A TOTALLY NEW SPECTATOR EXPERIENCE

We are the best at what we do!
For the past two years, a group of technically skilled glider pilots have started to use traffic awareness data messages, sent by "anti-collision" devices, as received by ground stations.

Initially it was all about safety in and around traffic areas of airports whilst allowing for automated logbook keeping. Their success encouraged a group of the developers to take their program to an even higher level by relaying the decrypted position data over the Internet.

My club in Varese, Italy, uses a regular Flarm unit connected to a PC, in order to keep track of all aircraft movements, as required by the local law. This is one of the reasons why Flarm is compulsory equipment at our club. By the way, the club’s website shows a map of the airport traffic area where anyone can see all detected aircraft (and you can even listen to the radio chat, live).

Nice, or harsh, if you’re sitting at work or in bed with flu, depending on your mood! For me it’s a joy to see that there’s gliding activity even in less gorgeous days.

THE ENCRYPTION

The Flarm data transmission protocol is encrypted, but in 2008 it was cracked by a mysterious hacker who published a comprehensive document (a link in the Flarm Wikipedia leads to the text) and signed it with the serial numbers of his own wristwatch and of a GPS, so if someday he reveals himself, we can be sure it’s really him.

This document allowed the development of hardware devices which proved to be compatible with the Swiss traffic-awareness system.

By the way, let me declare my admiration for the simple concept and the effectiveness of the Flarm device.

I have no doubt that it has greatly helped reduce the number of in-flight collisions between gliders and against ground obstacles in the Alps (wires, antennas).

Above: A view of the <Live.Glidernet.org> page, when one clicks over the icon representing one particular aircraft. The menu in the right box shows as many details as possible about that TMG.
Collisions are rare, but the human implications are always dramatic to say the least, as they involve responsibilities towards other individuals, and their families as well. While I’m deeply grateful for this addition to the safety of gliding, I would have firmly preferred an “open” system as was the original declaration by the Swiss development group back in 2003. But more on this later.

**BEST RANGE**

Off-the-shelf hardware can be used to set up a receiver station, thanks to the decryption document and using a good antenna, a USB broadcast television receiver, a small processing module like a Raspberry Pi or similar (Banana Pi, Cubieboard 2, Odroid U3, or simply a partition on a PC).

In the best conditions, a reception range of Flarm devices is 100 km which has been achieved. Impressive! The data can then be sent to a server on the Internet, which makes it visible for anyone as it is superimposed over a world map.

As I’m writing, I’m in a house in Germany, the sky is grey and foggy, but on http://live.glidernet.org I can see a Super Dimona spiralling up the Engelberg mountain at 2,900 metres in Switzerland. Its signal is being received by a ground station in Interlaken, some 50 km away.

At the same time, a Twin Astir is lazily maintaining altitude in Scotland in a weak “one-knotter”.

As I click on the aircraft’s own icon, a small window opens with all the details the owner has indicated and authorised when setting the preferences of his Flarm device. They range from a maximum of indetermination, to specific details such as registration marks, make and model, even the name of the pilot.

Lacking basic info, the website assigns a casual set of characters. More and more aircraft have a Flarm onboard in Europe, especially in Germany with the whole Alpine territory, including helicopters and
You may want to make your own experiments, or follow the available set of instructions published by the Open Glider.

### SOFTWARE AND DATA

You can easily find the Open Glider Network group of developers. Some of them are also working on a small compatible transmitter as a side project, with the aim of producing an open-source "tracking system" for gliders. They explicitly declare that they are not willing to provide an alternative anti-collision device. A lot of opportunities may be traced, especially if they haven't taken any care about what can be broadcast. For example, it took me less than a minute to identify the motorglider over the Engelberg as a Super Dimona, and to find in Google the official base airport and the name of the owner. So, if you care about privacy, select "no" to the "send Flarm ID menu" and registration in your device settings.

Imagine if you made up an excuse with your boss to go gliding on a beautiful day, and he catches you having fun in the Alps at 3,000 metres. Alleged airspace incursions might also be detected, but a lawyer would demonstrate (at a cost!) that a non-certified data source can't be proof enough for a guilty sentence. Nevertheless, please respect airspace rules, as from them comes the future of our sport. Already too many lobbies are working to segregate VFR flights in restricted areas.

### LET'S BUILD

You may want to make your own experiments, or follow the available set of instructions published by the Open Glider. All this spreading of information comes with an impact. Anyone can observe Flarm traffics (or ADS-b traffics on similar websites) where some ground stations have been connected to the Internet. Flarmnet already offers a database of devices, so the pilots should be aware that they can be traced, especially if they haven't taken any care about what can be broadcast. For example, it took me less than a minute to identify the motorglider over the Engelberg as a Super Dimona, and to find in Google the official base airport and the name of the owner. So, if you care about privacy, select "no" to the "send Flarm ID menu" and registration in your device settings.

Imagine if you made up an excuse with your boss to go gliding on a beautiful day, and he catches you having fun in the Alps at 3,000 metres. Alleged airspace incursions might also be detected, but a lawyer would demonstrate (at a cost!) that a non-certified data source can't be proof enough for a guilty sentence. Nevertheless, please respect airspace rules, as from them comes the future of our sport. Already too many lobbies are working to segregate VFR flights in restricted areas.

Third, the antenna. The small standard DVB-t antenna will be good for the first ground tests, but will have a limited range. There are two better alternatives: a Ground-plane antenna (a very common type for amateur radio) with a preamplifier, and the Collinear antenna design. The latter looks like a long plastic tube, inside of which are a series of skilfully cut and soldered pieces of coaxial cable of precise dimensions. If you have an interest about this antenna, please have a look at the ARRL Antenna Book, page 248 (online at: http://bit.do/TgXW).

Flarm units, when operated in Europe, use the 868 MHz band, which is licence-free for small airplanes on file.

**BIG BROTHER**

All this spreading of information comes with an impact. Anyone can observe Flarm traffics (or ADS-b traffics on similar websites) where some ground stations have been connected to the Internet. Flarmnet already offers a database of devices, so the pilots should be aware that they can be traced, especially if they haven't taken any care about what can be broadcast. For example, it took me less than a minute to identify the motorglider over the Engelberg as a Super Dimona, and to find in Google the official base airport and the name of the owner. So, if you care about privacy, select "no" to the "send Flarm ID menu" and registration in your device settings.

Imagine if you made up an excuse with your boss to go gliding on a beautiful day, and he catches you having fun in the Alps at 3,000 metres. Alleged airspace incursions might also be detected, but a lawyer would demonstrate (at a cost!) that a non-certified data source can't be proof enough for a guilty sentence. Nevertheless, please respect airspace rules, as from them comes the future of our sport. Already too many lobbies are working to segregate VFR flights in restricted areas.

**LET'S BUILD**

You may want to make your own experiments, or follow the available set of instructions published by the Open Glider.
Power devices like remote controls and intruder alarms. TV accessories work at very similar frequencies, so there’s plenty to choose from in terms of amplifiers and receivers. A good collinear antenna perfectly matched for Flarm application in the 868 band can be ordered from a Chinese workshop through Alibaba: http://bit.do/TgW3

Fourth, comes installation. The ideal location has a complete view of the sky in the desired direction, without tall concrete buildings and trees at least a dozen meters away. Top of a hill, if you can provide power, connection and service would be best. During a lightning storm, the antenna should be disconnected from the receiver, or at least this should be unplugged from the power source. Don’t make a “ground” connection, or the antenna will work very well as a lighting rod.

CONCLUSION

Flarm has announced the 6th version of the firmware for their devices. Update is mandatory by the end of March 2015 as the older v5 will stop working. This has happened in the past, as programmed and clearly stated by the factory “in the interest of implementing the best possible effectiveness”. There are differences, though. This time, the press-releases introduce a new worldwide tracking system based on Flarm’s servers, which is described as allowing to preserve the full rights to the pilots’ privacy. The server will allow the development of a Flarm proprietary tracking system for clubs and communities, while permitting also easy access to data for Search and Rescue operations. It’s easy to understand that, in order to allow all this, the transmitted data will be encrypted with a new code.

The small Atmel processor installed in Flarm devices can’t support the very high calculation properties necessary for a very strong encryption, but nevertheless some experts have identified some tricks which, if adopted by Flarm, might make an independent decryption very time consuming, in the region of many weeks or months of hard work.

This is to say that all this nice Gildernet traffic service may shortly fall into the control of the Flarm factory.

Whether the firm will be able to immediately provide a similar service, or we may have to wait some time, I don’t have a clue. The OGN tracking system might as well continue on its original path, separating from the Flarm legacy.

Whatever, we’ll see.
Progress is good and nobody can stop it.

Aldo Cernezezi