Do drones need a “front door”?

Sky Hopper UAVs on multiple unit mission in rural area

A door to secure flights

We hear a lot about “back doors” in communications firmware; entry points for elicit or state-sponsored access to data that should normally be private. This debate is also relevant to the world of both low mass “drones” and larger UAV systems.

The recent attacks on oil assets in Saudi Arabia by unknown players suggests that the need to “do something” has become more acute. Commentators are recognising that there is a “dark side” to the future here. See: https://thebulletin.org/2019/10/the-dark-side-of-our-drone-future/

None of this is news to the authorities; the CAA and FAA have been enlightened but increasingly cautious about what open-source digital location software and autonomous mission capabilities acting together could lead to when used in aerial platforms in the hands of bad people.

Those in the Sky Hopper project, where we are building our electronics demonstrator and enabling its firmware, are acutely conscious of our responsibilities if we bring higher mass capabilities to market. We can do a lot of damage.

Respecting the rules

Constraint measures are well established in the certified aerospace world, but if we are targeting exports to markets where property rights and the law are less respected, we need to get real about those responsibilities in our less regulated domain. And even in the UK, we know that entities like Extinction Rebellion have a mind-set that appears to disregard expected behaviours.

There is also a commercial opportunity here. Sorting out drone safety plays into the strengths of our institutions; compliance, audit, self-regulation, civil adminstration and legal contracting are good earners for the UK worldwide.

As usual with technical matters, however, governments and politicians are essentially useless at rational discretionary decision making; they tend to over-egg restraint through precautionary excess, favour rent-seeking larger players in the market as first movers; then invent complex policy and destroy innovation and economic advance as a result. General rules of good law and economics get replaced by tortuous regulations in poorly drafted legislation. The bad guys then ignore or avoid the intended outcomes.

Another layer in the control cake

One possible way forward is for the industry to accept that any drone needs a "front door" that the industry itself adopts as a ruling without which no flight can take place.

What would this front door be? Well, in communications technology we always have the same layer cake of hardware, firmware, data handling and data communications. Any door is likely to involve, to some extent, all of these. While raw data can always be seen, compiled firmware within a hardware processor, particularly if the latter includes the requirement of sourcing from a third party supplier is likely to offer some sort of initial lock. Add to that encrypted protocols again made accessible only through a separated supply chain and you begin to get towards a potential solution.

There are precedents here. In internet shopping solutions the PCI-DSS standards have cleaned out a great deal of fraud; hardware dongles and other encrypted licence codes provide security across the communications software business. HTTPS secure certificates are now the norm for IP data.

The real issue is the institutional wrapper through which these technical solutions can be provided. These need to define compliance in such a way that it does not impose a huge burden on innovative smaller players. As explained above, it is the wider industry rather than big players or the government that needs to lead here. The government could be limited to a generalised statue requiring secure compliance; stating that there has to be a wall between the door provider and the drone supplier, but not the shape or kind of door.

Separating controller from control

What the industry needs to do is organise the front door supplier(s) and keep them separated from the fliers. Organisations like the RAeS or others could help police the separation, with NATS and the CAA providing consulting expertise. Insurers would be a lot happier if they too were involved.

If this separation is achieved, a question arises as to who owns the front door, or doors. Once again, one wants to leave levels of innovation in the use of the door to developers. For example, in our Sky Hopper mid-mass industrial UAV platform our engineers have worked out a way that they believe offers real-time monitoring of cargoes and instrumentation. Anyone swapping these for a few loose grenades would be interdicted by no-fly measures, or even a take-off followed by auto re-routing to a secure compound. Triggering those interdictions would be instigated by the presence of the door with its compliance envelope, but not be part of the door itself.

We think there are measures that could be mandated that are no more expensive or onerous than some auto-industry safety regulations. Pre-flight mission logging compliance, in-flight mission progress checking, and separate-mode communications control between in-cruise flight and near-field operations that involves shared handshakes. Again, the issue is whether an open skies approach as in G-class airspace is ever going to be viable. We think not, take the pilot away and you not only remove the cognition and logic of control, you remove the moral presence that understands the value of human life. It's probably not ethical to allow any BVLOS UAV operations without secure oversight based on the well-honed ethics of safety that imbue the aerospace industry.

So, perhaps we all need to lay down the challenge – how do we design a front door for the UAV universe that allows the industry to develop worldwide in safety and with advantage to the UK?

Eben Wilson, MA Hons Econ – Project Leader, Sky Hopper (www.skyhopper.co.uk)