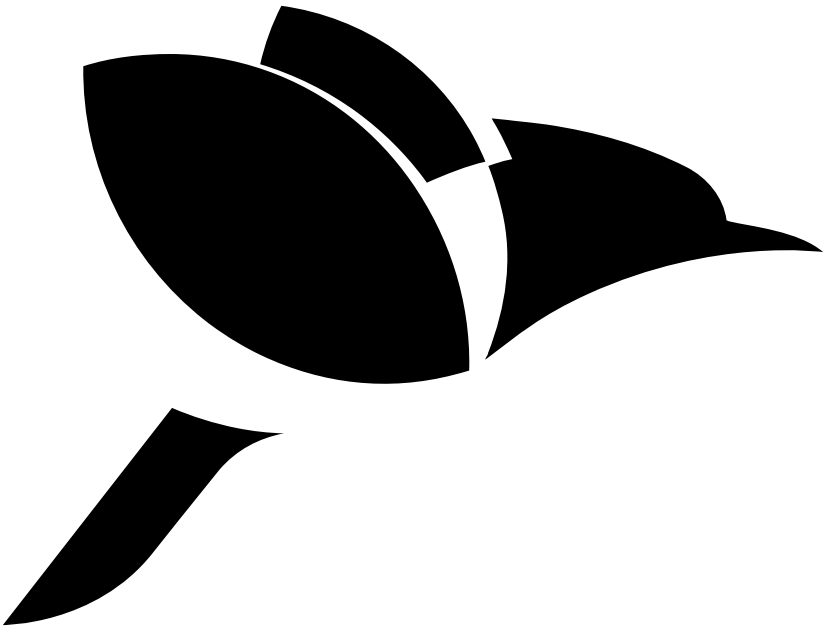

Kite-B - Supplement - Functional Hazard Assessment

Version	Document Number	Release Date
1.1.0	1863681304	02 Oct 2023

SWOOPAERO

Title	Kite-B - Supplement - Functional Hazard Assessment
Accountable Person	Chief Regulatory Officer
Manager Responsible	Flight Test Lead
Version	1.1.0
Status	PUBLISHED
Reference	DSN-KIT-MAN-AFM-SUP-FHA
Type	MANAGED PLATFORM
Fleet	Kite-B
Effective Date	02 Oct 2023
Review Date	02 Oct 2024

SWOOPAERO

Table of Contents

0. Administration

0.1 Revision Log

This table contains information from the latest revision to the document. For the full revision history, please see *Table A1-1*.

Version	Date	Summary		Author	Authorisation
1.1.0	02 Oct 2023		Response to CASA feedback	@ Aidan Biggar	@ Zac Kennedy
1.0.0	06 Jan 2023	N/A	N/A	@ Aidan Biggar	@ Zac Kennedy

Table 0-1: Revision history

0.2 Definitions

Term	Definition
Atypical airspace	Atypical Airspace is defined as; a) Restricted Airspace or Danger Areas; b) Airspace where normal manned aircraft cannot go (e.g. airspace within 100 ft. of buildings or structures); c) Airspace characterisation where the encounter rate of manned aircraft (encounter is defined as proximity of 3000 ft. horizontally and ± 350 ft. vertically) can be shown to be less than 1E-6 per flight hour during the operation); d) Airspace not covered in Airspace Encounter Categories (AEC) 1 through 12
BVLOS	Beyond Visual Line of Sight
CFIT	Controlled Flight into Terrain
CRP	Chief Remote Pilot
DAL	Development Assurance Level
Emergency landing	The system used to safely descend the RPA to the ground in case of extended hover assist activation or risk of containment volume breach.
ESC	Electronic Speed Controller
FC	Flight Controller
fGRC	Final Ground Risk Class
FHA	Functional Hazard Assessment
FTA	Fault Tree Analysis
GRC	Ground Risk Class
Hover assist	The primary subsystem used to reduce the severity of an RPA failure. This subsystem activates in case of non-normal behaviour from the RPA. The subsystem, in addition to the emergency landing functionality, constitutes the aircraft flight assistance and recovery system.
IMU	Inertial Measurement Unit
JARUS CS-UAS	Joint Authorities in Rule-Making for Unmanned Systems, Certification Specification for Unmanned Aerial Systems
MAC	Mid-air Collision
Near mid-air collision (NMAC)	A situation where two aircraft come within 30.5m (100 ft) vertically and 152.4m (500 ft) horizontally of each other while in flight.
NMAC	Near Mid-air Collision
OBC	Onboard Computer
OEM	Original Equipment Manufacturer
PRD	Prohibited, Restricted, Danger Area
RF	Radiofrequency

RFI	Radiofrequency Interference
RP	Remote Pilot
RPA	Remotely Piloted Aircraft
RPAS	Remotely Piloted Aircraft System
Serviceable	A state where the RPA can be flown safely, is released to service, and has been signed off as such by an authorised maintainer (or automated serviceability checks).
SPOF	Single Point of Failure
SRTM/DTED	Shuttle Radar Topography Mission/Digital Terrain Elevation Data
SSA	Systems Safety Assessment

Table 0-2: Definitions

0.3 Referenced Standards

The standards referenced below have been used to inform the contents of this document.

Organisation	Reference	Title
ASTM	ASTM F3389	Standard Test Method for Assessing the Safety of Small Unmanned Aircraft Impacts
FAA	AC23.1309 - 1E	System Safety Analysis and Assessment for Part 23 Airplanes
JARUS	AMC RPAS 1309	Safety Assessment of Remotely Piloted Aircraft Systems
SAE	ARP4761	Guidelines And Methods For Conducting The Safety Assessment Process On Civil Airborne Systems And Equipment
SAE	ARP4754A	Guidelines for Development of Civil Aircraft and Systems

Table 0-3: Referenced Standards

1. General

The Functional Hazard Assessment (FHA) has been developed on guidance from ARP4761 and AC23.1309 - 1E. The FHA forms the basis for other hazard analyses (for example, a Systems Safety Assessment). The FHA is a critical step in ensuring the safe operation of the RPA. It helps identify potential hazards and risks associated with the aircraft's functions and activities.

The purpose of the FHA is to identify and classify failure conditions of the functions (aircraft or system) according to their severity. The output of the FHA is the starting point for generating safety requirements. These derived requirements should be captured as requirements in aircraft and system specifications.

The FHA in section 2 focuses on the impact of total or partial loss of an aircraft function and the impact of misleading information or malfunction without warning to the pilot. The analysis reviews the detection mechanisms, procedural and technical mitigations, and system design elements that reduce the risk of the failure of that function. This includes, where applicable, reviews of redundancy, independence, and engineering analysis.

1.1 General Risk Reduction

For this FHA, it is assumed the Kite-B will be flown over low- to medium-risk areas. As a result, it is reasonable to assume the ground risk generally is significantly reduced. This assumption then reduces the level of analysis required (qualitative argument) to verify the hazards are adequately mitigated. The required level of analysis and mitigations are defined in *Section 1.3*.

1.2 Failure Severity

The following failure conditions have been used in the determination of classification for each of the functional failures. This is largely based on the JARUS 1309 document, where consensus has been shown or decided.

Classification	Failure Conditions	Example
No Safety Effect	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 remote crew workload.	Partial loss of telemetry to RPA
Minor	Failure conditions that would not significantly reduce RPAS safety and that involve remote crew actions that are within their capabilities. Minor failure conditions may include a slight reduction in safety margins or functional capabilities, or a slight increase in remote crew workload, such as flight plan changes.	Contingency landing
Major	Failure conditions that would reduce the capability of the RPAS or the ability of the remote crew to cope with adverse operating conditions to the extent that there would be a significant reduction in safety margins, functional capabilities or separation assurance. In addition, the failure condition has a significant increase in remote crew workload or impairs remote crew efficiency.	Emergency landing
Hazardous	Failure conditions that would reduce the capability of the RPAS or the ability of the remote crew to cope with adverse operating conditions to the extent that there would be the following: 1. Loss of the RPA where it can be reasonably expected that a fatality will not occur, or 2. A large reduction in safety margins or functional capabilities, or 3. High workload such that the remote crew cannot be relied upon to perform their tasks accurately or completely.	Crash, with low threat to humans (i.e. collision with obstacles)
Catastrophic	Failure conditions that could result in one or more fatalities.	Crash, with high threat to humans (i.e. CFIT or crash during hover)

Table 1-1: Severity definitions

1.2.1 Failure Probability

As shown in *Table 1-2*, the methodology to verify the safety objectives depends on the severity of the failure. In the case of the initial FHA, the quantitative probabilities are not applicable.

Section 1.3 modifies *Table 1-2* with the applied risk reduction from *Section 1.1*.

Classification	Safety Objective Verification Approach	Allowable Qualitative Probability	Allowable Quantitative Probabilities	Development Assurance Level
No Safety Effect	FHA summary	No probability requirement	No probability requirement	E
Minor	FHA summary	Probable	~10^-4	D
Major	Qualitative analyses	Remote	~10^-5	C
Hazardous	Qualitative and quantitative analyses	Extremely remote	~10^-6	B
Catastrophic	Qualitative and quantitative analyses	Extremely improbable	~10^-7	A

Table 1-2: Probability requirements and verification approach

Verification levels are defined using AC23.1309-1E

1.2.2 External Event Probability

The risk reduction highlighted above can be defined more concretely using external event probabilities and probability theory. For the Kite-B operating in a “standard” operation with fGRC of 3-4, the severity can be calculated as a function of the given population density, critical area, exposed population fraction, and probability of fatality given an impact.

As noted by CASA, this results in the following:

SAIL Comparison	fGRC Comparison	$D_{pop} \times A_c \times F_{exp} \times P(\text{fatality} \mid \text{impact})$	P(Catastrophic | EE)	Comparative “Severity” in the same category	Assessment Effort
3	4	0.001	$\leq 10^{-4}$	Minor	FHA with design and installation appraisal
2	3	0.0001	$\leq 10^{-3}$	Minor	FHA with design and installation appraisal

Table 1-4: External event probabilities

1.3 Required Analysis

In Table 1-5 below, the required level of analysis for failures in the FHA is outlined, considering the general risk mitigation in section 1.1.

Classification	Required Analysis
Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
Hazardous	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations
Minor	• Qualitative analysis • Review of technical and procedural mitigations
No Safety Effect	• Qualitative analysis

Table 1-5: Swoop Analysis

1.4 Emergency Landing

The emergency landing functionality is categorised as major in severity. This is due to the increased pilot workload and, to a lesser extent, the risk of damage to the aircraft where the emergency landing occurs on a tree or during retrieval.

The emergency land system functionality has been verified through demonstrated flight testing. The impact velocity is nominally 0.5m/s, with possible simultaneous failures resulting in a 2m/s descent rate. This is well below the threshold for structural damage to the RPA and would not result in projectiles that could cause a hazard to bystanders. Using hover motors during an emergency landing results in a distinctive and attention-capturing noise, complemented by an alarm bell that sounds from the initiation of the emergency landing until the RPA has been disarmed for 45 seconds. This noise would cause any bystanders to move clear of the descending RPA.

Per the definitions in *Table 1-1/1-2*, a major severity is appropriate as the execution of the landing does not significantly reduce RPAS safety, nor does it require unusual or complex crew actions.

Swoop Aero view the execution of an emergency land as a safe and appropriate action to take within the concept of operations.

The RPA emergency landing is automated (landing occurs without pilot input), and pilots are required to complete a tabletop exercise of the Emergency Response Plan to familiarise themselves with the requirements of the ERP. Additionally, the pilot may also choose to initiate an emergency landing manually. The software behaviour is identical in both cases.

The hover system used for emergency landing is tested in every takeoff (it is the same system), and the loss of any single hover motor or likely dual hover motor combination will not increase the descent rate or result in loss of control of the RPA.

1.5 Detect and Avoid

Current Swoop Aero operations occur in regions with low encounter rates and airspace density. The risk of MAC or NMAC is strategically and tactically reduced using mitigations such as NOTAMs, stakeholder engagement, UTM/system feeds, and electronic conspicuity to form part of the holistic DAA solution.

ADS-B In (and Out if operationally required/permissible) is the primary mitigation for cooperative traffic. The ADS-B In on the Kite-B is the uAvionix PingRX Pro, and the ADS-B In/Out is the Ping1090i or the Ping200X.

There is a functional explanation of the DAA system in the Kite-B - Supplement - Detect and Avoid.

The Detect and Avoid equipment/approach has not been certified by any regulator as there is currently no method provided to do so.

In many cases, the Kite-B is likely to operate in airspace that is “effectively” atypical due to the nature of the operation

2. Functional Hazard Assessment

The following FHA was completed using the template provided in AC23.1309 Appendix 2.

The failure severity for the type of failure is shown in the following rows:

- Total Loss of Function
- Loss of Primary Means of Providing Function
- Misleading / Incorrect Information
- Malfunction Without Warning

The relevant qualitative analysis, engineering analysis and review of technical and procedural mitigations are described in the final column.

In the relevant function section, there is a description of the purpose of the function and how the Kite-B system undertakes each function (including the systems used).

ⓘ The risk classification is based on the severity of the outcome before any mitigations. Thus, the classification is effectively set by the “Effect of Failure Condition (Crew/RPA)” column. Mitigations are included to justify the overall safety of the system in the context of that risk classification.

ⓘ Given the single point of failure nature of the flight controller, it is broadly excluded from the FHA and analysis of the failure of the FC itself is detailed in section 2.11.

2.1 Stability and Control

2.1.1 Function Description

This function is responsible for maintaining the stability and control of the RPA. This includes controlling the attitude, altitude and speed of the RPA and responding to external forces like wind. This function is also responsible for controlling airspeed, heading, and rates of the RPA in both hover and cruise.

In hover, this system relies on sensors such as the redundant Lidar, redundant GNSS, and redundant IMUs, and then executes commands to the ESCs to control the hover motors to maintain stable hover. In cruise flight, the system relies on the redundant GNSS, barometer, and redundant IMUs. A failure of this function is almost always catastrophic, as the RPA is no longer able to maintain stable flight.

2.1.2 Hazard Assessment

	Function #	Function	Failure Condition Hazard Description	Phase	Effect of Failure Condition (Crew/RPA)	FHA Summary	Classification	Verification Requirements
1	1.1	Determine attitude and speed	**Loss of all means of attitude and speed information**	Cruise	A full loss of all means of determining attitude and speed would likely result in an emergency landing or crash. The pilot's workout would be increased in response to the emergency and communicating with emergency responders and completing planned procedures.	• The Kite-B has redundant systems for attitude and speed estimation and would require simultaneous failure for total loss of the function. Detection is completed via comparison to alternative sensors (for example the values from one IMU compared to the other two IMUs) and using the onboard flagging system in the flight controller. These failures are shown to the pilot with alerts.	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
2			Loss of Primary Means of Providing Function	Cruise	A loss of the primary means of providing attitude and speed information would show alerts to the pilot who may need to take an action per the checklist. This increases the pilot workload.	• Partial loss will utilise a fallback system, for example, loss of GNSS yaw (primary system for heading estimation) will use the compass which has been validated with thousands of flight hours. Loss of both sources of heading estimate will use IMU data to correct which has multiple layers of redundancy with three IMUs in the flight controller.	Minor	• Qualitative analysis • Review of technical and procedural mitigations
3			Misleading / Incorrect Information	Cruise	Misleading information could cause the pilot to command an inappropriate action.	• The worst case of the pilot commanding an inappropriate action is emergency landing, which is major in severity.	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations
4			Malfunction Without Warning	Cruise	With no warning, the pilot would not take an action; however, the outcome is likely a crash which requires the pilot to coordinate the emergency response per the applicable procedures.	• Any failure in this system is shown to the pilot as a flag, and depending on the failure mode may cause an automated action such as contingency landing. This behaviour may increase pilot workload so is classified as minor. • A malfunction could cause the aircraft to believe it is at the correct altitude when it is not (much higher or much lower), or alternatively think it is going much faster/ slower than it should be. • The detection for this failure utilises the sensor redundancy to detect any failures in the primary systems. For example, a failure in a single airspeed sensor is immediately reported (based on probability of failure) to the flight controller which begins rejecting data from that sensor.	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures

5	1.2	Stabilise perturbations	Total Loss of Function	All	Perturbations may be able to increase in severity such that a possible deviation or departure from controlled flight (or damage to structure) is possible. When the system is functioning normally, any perturbations (for example due to wind) are quickly damped out.	• The Kite-B is required to only be flown in environmental conditions that are within the limits of the aircraft. The pilot is required to ensure environmental conditions are suitable for flight for the entirety of the duration of the mission. The RPS shows weather radar inputs (where available) which also assists in mitigating the risk of flight into environmental conditions outside the aircraft limits. • If very large oscillations cause a structural failure, the outcome is catastrophic. Prior to any such failure, alerts are shown to the pilot.	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
6			Loss of Primary Means of Providing Function	All	The Kite-B has eight hover motors, so the loss of any single hover motor would not cause the loss of this function. In this scenario, the pilot may need to command an action (such as contingency landing) or the aircraft may execute a safe automated action.	• All motors and control surfaces are redundant, so the loss of a single aileron (for example) would not result in the inability to control roll perturbations.	Minor	• Qualitative analysis • Review of technical and procedural mitigations
7			Misleading / Incorrect Information	All	Misleading information could cause the pilot to command an inappropriate action. The worst case is emergency landing, which is major in severity.	• The FC has redundant IMUs to estimate attitude and will raise an alert to the pilot and reject the data from an unhealthy IMU.	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations
8			Malfunction Without Warning	All	If the function fails without warning, the RPA may use inaccurate attitude data from an unhealthy IMU or may have an unhealthy motor or control surface that is not reported to the FC/RP.	• The aircraft has flags for vibration (ascending in severity for the magnitude of detected vibration) as detected by the flight controller and will execute appropriate automated actions based on these flags. • If the aircraft is not able to sustain a safe flight, it will initiate an automated emergency landing.	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations
9	1.3	Maneuvre RPA	Total Loss of Function	All	If the aircraft lost a significant number of motors, the RPA would no longer be able to manoeuvre correctly along the planned path.	• At worst, an unstable flight could result in an automated emergency landing which is classified as major. The emergency landing is triggered by a divergence between desired and actual attitude, airspeed or altitude.	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations
10			Loss of Primary Means of Providing Function	All	As noted previously, the loss of a single motor or attitude sensor will use the redundant systems to ensure no loss of flight.	• As above.	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations

11			Misleading / Incorrect Information	All	False alerting is likely inconsequential to the FC. At worst, the FC may use incorrect attitude data and have an inaccurate attitude estimate as a result.	• Misleading information could cause the pilot to command an inappropriate action. The worst case is emergency landing, which is major in severity.	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations
12			Malfunction Without Warning	All	If the FC has an issue, the FC may use incorrect attitude data and have an inaccurate attitude estimate as a result.	• The aircraft has flags for both hover and forward powertrains, and a failure would be detected by the ESC and reported to the pilot.	Minor	• Qualitative analysis • Review of technical and procedural mitigations
13	1.4.1	Control airspeed	Total Loss of Function	Cruise	A failure to decrease airspeed when requested could result in a CFIT event, at worst. This would require simultaneous corruption of forward motor commands to both forward motors. Such corruption has not been observed in the thousands of operational flight hours.	• The ESCs have an internal verification for the commands they receive and will not act on erroneous commands. A failure of the forward motors leading to the inability to maintain the desired airspeed would result in an automated emergency landing.	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
14			Loss of Primary Means of Providing Function	Cruise	As above	• Given the forward motors are the only system responsible for controlling airspeed in forward flight, the loss of the primary means of providing this function is analogous to the full loss of function.	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
15			Misleading / Incorrect Information	Cruise	N/A	• Misleading information could cause the pilot to command an inappropriate action. The worst case is emergency landing, which is major in severity.	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations
16			Malfunction Without Warning	Cruise	If the RPA does not detect the erroneous motor commands, the worst case outcome is CFIT.	• Given the forward motors are the only system responsible for controlling airspeed in forward flight, the loss of the primary means of providing this function is analogous to the full loss of function. If the control airspeed function activates when it is not required this could cause similar outcomes to the above.	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures

17	1.4.2	Control altitude and rate	Total Loss of Function	Hover (takeoff, transition, and landing)	A failure to control altitude could result in hover battery depletion or CFIT, at worst.	• This is mitigated through technical (altitude prioritised in the autopilot) and procedural (route planning and crosscheck) controls. • The altitude and rate estimates use redundant sensors (GNSS, Lidar, barometer for altitude and three independent IMUs for rates) which ensures no SPOF for these estimates.	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
18			Loss of Primary Means of Providing Function	Hover (takeoff, transition, and landing)	N/A	• Loss of a hover motor would reduce the capacity of the RPA to respond to altitude or rate commands; however, the RPA is able to land under control with the failure of a single hover motor.	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations
19			Misleading / Incorrect Information	Hover (takeoff, transition, and landing)	Misleading information could cause the pilot to command an inappropriate action. The worst case is emergency landing, which is major in severity.	• Altitude estimates from the RPA use redundant sensors and are filtered in the EKF, so the likelihood of a false altitude estimate is significantly reduced.	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations
20			Malfunction Without Warning	Hover (takeoff, transition, and landing)	Malfunction without warning would have a catastrophic outcome if the flight controller is not aware of the deviation from the desired altitudes or rates. In this scenario, there is a significant risk of CFIT.	• This is mitigated through the use of three different sensors for hover altitude estimation (GNSS, Lidar, and barometer) which protects against single sensor failure escalating to a full function malfunction.	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
21	1.4.3	Control heading	Total Loss of Function	Hover (takeoff, transition, and landing)	Inability to control heading could result in a CFIT if the RPA erroneously commands a heading that is not achieved or if the RPA is not able to yaw accurately into the wind.	• The Kite-B has redundant systems for heading estimation (GNSS yaw, compass, and IMU) and would require simultaneous failure for total loss of function. The eight hover motors are responsible for heading control in hover, and the loss of any single motor would not result in the loss of heading control.	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures

22			Loss of Primary Means of Providing Function	Hover (takeoff, transition, and landing)	Partial loss of the control heading function could occur with a loss of hover motor or failure of GNSS yaw.	• Partial loss will utilise a fallback system, for example, loss of GNSS yaw (primary system for heading estimation) will use the compass which has been validated with thousands of flight hours on the Kookaburra MkIII RPA. Loss of both sources of heading estimate will use IMU data to correct which is doubly redundant with three IMUs in the flight controller. • Any failure in this system is shown to the pilot as a flag, and depending on the failure mode may cause an automated caution such as contingency landing. This behaviour may increase pilot workload so is classified as minor.	Minor	• Qualitative analysis • Review of technical and procedural mitigations
23			Misleading / Incorrect Information	Hover (takeoff, transition, and landing)	N/A	• Misleading information could cause the pilot to command an inappropriate action. The worst case is emergency landing, which is major in severity.	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations
24			Malfunction Without Warning	Hover (takeoff, transition, and landing)	Inability to control heading could result in a CFIT if the RPA erroneously commands a heading that is not achieved or if the RPA is not able to yaw accurately into the wind. This is analogous to the total failure case if the aircraft cannot detect the failure.	• The Kite-B has redundant systems for heading estimation (GNSS yaw, compass, and IMU) and would require simultaneous failure for total loss of function. The eight hover motors are responsible for heading control in hover, and the loss of any single motor would not result in the loss of heading control.	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures

Table 2-1: Stability and Control Hazard Assessment

2.2 Air Navigation

2.2.1 Function Description

This function is responsible for ensuring that the RPA can safely and effectively navigate through airspace while performing its intended tasks. This includes the ability to determine the position, heading, and altitude of the RPA (in both hover and forward flight) and feed the “Stability and Control” function to maintain the desired positions, headings, and altitudes. This function is also responsible for managing the flight plan (route) and ensuring the aircraft is maintaining accurate track relative to that flight plan.

For this function, the dual GNSS modules are the most critical sensors to estimate position, heading, and altitude.

2.2.2 Hazard Assessment

	Function #	Function	Failure Condition Hazard Description	Phase	Effect of Failure Condition (Crew/RPA)	FHA Summary	Classification	Verification Requirements
1	2.1.1	Determine position, heading, and altitude	Total Loss of Function	Cruise	A total loss of the ability to determine the position, heading, or altitude would result in a CFIT or flyaway event. This would require a failure of both GNSS modules.	• The Kite-B has redundant systems for heading estimation (GNSS yaw, compass, and IMU) and would require simultaneous failure for total loss of function. • The Kite-B also has redundant sensors for position and altitude estimation in cruise with dual GNSS for position and altitude and fallback to barometer altitude control in the case of poor altitude estimates from both GNSS modules. • The aircraft is able to detect these failures using the redundant sensor	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures

	Function #	Function	Failure Condition Hazard Description	Phase	Effect of Failure Condition (Crew/RPA)	FHA Summary	Classification	Verification Requirements
2			Loss of Primary Means of Providing Function	Cruise	Loss of the primary means of estimating the position, heading, or altitude would use the fallback system and would not have a safety impact on the RPA. The pilot workload may increase as an alert will be shown and may require pilot command action.	• Partial loss will utilise a fallback system, for example loss of GNSS yaw (primary system for heading estimation) will use the compass which has been validated with thousands of flight hours on the Kookaburra RPA. Loss of both sources of heading estimate will use IMU data to correct which is doubly redundant with three IMUs in the flight controller. After an extended period in this mode, the RPA will automatically conduct an emergency landing. • Any failure in this system is shown to the pilot as a flag, and depending on the failure mode may cause an automated action such as contingency landing. This behaviour may increase pilot workload so is classified as minor.	Minor	• Qualitative analysis • Review of technical and procedural mitigations
3			Misleading / Incorrect Information	Cruise	Misleading information fed to the RPA about the health of any sensor could possibly cause the aircraft to reject useful data from a truly “healthy“ sensor. The pilot would be shown an alert which could be as high as a warning level (emergency landing).	• Misleading information could cause the pilot to command an inappropriate action. The worst case is emergency landing, which is major in severity.	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations
4			Malfunction Without Warning	Cruise	Malfunction without warning could cause the aircraft to use poor data from a sensor (i.e. bad GNSS data) instead of rejecting the data. This has a significant risk of CFIT.	• The detectability of a failure of this function is high due to the redundant nature of all sensors for performing this function. Erroneous data will be flagged by the EKF and rejected.	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures

	Function #	Function	Failure Condition Hazard Description	Phase	Effect of Failure Condition (Crew/RPA)	FHA Summary	Classification	Verification Requirements
5	2.2	Store/update mission route	Total Loss of Function	All	If the RPA loses the route file entirely while in flight, there is a risk of emergency landing or possible CFIT.	• The route is stored in the flight controller with corruption checks to ensure the route cannot be loaded or flown with corrupt inputs. Route file corruption has not been observed during the thousands of operational flights with the Kookaburra RPA. Corruption checks are completed on the route file which is sent from Swoop Planner and the Compute Core to the flight controller onboard the RPA. • Total or partial failure of the route file on the flight controller could cause a CFIT event.	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
6			Loss of Primary Means of Providing Function	All	There is no plausible loss of primary means of providing function, so it is treated as a full loss.	• As above	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
7			Misleading / Incorrect Information	All	Misleading or incorrect information could cause the aircraft to follow a different route (due to corrupt waypoints) or initiate an emergency landing because it believes it is outside of the contingency volume. Misleading information could cause the pilot to believe the aircraft is in a different location than their expectation, which could significantly increase the pilot's workload and stress.	• See total loss.	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
8			Malfunction Without Warning	All	Failure of the route file on the FC without warning is analogous to the total loss of the function.	• Total or partial failure of the route file on the flight controller could cause a CFIT event. • See total loss mitigations.	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures

	Function #	Function	Failure Condition Hazard Description	Phase	Effect of Failure Condition (Crew/RPA)	FHA Summary	Classification	Verification Requirements
9	2.3	Monitor/ correct actual route vs. planned route	Total Loss of Function	Cruise	Total loss of the function could result in flight away from the desired track, potentially causing a CFIT or flight into an unplanned area (for example controlled airspace). This outcome is catastrophic.	• The aircraft has redundant GNSS modules to accurately track the position of the aircraft relative to the desired track. Any failure in this system will, at worst, cause an emergency landing. Significant deviation from the desired route would result in an automated emergency landing for a projected breach of the contingency volume. • Failure of the primary system for path tracking would cause, at worst, an emergency landing	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
10			Loss of Primary Means of Providing Function	Cruise	Loss of the primary means of tracking the desired path would likely result in breaching the allowable contingency volume and cause an automated emergency landing.	• The aircraft has redundant GNSS modules to accurately track the position of the aircraft relative to the desired track. Any failure in this system will, at worst, cause an emergency landing. Significant deviation from the desired route would result in an automated emergency landing for projected breach of the contingency volume. • Failure of the primary system for path tracking would cause, at worst, an emergency landing	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations
11			Misleading / Incorrect Information	Cruise	Given the flight controller has significant authority to instigate maneuvers based on the deviation from the path, should the ability to monitor the actual path vs. intended path be corrupted, this could lead to the aircraft navigating to unplanned areas where potential CFIT/ incursions could occur. Misleading information could cause the pilot to believe the aircraft is in a different location than their expectation, which could significantly increase pilot's workload and stress.	• See total loss mitigations.	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures

	Function #	Function	Failure Condition Hazard Description	Phase	Effect of Failure Condition (Crew/RPA)	FHA Summary	Classification	Verification Requirements
12			Malfunction Without Warning	Cruise	A failure to accurately determine the position relative track that is not detected by the flight controller could result in CFIT. This outcome is catastrophic.	• See total loss mitigations.	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
13	2.4.1	Determine hover position, heading, and altitude	Total Loss of Function	Hover (takeoff, transition, and landing)	A failure to accurately determine hover position, heading, or altitude could result in a catastrophic occurrence (CFIT).	• The position and altitude are estimated using redundant sensors (dual Lidar, dual barometer, dual GNSS). The heading is estimated using redundant sensors (quad compass, IMU, and GNSS for yaw). This redundancy ensures the likelihood of catastrophic failure is extremely low.	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
14			Loss of Primary Means of Providing Function	Hover (takeoff, transition, and landing)	A loss of the primary means of performing this function would use the fallback sensors and potentially require a pilot action.	• All sensors on the RPA have operationally proven high reliability and robustness so the likelihood of a single sensor failure is relatively low.	Minor	• Qualitative analysis • Review of technical and procedural mitigations
15			Misleading / Incorrect Information	Hover (takeoff, transition, and landing)	A misleading warning or malfunction without warning could, at worst, result in the RPA operating as if it is at the correct position, heading, or altitude when it is not, which would lead to CFIT.	• All sensor data is compared to existing sensors in the EKF, so incorrect data can be readily filtered and removed from the overall state estimate.	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
16			Malfunction Without Warning	Hover (takeoff, transition, and landing)	A failure to accurately determine hover position, heading, or altitude could result in a catastrophic occurrence (CFIT).	• The redundant sensors ensure the likelihood of undetected failures is significantly reduced.	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
17	2.4.2	Monitor/ correct actual vs. planned profile	Total Loss of Function	Hover (takeoff, transition, and landing)	A failure to maintain/correct position in hover could, at worst, cause a CFIT if the RPA is unable to maintain the desired landing profile or position relative to track.	• The RPA has redundant sensors to estimate the position, and eight hover motors for maintaining position and control during hover. Any single point of failure would not result in total loss of function.	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures

	Function #	Function	Failure Condition Hazard Description	Phase	Effect of Failure Condition (Crew/RPA)	FHA Summary	Classification	Verification Requirements
18			Loss of Primary Means of Providing Function	Hover (takeoff, transition, and landing)	Loss of primary means would utilise the fallback system (redundant hover motors, redundant GNSS etc.)	• Partial loss could potentially trigger an emergency landing for full GNSS loss or projected breach of the contingency volume.	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations
19			Misleading / Incorrect Information	Hover (takeoff, transition, and landing)	Misleading information could cause the pilot to command an inappropriate action. The worst case is emergency landing, which is major in severity.	• All sensor data is compared to existing sensors and only used when it is considered “valid” by the EKF.	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations
20			Malfunction Without Warning	Hover (takeoff, transition, and landing)	If there is no warning, the aircraft or pilot may think they are following the planned profile while in reality, the aircraft is flying some unknown path that could cause CFIT/airspace incursion/loss of containment.	• See misleading case.	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures

Table 2-2: Air Navigation Hazard Assessment

2.3 State Transition

2.3.1 Function Description

This function is responsible for determining when the aircraft is in the air and when it is on the ground. It is critical to safely determine this transition in order to safely disarm the motors at the end of a mission and also to ensure the motors are never erroneously disarmed while the RPA is airborne. The key sensors to complete this detection are the AGL sensor (Lidar) to determine height above ground in hover and the IMUs for detecting impacts with the ground.

This function is also responsible for determining when the aircraft should switch from hover to cruise flight or vice versa.

2.3.2 Hazard Assessment

	Function #	Function	Failure Condition Hazard Description	Phase	Effect of Failure Condition (Crew/RPA)	FHA Summary	Classification	Verification Requirements
1	3.1	Determine air/ground transition	Total Loss of Function	Transition/Landing	The worst-case outcome of the failure of this function would be the RPA disarming while airborne.	• The Kite-B disarm logic is sophisticated and considers the velocity (from the GNSS), the throttle (from the FC), and the position. A series of checks must simultaneously be true for the disarm to occur.	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
2			Loss of Primary Means of Providing Function	Transition/Landing	Loss of primary means of providing the function could result in a delayed disarm (possible bouncing on the ground). This could possibly result in minor damage to the RPA.	• Any partial failure in this system is shown to the pilot as a flag, and depending on the failure mode may cause an automated action such as an aborted takeoff or emergency landing. This behaviour may increase pilot workload so is classified as minor.	Minor	• Qualitative analysis • Review of technical and procedural mitigations
3			Misleading / Incorrect Information	Transition/Landing	If the FC receives erroneous data, it could possibly act to disarm at an inappropriate time. The worst case is a disarm while in the air resulting in loss of the RPA.	• All sensor data is cross-checked and multiple simultaneous checks must be true for the RPA to disarm.	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures

	Function #	Function	Failure Condition Hazard Description	Phase	Effect of Failure Condition (Crew/RPA)	FHA Summary	Classification	Verification Requirements
4			Malfunction Without Warning	Transition/Landing	Malfunction without warning could result in the RPA transitioning at a very low altitude or incorrectly while in cruise flight. This could result in CFIT or other loss of flight.	• The Kite-B has redundant systems for altitude and would require simultaneous failure for total loss of function. This is mitigated through several different systems, including an independent check at the time of arming which ensures that the transition point is at least 32m above the current location. This check ensures that no single failure could result in a “low” transition.	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures

Table 2-3: State Transition Hazard Assessment

2.4 Manage Datalink

2.4.1 Function Description

This function is responsible for monitoring communications links with the pilot and ensuring the most appropriate (aka strongest) is selected at given points during a mission. The RPA has three communication methods, cellular, Wi-Fi, and Satcom. Where multiple are available, the RPA will use the strongest signal to communicate with the pilot and switch as needed if a connection becomes unreliable.

The onboard computer receives signal quality information from the three communications links and is responsible for selecting the most appropriate.

2.4.2 Hazard Assessment

	Function #	Function	Failure Condition Hazard Description	Phase	Effect of Failure Condition (Crew/RPA)	FHA Summary	Classification	Verification Requirements
1	4.1.1	Determine signal strength	Total Loss of Function	All	Signal strength does not affect automated flight. If the signal strength degrades sufficiently, the pilot workload may increase due to uncertainty about the exact RPA position and alerts. The worst-case outcome is that the pilot is required to execute an emergency landing but is unable to do so.	• Changes in the terrestrial connection due to poor connection with cellular or Wi-Fi networks will utilise the redundant Satcom system. See the Kite-B RPAFM for further information on communications links and the C3 architecture.	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations
2			Loss of Primary Means of Providing Function	All	Signal strength does not affect automated flight. If the signal strength degrades sufficiently, the pilot workload may increase due to uncertainty about the exact RPA position.	• Changes in the terrestrial connection due to poor connection with cellular or Wi-Fi networks will utilise the redundant Satcom system. See the Kite-B RPAFM for further information on communications links and the C3 architecture.	No Safety Effect	• Qualitative analysis
3			Misleading / Incorrect Information	All	Misleading information could result in the RPA switching to Satcom erroneously (which leads to increased latency) or not switching when required (which would cause a full loss of telemetry). The worst-case outcome is that the pilot is required to execute an emergency landing but is unable to do so.	• The cellular and Wi-Fi modules are COTS products that are tested extensively by the manufacturer and by Swoop Aero to ensure the likelihood of incorrect information is extremely low.	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations

	Function #	Function	Failure Condition Hazard Description	Phase	Effect of Failure Condition (Crew/RPA)	FHA Summary	Classification	Verification Requirements
4			Malfunction Without Warning	All	A failure of the RPA to detect a loss of signal strength and subsequently switch to Satcom would result in loss of telemetry to and from the RPA. The worst-case outcome is that the pilot is required to execute an emergency landing but is unable to do so. T	• The cellular and Wi-Fi modules are COTS products that are tested extensively by the manufacturer and by Swoop Aero to ensure the likelihood of malfunction without warning is extremely low. • If the Satcom communication link fails, an alert is shown to the RP.	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations

Table 2-4: Datalink Hazard Assessment

2.5 Manage Payload

2.5.1 Function Description

This function is responsible for ensuring any payloads in the RPA do not adversely impact flight safety. The RPA is designed such that any payload within the AFM weight limits will have a corresponding centre of gravity (CG) position that is within the safe range (ensuring the operator is not responsible for checking CG prior to flight). The operator is responsible for weighing the payload before every mission for safety and tracking purposes.

This function is primarily managed procedurally, without the use of specific onboard sensors or systems. The procedural controls ensure the payload remains within the stable CG range for the RPA.

2.5.2 Hazard Assessment

	Function #	Function	Failure Condition Hazard Description	Phase	Effect of Failure Condition (Crew/RPA)	FHA Summary	Classification	Verification Requirements
1	5.1	Payload doesn't negatively affect flight performance	Total Loss of Function	All	A total loss of the function could result in oscillatory flight (due to incorrect CG position) or motor saturation (due to excessive weight). Either of these outcomes could result in a CFIT in the absolute worst case.	• Total failure would be a procedural failure where a payload which is either, too heavy, too large or unbalanced is inserted and flown on the aircraft. • Mass and volume are procedurally mitigated via checklists and training. Balance is mitigated via engineering whereby a mass-appropriate payload cannot unbalance the aircraft. • A CG outside of limits would be captured by the automated hover assist (for attitude control) and subsequent emergency landing.	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
2			Loss of Primary Means of Providing Function	All	A loss of the primary means is equivalent to total loss.	• See total loss.	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures

	Function #	Function	Failure Condition Hazard Description	Phase	Effect of Failure Condition (Crew/RPA)	FHA Summary	Classification	Verification Requirements
3			Misleading / Incorrect Information	All	Misleading or incorrect information could lead to an unbalanced payload or overweight payload. This is analogous to the total loss of the function.	• See total loss.	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
4			Malfunction Without Warning	All	Malfunction without warning would be a payload that was of unknown mass causing negative effects on flight performance. At worst, this could result in a CFIT.	• See total loss.	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures

Table 2-6: Payload Hazard Assessment

2.6 Monitor Mission Progress

2.6.1 Function Description

This function is responsible for monitoring the progress of the mission, including RPA health, weather conditions, and any required contingency actions.

2.6.2 Hazard Assessment

	Function #	Function	Failure Condition Hazard Description	Phase	Effect of Failure Condition (Crew/ RPA)	FHA Summary	Classification	Verification Requirements
1	6.1	Telemeter RPA status to RPS	Total Loss of Function	All	A failure of this function will not have any effect on the automated functions of the RPA. Whilst the pilot may not have full capacity to command the aircraft, it will continue to execute the mission as planned. Total loss of telemetry could, at worst, cause the pilot to be unable to command an emergency landing when required.	• The RPA has redundant telemetry links. These links are constantly monitored by the OBC for health and signal strength and switching to use the most appropriate connection at a given moment. The connection links are fully independent (for hardware and firmware), so a failure of one link does not impact either of the other two links.	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations
2			Loss of Primary Means of Providing Function	All	Partial loss, for example through loss of cellular networks, would utilise the fallback satellite communication system, with no impact on safety or pilot workload.	• N/A	No Safety Effect	• Qualitative analysis
3			Misleading / Incorrect Information	All	Misleading information would not reduce the capability of the RPA; however, may cause a slight increase in workload for the remote crew which is classified as minor.	• N/A	Minor	• Qualitative analysis • Review of technical and procedural mitigations

	Function #	Function	Failure Condition Hazard Description	Phase	Effect of Failure Condition (Crew/ RPA)	FHA Summary	Classification	Verification Requirements
4			Malfunction Without Warning	All	A failure of this function will not have any effect on the automated functions of the RPA. Whilst the pilot may not have full capacity to command the aircraft, it will continue to execute the mission as planned. Total loss of telemetry could, at worst, cause the pilot to be unable to command an emergency landing when required.	• See total loss	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations
5	6.2.1	Weather awareness enroute	Total Loss of Function	All	A total loss of this function could result in flight into unacceptable weather conditions. In the worst case, this could result in loss of flight or CFIT.	• Procedural mitigations relating to pilot awareness of weather enroute mitigate total loss of failure. The pilot is required to check the weather forecast and monitor weather conditions throughout the flight. Radar data is shown directly to the pilot via an overlay on the RPS screen.	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
6			Loss of Primary Means of Providing Function	All	Loss of the primary means of providing the function could increase the likelihood of flight into unacceptable weather conditions. If we cannot use the primary weather source to get information, other weather sources must be used or flight is unacceptable.	• See total loss	Minor	• Qualitative analysis • Review of technical and procedural mitigations
7			Misleading / Incorrect Information	All	Misleading weather information or forecasting could increase the likelihood of flight into unacceptable weather conditions. Likely the outcome is analogous to total loss of the function.	• See total loss	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
8			Malfunction Without Warning	All	Malfunction without warning could increase the likelihood of flight into unacceptable weather conditions. Likely the outcome is analogous to total loss of the function.	• See total loss	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures

	Function #	Function	Failure Condition Hazard Description	Phase	Effect of Failure Condition (Crew/ RPA)	FHA Summary	Classification	Verification Requirements
9	6.2.2	Assess weather proximity to planned route	Total Loss of Function	All	See section 6.2.1	• See section 6.2.1	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
10			Loss of Primary Means of Providing Function	All	See section 6.2.1	• See section 6.2.1	Minor	• Qualitative analysis • Review of technical and procedural mitigations
11			Misleading / Incorrect Information	All	See section 6.2.1	• See section 6.2.1	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
12			Malfunction Without Warning	All	See section 6.2.1	• See section 6.2.1	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
13	6.3	Determine nearest safe contingency landing area	Total Loss of Function	All	Total loss of this function could result in the aircraft failing to divert when required due to a pilot command or automated aircraft response to an issue. If this is the case then the aircraft would have lost significant safety margins (i.e. in an adverse operating condition the crew could not effect the outcomes they want).	• The primary mitigation against the failure of this function is the Swoop Planner tool. Contingency landing areas are determined preflight by a route planner and cross-checked with a route authoriser. Route planning has procedural mitigations to reduce probability and risk. • When a contingency divert is requested, the aircraft calculates the least cost path to the contingency landing location. Any failure of this system is shown to the pilot as an alert.	Hazardous	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures

	Function #	Function	Failure Condition Hazard Description	Phase	Effect of Failure Condition (Crew/ RPA)	FHA Summary	Classification	Verification Requirements
14			Loss of Primary Means of Providing Function	All	The worst case outcome is a delayed contingency action. This is minor in severity due to the slightly increased pilot workload.	• Contingency landing sites are chosen and preplanned based on their availability and safety against a set of criteria. The aircraft does not assess the safety of a contingency landing location in real-time. If a contingency landing is required, the aircraft will calculate the quickest path to an approved contingency landing location.	Minor	• Qualitative analysis • Review of technical and procedural mitigations
15			Misleading / Incorrect Information	All	Misleading or incorrect information could cause the pilot to command an inappropriate pilot action. The most severe is emergency landing which is major.	• N/A	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations
16			Malfunction Without Warning	All	Similar to the total loss case	• See total loss	Hazardous	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures

Table 2-6: Mission Progress Hazard Assessment

2.7 Manage Flight Systems

2.7.1 Function Description

This function is responsible for maintaining and managing flight systems during a mission. This includes executing the contingency or emergency landing functions as required to maintain the safety of flight or as commanded by the Remote Pilot. This function monitors for contingency or emergency landing commands throughout the mission and ensures they are safely executed if and when required.

2.7.2 Hazard Assessment

	Function #	Function	Failure Condition Hazard Description	Phase	Effect of Failure Condition (Crew/RPA)	FHA Summary	Classification	Verification Requirements
1	7.1	Determine flight system status	Total Loss of Function	All	A total or partial failure in the system could result in an automated or pilot-commanded emergency landing which is classified as major.	• N/A	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations
2			Loss of Primary Means of Providing Function	All	A total or partial failure in the system could result in an automated or pilot-commanded emergency landing which is classified as major.	• N/A	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations
3			Misleading / Incorrect Information	All	Misleading information could cause the pilot to command an inappropriate action. The worst case is emergency landing, which is major in severity.	• N/A	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations
4			Malfunction Without Warning	All	A malfunction of this function without warning could result in the FC or RPA believing that systems are fully operational when there is an issue; however, this would require a simultaneous failure of this function and one (or more) aircraft systems monitored by this system to fail.	• N/A	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations
5	7.2.1	Contingency landing divert	Total Loss of Function	Cruise	Total loss of function would result in the aircraft not taking a contingency landing that was commanded (either autonomously or from the pilot). Thus, in a failure the aircraft would not divert. At worst, this could cause an emergency landing.	• N/A	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations

	Function #	Function	Failure Condition Hazard Description	Phase	Effect of Failure Condition (Crew/RPA)	FHA Summary	Classification	Verification Requirements
6			Loss of Primary Means of Providing Function	Cruise	A partial loss of the system could cause the aircraft to continue the planned mission (without executing the contingency landing). This may slightly increase pilot workload so is classified as minor.	• N/A	Minor	• Qualitative analysis • Review of technical and procedural mitigations
7			Misleading / Incorrect Information	Cruise	Misleading information could cause significantly increased workload for the team due to an aircraft landing at an unexpected location or the aircraft reporting that it is diverting but not successfully diverting. This is classified as major.	• N/A	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations
8			Malfunction Without Warning	Cruise	A malfunction without warning could also result in an erroneous contingency landing or failed contingency landing. The worst case is an emergency landing.	• N/A	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations
9	7.2.2	Emergency landing	Total Loss of Function	All	• The emergency landing system is a key part of the safety system of the RPA. Failure to execute emergency landing when required could result in a CFIT (for example, in the case of an aerodynamic stall or adverse weather conditions).	• The emergency landing system is tested in simulation and flight validation for all software changes, and the hover system is verified during every takeoff, and the takeoff is aborted if there is a fault found in the hover system.	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
10			Loss of Primary Means of Providing Function	All	A partial failure could also cause a catastrophic outcome if the system does not activate as intended. See section 1.4 for more information.	• N/A	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
11			Misleading / Incorrect Information	All	Misleading information could cause the pilot to command an inappropriate action. The worst case is emergency landing, which is major in severity.	• N/A	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations

	Function #	Function	Failure Condition Hazard Description	Phase	Effect of Failure Condition (Crew/RPA)	FHA Summary	Classification	Verification Requirements
12			Malfunction Without Warning	All	The worst case of a malfunction without warning is initiating an emergency landing when it is not commanded (or failing to execute an emergency landing when one is required). This is catastrophic.	• N/A	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures

Table 2-7: Flight Systems Hazard Assessment

2.8 Preflight Preparations

2.8.1 Function Description

This function ensures preparation for flight is successfully completed prior to any mission being flown. This includes validating routes are safe and legal to fly (clear of terrain and obstacles, clear of controlled airspace, clear of PRD areas etc.) and that all preflight requirements are met (charged batteries, mission loaded correctly on the RPA, and all preflight systems tests complete successfully).

This function is predominantly completed using Platform tools (i.e. Swoop Planner), operational controls, and the automated self-test functionality on the Kite-B.

2.8.2 Hazard Assessment

	Function #	Function	Failure Condition Hazard Description	Phase	Effect of Failure Condition (Crew/RPA)	FHA Summary	Classification	Verification Requirements
1	8.1.1	Plan safe mission	Total Loss of Function	All	A total loss of this function could, at worst, result in an unacceptable mission being loaded to the RPA.	• Mission planning is completed exclusively in Swoop Aero's internal software system, Swoop Planner, under strict software validation and procedure. All stages of mission planning are cross-checked to ensure missions reduce risk. • The primary mitigation against the catastrophic failure of this function is the Swoop Planner tool. The software validation checks the entire containment volume for a number of validations to ensure the route is within acceptable limits. • The route planning process also relies on an independent crosscheck (in addition to the software validator). • The OBC has a check to ensure that the route file provided to the FC is not corrupt.	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations
2			Loss of Primary Means of Providing Function	All	Partial failure would have no effect on safety due to being doubly redundant in software, route cross-checking and pilot mission selection.	• See total loss	No Safety Effect	• Qualitative analysis

	Function #	Function	Failure Condition Hazard Description	Phase	Effect of Failure Condition (Crew/RPA)	FHA Summary	Classification	Verification Requirements
3			Misleading / Incorrect Information	All	Misleading information could cause the route approver to allow a mission to be selected by the pilot and would have the same outcome as total loss of function.	• All routes are human cross-checked to ensure they meet route planning guidelines.	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations
4			Malfunction Without Warning	All	The worst case of a malfunction without warning is a total loss of the function.	• See total loss	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations
5	8.1.2	Obstacle location awareness	Total Loss of Function	All	A total failure of this system could, at worst, cause the aircraft to impact a ground obstacle such as a tree or building. This poses a very significant risk to the RPA but is unlikely to cause a fatality.	• As above, mission planning is completed in Swoop Planner. Location creation and site surveying have a set of defined procedures and cross-checks to reduce the chance of total failure. All locations include a mandatory explicit description and location of obstacles within 2000m of the landing zone. These obstacles are then included in Swoop Planner as a 2D record for all future routes planned from that location. The sites must also be re-surveyed every 12 months to mitigate the risk of changes in obstacles.	Hazardous	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
6			Loss of Primary Means of Providing Function	All	Partial loss utilises redundancy to prevent undesirable outcomes; thus would need simultaneous failures to have a safety effect.	• See total loss	No Safety Effect	• Qualitative analysis
7			Misleading / Incorrect Information	All	Misleading or incorrect information could result in an erroneous route plan into an obstacle. This is ultimately akin to total loss of the function.	• See total loss	Hazardous	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures

	Function #	Function	Failure Condition Hazard Description	Phase	Effect of Failure Condition (Crew/RPA)	FHA Summary	Classification	Verification Requirements
8			Malfunction Without Warning	All	This is akin to total loss as a malfunction without warning could result in a route planned into an obstacle.	• See total loss	Hazardous	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
9	8.1.3	Terrain awareness	Total Loss of Function	All	A total failure of this system could, at worst, cause the aircraft to impact a ground obstacle such as a tree or building. This poses a very significant risk to the RPA but is unlikely to cause a fatality.	• Terrain separation is defined in the route validation in Swoop Planner. The planner validator compares the full containment volume of the planned route against SRTM terrain data. This dataset has been validated to be within 15m at all times, and thus with an absolute minimum terrain separation of 40m in the route planning rules, CFIT is not possible due to terrain awareness. • Routes cannot be approved with a forward flight segment lower than 80m AGL outside of R&D. Missions must account for possible maximum SRTM errors with sufficient battery overhead to avoid an adverse outcome. This is enforced procedurally and through software controls.	Hazardous	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
10			Loss of Primary Means of Providing Function	All	Partial loss utilises redundancy to prevent undesirable outcome thus would need simultaneous failures to have a safety effect.	• N/A	No Safety Effect	• Qualitative analysis
11			Misleading / Incorrect Information	All	Misleading or incorrect information could result in an erroneous route plan into terrain. This is ultimately akin to total loss of the function.	• See total loss	Hazardous	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures

	Function #	Function	Failure Condition Hazard Description	Phase	Effect of Failure Condition (Crew/RPA)	FHA Summary	Classification	Verification Requirements
12			Malfunction Without Warning	All	This is akin to total loss as a malfunction without warning could result in a route planned into terrain.	• See total loss	Hazardous	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
13	8.1.4	PRD area awareness	Total Loss of Function	All	This function is doubly redundant, however total failure could cause the pilot to command a worst case emergency landing (in the case of an NMAC), which is major in severity. The pilot workload may also increase due to the possible increase in air traffic.	• The route planner, route authoriser, and pilot are required to ensure the aircraft is flying within regulatory guidelines at all times. There is an explicit procedure for each person to understand the airspace being used.	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations
14			Loss of Primary Means of Providing Function	All	Partial loss utilises redundancy to prevent undesirable outcome thus would need simultaneous failures to have a safety effect.	• N/A	No Safety Effect	• Qualitative analysis
15			Misleading / Incorrect Information	All	Misleading information could cause the route to travel through a PRD area which could have an increased risk of the pilot commanding an inappropriate action. The worst case is emergency landing, which is major in severity.	• N/A	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations
16			Malfunction Without Warning	All	Malfunction without warning is equivalent to total loss of the function.	• See total loss.	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations

	Function #	Function	Failure Condition Hazard Description	Phase	Effect of Failure Condition (Crew/RPA)	FHA Summary	Classification	Verification Requirements
17	8.1.5	Controlled airspace awareness	Total Loss of Function	All	In the absolute worst case, flight into controlled airspace could increase the risk of MAC; however there are external events that would need to occur. It is reasonable to assume the worst case outcome is an emergency landing. The pilot workload may also increase due to the possible increase in air traffic.	• The route planner, route authoriser, and pilot are required to ensure the aircraft is flying within regulatory guidelines at all times. There is an explicit procedure for each person to understand the airspace being used.	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations
18			Loss of Primary Means of Providing Function	All	Partial loss utilises redundancy to prevent undesirable outcome thus would need simultaneous failures to have a safety effect.	• N/A	No Safety Effect	• Qualitative analysis
19			Misleading / Incorrect Information	All	Misleading information could cause the route to travel through controlled area which could have an increased risk of the pilot commanding an inappropriate action. The worst case is emergency landing, which is major in severity.	• N/A	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations
20			Malfunction Without Warning	All	Malfunction without warning is equivalent to total loss of the function.	• See total loss.	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations
21	8.2.1	Recharge consumables	Total Loss of Function	All	At worst, this would prevent flight due to a discharged battery. This has no safety impact.	• The aircraft monitors the battery remaining at all times during flight and will execute an automated closest base if the nearest base is projected to become unreachable due to battery life. If the battery life becomes extremely life, an alert is shown to the RP to execute an emergency landing.	No Safety Effect	• Qualitative analysis

	Function #	Function	Failure Condition Hazard Description	Phase	Effect of Failure Condition (Crew/RPA)	FHA Summary	Classification	Verification Requirements
22			Loss of Primary Means of Providing Function	All	Analogous to total loss	• See total loss	No Safety Effect	• Qualitative analysis
23			Misleading / Incorrect Information	All	At worst, this could result in the battery showing as charged on the charger but in reality not being charged. This could result in a reduced flight time and automated closest base. This increases pilot workload so is minor in severity.	• N/A	Minor	• Qualitative analysis • Review of technical and procedural mitigations
24			Malfunction Without Warning	All	Analogous to total loss	• See total loss	No Safety Effect	• Qualitative analysis
25	8.2.2	Preflight systems test	Total Loss of Function	All	A total loss of this function would prevent the aircraft arming due to not passing the preflight checks. This would slightly increase pilot workload.	• N/A	Minor	• Qualitative analysis • Review of technical and procedural mitigations
26			Loss of Primary Means of Providing Function	All	Analogous to the total loss.	• N/A	Minor	• Qualitative analysis • Review of technical and procedural mitigations
27			Misleading / Incorrect Information	All	The worst case outcome of misleading information would be an indication to the pilot that the preflight checks had passed, when in fact they had failed. The aircraft would abort the takeoff.	• N/A	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations

	Function #	Function	Failure Condition Hazard Description	Phase	Effect of Failure Condition (Crew/RPA)	FHA Summary	Classification	Verification Requirements
28			Malfunction Without Warning	All	The worst case of a malfunction without warning would be permitting flight without successfully passing the preflight checks. This could result in an emergency landing or aborted takeoff when the aircraft began the takeoff. This is major in severity.	• N/A	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations
29	8.2.3	Upload mission plan	Total Loss of Function	All	A failure to upload the mission plan could cause some operational nuisance and a slight increase in pilot workload. This is minor.	• N/A	Minor	• Qualitative analysis • Review of technical and procedural mitigations
30			Loss of Primary Means of Providing Function	All	There is only one method of uploading the mission plan.	• See total loss	No Safety Effect	• Qualitative analysis
31			Misleading / Incorrect Information	All	Misleading information could, at worst, result in the aircraft saying it had successfully loaded a route when in fact it had not. This has no impact.	• Route files are checked for corruption prior to being loaded on the RPA and allowing arming.	No Safety Effect	• Qualitative analysis
32			Malfunction Without Warning	All	A malfunction without warning could result in a slight increase in pilot workload as the RPA would not be able to arm.	• N/A	Minor	• Qualitative analysis • Review of technical and procedural mitigations

Table 2-8: Preflight Preparations Hazard Assessment

2.9 Manage Communications

2.9.1 Function Description

This function works alongside the manage datalink function to ensure the most appropriate connection method is used to communicate between the RPA and RP.

2.9.2 Hazard Assessment

	Function #	Function	Failure Condition Hazard Description	Phase	Effect of Failure Condition (Crew/RPA)	FHA Summary	Classification	Verification Requirements
1	9.0	Manage communications	Total Loss of Function	All	See sections 4.1.1 and 6.1	See sections 4.1.1 and 6.1	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
2			Loss of Primary Means of Providing Function	All	See sections 4.1.1 and 6.1	See sections 4.1.1 and 6.1	No Safety Effect	• Qualitative analysis
3			Misleading / Incorrect Information	All	See sections 4.1.1 and 6.1	See sections 4.1.1 and 6.1	Minor	• Qualitative analysis • Review of technical and procedural mitigations
4			Malfunction Without Warning	All	See sections 4.1.1 and 6.1	See sections 4.1.1 and 6.1	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures

Table 2-9: Communications Hazard Assessment

2.10 Collision Avoidance

2.10.1 Function Description

This function is responsible for monitoring nearby airspace for collision threats and executing automated actions as required to avoid a possible collision. This includes detecting traffic, calculating the track (and thus collision risk) of any detected traffic, and, if required, subsequently maintaining separation from traffic through an evasive maneuver.

This function relies primarily on the DAA hardware (ADS-B In as standard) for detecting and the onboard computer for relative track calculation and completion of the evasive manoeuvres.

2.10.2 Hazard Assessment

	Function #	Function	Failure Condition Hazard Description	Phase	Effect of Failure Condition (Crew/RPA)	FHA Summary	Classification	Verification Requirements
1	10.1	Detect traffic	Total Loss of Function	All	A total loss of the function could result in an undetected aircraft transiting through the same airspace as the RPA. The worst case outcome of this is a mid-air collision.	• Current Swoop Aero operations occur in regions with low encounter rates and airspace density. The risk of MAC or NMAC is strategically and tactically reduced using mitigations such as NOTAMs, stakeholder engagement, UTM/system feeds, and ADS-B, to form part of the holistic DAA solution. • The PingRx Pro is a COTS device that is tested extensively by the OEM.	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
2			Loss of Primary Means of Providing Function	All	Given the hardware used is not redundant, a loss of the primary means is analogous to total loss.	• See total loss	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
3			Misleading / Incorrect Information	All	Misleading information could cause the pilot to command an inappropriate action. The worst case is emergency landing, which is major in severity.	• N/A	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations

	Function #	Function	Failure Condition Hazard Description	Phase	Effect of Failure Condition (Crew/RPA)	FHA Summary	Classification	Verification Requirements
4			Malfunction Without Warning	All	Malfunction without warning could result in the aircraft failing to detect nearby traffic, which is the same as a total loss.	• See total loss	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
5	10.2	Determine traffic relative track	Total Loss of Function	All	A total loss (pilot and system failure) could result in a mid-air collision.	• DAA is based off the current known aircraft heading. It does not account for imminent manoeuvres. The onboard aircraft embedded system is the primary tool for determining aircraft traffic relative track. The pilot has full awareness of the position of airspace users detected thus pilot procedures are the secondary mitigation to command the aircraft as necessary.	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
6			Loss of Primary Means of Providing Function	All	The worst case outcome of a pilot needing to action an aircraft which has not successfully determined traffic relative track is a small increase in pilot workload and/or an emergency landing, which is major in severity. In this case, the pilot is able to simultaneously perform the same calculation that the aircraft is doing, and execute emergency landing if required.	• N/A	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations
7			Misleading / Incorrect Information	All	Misleading information could cause the aircraft or pilot to automate or command an inappropriate action. The worst case is emergency landing, which is major in severity.	• N/A	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations

	Function #	Function	Failure Condition Hazard Description	Phase	Effect of Failure Condition (Crew/RPA)	FHA Summary	Classification	Verification Requirements
8			Malfunction Without Warning	All	Analogous to the total loss.	• See total loss	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
9	10.3	Maintain traffic separation	Total Loss of Function	All	The aircraft's ability to maintain traffic separation is dependent on the above two rows in this table (Detect traffic & Determine traffic relative track) as well as the aircraft determining its own position. Total loss of function has the failure conditions of each of these individual functions therefore loss of any of these functions has the same failure condition.	• N/A	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
10			Loss of Primary Means of Providing Function	All	Given the sensors are not redundant, loss of primary means can be considered analogous to total loss.	• As above	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
11			Misleading / Incorrect Information	All	Misleading information could cause the pilot to command an inappropriate action. The worst case is emergency landing, which is major in severity.	• N/A	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations
12			Malfunction Without Warning	All	A malfunction of this system without warning is equivalent to the total loss of the function.	• See total loss	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures

	Function #	Function	Failure Condition Hazard Description	Phase	Effect of Failure Condition (Crew/RPA)	FHA Summary	Classification	Verification Requirements
13	10.4	Collision emergency evasion	Total Loss of Function	All	A total loss of the function could, at worst, result in a mid-air collision.	• Collision evasion failure conditions are considered sufficient when in alignment with the Air Risk Class TMPR Requirements. It may be that the 1309-esque failure rates are not achieved in all instances however this is solely related to detection, and not hardware reliability.	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
14			Loss of Primary Means of Providing Function	All	Given the emergency evasion is commanded from the compute core, a loss of this system is equivalent to the total loss of the function (as the RPA would be unable to execute any required DAA manoeuvres).	• See total loss	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
15			Misleading / Incorrect Information	All	Misleading information could cause the pilot to command an inappropriate action. At worst, this could result in a mid-air collision.	• See total loss	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures
16			Malfunction Without Warning	All	A malfunction without warning of this system could, at worst, be analogous to a total loss of the system. This is catastrophic.	• See total loss	Catastrophic	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures

	Function #	Function	Failure Condition Hazard Description	Phase	Effect of Failure Condition (Crew/RPA)	FHA Summary	Classification	Verification Requirements
17	10.5	Conspicuity to air traffic	Total Loss of Function	All	If the RPA is required to be conspicuous but is not broadcasting appropriately, other air traffic or ATC may not be aware of the RPA position. This is a hazardous outcome.	• The RPA, when equipped with ADS-B broadcasting, is capable of self-testing for broadcast health. In the case of failure of the ADS-B broadcast an alert is shown to the pilot and flight is blocked. • The broadcast module is a COTS product that is tested extensively by the OEM. • The aircraft has bright navigation lights for conspicuity to other airspace users.	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations
18			Loss of Primary Means of Providing Function	All	Given there is only one module, loss of the primary means is analogous to total loss. Loss of navigation lights is similar.	• See total loss	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations
19			Misleading / Incorrect Information	All	Misleading alerting to the pilot could result in an unnecessary pilot action.	• N/A	Major	• Qualitative analysis • Engineering analysis and review of technical and procedural mitigations
20			Malfunction Without Warning	All	If the RPA is required to be conspicuous but is not broadcasting appropriately, other air traffic or ATC may not be aware of the RPA position. This is a hazardous outcome.	• See total loss	Hazardous	• Qualitative analysis • Detailed engineering analysis and review of technical and procedural mitigations • Review of redundancy and system independence to ensure no common mode failures

Table 2-10: Collision Hazard Assessment

2.11 Flight Controller Failure

As noted at the beginning of the FHA, the Kite-B has one flight controller, and as such, failure of this hardware is a catastrophic outcome. Many other sensors are redundant (GNSS, Lidar, airspeed etc.); however, this redundancy does not provide additional safety benefits if there is a failure of the flight controller.

The flight controller hardware is a COTS product that has been extensively tested by the manufacturer. The software run on the flight controller has thousands of hours of safe flight time, and any changes to the flight controller software are cross-checked by a human and then tested in automated and manual simulation tests before proceeding to full-scale flight testing. Once the flight testing is completed, these changes can be rolled out to the operational RPA.

The flight controller is powered with redundant 5V power rails, such that the loss of one system (for example, due to battery failure) does not result in a loss of power to the FC.

3. FHA Diagram

Kite-B - Supplement - Systems Safety Assessment

3.1 RPAS Function Tree

The Function Tree below is the source for the functions outlined in the FHA above.

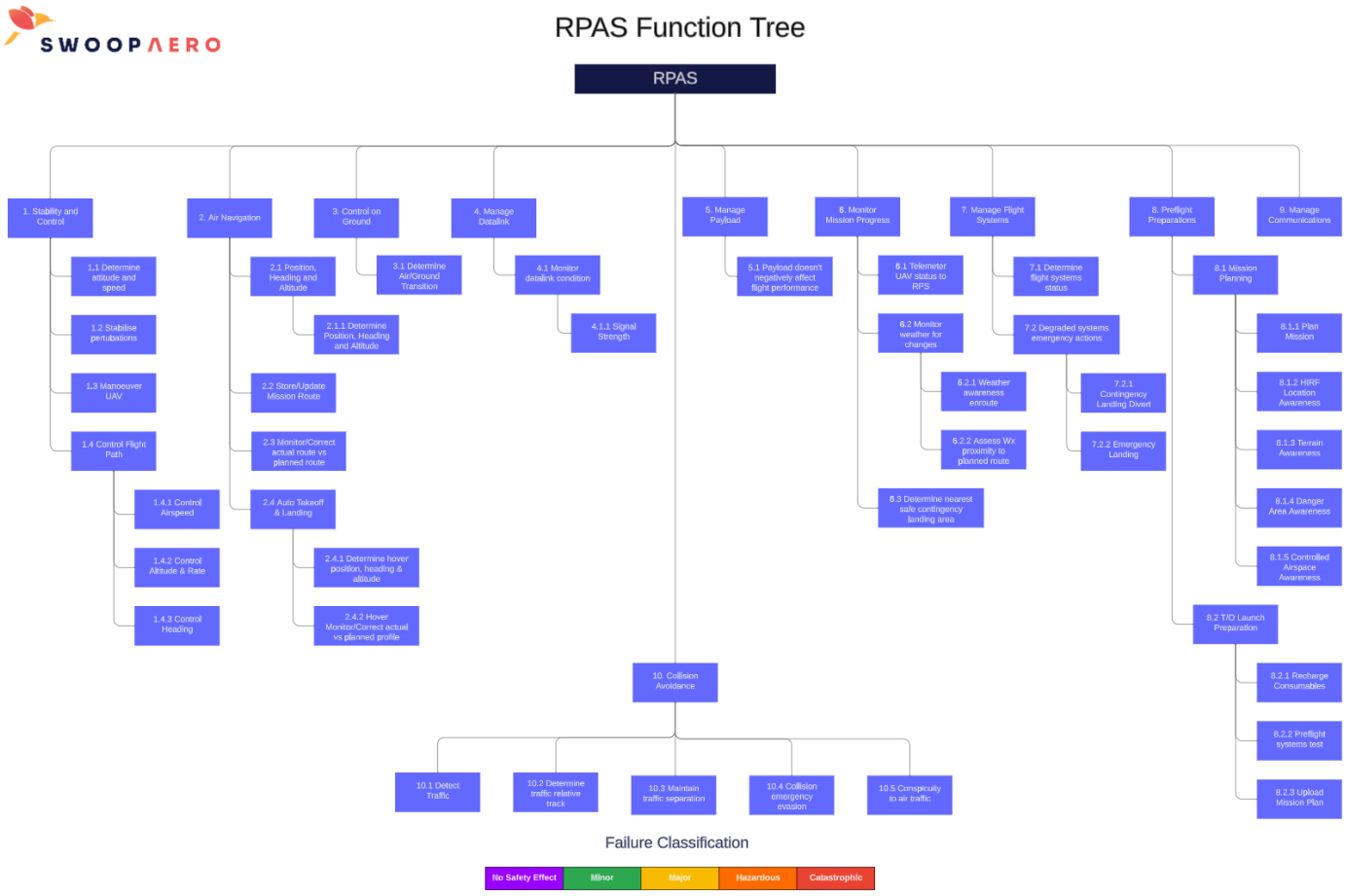

Figure 3-1: RPAS Function Tree

Appendices

Appendix 1 - Revision History

Version	Date	Summary		Author	Authorisation
1.1.0	02 Oct 2023		Response to CASA feedback	@ Aidan Biggar	@ Zac Kennedy
1.0.0	06 Jan 2023	N/A	N/A	@ Zac Kennedy	@ Zac Kennedy

Table A1-1: Revision History

Appendix 2 - Supporting Documentation

Reserved

SWOOPAERO

Port Melbourne, Australia

safety@swoop.aero