Safety Memo

Simone Duranti
Dept. of Computer and Information Science
Linköpings Universitet
SE-581 83 Linköping, SWEDEN

September 2007

General

Safety has been the primary concern throughout all research activities within the UAVTech group at Linköping University, since the early times in the middle 90-ies, when research activity was carried out in the frame of WITAS project [1]. Throughout the years the group has matured the capability to design, manufacture, maintain and operate a variety of UAV demonstrators, ranging from MicroUAVs in the "<1 kg" class up to the Yamaha RMAX Unmanned Helicopter (100 kg), for the operation of which the group has obtained a formal permit to fly released by the Swedish Airworthiness Authority (Luftfartsverket, [2]).

During all these years of intense design and flight test activity, we have NEVER incurred into mishaps that have led either to injuries to people or goods, or to flyaways of our unmanned platforms.

The safety philosophy that the pingWing development has been based on embodies:

- Design simplicity. Few moving parts, electric motor propulsion, mature technology battieries, etc.
- Manufacturing by skilled personnel. The *pingWing* has been manufactured by David Lundström, who is current Nordic Champion in model aerobatics (class F3A). Some parts have been manufactured by the University Workshop, and assembled by David.
- High quality components. The *pingwing* has been built with "top of the line" components (autopilot, servos, receiver, etc).
- Rigorous ground and flight testing prior to public exhibitions/competitions

The ground station is based on the well proven Horizon software, supplied by Micropilot. The safety area has been clearly marked on the moving map loaded into the ground station, to increase the situation awareness of the safety operator during the competition flight.

Notations

We introduce the following notations:

- N	Life time in amount of charge / discharge cycle
- e	Endurance (h)
- h	Cruise Altitude (m)
- L/D	Lift-to-Drag ratio
- ws	Wind speed (m/s)
- as	Air speed (m/s)

System properties

The vehicle

Name	*pingWing*
Weight	437 g (including paintball)
Wingspan	40,5 cm
Propulsion	1 Electric Brushless Motor
Endurance	30 minutes

Transmission systems

- 2.4 GHz Analog transmitter for the video downlink. (200 mW)
- 868 MHz Digital modem for uplink and downlink telemetry and data (250 mW)
- 72 MHz or 35 MHz RC transmitter for safety RC Link. (100mW).

Autopilot system overview

The *pingWing* is equiped with a Micropilot MP2028 autopilot board.
The board is sold to 350 customers in 51 countries, including NASA Ames Research Center, Goddard Space Flight Center, Jet Propulsion Laboratory, Wallops Flight Facility, Langley Research Center [3].

Due to large scale production, and to the maturity of this product having been on the market since several years, we believe that the level of reliability of the MP2028 is at least one order magnitude greater than any other prototypic autopilot board operated during the MAV07 outdoor competition.

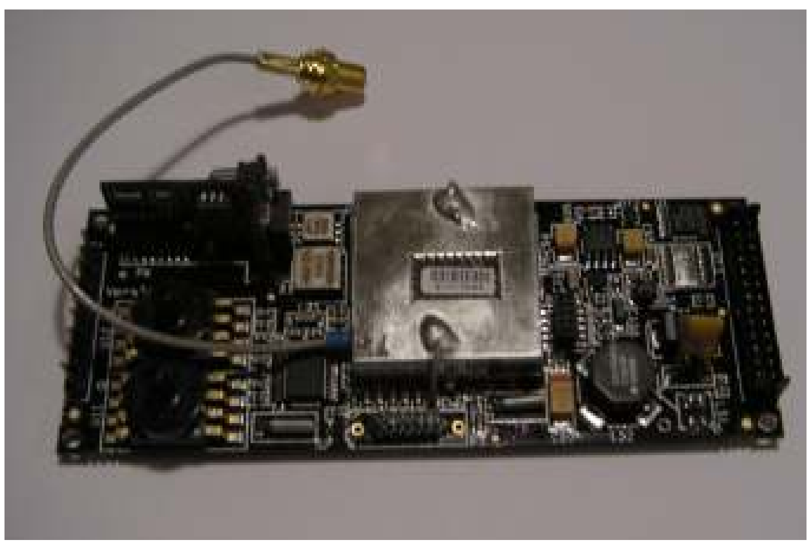


Figure 1 – The Micropilot MP2028 board

The board has following technical specifications:

CPU Motorola MC68332 32bit 16MHz

Sensors

- 3 axis accelerometer
- 3 axis rate gyro
- 2 pressure transducers (static/differential)
- 3 axis magnetometer
- 4hz GPS

We distinguished 3 non degenerated modes which can be selected with a button on the RC Link of the pilot:

1. Manual: Pilot (stick) commands are directly sent to servos, via RC link.
2. Auto1: Pilot commands go through attitude stabilization filters. If pilot doesn't send command the Micro Air Vehicle goes on a straight line ("arcade" mode according to Micropilot nomenclature).
3. Auto2: Pilot commands aren't sent. The Micro Air Vehicle follows a flight plan, which can be modified by moving waypoints on ground station (via datalink).

The MP2028 has been previously operated by our team on board the LinkMAV rotary wing MAV [4], and is currently operated on the fixed wing MAV *pingWing*. Over more than 250 flight hours we hadn't experienced any autopilot failure. We assume therefore that the probability of autopilot failure is less than 1 every 250 flight hours.

Flight Zone Computation

The safety area for the outdoor competition is defined by the coordinates given in Figure 2. The safety area has an approximate surface of 1.3 km^2.

Lat (deg)	Long (deg)
43.5389	1.2433
43.5425	1.2469
43.5447	1.2511
43.5447	1.2636
43.5358	1.2608
43.5328	1.2581

Figure 2 - Safety flight area

To simplify the computations we will assume in the following that (see Fig. 3):

1. The safety are is a 1.3 km square
2. The flight area is a 1.0 km square (conservative assumption).

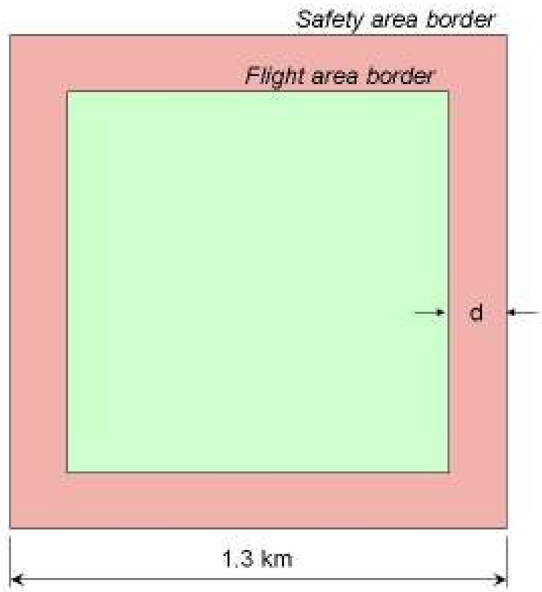
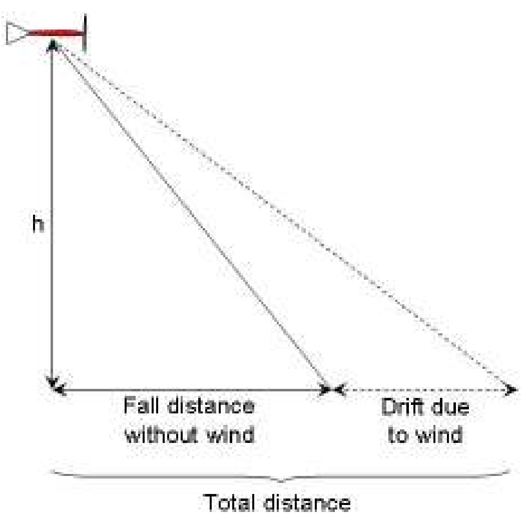


Figure 3 – Safety and Flight equivalent Area



$$d = L/D \cdot h + \frac{\sqrt{h^2 + (L/D \cdot h)^2}}{as} \cdot ws$$

Figure 4 – Fall distance

The *pingWing* cruise speed is around 15 m/s.

According to Competition Rules a worse case scenario of "wind gusting up to 10 m/s" is defined. We assume that the average wind corresponding to this scenario is 5 m/s, and we consider this averaged value for the following calculations.

Therefore we have a distance (see Figure 5):

d = 105 meters (flight altitude 50 m)

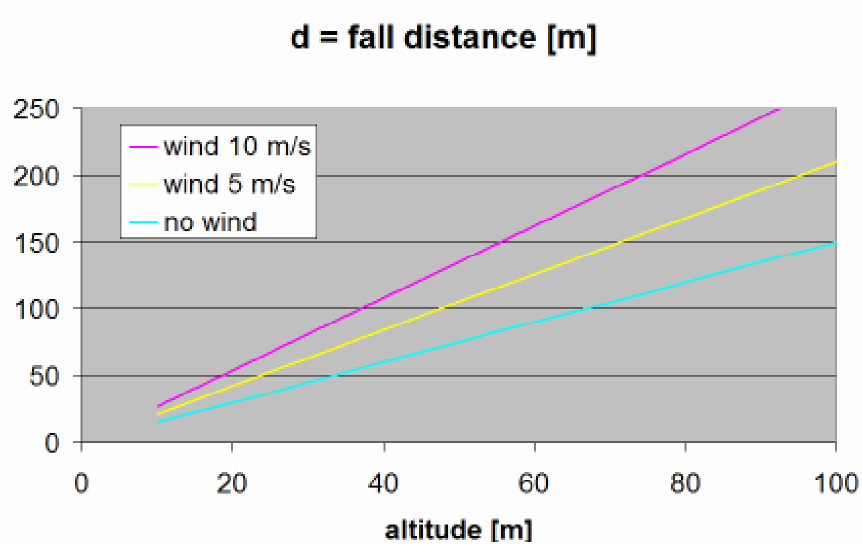


Figure 5 – Fall distance graph, as function of flight altitude and average wind speed

Probability to exit a given flight zone

To prevent Micro Air Vehicle from causing accidents we need to classify flight failure and provide maneuvers and failsafes to prevent these failures to be responsible for an accident. To do so a Micro Air Vehicle mustn't exit a given flight zone with the probability of 10^{-4} per flight hour.

We identify 3 major failure modes:

1. power supply failure, probability P(1)
2. GPS failure, probability P(2)
3. autopilot failure, probability P(3)

and we define the probability to exit a given flight zone as the sum of the probabilities of these three events:

$$P = P(1) + P(2) + P(3) < 8.94 \times 10{-}5 \text{ per hour} < 0.0001 \text{ per hour}$$

Being

$$P(1) = 7.4 \times 10{-}5 \text{ per hour}$$
$$P(2) = 3 \text{ x } 10\text{-}6$$
$$P(3) = 1.24 \times 10{-}5 \text{ per hour}$$

These latter values are derived in detail in the following paragraphs.

Power supply failure

A power supply failure will automatically and immediately cause a crash of the MAV, after a pseudo-ballistic trajectory with frozen control surfaces. We assume that the average L/D ratio during this phase is 1.5.

We define the following events, which are independent:

A Failure of the battery of the Micro Air Vehicle.
B The Micro Air Vehicle crash outside of the borders of the flight zone.

The Li-Po battery commonly used have a 3000 charge and discharge cycle, and provides a 0.5 hour endurance.

$$P(A) = \frac{1}{n \cdot e} = \frac{1}{3000 \cdot 0.5} = 6.7 \cdot 10^{-4} \text{ per hour}$$

$$d = L/D \cdot h + \frac{\sqrt{h^2 + (L/D \cdot h)^2}}{as} \cdot ws$$

$$P(B) = \frac{surface(strip\_within\_d\_to\_borders)}{surface(flight\_zone)} = \frac{d \cdot 1000}{1000^2} = \frac{d}{1000} = 0.105$$

P(A) × P(B) = 7.4 × 10−5 per hour

GPS failure

If the Micro Air Vehicle lose the GPS fix more than 2s, the only way to avoid the MAV to exit the flight zone is the safety RC link. If the RC link is also lost we shut down the throttle automatically to make it crash safely.

We consider the events:

A GPS signal failure
B RC link failure
C Micro Air Vehicle crash outside the flight zone

Based on previous flight experience (more than 250 flights of 20 minutes average since 2003 with the MP2028) we had no GPS fix failure during flight. We do a conservative assumption of typical GPS failure probability for similar autopilots estimated to:

$$P(A) = 7.5 \times 10{-}3 \text{ per hour}$$

Based on FFAM estimated figures of year 2006 of 5 accidents due to lost of RC link per year and per club with 737 clubs and 23692 members (50 h/yr/member) the probability of losing RC link can be estimated to:

$$P(B) = \frac{5 \cdot 737}{50 \cdot 23692} = 3.11 \cdot 10^{-3}$$

From previous section we have:

$$P(C) = 1.3 \times 10^{-1}$$

Therefore, as A, B, and C are independent events:

$$P(A \cap B \cap C) = P(A) \times P(B) \times P(C) = 3 \cdot 10^{-6}$$

Autopilot failure

If the autopilot fails (there are several failure modes) the only way to get the aircraft on the ground and inside the flight zone is to use the safety RC link. Let A = Autopilot fails and B = Lost RC link.

$$P(A) < 1/250 = 4 \times 10{-}3$$

$$P(B) = 3.11\ 10\text{-}3$$

$$P(A \cap B) = P(A) \times P(B) = 1.24 \cdot 10^{-5}$$

References

[1] P. Doherty. “Advanced research with autonomous unmanned aerial vehicles.” In Proc. Of the 9th International Conference on the Principles of Knowledge Representation and Reasoning, pages 731–732, June 2004.

[2] Godkännande av verksamhet med Obemannad Autonom luftfarkost (UAV hkp) för IDA Autonomous UAV Technologies group. UAV Tillstånd nr: Sv502. LS2005-0040, 2005-01-28

[3] http://www.micropilot.com/

[4] S. Duranti, G. Conte, D. Lundström, P. Rudol, M. Wzorek and P. Doherty LinkMAV, “LinkMAV, a Prototype Rotary Wing Micro Aerial Vehicle”, in Proceedings of the 17th IFAC Symposium on Automatic Control in Aerospace (ACA2007), 25 - 29 June 2007, Toulouse, France