2018

RISK CONTROLS FOR UAS OPERATIONS

V1.0 – March 2018

An Advisory Circular (AC) is issued by the Authority to promulgate important information to the Defence Aviation community, but does not mandate any action. This includes informing the community on aviation safety/airworthiness matters, information that enhances compliance understanding for existing regulation, or policy guidance for aviation issues not yet regulated that requires further understanding.

Audience

This AC 001/2018 applies to:

Applicants for Unmanned Aircraft System Operating Permits (UASOP), Command or Defence Group members who are responsible for authorising Defence Unmanned Aircraft System (UAS) operations, and any other persons who contribute to eliminating or otherwise minimising safety risks due to Defence UAS operations.

Purpose

This AC presents an expansive, but non-exhaustive, list of candidate risk controls for UAS operations. It also presents a tool to help identify where risk controls may be required to improve the safety of UAS operations.

For further information

For further information on this AC, contact DAVCERT-DASA UAS Section at DASA.UAS@defence.gov.au

Status

Version	Date Approved	Released By	Details
1.0	March 2018	DAVCERT	Initial release

Unless specified otherwise, all regulation referenced in this AC are references to the Defence Aviation Safety Regulation (DASR).

1. Reference Material

1.1. Acronyms

AC	Advisory Circular
ACAS	Airborne Collision Avoidance System
ADS-B	Automatic Dependant Surveillance - Broadcast
AMC	Acceptable Means of Compliance
ARS	Autonomous Recovery System
ATC	Air Traffic Control
ATMP	Air Traffic Management Plan
CRM	Crew Resource Management
DASA	Defence Aviation Safety Authority
DASR	Defence Aviation Safety Regulation
EO/IR	Electro-Optical/Infrared
ERP	Emergency Response Plan
EVLOS	Extended Visual Line of Sight
FTS	Flight Termination System
GDT	Ground Data Terminal
GM	Guidance Material
GNSS	Global Navigation Satellite System
GP	General Public
HF	Human Factors
HMI	Human Machine Interface
IMU	Inertial Measurement Unit
JARUS	Joint Authorities for Rulemaking on Unmanned Systems
MAO	Military Air Operator
MEP	Mission Essential Personnel
MTOW	Maximum Take-Off Weight
NOTAM	Notice to Airmen
OEM	Original Equipment Manufacturer
PCAS	Portable Collision Avoidance System
PPE	Personal Protective Equipment
RF	Radio Frequency
RP	Remote Pilot
RPS	Remote Pilot Station

SORA	Specific Operations Risk Assessment
SSR	Secondary Surveillance Radar
TCAS	Traffic Alert and Collision Avoidance System
UA	Unmanned Aircraft
UAS	Unmanned Aircraft System
UASOP	Unmanned Aircraft System Operating Permit
VLOS	Visual Line of Sight
VMC	Visual Meteorological Conditions

1.2. Definitions

The definitions below are specific to the UAS context. Further information on these definitions, including their source, is available in the Guidance Material (GM) to DASR UAS.10.

1.2.1. **Mission Essential Personnel (MEP).** All persons directly associated with the operation of the UAS or briefed as part of the UAS mission.[1]

1.2.2. **General Public (GP).** All persons not classed as MEP, including all persons not directly associated with the operation of the UAS or briefed as part of the UAS mission.

1.2.3. **Critical Infrastructure.** A facility that, if damaged by a UA, may have an immediate and adverse effect on MEP or GP health and safety. Examples may include chemical plants, armament storage facilities, and fuel storage facilities.

1.2.4. **UAS Operator.** The organisation (eg MAO) or person with Operational Control (OPCON) or tasking authorisation for the UAS.

1.2.5. **Populous Area.** An area in relation to the operation of an unmanned aircraft that has a sufficient density of population for some aspect of the operation, or some event that might happen during the operation (in particular, a fault in, or failure of, the unmanned aircraft) to pose an unreasonable risk to the life or safety of somebody who is in the area, but is not connected with the operation.

[1] MEP includes all persons directly associated with the operation of the UAS or briefed as part of the UAS mission. MEP is broader than personnel directly associated with the launch, recovery and control during flight of the UAS. MEP may, depending on the UAS mission, include civilians, Defence personnel, and/or foreign defence personnel. MEP must be aware of the UAS operations, the associated hazards and be essential to the conduct of the UAS task. MEP may include ground troops within a Defence joint operation/exercise area, troops on a Defence ship or civilian personnel operating as part of counter terrorism tasking.

1.2.6. **Remote Pilot (RP)**. The person in direct command/control of the UAS, including manipulating flight controls or programming waypoints during flight.

1.2.7. **Remote Pilot Station (RPS).** A station at which the RP manages the flight of an unmanned aircraft.

1.2.8. **Segregated Airspace.** Airspace of specified dimensions allocated for exclusive use to a specific user(s).

1.2.9. **Unmanned Aircraft (UA).** An air vehicle that flies under remote control or autonomous programming without a human on board in control.

1.2.10. **Unmanned Aircraft System (UAS).** The entire system consisting of the UA, RPS, communications/data links, networks, launch and recovery systems, and personnel required to fly/control the UA.

1.3. References

1.3.1. AAP 8000.011 Defence Aviation Safety Regulations

1.3.2. Work Health and Safety Act 2011 (WHS Act) and Work Health and Safety Regulations 2011 (WHS Regulations)

1.3.3. Safe Work Australia Interpretive Guideline—Model Work Health and Safety Act: The Meaning of ‘Reasonably Practicable’

1.3.4. AAP 7001.054 Electronic Airworthiness Design Requirements Manual (eADRM)

1.3.5. Joint Authorities for Rulemaking on Unmanned Systems (JARUS) guidelines on Specific Operations Risk Assessment (SORA)

2. Background

2.1. The December 2017 release of DASR UAS (ref 1.3.1) presents a substantial change to how Defence regulates UAS. The regulations introduce three categories for UAS operations, namely Certified, Specific and Open. Specific category UAS operations are further sub-categorised into Specific Type A (operations under a UASOP) and Specific Type B (operations under a Standard Scenario).

2.2. A prerequisite for Command/Group authorisation of a UAS operation, regardless of UAS category, is to ensure that risks to health and safety have been eliminated or otherwise minimised so far as is reasonably practicable. Identifying and then applying robust and appropriate risk controls is a key contributor to satisfying this requirement.

2.3. For UAS operated under Open category or Specific Type B, the risk controls listed in the respective DASR UAS regulation and associated AMC should make a substantial contribution to satisfying this requirement.

2.4. Operations under a UASOP, on the other hand, are often typified by a more complex operating environment, and consequently identifying robust and appropriate risk controls can be challenging.

2.5. This AC presents applicants for a UASOP under DASR UAS.30 with tools to assist them in identifying and applying robust and appropriate risk controls. It provides:

2.5.1. a tool for identifying where risk controls might contribute to managing hazards presented by a particular UAS in a particular operating environment, and

2.5.2. a non-exhaustive list of candidate risk controls.

2.6. Finally, while not the primary audience for this AC, Command/Group authorising UAS operations under Open or Specific Type B may use the list of candidate risk controls in this AC to identify additional risk controls beyond those required by DASR UAS.

3. Defence’s approach to risk decisions

3.1. Before presenting the subject UAS tool and risk controls, readers should first understand how this information contributes to satisfying Duty Holder obligations under Australia’s WHS Legislation (ref 1.3.2).

3.2. The WHS legislation requires Duty Holders to eliminate or otherwise minimise risks to health and safety so far as is reasonably practicable. Defence’s approach involves the following six steps:

3.2.1. Establish hazard and risk context

3.2.2. Be reasonably informed (of the risk and possible controls)

3.2.3. Eliminate risk so far as is reasonably practicable

3.2.4. Minimise risk so far as is reasonably practicable by applying hierarchy of control measures

3.2.5. Characterise risk

3.2.6. Decision-to-proceed.

3.3. In executing these six steps, Duty Holders are required to:

3.3.1. consult, co-operate and co-ordinate with other Duty Holders throughout the process

3.3.2. maintain and review the control measures to ensure their effectiveness in ensuring that the risk is eliminated or otherwise minimised so far as is reasonably practicable.

3.4. Figure A-1 depicts this process.

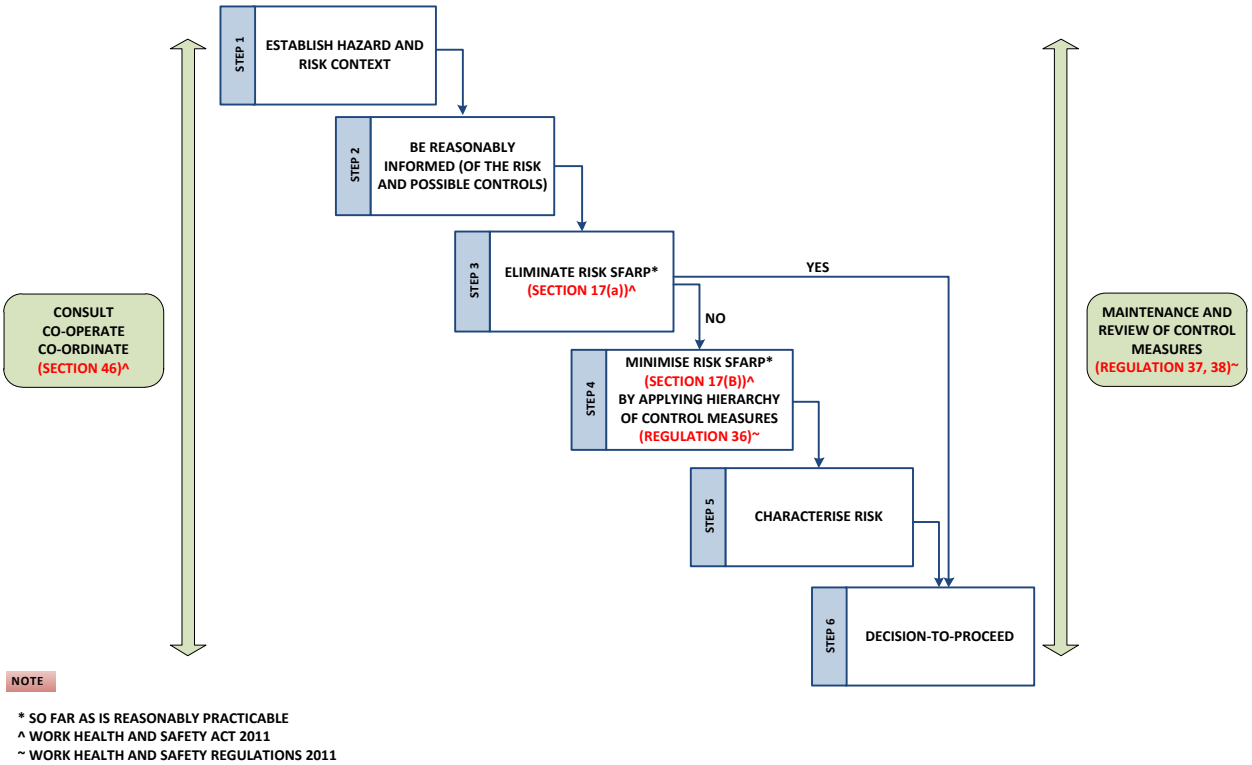

Figure A-1: Defence's approach to risk decisions

3.5. This AC is particularly applicable to Step 2 of this process, since it assists Duty Holders in their endeavours to be reasonably informed of the risk and possible risk controls.

4. A tool for assessing UAS risk controls

4.1. UAS operations present a hazard to other aircraft and to people and critical infrastructure on the ground[2]. Given the potential complexity of some UAS operating environments, a tool to assist in assessing UAS risks can be useful[3]. Some of the more commonly used methods for exploring safety-related risks and risk controls include: Failure Modes and Effects Analysis (FMEA); Hazard and Operability Study (HAZOP); Hazard Identification (HAZID); Fault Tree Analysis (FTA); and Bowtie analysis.

4.2. Each of these methods has its own strengths and weaknesses, and each may contribute a different perspective to the Command/Group's endeavours to robustly manage UAS risks. Defence has previously found the Bowtie analysis to be useful for exploring UAS risk controls.

4.3. Annex A to this AC presents two Bowties that have been developed around key UAS threats and consequences. They may provide the relevant Command/Group with a useful tool for identifying where risk controls are needed, and for producing well-focused risk controls.

4.4. Importantly, these Bowties do not necessarily present a complete solution for every UAS and operating environment; novel UAS applications may present novel hazards, and therefore require expansion of the Bowties.

5. Candidate risk controls for UAS operations

5.1. Risk management for manned aircraft operations has been refined by Defence over many decades, and consequently the available risk controls are generally well understood. Risk management for UAS operations, on the other hand, is rapidly evolving within Defence and the international aviation community. Consequently, knowledge of the hazards presented by UAS operations and identification of available risk controls that best target those hazards, is still developing.

5.2. Annex B to this AC presents a list of candidate risk controls for UAS operations, developed utilising the Bowties at Annex A, encompassing:

5.2.1. UAS design features

5.2.2. RP training and management

5.2.3. Maintenance and engineering

5.2.4. Operational limitations

[2] Throughout this AC, references to people and infrastructure on the ground apply equally to people and infrastructure on the water (eg oil rigs, ships).

[3] DASR UAS does not mandate the employment of a risk assessment tool. It does, however, emphasise the statutory requirement for safety risks to be eliminated or otherwise minimised so far as is reasonably practicable. A tool may assist the relevant Command/Group in that endeavour, particularly for more complex operating environments.

5.2.5. Operational procedures

5.2.6. Operational planning.

5.3. Each candidate risk control is accompanied by a description of the particular hazard/s it aims to manage (extracted from the Bowties at Annex A), and some of the features that would improve its effectiveness. This list is context dependent and as such not every control will be relevant to every UAS operation.

5.4. The list of candidate risk controls at Annex B is not exhaustive. First, novel UAS applications may present novel hazards, and therefore may require additional risk controls. Secondly, those persons directly associated with a particular UAS and its operation (eg UAS Operators, RPs, engineers, trainers) are best placed (and responsible) to identify and implement other reasonably practicable controls[4].

6. Sequence of applying risk controls

6.1. This AC provides no advice on the sequence in which controls must be applied to ensure that UAS hazards are eliminated[5] so far as is reasonably practicable; and if this is not possible, to ensure that UAS risks are minimise[6] so far as is reasonably practicable by applying the mandated hierarchy of controls[7]. Such decisions are context dependant, and remain the duty of the persons designing, manufacturing, maintaining, importing, supplying, commissioning and/or operating the UAS for Defence purposes.

7. AC Currency

7.1. This AC will remain current until cancelled by DASA.

Annexes:

A. Bowties for assessing UAS risk controls
B. Candidate risk controls for UAS operations

[4] *WHS Act 2011* Section 18
[5] *WHS Act 2011* Section 17.a
[6] *WHS Act 2011* Section 17.b
[7] WHS Regulation 36

BOWTIES FOR ASSESSING UAS RISK CONTROLS

1. Due to the potential complexity of some UAS operating environments, a risk assessment tool can assist in assessing UAS risks. This annex presents Bowties that have been developed around selected UAS hazards and consequences. Importantly, these Bowties do not present a complete representation for every UAS and operating environment.

Note: This annex expects the reader to be familiar with the Bowtie methodology.

2. Risk context

2.1. UAS operations present a hazard to other (manned) aircraft, and to people on the ground (either directly or through damaging critical infrastructure[8]). There are differences in risk context, and therefore risk treatments, between these groups, so it makes sense to create two separate Bowties. The following two sections of this annex present the two Bowties.

3. Bowtie for assessing hazards to other aircraft

3.1. This section presents a Bowtie for situations where UAS operations may present a hazard to other (manned) aircraft.

3.2. The Bowtie methodology initially requires identification of possible adverse consequence(s), a description of the unwanted (or 'top') event, and identification of the potential threats. For the context of a UAS presenting a hazard to other aircraft, the following have been selected:

3.2.1. ***Possible adverse consequence.*** In the case of a collision between a UAS and an aircraft, it is appropriate to simply consider the worst credible outcome, namely catastrophic damage to the other aircraft as a result of a mid-air collision.

3.2.2. ***Unwanted event.*** Several different unwanted (or 'top') events could correctly and usefully be used in this Bowtie. In this AC we have settled on the event of "separation breakdown", since as soon as a loss of separation occurs, safety margins begin to deplete. Separation standards and requirements vary based on the type of airspace and are defined by the Air Traffic Service (ATS) provider.

3.2.3. ***Threats.*** In this AC we have settled on the following five threats that could lead to separation breakdown:

[8] The DASR UAS context for Critical Infrastructure may differ to other domains. Refer to the definition at paragraph 1.2 of this AC.

1. loss or degradation of datalink[9]
2. loss or degradation of positional information[10]
3. UAS technical failure rendering the UA unresponsive[11]
4. other airspace users[12]
5. RP error or loss of situational awareness[13].

Note: These threats could be further decomposed or grouped differently, and could still result in a valid and useful Bowtie. The approach employed in this AC was to compile an extensive list of root causes, and then aggregate them into 'threats' that would later be meaningful for the creation of well-focused risk controls. The list of root causes has been included at Appendix 1 to this annex, since they provide clarity on the meaning of each of these five threats.

3.3. Figure A-2 presents the resulting Bowtie that covers hazards to other aircraft. It shows that the five identified threats could lead to the unwanted event (separation breakdown), and this could lead to the identified adverse consequence (catastrophic damage to other aircraft).

3.4. The Bowtie also makes provision for the implementation of 'barriers' (ie risk controls). The 'threat barriers' on the left are aimed at reducing the likelihood of the top event, while the 'harm barriers' on the right are aimed at reducing the likelihood and/or severity of the adverse consequence. Candidate barriers are presented in Annex B to this AC.

[9] The availability, reliability, continuity and integrity of the datalink is a key enabler for the RP's ability to control the UA inflight even if the UA does not require active control at all times. Loss or degradation of datalink will impede the RP's ability to control the UA and can therefore lead to separation breakdown.
[10] Positional information of suitable accuracy, integrity, continuity and functionality can be critical for aircraft separation. Loss or degradation of positional information (including misleading positional information) will impede the RP's ability to maintain safe separation with another aircraft.
[11] UAS technical failures can result in a loss of positive control due to the UA being unresponsive to commands or responding unpredictably. In these cases a separation breakdown can occur.
[12] The presence of other airspace users is a contributing factor to separation breakdown. If there is a failure in planning or procedures by the UAS operator or other airspace users, or if there is an error by another airspace user or technical failure with another aircraft, then a separation breakdown can occur.
[13] An error by the RP can be a contributing factor to a separation breakdown with another aircraft. Errors include incorrect or no commands (in a case where RP intervention is needed). The unique nature of UAS operations, with the pilot removed from the aircraft, increases the likelihood of RP errors and loss of situational awareness.

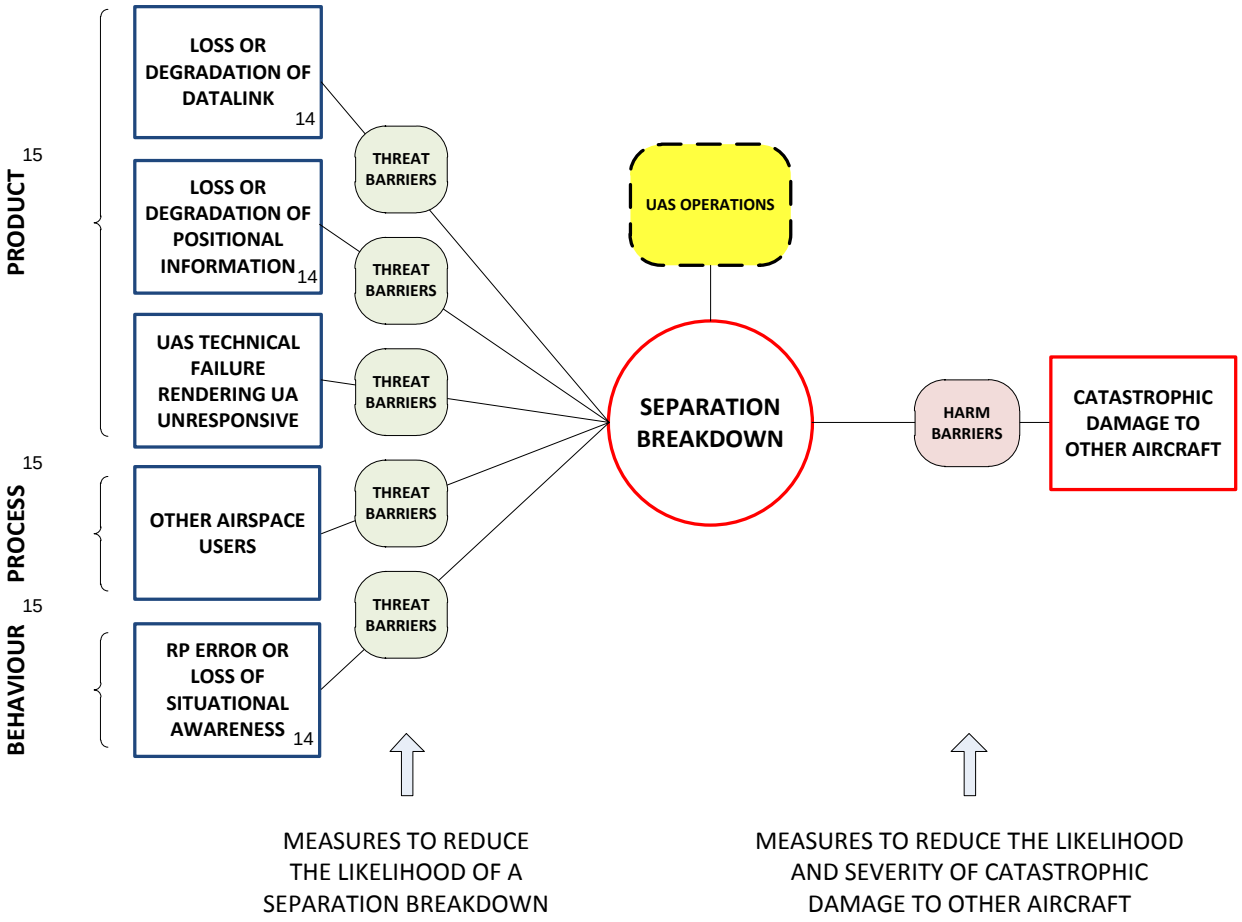

Figure A-2: Bowtie for assessing hazards to other aircraft

4. Bowtie for assessing hazards to people on the ground and critical infrastructure

4.1. This section presents a Bowtie for situations where UAS operations may present a hazard to people and/or critical infrastructure on the ground.

4.2. The Bowtie methodology initially requires identification of the possible adverse consequence(s), a description of the unwanted (or 'top') event, and identification of the range of threats. For the context of a UAS presenting a hazard to people on the ground (either directly or through damaging critical infrastructure), the following have been selected:

4.2.1. ***Possible adverse consequences.*** Three separate consequences have been defined for this Bowtie, as follows:

- injury/fatality to the General Public

[14] Common to both Bowties.
[15] It is common in Defence Aviation Safety to employ Bowties that utilise threat lines to address threats related to product, process or behaviour integrity. The association of product, process and behaviour to threats identified for hazards presented by UAS operations has been clarified in the figure.

- injury/fatality to Mission Essential Personnel

- damage to critical infrastructure.

Note: While injury and fatality could have been included as separate consequences, the risk controls are often identical so they have been combined. Conversely, even though GP and MEP are owed the same duty of care under law, the risk controls for GP and MEP can potentially be quite different, so it makes sense for GP and MEP risk controls to be separately identified. Finally, while damage to critical infrastructure could be directly considered during these GP/MEP assessments, separating it provides for more focused risk controls.

4.2.2. ***Unwanted event.*** Several different unwanted (or 'top') events could correctly and usefully be used in this Bowtie. In this AC we have settled on the event of "unintended descent", since this is the point at which safety margins for people on the ground begin to deplete. Unintended descent is also used to cover controlled flight into terrain.

4.2.3. ***Threats.*** In this AC we have settled on the following five threats that could lead to unintended descent:

1. loss or degradation of datalink[16]

2. loss or degradation of positional information[17]

3. UAS technical failure precluding continued flight[18]

4. adverse operating conditions[19]

5. RP error or loss of situational awareness[20].

Note: These threats could be further decomposed or grouped differently, and could still result in a valid and useful Bowtie. The approach employed in this AC was

[16] The availability, reliability, continuity and integrity of the datalink is a key enabler for the RP's ability to control the UA inflight even if the UA does not require active control at all times. Loss or degradation of datalink will impede the RP's ability to control the UA and can therefore lead to an unintended descent.
[17] Positional information of suitable accuracy, integrity, continuity and functionality can be critical for terrain avoidance and for maintaining planned separation from communities and infrastructure. Loss or degradation of positional information (including misleading positional information) can jeopardise this separation.
[18] UAS technical failures can preclude continued flight of the UA and lead to an unintended descent. In some cases the RP may retain limited control of the UA (eg engine failure causing the UA to descend but RP is able to control the glide) or the RP may have no control (eg catastrophic structural failure).
[19] Adverse operating conditions may affect UA systems and cause an unintended descent. Adverse conditions include weather conditions beyond UAS design limits (eg rain, turbulence, lightning) and impact damage (eg hail, hostile fire, birds, another aircraft).
[20] An error by the RP can be a contributing factor to an unintended descent. Errors include incorrect or no commands (in a case where RP intervention is needed). The unique nature of UAS operations, with the pilot removed from the aircraft, increases the likelihood of RP errors and loss of situational awareness. Controlled flight into terrain, when the RP is in full control of the UA, is also considered an RP's error in failing to initiate relevant manoeuvres.

to compile an extensive list of root causes, and then aggregate them into 'threats' that would later be meaningful for the creation of well-focused risk controls. The list of root causes has been included at Appendix 1 to this annex, since they provide clarity on the meaning of these five threats.

4.3. Figure A-3 presents the resulting Bowtie that covers hazards to people on the ground (either directly or through damaging critical infrastructure). It shows that five threats could lead to an unwanted event (unintended descent), and this could lead to three adverse consequences.

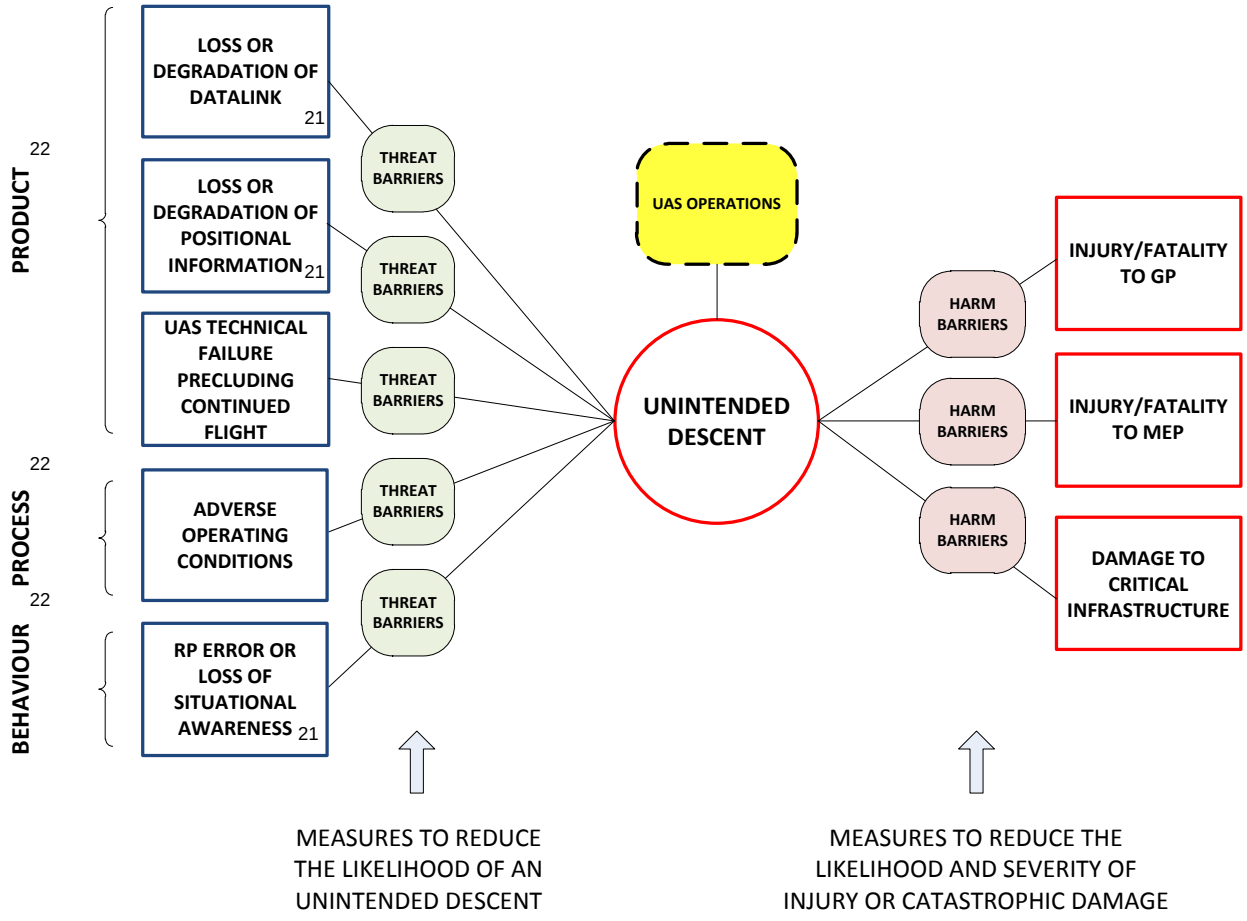

Figure A-3: Bowtie for assessing hazards to people on the ground

4.4. The Bowtie also makes provision for the implementation of 'barriers' (ie risk controls). The 'threat barriers' on the left are aimed at reducing the likelihood of the top event, while the 'harm barriers' on the right are aimed at reducing the likelihood and/or severity of the adverse consequences. Candidate barriers are presented in Annex B to this AC.

[21] Common to both Bowties.
[22] It is common in Defence Aviation Safety to employ Bowties that utilise threat lines to address threats related to product, process or behaviour integrity. The association of product, process and behaviour to threats identified for hazards presented by UAS operations has been clarified in the figure.

4.5. Note that the threats identified in the two Bowties are mostly the same, representing a total of seven separate threats. The reader might question whether the two Bowties should be combined into one Bowtie which alone depicts the seven threats. While this is an option, the risk controls can be quite different in terms of approach and criticality, so the recommendation in this AC is to keep the two Bowties separate.

Appendix:

1. Root cause identification for UAS threats

ROOT CAUSE IDENTIFICATION FOR UAS THREATS

1. This appendix contains seven tables providing the most credible root causes which could lead to each threat that was identified in Annex A. These lists are not intended to be exhaustive but rather intended to highlight likely causes for each threat to assist in identifying well-focused risk controls.

Table 1A-1: Loss or degradation of datalink

Root Cause for this Threat	Explanation
UA datalink hardware failure	Failure in an antenna, receiver or an associated system can cause datalink to be lost.
Ground based datalink hardware failure	Failure in the RPS, the Ground Data Terminal (GDT) or ground antennae can cause datalink to be lost.
Datalink system software failure	Failure in software in the UA or the ground datalink system can cause the datalink to be lost.
Data processing delays	Delays due to datalink overload can cause a degradation of the datalink.
Flight beyond datalink range or satellite coverage	Shadowing by obstacles or simply exceeding the range of the link can cause loss of datalink.
Adverse weather conditions	Weather such as lightning and rain can affect datalink quality or availability.
Spectrum conflict	Conflict on the spectrum that the UAS is operating can cause loss or degradation of the datalink.
Electromagnetic interference	Electromagnetic interference, both unintentional and malicious, can cause loss or degradation of the datalink.

Table 1A-2: Loss or degradation of positional information

Root Cause for this Threat	Explanation
Navigation system hardware failure	Failure in hardware in the UA or RPS can cause positional information to be lost or degraded.
Navigation system software failure	Failure in software in the UA or RPS can cause the positional information to be lost or degraded.
Navigation source error	Errors in the navigation source (eg signal multipath, satellite error) can cause degraded positional information
Satellite unavailability	Shadowing or other causes of satellite unavailability can cause a loss of positional information.
Loss of sight of the UA in VLOS or EVLOS	Operation in VLOS or EVLOS requires eyesight to be the primary source of positional information, so loss of visual contact will result in the loss of that positional information.
Loss or degradation of datalink	This is covered as a separate threat.

Table 1A-3: UAS technical failure precluding continued flight

Root Cause for this Threat	Explanation
UA hardware failure	Failure of UA hardware such as sensors, or mechanical, hydraulic or other systems, can preclude continued flight of the UA.
Ground based hardware failure	Failure of hardware in the RPS can preclude continued flight of the UA.
Software failure	Failure of software in the UA or the RPS can preclude continued UA flight.
UA structural failure	Failure of the UA structure, either due to operating beyond structural limits or failure in design, can preclude continued flight of the UA.
UA propulsion failure	Failure of the propulsion on the UA can preclude continued flight of the UA.
UA battery or fuel depletion	Fuel or battery depletion, either due to planning errors or a technical problem in the fuel/battery system, can preclude continued flight of the UA.
Loss or degradation of datalink	This is covered as a separate threat.
Adverse operating conditions	Exposure to extreme environmental conditions can cause in-flight impact damage or affect UA systems and result in a technical failure. This is covered as a separate threat.

Table 1A-4: UAS technical failure rendering UA unresponsive

Root Cause for this Threat	Explanation
UA hardware failure	Failure of UA hardware such as the flight computer or associated systems can render the UA unresponsive or cause it to respond unpredictably.
Ground based hardware failure	Failure of the hardware in the RPS can inhibit control of the UA.
Software failure	Failure of software in the UA or the RPS can render the UA unresponsive or cause it to respond unpredictably.
Loss or degradation of datalink	This is covered as a separate threat.

Table 1A-5: RP error or loss of situational awareness

Root Cause for this Threat	Explanation
Poor Human Machine Interface (HMI) design	Poor HMI design of the RPS can increase RP workload and increase the likelihood of errors.
Inaccurate terrain data	Inaccurate terrain data can cause the RP to lose situational awareness or can contribute to a controlled flight into terrain.
Inadequate training	Inadequate RP training can lead to errors.
Low RP experience	Low RP experience, especially when operating in complex situations, can lead to loss of situational awareness or increase the likelihood or errors.
Lack of adequate Crew Resource Management (CRM)	Inadequate CRM can lead to RP overload and cause errors.
RP fatigue	Fatigue can diminish RP effectiveness and lead to errors.
Handover from one RP to another	If handover between RPs is not completed effectively it can lead to errors or loss of situational awareness.
Handover from one RPS to another	If handover between RPS is not completed effectively it can lead to errors.
Exposure to low visibility conditions if operating in VLOS/EVLOS	Operation in VLOS or EVLOS requires eyesight to be the primary source of positional information, so operating in low visibility conditions can reduce awareness of the UA and lead to errors.
Loss of, degradation of and misleading positional information	This is covered as a separate threat.

Table 1A-6: Adverse operating conditions

Root Cause for this Threat	Explanation
Exposure to excessive water or moisture	Water or excessive moisture can cause damage to systems on the UA.
Exposure to icing conditions	Icing on the aircraft can cause controllability issues.
Exposure to high winds or turbulence	Winds and turbulence can affect the controllability of the UA, especially if it is a light UA, or cause damage to structure and control surfaces.
Lightning strike	A lightning strike can cause damage to UA systems or structure.
Hail	Hail can cause a structural failure of the UA.
Bird strike	Bird strikes can cause structural failures or affect the propulsion system of the UA.
Aircraft	Collision with another aircraft (either manned or unmanned) can cause structural failure of the UA.

Table 1A-7: Other airspace users

Root Cause	Explanation
Failure of UAS procedures for operations in shared airspace	If procedures for UAS operations in shared airspace are not adequate this can lead to a separation breakdown.
Failure of UAS planning for operations in shared airspace	If the planning for UAS operations in shared airspace is not adequate this can lead to a separation breakdown.
Error by other aircraft pilot or technical failure of other aircraft	Even when there is no failure with the UAS, the procedures or the RP, a separation breakdown can be caused by another aircraft.

CANDIDATE RISK CONTROLS FOR UAS OPERATIONS

1. This annex presents candidate risk controls (or 'barriers' in Bowtie parlance) for UAS operations.

1.1. As stated in the main body of this AC, this list is not exhaustive, and the responsibility as per ref 1.3.2, to eliminate or otherwise minimise risks so far as is reasonably practicable, lies with persons directly associated with a particular UAS. They must continually identify and implement other reasonably practicable risk controls, in addition to this list. The annex does, however, present a significant list of risk controls that have been identified by the DASA through:

1.1.1. local UAS risk management research, as captured in AAP 7001.054 (ref 1.3.4) Section 4 Chapter 3

1.1.2. the UAS SORA work completed by JARUS (ref 1.3.5)

1.1.3. previous Defence UAS risk management experience, including Heron and Shadow operations.

1.2. This annex is structured as follows:

1.2.1. Table B-1 presents a list of identified risk controls for UAS operations, grouped into six major categories.

Note: The risk controls have not been grouped or presented in a 'hierarchy of controls'[23] format. The responsibility to eliminate risks by applying suitable risk controls, or to otherwise minimise risks through the application of hierarchy of suitable risk controls, remains the responsibility of persons directly associated with a UAS operation, as per ref 1.3.2.

1.2.2. The remainder of the annex expands on each of the risk controls in Table B-1, presenting a description of the particular hazard it aims to manage (extracted from the Bowties at Annex A), and some features that would improve its effectiveness.

2. Risk controls for UAS operations

[23] Ref 1.3.2 regulation 36 – 'Hierarchy of Control Measures' defines the hierarchy of risk controls by which a duty holder must minimise risks so far as is reasonably practicable, if it is not reasonably practicable to eliminate them. The hierarchy is:
(1) doing one or more of:
  (a) substituting (wholly or partly) the hazard giving rise to the risk with something that gives rise to a lesser risk,
  (b) isolating the hazard from any person exposed to it,
  (c) implementing engineering controls;
(2) If a risk then remains, the duty holder must minimise the remaining risk, so far as is reasonably practicable, by implementing administrative controls;
(3) If a risk then remains, the duty holder must minimise the remaining risk, so far as is reasonably practicable, by ensuring the provision and use of suitable personal protective equipment.

2.1. The risk controls presented in this annex have been grouped into the following six major categories:

2.1.1. UAS design features

2.1.2. RP training and management

2.1.3. Maintenance and engineering

2.1.4. Operational limitations

2.1.5. Operational procedures

2.1.6. Operational planning.

Table B-1: Risk controls for UAS operations

Design Features			RP Training & Management	Maintenance & Engineering	Operational Limitations	Operational Procedures	Operational Planning
UA Features ARS FTS Parachute Geo-fencing Obstacle avoidance Programmable minimum operating height Secondary system for positional information Positional system independent of external sources EO/IR camera GNSS with augmentation Altitude and positional information equipment	ADS-B SSR transponder Collision avoidance system (ACAS/TCAS/PCAS) Communication equipment Secondary means of communicating with ATC Weather radar Impact resistance Resistance to environmental conditions Mass restriction Frangibility Lighting Hi-visibility paint Radar visibility	**RPS Features** Datalink strength display Diagnostics and monitoring Battery or fuel indicator Emergency power supply Redundant RPS bay RPS handover function UA differentiation HF design **Datalink Features** Redundancy in datalink systems	Training Emergency procedure training Categorisation system CRM Fatigue management HF assessment Workload assessment	Maintenance and testing Maintenance support system Engineering support system	Single UA operations Minimum operating height Minimum distance from GP Minimum distance from MEP Overflight of GP restriction Overflight of MEP restriction Area restrictions to avoid GP Area restrictions to avoid MEP Visibility conditions when operations in VLOS/EVLOS Airspace restrictions Airspace buffers	Documented UA limitations Pre-flight checks Airspace procedures Emergency procedures Communications procedures Handover procedures Minimum fuel/battery reserves	NOTAMs Datalink and satellite shadowing Adverse weather conditions Airspace planning Airspace co-ordination Spectrum assessment RF survey Security threat assessment Emergency landing sites Area mapping Access restrictions ARS route planning Awareness briefings for GP Briefings for MEP Operational coordination PPE

3. The remainder of this annex expands on each of the risk controls in Table B-1. Each is structured in the same way. First it provides a brief description of the risk control. Next is an indication of how it acts as a threat and/or harm barrier linking to the Bowties presented at Annex A. Finally it identifies (non-exhaustively) some features that might improve the effectiveness of the risk control.

4. **Design Features**

4.1. **UA design features.** The following UA design features can act as risk controls for UAS operations:

4.1.1. **Autonomous Recovery System (ARS).** ARS can trigger automatic flight actions (loiter or auto return home) when specific failure conditions occur. It can reduce the likelihood of:

- a loss or degradation of datalink progressing to a separation breakdown or an unintended descent.

4.1.2. An effective ARS should:

- be capable of being pre-programmed to engage when specific conditions occur
- execute a predictable route and altitude plan
- provide an override capability to the RP upon re-establishing datalink
- display the pre-programmed ARS route to the RP
- have a comprehensive list of actions to be taken by the RP when ARS is activated documented in the Flight Manual or equivalent document
- be supported by information in the Flight Manual or equivalent document describing the operation and limitations of the system.

4.1.3. **Flight Termination System (FTS).** A FTS, that can be initiated automatically when certain conditions occur or remotely activated by the RP, will allow immediate termination of the UA flight and prevent escape. It can reduce the likelihood of:

- a loss or degradation of positional information progressing to a separation breakdown
- a UAS technical failure which renders the UA unresponsive progressing to a separation breakdown.

4.1.4. An effective FTS should:

- be capable of being activated from the RPS
- be capable of being pre-programmed for automatic activation when specific failure conditions occur
- be supported by information in the Flight Manual or equivalent document describing the operation and limitations of the system.

4.1.5. **Parachute.** An automatic or manually deployable parachute can reduce the impact speed of the UA. It can reduce the likelihood or consequence of:

- an unintended descent progressing to an injury/fatality to GP/MEP
- an unintended descent progressing to damage to critical infrastructure.

4.1.6. An effective parachute system should:

- be capable of being activated from the RPS
- be capable of being pre-programmed for automatic deployment when specific failure conditions occur
- be supported by information in the Flight Manual or equivalent document describing the operation and limitations of the system.

4.1.7. **Geo-fencing.** A geo-fence (ie a virtual geographic boundary) can assist in the containment of a UA within a pre-programmed volume. It can reduce the likelihood of:

- a loss or degradation of datalink progressing to a separation breakdown
- an RP error progressing to a separation breakdown or an unintended descent
- a UAS technical failure which renders the UA unresponsive progressing to a separation breakdown
- an unintended descent progressing to an injury/fatality to GP/MEP
- an unintended descent progressing to damage to critical infrastructure.

4.1.8. An effective geo-fencing feature should:

- be capable of being pre-programmed
- be capable of operating without an active datalink

- be supported by information in the Flight Manual or equivalent document describing the actions taken by the UA on reaching the geo-fence boundary (eg ARS activated, UA ditched) and the operation and limitations of the system.

4.1.9. **Obstacle avoidance.** An obstacle avoidance design feature can detect and autonomously avoid obstacles in the UA's flight path. It can reduce the likelihood of:

- an unintended descent progressing to damage to critical infrastructure.

4.1.10. An obstacle avoidance design feature should:

- be supported by information in the Flight Manual or equivalent document describing the operation and limitations of the system.

4.1.11. **Programmable minimum operating height.** A design feature to maintain a minimum operating height can preserve a buffer between the UA and terrain. This can reduce the likelihood of the UA being on a collision course with terrain and provide additional time to recover in case of a technical issue or an error. It can reduce the likelihood of:

- a loss or degradation of datalink progressing to an unintended decent

- an RP error or loss of situational awareness progressing to an unintended decent.

4.1.12. An effective minimum operating height design feature should:

- display the programmed minimum operating height to the RP

- execute a predictable response when the RP attempts to fly below the minimum set height

- be capable of operating without an active datalink

- be supported by information in the Flight Manual or equivalent document describing the operation and limitations of the system.

4.1.13. **Secondary system for positional information.** A secondary system for positional information can enable the RP to continually verify the accuracy of positional information and provides the ability to safely recover the UA when the primary positional information is lost. It can reduce the likelihood of:

- a loss or degradation of positional information which could progress to a separation breakdown or an unintended descent.

4.1.14. An effective secondary system for positional information should:

- be an independent system to the primary positional information system
- receive positional information from an independent source to the primary positional information system
- be supported by operational procedures to cross-reference data
- be supported by information in the Flight Manual or equivalent document describing the limitation, and resultant uncertainty in aircraft position, when using the system.

4.1.15. **Positional system independent of external sources.** A system for positional information that is independent of external sources such as satellites (eg inertial measurement unit (IMU)) can provide augmentation to a primary positional information source and provide redundancy when the primary information source is lost. It can reduce the likelihood of:

- a loss or degradation of positional information which could progress to a separation breakdown or an unintended descent.

4.1.16. An effective source of positional information independent of external sources should:

- be supported by information in the Flight Manual or equivalent document, describing the operation and limitations (eg uncertainty in aircraft position with time), when using the system.

4.1.17. **Electro-optical/Infrared (EO/IR) cameras**. EO/IR cameras can act as a secondary source of positional information and provide the RP with a visual aid to verify the terrain and confirm positional information. It can reduce the likelihood of:

- a loss or degradation of positional information which could progress to a separation breakdown or an unintended descent
- RP error or loss of situational awareness which could progress to an unintended decent.

4.1.18. An effective EO/IR camera feature should:

- be supported by operational procedures to cross-reference terrain data with positional information.

4.1.19. **Global Navigation Satellite System (GNSS) with augmentation.** Using a GNSS with an augmentation system such as Receiver Autonomous Integrity

Monitoring (RAIM) will provide higher integrity positional information by detecting satellite failures or errors. It can reduce the likelihood of:

- a loss or degradation of positional information which could progress to a separation breakdown or an unintended descent.

4.1.20. An effective GNSS system with augmentation should:

- include a performance augmentation system that provides at least Fault Detection (FD) capability

- be supported by information in the Flight Manual or equivalent document describing the operation and limitations of the system.

4.1.21. **Altitude and positional information equipment.** Positional information and altitude information sources that meet required standards are important to maintaining safe separation if a UAS is to operate in non-segregated airspace. They can reduce the likelihood of:

- a loss or degradation of positional information which could progress to a separation breakdown or an unintended descent.

4.1.22. Effective altitude and positional information equipment should:

- meet the requirements of ref 1.3.4 Section 4 Chapter 3.

4.1.23. **Automatic Dependant Surveillance – Broadcast (ADS-B).** ADS-B can broadcast the position and altitude of the UA to ATC and other co-operative aircraft to improve traffic management and aircraft separation. It can reduce the likelihood of:

- a loss or degradation of datalink progressing to a separation breakdown

- a UAS technical failure which renders the UA unresponsive progressing to a separation breakdown

- the presence of other airspace users progressing to a separation breakdown.

4.1.24. An effective ADS-B feature should:

- meet the same design, installation and test requirements as manned aircraft.

4.1.25. **Secondary Surveillance Radar (SSR) Transponder.** An SSR transponder can provide ATC with aircraft information to assist safe separation, and has the ability to squawk emergency codes to ATC. It can reduce the likelihood of:

- a loss or degradation of datalink progressing to a separation breakdown
- loss or degradation of positional information progressing to separation breakdown
- UAS technical failure which renders the UA unresponsive progressing to a separation breakdown
- RP error or loss of situational awareness progressing to separation breakdown
- the presence of other airspace users progressing to separation breakdown.

4.1.26. An effective SSR transponder should:

- meet the requirements of ref 1.3.4 Section 4 Chapter 3
- be programmed with emergency codes designated or agreed to by ATC
- automatically squawk preset codes when specific failure conditions occur
- provide the RP the ability to manually select codes and squawk during flight
- provide the RP the ability to turn the transponder on/off remotely during flight
- be supported by information in the Flight Manual or equivalent document describing the operation and limitations of the system.

4.1.27. **Collision avoidance system (ACAS/TCAS/PCAS).** An aircraft collision avoidance system can assist in resolution action for both the UA and the other aircraft if a separation breakdown occurs. It can reduce the likelihood of:

- a separation breakdown progressing to catastrophic damage to other aircraft.

4.1.28. An effective collision avoidance feature should:

- meet the same design, installation and test requirements as manned aircraft
- be capable of transparently interacting with manned aircraft equipped with ACAS
- be employed on a UAS that can meet the ACAS bank, climb and other performance requirements

- be supported by information in the Flight Manual or equivalent document describing the operation and limitations of the system.

4.1.29. **Communication equipment.** Meeting specific requirements for communications equipment will improve the ability of the RP to communicate with ATC and other airspace users when operating in non-segregated airspace. It can reduce the likelihood of:

- loss or degradation of datalink progressing to separation breakdown
- loss or degradation of positional information progressing to separation breakdown
- UAS technical failure which renders the UA unresponsive progressing to a separation breakdown
- RP error or loss of situational awareness progressing to separation breakdown
- the presence of other airspace users progressing to separation breakdown.

4.1.30. Effective communication equipment should:

- meet the requirements of ref 1.3.4 Section 4 Chapter 3, or
- have any deficiencies from those requirements analysed and treatments (such as operational procedures) implemented.

4.1.31. **Secondary means of communicating with ATC.** Having a secondary means of communicating with ATC (eg communication by phone) provides redundancy in the event of a failure of the primary communication method. It can reduce the likelihood of:

- loss or degradation of datalink progressing to a separation breakdown, where the primary means of communication was being routed through the UA
- UAS technical failure which renders the UA unresponsive progressing to a separation breakdown.

4.1.32. An effective secondary means of communicating with ATC should:

- not be routed through the UA if the primary communication means is routed through the UA

- be independent of the primary RPS communication system (including power supply).

4.1.33. **Weather radar.** Adverse weather, such as rain and thunderstorms, can affect the operation of the UA if it is not designed to withstand those conditions (eg water ingress for a UA that is not waterproof leading to failure of systems). Weather conditions such as thunderstorms can also interfere with a datalink signal. The ability to monitor weather real-time, either through an on-board system in the UA or through monitoring of an external weather radar from the RPS, can assist in identifying adverse weather conditions that may affect UA operation so the RP can take steps to avoid them. It can reduce the likelihood of:

- a loss or degradation of datalink which could progress to a separation breakdown or an unintended descent

- adverse operating conditions progressing to an unintended descent.

4.1.34. An effective weather radar capability should:

- provide real-time weather information

- be capable of covering the same range as the UA

- be supported by information in the Flight Manual or equivalent document describing the operation and limitations of the system.

4.1.35. **Impact resistance.** A UA that is designed to withstand impact can minimise the effect of hail, projectiles, birds and so on. It can reduce the likelihood of:

- adverse operating conditions progressing to an unintended descent.

4.1.36. A UA’s impact resistance ability should:

- be suitable for the conditions in which it is expected to operate.

4.1.37. **Resistance to environmental conditions.** A UA that is designed to be resistant to a range of environmental conditions, such as rain, turbulence and lightning, can reduce the risk of failure due to inadvertent exposure. It can reduce the likelihood of:

- adverse operating conditions progressing to an unintended descent.

4.1.38. A UA’s resistance to environmental conditions should:

- be compatible with the environment in which it is expected to operate

- be supported by information in the Flight Manual or equivalent document describing the environmental condition limits of the UA.

4.1.39. **Mass restriction.** The mass of a UA has a large impact on the amount of damage that results from a collision. Operation of a UA with a limitation on the maximum take-off weight (MTOW) can reduce the severity of:

- damage to other aircraft as a result of a separation breakdown
- an injury to GP/MEP as a result of an unintended descent
- damage to critical infrastructure as a result of an unintended descent.

4.1.40. **Frangibility.** A UA of frangible construction can break apart in the event of a collision, therefore reducing the amount of damage to the other aircraft, person or object. It can reduce the severity of:

- damage to other aircraft as a result of a separation breakdown
- an injury to GP/MEP as a result of an unintended descent
- damage to critical infrastructure as a result of an unintended descent.

4.1.41. **Lighting.** Anti-collision and position lights can act as an alert or source of information to other aircraft about the UA's position. It can reduce the likelihood of:

- a separation breakdown progressing to catastrophic damage to other aircraft.

4.1.42. Effective lighting should:

- meet the requirements of ref 1.3.4 Section 4 Chapter 3, or
- have any deficiencies from those requirements analysed and treatments (such as operational procedures) implemented.

4.1.43. **Hi-visibility paint.** UA painted in a hi-visibility paint scheme can act as an alert or source of information of the UA's position to other aircraft. It can reduce the likelihood of:

- a separation breakdown progressing to catastrophic damage to other aircraft.

4.1.44. **Radar visibility.** When a UA is operating in an area where radar is contributing to the safe separation of aircraft, the UA must be visible to the radar to enable effective traffic detection, separation and collision avoidance. Radar visibility can reduce the likelihood of:

- operations in the vicinity of other airspace users progressing to separation breakdown.

4.1.45. Effective radar visibility should:

- be determined through analysis and/or test at worst-case ranges and elevations
- have any deficiencies analysed and treatments (such as operational procedures) implemented, if the radar visibility is not adequate.

4.2. **RPS Design Features.** The following RPS design features can act as risk controls for UAS operations:

4.2.1. **Datalink strength display.** A datalink strength display in the RPS can enable the RP to actively monitor datalink strength and be aware of the limit of the datalink range. It can reduce the likelihood of:

- a loss of datalink which could progress to a separation breakdown or an unintended descent.

4.2.2. The datalink strength display should:

- provide continuous indication of link strength
- provide indication of the predicted maximum limit range for the UA.

4.2.3. **Diagnostics and monitoring.** Having diagnostic and monitoring capability for the air vehicle in the RPS can alert the RP to technical issues and enable them to take action as required. It can reduce the likelihood of:

- a UAS technical failure precluding continued flight progressing to an unintended descent.

4.2.4. An effective diagnostic and monitoring capability should:

- clearly advise the RP of any degraded mode of operation due to any failure
- clearly advise the RP in cases when there is an automatic switching to backup mode for a system due to failure
- be supported by information in the Flight Manual or equivalent document describing the operation and limitations of the system.

4.2.5. **Battery or fuel indicator.** A battery or fuel indicator in the RPS can enable the RP to monitor and avoid battery or fuel depletion. It can reduce the likelihood of:

- a UAS technical failure precluding continued flight progressing to an unintended descent.

4.2.6. **Emergency power supply.** An emergency power supply for the RPS can allow the RP to initiate emergency procedures or to retain control of the UA until primary power is restored. It can reduce the likelihood of:

- UAS technical failure progressing to an unintended descent or a separation breakdown.

4.2.7. An emergency power supply should:

- be supported by information in the Flight Manual or equivalent document describing the operation and limitations of the system.

4.2.8. **Redundant RPS bay.** A redundant RPS bay can provide a backup in the event of an RPS failure. It can reduce the likelihood of:

- a loss of datalink, due to an RPS failure, progressing to a separation breakdown or an unintended descent

- a loss of positional information, due to an RPS failure, progressing to a separation breakdown or an unintended descent

- UAS technical failure which renders the UA unresponsive, due to an RPS failure, progressing to a separation breakdown.

4.2.9. A redundant bay should:

- be independent of the primary bay

- be subjected to a comprehensive safety assessment if it has reduced functionality to the primary bay

- provide a means of readily configuring the redundant bay to match the primary bay or of verifying the configuration of both bays is identical if configuration is done manually

- be supported by information in the Flight Manual or equivalent document describing the operation and limitations of the system.

4.2.10. **RPS handover function.** Where more than one RPS is used to control a UA in a single flight, the capability for automatic set-up or checking of the RPS settings can minimise errors during the handover process. It can reduce the likelihood of:

- RP error or loss of situational awareness which could progress to a separation breakdown or an unintended descent.

4.2.11. An effective RPS handover function should:

- enable the controlling RPS to automatically configure the other RPS prior to handover, or

- provide a means of verifying that the configuration data of both RPS is identical.

4.2.12. **UA differentiation.** Where an RPS is designed to command, control and monitor multiple UA, the ability to clearly identify which UA is being controlled or displayed at any time is important to minimise potential errors. It can reduce the likelihood of:

- RP error or loss of situational awareness progressing to a separation breakdown or an unintended descent.

4.2.13. Effective UA differentiation requires:

- all controls, indicators and warnings to be presented in a manner that prevents confusion over which UA the information is relevant to, and prevents inadvertent operation of the wrong UA

- a means to clearly indicate to the RP the UA over which he/she has command and control.

4.2.14. **HF design.** An RPS that is designed with consideration of HF can reduce RP workload and assist in avoiding RP errors. It can reduce the likelihood of:

- an RP error or loss of situational awareness which could progress to a separation breakdown or an unintended decent.

4.2.15. An effective HF design should:

- ensure the RPS displays clear and unambiguous aircraft system status information, and navigation, flight and other data, to the RP to enable safe operation

- be supported by a HF assessment to identify any deficiencies and any possible design treatments

- ensure any residual deficiencies are managed through training or operational treatments.

4.3. **Datalink features.** The following datalink features can act as risk controls for UAS operations:

4.3.1. **Redundancy in datalink systems.** Having redundancy in datalinks can facilitate continued datalink in the event of a failure or interference. It can reduce the likelihood of:

- a loss of datalink which could progress to a separation breakdown or an unintended descent.

4.3.2. Redundancy in the datalink system can be provided as:

- an end-to-end redundant datalink system, or
- redundancy in the datalink components such as:
  - multiple antennas
  - broadcast over multiple frequencies.

5. **RP Training and Management**

5.1. The following RP training and management procedures can act as risk controls for UAS operations:

5.1.1. **Training.** RP training can reduce the likelihood of:

- a loss or degradation of datalink which could progress to a separation breakdown or an unintended descent
- a loss or degradation of positional information which could progress to a separation breakdown or an unintended descent
- an RP error or loss of situational awareness which could progress to a separation breakdown or an unintended descent
- the presence of other airspace users progressing to separation breakdown.

5.1.2. RP training should enable the RP to:

- understand the limitations of the datalink (range, azimuth and required signal strength) and operate the UA within those limitations
- regularly verify positional information to identify cues of erroneous information

- understand the design limitations of the UAS and operate within those limitations
- maintain safe separation from other airspace users.

5.1.3. RP training should:

- be documented in a training management plan or equivalent document.

5.1.4. **Emergency procedure training.** RP emergency procedure training can reduce the likelihood of:

- a loss or degradation of datalink progressing to a separation breakdown or an unintended descent
- a loss or degradation of positional information progressing to a separation breakdown or an unintended descent
- a UAS technical failure which renders the UA unresponsive progressing to a separation breakdown
- an RP error or loss of situational awareness progressing to separation breakdown or unintended descent
- adverse operating conditions progressing to an unintended descent
- a separation breakdown progressing to catastrophic damage to other aircraft
- an unintended descent progressing to an injury/fatality to GP/MEP or damage to critical infrastructure.

5.1.5. RP emergency procedure training should enable the RP to carry out emergency procedures:

- if datalink cannot be re-established
- in case of loss or degradation of positional information
- in the event of technical failures
- following an RP error
- to avoid or react to adverse operating conditions
- upon separation breakdown
- upon unintended descent

- upon the UA being on collision course with terrain.

5.1.6. RP emergency procedure training should:

- be documented in a training management plan or equivalent document.

5.1.7. **Categorisation system.** A categorisation system for RPs can assist in balancing complexity of operations with RP experience and allow for supervision requirements or restricted operations for RPs with low experience. It can reduce the likelihood of:

- an RP error or loss of situational awareness which could progress to a separation breakdown or an unintended descent.

5.1.8. An RP categorisation system should:

- be documented in a training management plan or equivalent document.

5.1.9. **Crew Resource Management (CRM).** Effective CRM is important to manage RP workload and minimise errors. It can reduce the likelihood of

- an RP error or loss of situational awareness which could progress to a separation breakdown or an unintended descent.

5.1.10. CRM should:

- be included in RP training and currency requirements and documented in a training management plan or equivalent document.

5.1.11. **Fatigue management.** Effective management of fatigue is important to RP performance. It can reduce the likelihood of:

- an RP error or loss of situational awareness which could progress to a separation breakdown or an unintended descent.

5.1.12. Procedures for effective fatigue management can include:

- restriction on number of continuous hours that an RP can operate a UA without a break

- restriction on overall number of hours that an RP can work in a day or a week

- requirement for number of hours of rest between RP shifts.

5.1.13. Procedures for fatigue management should:

- be documented in local instructions.

5.1.14. **HF assessment.** An assessment to identify HMI design deficiencies in the RPS can assist in improved awareness and training to reduce HMI related errors. It can reduce the likelihood of:

- an RP error or loss of situational awareness which could progress to a separation breakdown or an unintended descent.

5.1.15. An effective HF assessment should:

- assess whether the RPS displays clear and unambiguous aircraft system status information, and navigation, flight and other data, to the RP to enable safe operation
- identify deficiencies in the HMI design and any potential operational treatments
- be supported by information in the Flight Manual or equivalent document describing the HMI limitations of the system.

5.1.16. **Workload assessment.** A workload assessment to determine manpower requirements to operate the system in normal and abnormal conditions can identify where manpower is insufficient for the workload. It can reduce the likelihood of:

- an RP error or loss of situational awareness which could progress to a separation breakdown or an unintended descent.

5.1.17. An effective workload assessment should:

- determine where the workload on the RP will exceed normal capacity and implement strategies to manage or minimise workload.

6. Maintenance and Engineering

6.1. The following maintenance and engineering support systems and procedures can act as risk controls for UAS operations:

6.1.1. **Maintenance and testing.** Maintenance and testing can decrease the occurrence of technical failures. It can reduce the likelihood of:

- a loss or degradation of datalink due to datalink hardware failures which could progress to a separation breakdown or an unintended descent
- a loss or degradation of positional information due to positional information hardware failures which could progress to a separation breakdown or an unintended descent

- a UAS technical failure precluding continued flight which could progress to an unintended descent

- a UAS technical failure rendering the UA unresponsive which could progress to a separation breakdown

- a separation breakdown progressing to catastrophic damage to other aircraft due to hardware failures (eg ADS-B failure, failure of anti-collision lighting).

6.1.2. Maintenance and testing should:

- be carried out as per OEM or locally established procedures

- include pre-flight inspections and activities (including checking and replenishment of all consumable fluids, gases etc)

- include conduct of repairs as per relevant engineering instructions

- be carried out by appropriately trained and experienced personnel

- be carried out under appropriate supervision

- be supported by a maintenance management plan or equivalent document.

6.1.3. **Maintenance support system.** A maintenance support system can decrease the occurrence of technical failures. It can reduce the likelihood of:

- a loss or degradation of datalink due to datalink hardware failures which could progress to a separation breakdown or an unintended descent

- a loss or degradation of positional information due to positional information hardware failures which could progress to a separation breakdown or an unintended descent

- a UAS technical failure precluding continued flight which could progress to an unintended descent

- a UAS technical failure rendering the UA unresponsive which could progress to a separation breakdown

- a separation breakdown progressing to catastrophic damage to other aircraft due to hardware failures (eg ADS-B failure, failure of anti-collision lighting).

6.1.4. An effective maintenance support system should:

- have a system for condition monitoring
- include an aircraft log to capture flights details
- include a log of maintenance and repair activities for each UA and RPS
- be supported by a maintenance management plan or equivalent document.

6.1.5. **Engineering support system.** An engineering support system can decrease the occurrence of technical failures. It can reduce the likelihood of:

- a loss or degradation of datalink due to datalink hardware failures which could progress to a separation breakdown or an unintended descent
- a loss or degradation of positional information due to positional information hardware failures which could progress to a separation breakdown or an unintended descent
- a UAS technical failure precluding continued flight which could progress to an unintended descent
- a UAS technical failure rendering the UA unresponsive which could progress to a separation breakdown
- a separation breakdown progressing to catastrophic damage to other aircraft due to hardware failures (eg ADS-B failure, failure of anti-collision lighting).

6.1.6. An effective engineering support system should include:

- failure and defect monitoring and investigation
- configuration management
- a design assurance system
- a process for developing and/or approving repairs and designs.

7. Operational Limitations

7.1. The following operational limitations can act as risk controls for UAS operations:

7.1.1. **Single UA operations.** Avoiding operation of multiple UA by a single operator can reduce RP workload. It can reduce the likelihood of:

- RP error or loss of situational awareness which could progress to a separation breakdown or an unintended descent.

7.1.2. **Minimum operating height.** An operational limitation to maintain a minimum operating height can reduce the likelihood of the UA being on collision course with terrain and therefore provide additional time to recover from a technical issue or an error. It can reduce the likelihood of:

- a loss or degradation of datalink progressing to an unintended descent
- a loss or degradation of positional information progressing to an unintended descent
- RP error or loss of situational awareness progressing to an unintended descent.

7.1.3. **Minimum distance from GP.** Restrictions on operating near GP can assist in minimising risk to people on the ground. It can reduce the likelihood of:

- an unintended descent progressing to an injury/fatality to GP.

7.1.4. **Minimum distance from MEP.** Restrictions on operating near MEP can assist in minimising risk to people on the ground. It can reduce the likelihood of:

- an unintended descent progressing to an injury/fatality to MEP.

7.1.5. **Overflight of GP restriction.** A restriction from operating overhead of GP can assist in minimising risk to people on the ground. If can reduce the likelihood of:

- an unintended descent progressing to injury/fatality to GP.

7.1.6. **Overflight of MEP restriction.** A restriction from operating over MEP can assist in minimising risk to people on the ground. If can reduce the likelihood of:

- an unintended descent progressing to injury/fatality to MEP

7.1.7. **Area restrictions to avoid GP.** Restrictions on areas that a UA can operate near or over can assist in minimising risk to people on the ground. It can reduce the likelihood of:

- an unintended descent progressing to injury/fatality to GP.

7.1.8. Area restrictions can include:

- operating only over Defence controlled land
- not operating over populous areas
- maintaining operational buffers from the edge of the intended operational area to reduce the likelihood of escaping the area.

7.1.9. **Area restrictions to avoid MEP.** Restrictions on areas that a UA can operate over can assist in minimising risk to people on the ground. It can reduce the likelihood of:

- an unintended descent progressing to injury/fatality to MEP.

7.1.10. Area restrictions can include:

- not operating over MEP congregations such as camps or headquarters
- maintaining operational buffers from the edge of the intended operational area to reduce the likelihood of escaping the area.

7.1.11. **Visibility conditions when operating in VLOS/EVLOS.** Restrictions on operating conditions when operating in VLOS/EVLOS can assist in maintaining visibility of the UA and visibility of other aircraft in the area. It can reduce the likelihood of:

- loss or degradation of positional information (which is primarily provided via visual contact with the UA in VLOS), which could progress to a separation breakdown or an unintended descent
- RP error or loss of situational awareness which could progress to a separation breakdown or an unintended descent
- the presence of other airspace users progressing to separation breakdown.

7.1.12. Operating condition restrictions can include:

- to operate only in daytime if not equipped with suitable lighting
- to operate only in visual meteorological conditions (VMC)
- not to operate in cloud
- not to operate in low visibility conditions such as smoke or fog.

7.1.13. **Airspace restrictions.** Restrictions on airspace, such as only operating in segregated airspace, can minimise interaction with other airspace users. It can reduce the likelihood of:

- loss or degradation of datalink progressing to a separation breakdown
- loss or degradation of positional information progressing to a separation breakdown

- a UAS technical failure which renders the RP unresponsive progressing to a separation breakdown

- RP error or loss of situation awareness progressing to a separation breakdown

- the presence of other airspace users which could progress to a separation breakdown.

7.1.14. **Airspace buffers.** Including a buffer between the UA operations and the edge of the intended or available airspace can minimise the likelihood of escape or provide time to recover in the case of an emergency. It can reduce the likelihood of:

- loss or degradation of datalink progressing to a separation breakdown

- loss or degradation of positional information progressing to a separation breakdown

- UAS technical failure which renders the RP unresponsive progressing to a separation breakdown

- RP error or loss of situation awareness progressing to a separation breakdown

- the presence of other airspace users which could progress to a separation breakdown.

7.1.15. Airspace buffers should:

- provide a buffer between the boundary for UA operations and the edge of the intended airspace.

8. Operational Procedures

8.1. The following operational procedures can act as risk controls for UAS operations:

8.1.1. **Documented UA limitations.** Documenting the limitations of the UAS can enable the RP to avoid operating outside those limits or take appropriate action if operating limits are inadvertently exceeded, therefore reducing the risk of a UAS technical failure. It can reduce the likelihood of:

- a loss or degradation of datalink which could progress to a separation breakdown or an unintended descent

- a loss or degradation of positional information which could progress to a separation breakdown or an unintended descent
- a UAS technical failure precluding continued flight which could progress to an unintended descent
- adverse operating conditions progressing to an unintended descent.

8.1.2. Documentation of UA limitations should cover:

- designed limits of the UAS, such as structural load limits of the UA and range limits of the datalink
- deficiencies of the UAS design, such as low integrity navigation systems providing inaccurate data
- performance of navigation systems whose accuracy drifts over time (eg IMU)
- weather limitations of the UA, such as wind gust limits or not to operate in rain.

8.1.3. UA limitations should be:

- well characterised and communicated to RPs
- documented in the flight manual or equivalent document.

8.1.4. **Pre-flight checks.** Checks carried out by the RP prior to take-off can identify functional deficiencies with the UAS. It can reduce the likelihood of:

- a technical failure precluding continued flight which could progress to an unintended descent.

8.1.5. Effective pre-flight checks should:

- confirm the functionality of any critical systems, such a control surfaces and navigation, prior to take-off
- be carried out in accordance with OEM or locally produced procedures
- be documented in a Flight Manual or equivalent document.

8.1.6. **Airspace procedures.** Operational procedures for operations in specific airspace classes can assist in maintaining safe separation from other airspace users. It can reduce the likelihood of:

- the presence of other airspace users progressing to a separation breakdown.

8.1.7. Effective airspace procedures should:

- present procedures for maintaining safe separation in all classes of airspace that the UAS will operate in
- be documented in an Air Traffic Management Plan (ATMP) or equivalent document.

8.1.8. **Emergency procedures**. Documenting emergency procedures can enable the RP to initiate required action in emergencies. It can reduce the likelihood of:

- a loss or degradation of datalink progressing to a separation breakdown or an unintended descent
- a loss or degradation of positional information progressing to a separation breakdown or an unintended descent
- a UAS technical failure which renders the UA unresponsive progressing to a separation breakdown
- an RP error or loss of situational awareness progressing to separation breakdown or unintended descent
- adverse operating conditions progressing to an unintended descent
- a separation breakdown progressing to catastrophic damage to other aircraft
- an unintended descent progressing to an injury/fatality to GP/MEP or damage to critical infrastructure.

8.1.9. Emergency procedures should cover:

- lost link and lost positional information events including steps to be taken to attempt to re-establish link
- recovery actions for all probable technical failure modes
- manual ditching or flight termination in an emergency
- procedures while RPS is on emergency power which could include:
    - o manual ditching or flight termination
    - o emergency landing
    - o manual activation of return home function

- evacuation plan if UA is on collision course with an area containing GP/MEP

- emergency response plan (ERP) to be activated in case of a collision with GP/MEP or critical infrastructure to limit severity of injuries.

8.1.10. Emergency procedures should be:

- documented in a Flight Manual or equivalent document.

8.1.11. **Communications procedures.** Procedures for communicating with other airspace users and ATC can improve RP situational awareness and alert other airspace users to the presence of a UA. It can reduce the likelihood of:

- loss or degradation of datalink progressing to a separation breakdown

- loss or degradation of positional information progressing to a separation breakdown

- UAS technical failure which renders the UA unresponsive progressing to a separation breakdown

- RP error or loss of situational awareness progressing to a separation breakdown

- the presence of other airspace users progressing to a separation breakdown.

8.1.12. Communication procedures should include:

- communication with ATC

- where primary ATC communication is via the UA, a secondary mean of communication with ATC which does not require an active datalink to the UA

- direct communication with other airspace users via radio broadcasts

- the periodicity of communication broadcasts

- communication requirements in case of:

  - loss of datalink and/or activation of ARS

  - loss of positional information

  - loss of control of UA due to technical failure.

8.1.13. Communication procedures should be:

- documented in a Flight Manual or equivalent document.

8.1.14. **Handover procedures.** Documented procedures for handover from one RP to another or from one RPS to another can ensure there is clarity over who is in control of the UA at all times and assist in minimising errors. It can reduce the likelihood of:

- RP error or loss of situational awareness which could progress to a separation breakdown or an unintended descent.

8.1.15. Handover procedures should include:

- handover checklists
- crew co-ordination
- aircrew monitoring during RPS handover.

8.1.16. Handover procedures should be:

- documented in a Flight Manual or equivalent document.

8.1.17. **Minimum fuel/battery reserves.** Maintaining a minimum fuel or battery reserve for UA operations can provide a reserve in case of an emergency that requires the UA to remain airborne. It can reduce the likelihood of:

- a loss or degradation of datalink progressing to an unintended descent
- an RP error or loss of situational awareness progressing to an unintended descent.

8.1.18. Fuel/battery reserves should:

- be documented in operational procedures
- be considered in flight planning.

9. Operational Planning

9.1. The following operational planning steps can act as risk controls for UAS operations:

9.1.1. **NOTAMs.** Issuing NOTAMs can alert other aircraft of a UA operating in the area. It can reduce the likelihood of:

- loss or degradation of datalink progressing to a separation breakdown

- presence of other airspace users progressing to a separation breakdown.

9.1.2. **Datalink and satellite shadowing.** Pre-flight planning can identify potential sources of datalink or satellite shadowing, allowing the RP or the Operator to plan routes that reduce shadowing. This can reduce the likelihood of:

- loss or degradation of datalink which could progress to a separation breakdown or an unintended descent

- loss or degradation of positional information which could progress to a separation breakdown or an unintended descent.

9.1.3. **Adverse weather conditions.** Pre-flight planning can identify weather conditions beyond the design limits of the UA, to enable the RP or Operator to plan routes that avoid or minimise exposure to these conditions. This can reduce the likelihood of:

- loss or degradation of datalink which could progress to a separation breakdown or an unintended descent

- adverse operating conditions progressing to an unintended descent.

9.1.4. Planning for adverse conditions should cover:

- weather forecasts

- wildlife planning

- avoiding low-visibility conditions such as smoke or cloud if operating in VLOS/EVLOS.

9.1.5. **Airspace planning.** Operational planning for the intended airspace class can assist in maintaining safe separation from other airspace users. It can reduce the likelihood of:

- the presence of other airspace users progressing to separation breakdown.

9.1.6. Airspace planning should cover:

- planning for operations in all classes of airspace that the UAS will operate in.

9.1.7. **Airspace co-ordination.** When operating as part of a military exercise or operation, co-ordinating operations with other airspace users can assist in de-confliction and maintaining safe separation. It can reduce the likelihood of:

- the presence of other airspace users progressing to separation breakdown.

9.1.8. **Spectrum assessment.** A spectrum assessment by a spectrum management authority prior to operation can reduce the likelihood of a spectrum conflict or interference. It can reduce the likelihood of:

- loss or degradation of datalink which could progress to a separation breakdown or an unintended descent.

9.1.9. **RF survey.** Conducting a radio frequency survey prior to operations can identify high intensity emitters in the operational area that may cause interference with the UAS. It can reduce the likelihood of:

- loss or degradation of datalink which could progress to a separation breakdown or an unintended descent.

9.1.10. **Security threat assessment.** A security threat assessment can assess the likelihood and possible sources of intentional interference with the UAS. It can reduce the likelihood of:

- loss or degradation of datalink which could progress to a separation breakdown or an unintended descent.

9.1.11. **Emergency landing sites.** Identification of emergency landing sites during operational planning can provide options to the RP in the case of an unintended descent where the RP still retains some control of the UA. It can reduce the likelihood of:

- an unintended descent progressing to an injury/fatality to GP/MEP or damage to critical infrastructure.

9.1.12. **Area mapping.** Conducting area mapping as part of operational planning can assist in identifying areas of GP, MEP and critical infrastructure to enable the RP to avoid or minimise time in those areas. It can reduce the likelihood of:

- an unintended descent progressing to an injury/fatality to GP/MEP or damage to critical infrastructure.

9.1.13. Area mapping should cover:

- GP in the vicinity of operations and implementation of barriers such as stand-off distances

- areas of congregation of MEP, such as operational headquarters or living areas, in the vicinity of operations and implementation of barriers such as overflight restrictions or reduced time in those areas

- critical infrastructure in the area of operations and plans to avoid or minimise time in those areas.

9.1.14. **Access restrictions.** Restricting GP access to areas where a UA is operating can minimise the number of people who are exposed to risk from the UA. It can reduce the likelihood of:

- an unintended descent progressing to an injury/fatality to GP.

9.1.15. **ARS route planning.** For UA fitted with an ARS, effective route planning can assist in avoiding flight over areas of GP/MEP or critical infrastructure. It can reduce the likelihood of:

- a loss or degradation of datalink progressing to a separation breakdown when ARS is activated

- an unintended descent progressing to an injury/fatality to GP/MEP or damage to critical infrastructure.

9.1.16. Effective ARS route planning should:

- avoid, where possible, any airspace that contains regular air traffic

- avoid flight over GP and ensure stand-off distances are maintained

- avoid or minimise flight over MEP

- avoid flight over critical infrastructure

- include independent checking of the ARS route parameters, to reduce the likelihood of input errors.

9.1.17. **Awareness briefings for GP.** Briefing GP in the area of a UAS operation can increase their awareness and provide them with actions to be taken in the case of an emergency. It can reduce the likelihood of:

- the presence of other airspace users progressing to a separation breakdown

- an unintended descent progressing to an injury/fatality to GP.

9.1.18. Awareness briefing should be provided to:

- any GP on the ground in or near the area of operation (eg nearby camp sites)

- any civilian operators of aircraft (manned or unmanned) in or near the area of operation (eg local flying clubs)

9.1.19. An effective awareness should cover:

- the intended timings and location of the UA operation in the area
- the airspace that the UA will be operating, for the civilian aircraft operators
- actions to be taken if advised of an emergency, such as taking shelter for GP on the ground.

9.1.20. **Briefings for MEP.** Briefing MEP in the area of the UAS operation can increase their awareness and provide them with actions to be taken in the case of an emergency. It can reduce the likelihood of:

- an unintended descent progressing to an injury/fatality to MEP.

9.1.21. An effective MEP briefing should cover:

- the intended timings and location of the UA operation in the area
- actions to be taken by MEP during the operation, such as wearing of PPE
- actions to be taken in the case of an emergency.

9.1.22. **Operational co-ordination.** When operating in the vicinity of MEP, co-ordinating UA operations with ground force operations and movement can assist in minimising flight time over MEP and increase MEP awareness of the UA operation. It can reduce the likelihood of:

- an unintended descent progressing to an injury/fatality to MEP.

9.1.23. **PPE.** Identifying PPE for MEP in the UAS operating area can reduce the severity of a collision. It can reduce the likelihood of:

- an unintended descent progressing to an injury/fatality to MEP.

10. Standard Risk Controls

10.1. For operations in particular areas or in the vicinity of particular activities, certain permissions may be required from other parties, such as Air Services, to assist in maintaining safety. While these are not stand-alone risk controls to be implemented by the UAS operator, they are essential when other parties are contributing to the safety of aircraft operations. The following standard risk controls may be required for UAS operations:

10.1.1. approval, from the authority controlling the area, to operate in a Prohibited Area, or a Restricted Area

10.1.2. approval, from the person in charge of the operation, to operate over an area where a fire, police or other public safety or emergency operation is being conducted

10.1.3. approval from the relevant authority to operate in the movement area or the approach or departure path of a runway of an aerodrome/ship

10.1.4. approval from the relevant airspace authority to operate within 3 nm (5.5 km) of the movement area of a controlled aerodrome

10.1.5. approval from the relevant airspace authority to operate in controlled airspace.