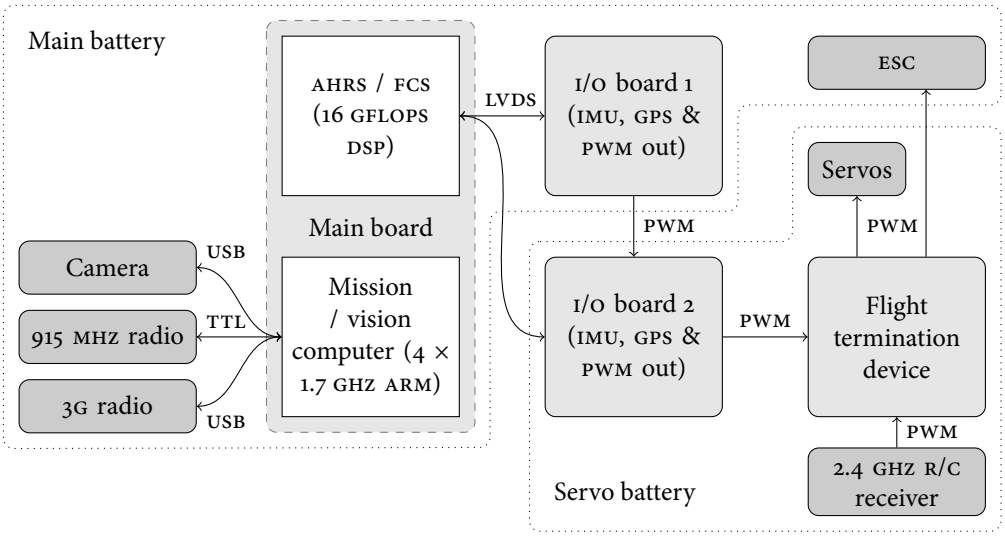
UAV Challenge – Outback Rescue 2014 – Search and Rescue Challenge

Deliverable 1: Technical Report & Risk Assessment

3rd August, 2013 / Prepared by Ben Dyer for [SFWA]

1 UAS design overview

- Skywalker X-8 flying wing airframe (2.1 m wingspan, 5 kg maximum take-off weight including 600 g *Search and Rescue Challenge* payload)
- On-board machine vision camera, image processing, target recognition and geo-referencing capability
- Expected 10 m geo-referencing error (95th percentile)
- Long-range 915–928 MHz and 3G data links
- Custom inertial measurement unit (IMU), attitude / heading reference system (AHRS) and flight control system (FCS) hardware
- Ground control station (GCS) based on BeagleBone Black GNU/Linux embedded computer with web interface
- Electromagnetic payload release system



Our team follows sound engineering practices drawn from the experience of our members in design and testing of hardware and firmware for embedded systems in safety-critical applications, as well as in the design and maintenance of medium-scale high-availability internet services.

Having reviewed reports by and about participants in previous years, it is apparent that while UAS technical capability appears to be have been sufficient to meet the *Search and Rescue Challenge* requirements for some time, hardware and software reliability remains a major obstacle. Thus, our main engineering objectives are improvements in worst-case performance, isolation of system faults, and simplification of overall system state management.

In support of this we have designed our IMU and AHRS / FCS hardware for maximum reliability, including individual overload protection on all major components and electrical isolation

between boards and between the flight electronics and servo/throttle control lines. We have verified correct operation of this system even while a short-circuit is applied to individual on-board components, as well as during repeated power-cycling and ±4 *g* vibration. Our IMUs incorporate high-resolution barometric pressure sensors referenced to current GCS pressure to avoid reliance on GPS altitude readings, which have proven to be unusuable during early testing.

Our software design has a similar focus on predictability and fault tolerance. The IMU firmware uses no interrupts for completely deterministic operation, and provides sensor updates every millisecond with less than 50 ns jitter even in the presence of I2C timeouts or complete sensor failure. Our AHRS uses a 22-state Scaled Unscented Kalman Filter (UKF) running at 1000 Hz, providing excellent handling of non-linearity and higher reliability than commonly-employed *ad hoc* approaches to sensor fusion. Flight control is based on a non-linear model predictive control approach, using a dynamics model of our UAV developed in X-Plane and verified experimentally. All communications between system components use 8-bit CRCs proven to detect up to four bit errors in the relevant packet sizes, and packet formatting is deterministic in space and time usage.

We are currently using the Skywalker X-8 airframe for development, and provided endurance testing is successful intend to use this airframe in the *Search and Rescue Challenge*. Key advantages of this airframe include the < 5 kg mass including payload, foam construction, and low cost. The relatively low mass reduces kinetic energy and therefore impact damage, while the foam provides some level of protection for the electronics. The low airframe cost enables us to test extensively and in a wider variety of conditions; in particular, full verification of the Loss of Data Link and Loss of GPS failure responses is required, as they are the only code paths not exercised during normal use.

2 Risk management

The fail-safe and flight termination requirements outlined in §§ 5.5–5.6 of the *Search and Rescue Challenge: Mission, rules and judging criteria [version 1.0]* (hereafter "*Rules*") are exceeded by our UAS. In accordance with the "*test like you fly*" principle, development and test flights involving autonomous control will be conducted with fail-safes and termination devices configured according to the outline below, with mission boundary and required waypoints set.

The devices involved in fail-safe system implementation are:

- Dual I/O boards, one powered from the main battery and one powered from the servo battery, which drive the electrically isolated servo PWM bus in a daisy-chain configuration;
- The flight control system, powered from the main battery, which is connected to both I/O boards via independent high-speed LVDS links;
- The termination device, which is connected between the I/O board daisy chain and the servos and ESC;
- A standard R/C receiver, which is connected to the termination device and may be used to assert manual control of the UAV if termination mode has not already been entered.

The system functions as follows:

- Our I/O hardware provides a PWM interface to control servos and throttle. We use two I/O boards, running from separate batteries and fully isolated from the PWM bus. Each I/O board is attached directly to a GPS module, and continuously monitors the raw GPS output to detect mission boundary crossings or loss of signal conditions. After the mission boundary is crossed, or 30 s after GPS signal is lost, the I/O board disables its PWM output.
- The I/O boards monitor the 1000 Hz heartbeat signal from the FCS; if longer than 10 ms has elapsed after the last hearbeat, the I/O board disables its PWM output.

- The FCS monitors the filtered position output from the UKF; if the horizontal or vertical position plus uncertainty in position crosses the mission boundary, the FCS ceases output of the heartbeat signal. If GPS signal is lost, the FCS enters LOSS OF GPS mode and attempts to loiter using dead reckoning for a period of 30 s, then ceases output of the heartbeat signal.
- The FCS monitors control surface and throttle response. If response deviates from the internal flight model by more than a certain amount (*e.g.* due to engine failure), the FCS ceases output of the heartbeat signal.
- The FCS monitors the telemetry and control link, which recieves 10 packets per second from the GCS. If the link is lost for longer than 10 s, the system enters LOSS OF DATA LINK mode. If LOSS OF GPS and LOSS OF DATA LINK modes are active simultaneously, the system ceases output of the heartbeat signal.
- The FCS ceases output of the heartbeat signal if an abort packet is received from the GCS (allowing for manual abort at any time).
- When an I/O board disables PWM output, it also disables its watchdog timer and enters an infinite loop; this mode holds until the I/O board is physically disconnected from power.
- The termination device powers off all other flight electronics while driving servo outputs and throttle to their minimum values if neither I/O board outputs a PWM pulse for 50 ms.
- If the termination device receives a manual override signal from the R/C receiver, and flight termination mode has not yet been entered, it powers off all other flight electronics and passes the R/C PWM signals through to the PWM bus.

In order to ensure flight termination systems and code paths are exercised as frequently as possible, the system will trigger termination at the conclusion of automated landing approaches, as a soft-disarm mechanism prior to power being physically disconnected.

Note that GCS lock-up (*Rules* § 5.5.7) is handled using the procedures for LOSS OF DATA LINK, as a GCS lock-up necessarily results in a loss of link due to heartbeat packets not being transmitted to the UAV.

3 Regulatory compliance

Our radio equipment is covered by ACMA class licences (*Radiocommunications (Low Interference Potential Devices) Class Licence 2000* Sch. 1 items 45 and 45A, and *Radiocommunications (Cellular Mobile Telecommunications Devices) Class Licence 2002*), so no additional licensing is required.

All flights are conducted in accordance with CASR Part 101, additionally following the guidance set out in CASA AC 101-3(0). Our local CASA office will be notified of our activities and forwarded copies of our *Search and Rescue Challenge* deliverables.

4 Insurance

Current development is covered by an Allianz home insurance policy (number 21-0034311-DHP) with a public liability limit of $20 million (not restricted or excluded for model aircraft, regardless of wingspan). A certificate of currency is available upon request. Injury to team members is covered by separate health insurance, life/TPD insurance and income protection insurance policies from Medibank Private, Australian Super, and the Commonwealth Bank.

Once the *Search and Rescue Challenge* 12-month insurance policy is made available, we will purchase that coverage in addition to our existing coverage.

5 Risk assessment

The following risks are rated with based on their expected frequency (in mean flight hours per occurrence) and expected severity of injury or property damage. The pre-mitigation frequency / severity rating is in the column labelled "F/S", and the post-mitigation rating is in the column labelled "Residual F/S". These frequency and severity ratings are based on MAAA MOP 022 § 9, and are detailed below.

Frequency

	Rating	Description
1	Very rare	Once per 10,000 + flight hours
2	Rare	Once per 1,000 flight hours (could be expected to occur once across all teams entering the *Search and Rescue Challenge*)
3	Infrequent	Once per 100 flight hours (could be expected to occur once per team in the *Search and Rescue Challenge*)
4	Frequent	Once per 10 flight hours
5	Very frequent	Once per flight hour

Severity

	Rating	Property damage	Injury
A	Very low	Less than $1,000	Minor cuts/bruises, no medical attention required
B	Low	Less than $10,000	Low-level medical treatment may be required (stitches, wound dressing); no long-term impact
C	Moderate	Less than $100,000	Hospital admission and in-patient treatment; risk of temporary disability or minor long-term disability
D	Severe	Less than $1,000,000	Extended hospital treatment; temporary disability and risk of moderate long-term disability
E	Extreme	$1,000,000 +	Death or permanent disability

5.1 UAV structure and control

Risk	Impact	F/S	Mitigation measures	Residual F/S
Servo failure	Loss of control	2/D	Test servos through full range prior to launch. FCS to detect condition and terminate flight. (CASR 101.395; *Rules* §§ 5.3, 5.6)	2/B
Motor failure	Loss of control	2/D	Test motor through full thrust range prior to launch. FCS to detect condition and terminate flight. (*Rules* §§ 5.3, 5.5.3)	2/B
Control surface detachment	Loss of control	2/D	Inspect control surfaces prior to launch, and after hard landings or other impact. Ensure tape hinges are fully attached, and tape not torn/punctured. FCS to detect condition and terminate flight. (CASR 101.395; *Rules* §§ 5.3, 5.6)	2/B
Wing detachment	Loss of control	1/D	Inspect wing attachment points prior to launch. FCS to detect condition and terminate flight. (CASR 101.395; *Rules* §§ 5.3, 5.6)	1/B

Risk	Impact	F/S	Mitigation measures	Residual F/S
Motor detachment	Loss of control	1/D	Inspect motor mount prior to launch, and after hard landings or other impact. Verify Loctite® on bolts remains intact. FCS to detect condition and terminate flight. (CASR 101.395; *Rules* § 5.6)	1/B
Propeller failure	Loss of control; injury from blade fragments	3/D	Inspect propeller prior to launch. Discard propeller if any cracks found, and after any hard landings or impact to propeller. (*Rules* § 5.3)	2/C
Unintended payload detachment	Injury / damage due to payload impact	3/D	Flight test with payload locked in place and release mechanism disabled. Only enable mechanism on specific payload drop tests under controlled conditions. Inspect and test release mechanism prior to launch. (CASR 101.090; *Rules* §§ 2.1.1, 2.1.3, 5.3)	1/D

5.2 UAS electronics

Risk	Impact	F/S	Mitigation measures	Residual F/S
Pitot failure	Reduction in accuracy of airspeed, α, β estimates; UAV controllability	2/C	Use dual pitot tubes. Check for blockage prior to launch. Calibrate periodically. Reduce manoeuvre load limit if airspeed error increases beyond acceptable bounds. (*Rules* § 5.6)	1/C
IMU failure	Loss of control	3/D	Use dual IMUs with results fused in AHRS. Ensure IMU power is overload protected, and isolate IMU inputs / outputs. Restart IMU if error detected. Terminate flight if both IMUs fail. (*Rules* § 5.6)	2/D
GPS failure	Reduction in lat / long and wind velocity estimate accuracy	5/A	Use dual GPS (different mfgrs). Weight GPS sensor covariance based on current PDOP and tracked SV count. Loss of GPS mode if both signals lost or out of tolerance for > 30 s. (*Rules* §§ 5.5.4, 5.6; *cf.* §§ 3.2, 3.3)	3/A
Radio link failure	Loss of manual controllability and monitoring, mission abort capability	3/D	Range test to ensure sufficient link margin available prior to launch. Monitor link margin during flight and adapt course if required. FCS firmware to enforce mission boundary, comms hold and home waypoints configuration for all flights. (*Rules* §§ 5.5.2, 5.5.5, 5.6)	2/B
PWM control failure	Loss of control	2/D	Flight termination device to activate within 60 ms. (*Rules* § 5.6)	2/B
Main battery failure	Loss of thrust and FCS	2/D	Flight termination device to activate within 60 ms. (*Rules* § 5.6)	2/B
Servo battery failure	Loss of control	2/D	Flight termination device to activate within 60 ms. (*Rules* § 5.6)	2/B
Rangefinder failure	Reduction in altitude accuracy during landing	2/A	None.	2/A
FCS failure	Loss of control	3/D	Flight termination device to activate within 60 ms. (*Rules* §§ 5.5.6, 5.6)	3/B
Mission computer failure	Loss of mission readiness	3/A	FCS to restart mission computer while proceeding to next waypoint.	3/A
GCS radio failure	Loss of data link	4/D	Activate Loss of Data Link mode within 10 s. Replace GCS with spare and terminate flight if link unrecoverable. (*Rules* §§ 5.5.2, 5.5.7)	2/B
GCS server failure	Loss of data link	3/A	Replace GCS with spare. (*Rules* § 5.5.7)	2/A

Risk	Impact	F/S	Mitigation measures	Residual F/S
GCS network failure	Loss of visual telemetry readout	3/A	Restart ground computers and GCS. Replace GCS with spare if necessary.	2/A
Battery fire	May spread to property or vegetation	2/E	Use more stable LiFePO4 batteries instead of LiPoly. Ensure no exposed metal near battery, and sufficient impact protection. Ensure Class ABE fire extinguisher available. Do not fly on elevated fire risk days (severe or above). (*Rules* § 5.17)	2/B

5.3 Human factors

Risk	Impact	F/S	Mitigation measures	Residual F/S
Contact with propeller	Severe cuts, loss of digits	3/C	Do not connect motor until immediately prior to launch. Ensure ISEA Level 5 cut / impact resistant glove worn. Ensure communication between team members and explicit confirmation of readiness prior to throttle up or launch. Ensure follow-through during hand launch.	2/B
Loss of concentration during R/C control	Loss of control	3/D	Ensure team roles clearly understood. Do not engage in other tasks during manual flight. Ensure fail-safes enabled during manual flight. (*Rules* § 5.2)	2/B
Set-up errors	Electrical damage, loss of control	4/A	Ensure all connectors are keyed. Enclose and permanently attach as many on-board systems as practical. Ensure servo and throttle operation is tested prior to launch.	2/A
Incorrect GCS configuration	Waypoints or mission boundary not enabled, unintended operation	3/D	FCS firmware to ensure UAV cannot be armed without mission boundary, comms hold and home waypoints configured. FCS firmware to enforce mission boundary within 10 km of current location; comms hold and home waypoints within 1 km. (*Rules* § 5.5.5)	1/D
Software configuration errors	Incorrect autopilot settings or modes used	4/D	Ensure autopilot settings are not user-accessible. Restrict autopilot modes as much as possible. Ensure fail-safes enabled regardless of mode.	3/B

5.4 External factors

Risk	Impact	F/S	Mitigation measures	Residual F/S
Wind	Loss of controllability in winds > 20 m/s	4/C	Check wind before flight and do not launch if > 10m/s. Abort mission if wind > 15m/s. (*Rules* § 2.4)	2/A
Rain	Damage to UAV electronics in moderate / heavy rain	3/B	Check weather before flight and do not launch in rain. Abort mission if light rain appears to be worsening. (*Rules* § 2.4)	2/A
Fog	Loss of visibility and control	3/D	Do not launch in fog. Abort mission if fog reduces visibility. (CASR 101.095, 101.385)	1/D
Other aircraft	Impact with aircraft	1/E	Do not fly in controlled airspace, near airfields, or near helipads. Abort mission if aircraft seen nearby. (CASR 101.055, 101.065–101.085, 101.400)	1/E