System Design and Compatibility

FLARM® is an affordable traffic alert and collision avoidance system for General Aviation. FLARM devices have been credited on many occasions with preventing collisions, resolving dangerous situations, and increasing situation awareness. FLARM is the most widespread alternative to expensive ACAS/TCAS systems found in commercial airliners.

FLARM is based on cooperative exchange of digital data through radio communication, similar to ADS-B. Devices measure position and predict the aircraft's trajectory. This is broadcast using a digital, encrypted radio channel. Devices in other nearby aircraft receive the data and compare it to their own predicted trajectory to assess the risk of a collision. If a dangerous situation is detected, an alert is issued in both aircraft so the situation can be resolved by the pilots.

The first FLARM devices were sold in 2004 through a crowd-funding initiative; they still operate today. Nearly 30'000 FLARM-compatible devices are now in use globally. FLARM has been hugely successful due to its simplicity, high functionality, and low price, all of which helped to kick-start the project and attain the critical mass needed. Consequently FLARM won the OSTIV prize 'for great contribution to safety', the FAI Worlds Air Sports Federation prize for 'Technical Advances in Sporting Aviation', the Flieger Magazin Innovation Award, the Aerosuisse Award and the Aerokurier Innovation Award.

The technology is extensively licensed to other manufacturers, thus the FLARM population today is very diverse: FLARM-compatible devices are used in gliders, powered airplanes, helicopters, military aircraft, hang-gliders, paragliders, r/c aircraft, and drones. There are currently nine independent manufacturers offering FLARM-compatible products for a wide range of applications. The majority of FLARM-compatible devices currently sold come from these manufacturers, competing with FLARM's own end-user products.

Due to the cooperative exchange of data amongst the devices, compatibility is critical: each device needs to speak the same language in order to be interpreted correctly. Innovation and improvements must happen while retaining full compatibility of the complete population at all times. The FLARM Licensing Framework is readily available to manufacturers and addresses this and other relevant issues. The following sections describe the FLARM Licensing Framework and the considerations leading to its design.

Licensing and Compatibility

Several layers of technical specifications must be considered to establish compatibility:

i. *Physical layer and radio protocol*: How is information encoded into bits and bytes? When and how often is it sent? How to avoid radio packet collisions, i.e. two devices sending at the same time?

ii. *Semantics of data*: What does the data mean? For instance, how is altitude encoded (above WGS-84 ellipsoid or AMSL, pressure or GNSS), what position encoding precision and ambiguity is required, how are the aircraft types defined, or how are ID's assigned?

iii. *Behavior layer*: How is the data to be processed and filtered? When is an alert to be issued? How does Stealth Mode work? What defines a valid configuration file? How are errors defined and shown to the user?

Any compatible device must implement all layers. While the physical layer is relatively easy to describe and implement, the semantics and behavioral layers are large and complex. To offer a Licensing Framework for manufacturers while ensuring full compatibility, two models are possible:

- *Compatibility by design*: All products use the same base electronic design and the same software, with only minor variations. Compatibility is inherent, since the specification is in the software code and the hardware design. Testing is only required across one design, for each update.
- *Compatibility by standards and certification*: The specification layers are precisely described in an extensive standards document. Manufacturers develop their own devices and software by reading, interpreting, and implementing the standards document. A certification procedure is developed with which conformance of the hardware and software to the standard is tested, verified, and published, all by a trusted and independent party. Thorough testing is essential to attain the reliability required in a safety system, for each update.

The first model is more efficient for small volumes whereas the latter is the typical choice for products selling in the millions. Creating robust standards documents, test and certification procedures and establishing trusted bodies is exceedingly costly, particularly for safety systems, but may pay off with increasing economies of scale.

FLARM has adopted the *compatibility by design* model since it believes it is the best solution for all stakeholders given the size and needs of the market. In the FLARM Licensing Framework, introduced in 2005, manufacturers may design their own hardware according to the FLARM specification. The software is delivered in binary form and is functionally identical for all device types except for some low-level hardware-specific adaptations. Since 2014, a complete ready-to-use OEM hardware module is also available, reducing development cost and increasing system performance consistency.

The following sections discuss technical and organizational challenges that were relevant for the choice of the FLARM Licensing Framework.

Technical Challenges for Compatibility

Particularly, the following aspects must be considered in depth:

- Each device has to act consistently and symmetrically. This requires the algorithms for motion prediction and collision risk assessment to be identical on all devices. Just comparing positions would lead to a lot of unnecessary alerts and rule out some important use cases where aircraft operate in close proximity intentionally, such as gliders in thermals. It also ensures all devices transmit and receive.
- Sensors and the processing of sensor data (such as filtering) needs to be consistent and good enough on all devices. Specifically in highly dynamic environments typical for aircraft the processing and filtering of sensor data has a large impact on the overall performance of the system.
- The radio bands FLARM uses can inherently become crowded. The bandwidth available to each device must thus be allocated in a fair, cooperative manner such that the system scales nicely and delivers critical information when it is needed.
- In some cases, a pilot may want to reduce the level of information that is available to other pilots about his own aircraft, e.g. to not give away tactical information during a competition (Stealth Mode option) or to avoid large-scale, ground-based tracking (No Track option). To ensure the traffic alert functionality the broadcasted data cannot be deteriorated; such restrictions have to be implemented in the receivers.
- Rules and regulations for RF emission compliance are diverse across the globe: only specific frequencies and transmit modes (e.g. frequency hopping) are legal to use, different in each region.

All of above is adequately addressed in the FLARM Licensing Framework: *Compatibility by design* ensures consistent behavior for all device types, adhering to rules and regulations where applicable. In addition, it gives valuable access to intellectual property such as patents, trademarks and brands.

Maintenance and Updates

Two conflicting drivers must be considered for maintaining a large distributed system: Innovation and stability. Innovation is needed to adapt to changes in the environment and implement new functionality. Stability is required for consistent performance and uninterrupted reliability of the entire population. FLARM's capabilities have been continuously extended in the past decade, also beyond traffic alert and collision avoidance. For instance, a novel skydiver and r/c aircraft solution, a framework to encode wind information to improve collision warnings, the no-track option, and various performance improvements – some to the benefit of ground-based receivers – were released in version 6 in 2015. Secure flight recording and fixed obstacle alerts were added years before. Enhancements like these add to the value of FLARM for every user yet require a software update of the entire population of devices. This allows functionality far beyond what other ADS-B implementations such as 1090ES can offer.

An update of the physical, semantical, or behavioral layers of FLARM consequently requires the coordination of all parties, manufacturers and pilots alike. Consensus on system updates is automatically established with the FLARM model by embedding expiration dates into the software for all device types and requiring periodic updates, as done in 2005, 2006, 2008, 2011, and 2015. This leads to a synchronized update process for all devices and manufacturers. Many useful features can be added with each update.

The first FLARM device was sold in 2004. Its microcontroller is less powerful than that of a modern PowerFLARM device, yet the two device families are still fully compatible. Maintaining software for old devices is challenging, time-consuming, and expensive. Nevertheless, FLARM remains committed to do so.

Privacy and Security

The data any FLARM-compatible device broadcasts is inherently sensitive: The identification and accurate position information may be used to identify and track an aircraft and thus its crew over time and in a large area. Only a few ground-based receiver stations are needed to collect huge sets of data. For example during a gliding competition, signals from distant aircraft disclose the location and strength of thermals giving a tactical advantage for trailing aircraft. Users may consequently choose to not disclose this information. The FLARM-compatible device must respect this by protecting data without impacting the main safety functions. The rules for this must be strict and symmetrical for all devices. The Licensing Framework ensures that the rules are obeyed.

Encryption of the radio protocol is a consequence of the requirements for privacy and security and was thus introduced nearly a decade ago: It protects the system from abuse but also from rogue devices implementing the protocol and system incorrectly or incompletely. The latter may have serious consequences for users of proper devices since incorrect data may lead to undefined behavior on the receiver end. The encryption applied is an industrial-strength symmetric cipher, fast enough to be run on all devices with no performance degradation. Since decryption or interception of encrypted communication is illegal in most countries, this also ensures the integrity of the system beyond the technical barriers. Furthermore, the encryption can be enhanced with software updates if security is compromised.

Conclusion

Since the launch of FLARM over a decade ago, the open ecosystem with many suppliers offering diverse, innovative products has been instrumental to its success. The FLARM Licensing Framework was fundamental to the instant and broad success of this technology: Based on *compatibility by design*, it is both efficient and economically sustainable, as demonstrated by the vast offering of compatible devices available and continuous enhancements of the technology.

As with every distributed system, compatibility is not trivial and details are important in the domains of technology, maintenance, and privacy/security. The FLARM Licensing Framework addresses these issues optimally, to the best interest of those who care the most: us pilots.