Safety Memo

Pierre-Selim Huard
École Nationale de l'Aviation Civile
7 avenue Edouard Belin, 31055, Toulouse, France

September 2007

Safety has been the primary concern throughout all phases of the Paparazzi[2] system development. The ground station has been redesign to improve its efficiency and usability. We emphasise our work on the alert situations detection and display. The airborne code has been created with an emphasis on simplicity and robustness, and all critical code has been segregated in both software and hardware for error tolerance and recovery. The critical code has been thoroughly analyzed with the help of formal methods[1] and regenerated from a high level specification in Lustre, a declarative and synchronous programming language[3], taking into account the real-time constraints.

Notations

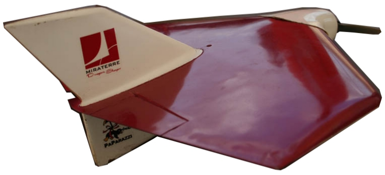
We introduce the following notations:

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)

1 System properties

The vehicle

Name	Mirateerre Dragonfly Slayer
Weight	300g
Wingspan	33cm
Propulsion	1 Electric Brushless Engine
Endurance	30 minutes



Transmission systems

- 2.4GHz analog transmitter for the video downlink. (50mW)
- Digital modem 868MHz for uplink and downlink telemetry and data (10mW)
- 72MHz RC transmitter for safety RC Link. (100mW).

Autopilot system overview

The system is equiped with Paparazzi Tiny board (see figure 1). It uses a integrated Ublox GPS reciever and 4 IR sensors for stabilisation and autonomous navigation.

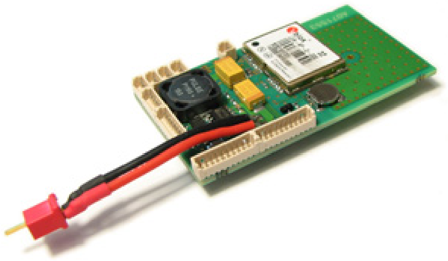


Figure 1: Paparazzi Tiny Board

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

1. Manual: Pilot commands are directly sent to flight commands.
2. Auto1: Pilot commands go through attitude stabilization filters. If pilot doesn't send command the Micro Air Vehicle goes on a straight line.
3. Auto2: Pilot commands aren't sent. The Micro Air Vehicle follows a flight plan.

2 Flight Zone Computation

The fall distance without wind is: $L/D \times h$
The fall duration is: $\frac{\sqrt{h^2+(L/D\times h)^2}}{as}$
The wind effect is: $\frac{\sqrt{h^2+(L/D\times h)^2}}{as} \times ws$
Therefore, we have (see figure 2):

$$d = L/D \times h + \frac{\sqrt{h^2+(L/D\times h)^2}}{as} \times ws \quad (1)$$

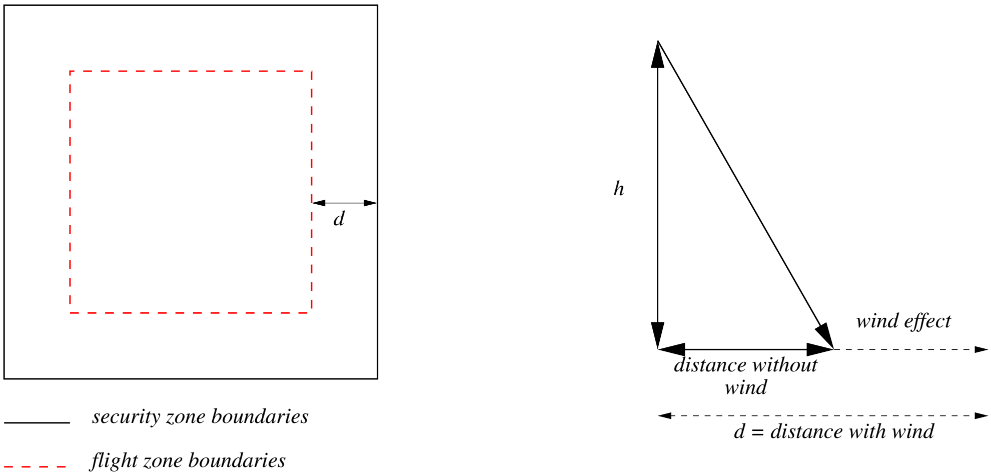


Figure 2: On the left: distance between the Security zone and the Flight zone. On the right: How the previous distance is computed

The Miraterre Dragonfly Slayer cruise speed is approximatively $20m/s$. At this speed the maximum Lift-to-Drag ratio is 1.1 with a nose-down attitude. In the worse case, we consider that the wind speed is $15m/s$. The Li-Po battery commonly used have a 3000 charge and discharge cycle, and provides a 0.5 hour endurance. Therefore we have a distance:

$$\boxed{\text{d=103 meters}}$$

3 Probability to exit a given flight zone

To prevent Micro Air Vehicle from causing accidents we need to classify flight failure and provide manoeuvers and failsafes to prevent this 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.

Power supply failure

A power supply failure will automatically and immediatly cause a crash of the MAV.

We define the following events, which are indepent:

A The battery of the Micro Air Vehicle is out of order.
B The Micro Air Vehicle crash outside of the borders of the flight zone.

$$\begin{aligned}
P(A) &= \frac{1}{n \times e} \\
&= 6.6 \times 10^{-4} \text{ per hour} \\
d &= L/D \times h + \frac{\sqrt{h^2 + (L/D \times h)^2}}{as} \times ws \\
&= 103 \text{ meters} \\
P(B) &= \frac{surface(\text{stripe within distance } d \text{ of the borders})}{surface(\text{flight zone})} \\
&= 0.125 \\
P(A) \cap B) &= P(A) \times P(B) \\
&= 8.3 \times 10^{-5} \text{ per hour}
\end{aligned}$$

To simplify the computation of the surface we considered that the flight zone was a 800 meters square.

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 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 400 flights of 20 minutes average since 2003) we had one GPS fix failure during a flight. Therefore, the typical GPS failure probability is estimated to:

$$P(A) = \frac{1}{400 \times \frac{20}{60}} = \frac{1}{120} = 7.5 \times 10^{-3} \text{ per hour}$$

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) we estimated the probability of losing RC link to:

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

From previous section we have:

$$P(C) = 1.25 \times 10^{-1}$$

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

$$P(A \cap B \cap C) = P(A) \times P(B) \times P(C) = 1.25 \times 10^{-6} \text{ per hour}$$

Autopilot failure

If the autopilot fails 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. Over more than 250 flight hours we hadn't experienced any autopilot failure, therefore:

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

We have:

$$P(A \cap B) = P(A) \times P(B) < 1.244 \times 10^{-5} \text{ per hour}$$

References

[1] Nicolas Albert. Certification du code embarqué d'un micro-drone. Master's thesis, University of Toulouse, 2005.

[2] P. Brisset, A. Drouin, M. Gorraz, P.-S. Huard, and J. Tyler. The Paparazzi solution. In *MAV2006*, Sandestin, Florida, November 2006.

[3] N. Halbwachs, P. Caspi, P. Raymond, and D. Pilaud. The synchronous data-flow programming language LUSTRE. *Proceedings of the IEEE*, 79(9):1305–1320, September 1991.