On-Board Safety Monitoring for Drones



Nick Tudor discusses some of the issues which have to be resolved before we see routine on-demand, commercially viable fully autonomous drone operations in our skies. He provides an overview of the regulations, their current means of compliance, and proposes an approach to help unblock the technical challenges being experienced in the industry.

There are a number of reasons why Unmanned Air Systems (UAS), Unmanned Air Vehicles (UAVs), Remotely Piloted Air Systems (RPAS), or 'drones', have yet to really deliver the vision of autonomous flight. Apart from the multiple labels for the same thing[1] , these range from legal and technological to regulatory and there have been numerous false starts. This paper will describe and touch on some of the issues which have to be resolved in order to enable on-demand, commercially viable fully autonomous operations. The focus of this article, however, is on a proposed approach to the resolution of some of the technological issues that could then lead to changes in the law that, in turn, might enable a change in regulatory policy and possibly affect insurance premiums for drone operations.

The Three Questions

While many in the autonomous systems world focus on capabilities, when it comes to engineering a solution (and from a regulatory perspective) showing what it does is only one part of the three-question set that have to be satisfactorily answered.

[1] Some might say that a UAV is only the aircraft, some might say that there has to be a 'pilot' and hence RPAS, some might say that there has to be a ground station and hence UAS; they're all correct to a greater or lesser degree, so it's not really a useful difference except perhaps in perception by different groups of people.

The questions are:

- What will it do?
- Can we give assurance that it won't do the things we don't want it to do?
- Can we describe what happens, when [not 'if'] things go wrong?

Largely it is accepted that developers can do the functions that they claim, otherwise they wouldn't be in the business in the first place. It is therefore relatively easy to answer the first question: what does it do? Most developers, however, do not focus on the other two questions. While current systems require a human to supervise autonomous operations, a human operator is limited in what they can do by the design of the vehicle, its ground system and the specifics of the environment in which the actual task is being conducted.

International Civil Aviation Organization (ICAO)

Role

Internationally, the driving agency for regulations is the International Civil Aviation Organization (ICAO). It is a United Nations specialised agency set up originally as a result of the Convention on International Civil Aviation (also known as Chicago Convention), that was signed on 7 December 1944 by 52 States.

While it is implicitly part of the ICAO Business Plan 23-25, there is only one specific mention of unmanned aircraft and that is in the message from the Secretary General. However, there is an annual ICAO Remotely Piloted Aircraft Systems Symposium/Drone Enable Symposium that seek to understand the latest developments and thinking in uncrewed aviation. There is also an ICAO RPAS Panel (RPASP), which includes representatives from the UK.

Safety

Managing and improving the safety of the global air transport system is ICAO's guiding and most fundamental Strategic Objective. One of the major initiatives of ICAO is the 'No Country Left Behind' initiative. This is to try to assist member States with implementation of globally harmonized, safe practices; this will apply to autonomous systems. Within aerospace, safety can largely be split into two broad topic areas: the airspace and the aircraft.

Airspace

Views on what the future holds vary significantly. Some think there will only be a small increase in the amount of air traffic by the introduction of uncrewed vehicles, restricted to niche use cases in remote areas. Others, however, think there will be a massive increase, including over dense population centres.

In remote areas, even with small numbers, there are significant impacts on existing air users and, particularly if there is a larger increase in numbers, the fundamental principles of Air Traffic Management (ATM) are being challenged. This is why there are significant initiatives on Unmanned Traffic Management (UTM). The thinking is that UAS are different and have to be treated differently, but they still have to be integrated into existing ATM as other air users need to be aware and be able to react to advice and direction from ground-based services – as well as using information from other aircraft, such as conspicuity devices. Simply segregating airspace for the sole use of UAS is not tenable in the medium term but is currently the only accepted approach for trials.

'Ground Control to Major Tom'[2]

While there are grand proposals, plans and in some cases, actual trials for lots of likely very expensive ground-based systems that purport to provide the safety backstop for the aircraft, ultimately, the decision for what the aircraft will actually do must reside with the aircraft. When, (not 'if') the communications fail, there is not a lot a now 'not-in-control' controller can do. They may be able to alert the authorities to the possibility of a vehicle being out of that person's control, but where it will be and what it's going to do is entirely in the gift of the aircraft; Major Tom is off on his own!

"When, (not 'if') the communications fail, there is not a lot a now 'not-in-control' controller can do"

Airworthiness of Aircraft

Developed by ICAO are the Standards and Recommended Practices (SARPS) contained in the nineteen Technical Annexes to the Convention on International Civil Aviation are applied universally and produce a high degree of technical uniformity.

Airworthiness

Airworthiness is the measure of an aircraft's suitability for safe flight. Certification of airworthiness is initially conferred by a certificate of airworthiness from a national aviation authority, and is maintained by performing the required maintenance actions. The application of airworthiness defines the condition of an aircraft and supplies the basis for judgment of the suitability for flight of that aircraft, in that it has been designed with engineering rigour, constructed, maintained and is expected to be operated to approved standards and limitations, by competent and approved individuals, who are acting as members of an approved organisation and whose work is both certified as correct and accepted on behalf of the State.

It is for each State to ensure that their aircraft have a certificate of airworthiness and that these certificates are recognised as valid by other states. For large aircraft (such as an Airbus or Boeing), within Europe there is Certification Specification 25 and similar documents have been developed for helicopters, smaller aircraft, gliders, etc, but until recently, there has been no guidance on and no equivalent for UAS; with Europe there now is JARUS CS-LUAS and EASA CS-LUAS.

Acceptable Loss

Flying aircraft presents a number of hazards which, through the design process of the aircraft, are expected to be mitigated in some way. There is a limit to what can be achieved to design, build and maintain an aircraft, so the approach is based upon the probability of a failure and the impact of that failure on the ability of the aircraft to continue to be operated. Loss of an aircraft/life is a defined as 'Catastrophic' and per aircraft Type (eg Airbus A320); this has been agreed to be $1x10^{-6}$, or one in a million flying hours as the overall hull loss

[2] This reference is to a David Bowie's 1969 song "Space Oddity". The lyrics tell the story of an astronaut named Major Tom who is informed by Ground Control that a malfunction has occurred in his spacecraft; but the astronaut does not get the message.

accident rate for an individual aircraft. An aircraft is built from various equipment, systems and installations and all are assessed to determine their contribution to safety. Figure 1 is a diagram that outlines the probability vs severity of failure principle of aircraft components and is used as part of the design process in order to mitigate hazards.

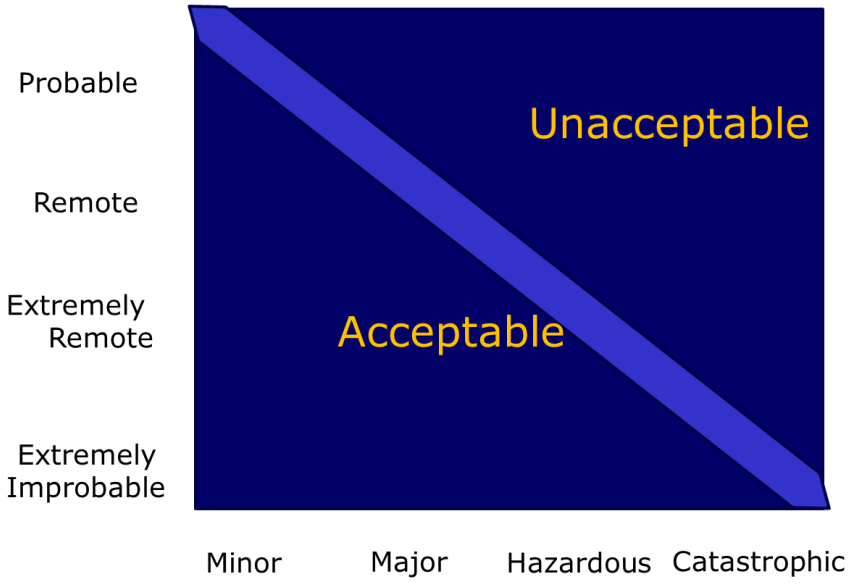


Figure 1 - Probability vs Severity

This is encapsulated in CS-25.1309 where not only must all components perform their intended functions in foreseeable operating conditions, but also that:

"The aeroplane systems and associated components, considered separately and in relation to other systems, must be designed so that -

(1) Any **catastrophic** failure condition

(i) is **extremely improbable**; and

(ii) does not result from a single failure; and

(2) Any **hazardous** failure condition is **extremely remote**; and

(3) Any **major** failure condition is **remote**.

Information concerning unsafe system operating conditions must be provided to the crew to enable them to take appropriate corrective action."

Extremely Improbable Failure Conditions for systems are those having an Average Probability Per Flight Hour of the order of $1x10^{-9}$ or less[3].

[3] This is the contribution per failure condition to the overall aircraft loss rate. More details on how this is calculated can be found at AMC 25.1309.

European Union Aviation Safey Agency (EASA) has issued Special Condition RPAS.1309 [1], which applies to any RPAS:

- for which a type certification is requested,
- for which the kinetic energy assessment in accordance with section 6 of the EASA policy E.Y013-01 results in an initial certification basis according to CS-VLA or CS-VLR, and
- with no occupant on board.

For this instantiation of paragraph 1309, it uses almost exactly the same wording in CS25.1309 for the treatment of likelihood and impact and hence acceptable loss (see Figure 1).

New EASA Policy – SAIL V and SAIL VI

The CAA has tended to mirror EASA policy since Brexit, which is why this new policy is interesting from a market perspective. There are three categories of UAS under the EASA approach to RPAS authorisation: Open (broadly light, very short range, Visual Line of Sight, etc ...), Specific (broadly getting heavier, Beyond Visual Line of Sight (BVLOS), operating closer to larger groups of people, etc..) and Certified (broadly: everything else). EASA have recently published "MOC Light-UAS High Risk.2510-01" [2] which apply to the upper end of the Specific category. This is targeted at UAS that are likely to be heavier, will be BVLOS and closer to people. The objective of Light-UAS.2510 is to ensure an acceptable safety level for equipment and systems as installed as part of the UAS. The safety objectives for each failure condition are reproduced from para 8.1 Safety Objectives per SAIL(Specific Assurance and Integrity Level) in the following table:

	Failure Condition Classification		
	Major	Hazardous	Catastrophic
	Allowable Qualitative Probability		
	Remote	Extremely Remote	Extremely Improbable
	Allowable Quantitative Probability and Functional Development Assurance Level (FDAL)		
SAIL VI	$\leq 10^{-4}$ FDAL D	$\leq 10^{-6}$ FDAL C	$\leq 10^{-8}$ FDAL B
SAIL V	$\leq 10^{-4}$ FDAL D	$\leq 10^{-5}$ FDAL C	$\leq 10^{-7}$ FDAL B

In the notes for this table, EASA make it clear that the quantitative safety objectives are expressed per flight hour and that an average flight profile (including the duration of flight phases) and an average flight duration should be defined. Furthermore, in a recognition that the drone industry does not use the same components/systems that might be used for manned aviation, it states that: "*component failure rate data may not be precise enough to enable accurate estimates of the probabilities of failure conditions.*" The resultant uncertainty must therefore be safely accounted for when calculating the estimated probability of each failure condition. There is quite a lot of guidance in the document which is a significant

enhancement on previous UAS.1309, especially as this now effectively requires use of ARP4754B/4761A and DO-178C for SAIL V/VI aircraft and changes the allowable quantitative probability numbers to be more stringent than previously defined.

The UK

The Civil Aviation Authority (CAA) provides the regulatory services for RPAS in the UK. The major problem all authorities have to deal with is how to authorise on-demand use of fully autonomous capable aircraft. While airspace can be segregated, Transponder Mandatory Zone (TMZ) and the like may provide at least a partial solution with conspicuity and even 'detect-and-avoid' systems being required on board aircraft, there still remains the question over trust: what will these aircraft actually do?

The Answer is On-Board

The decision for what the aircraft will actually do must reside with the aircraft. This is the case for manned aviation and the pilot is responsible for the safety of the aircraft (and passengers). While, for example, Air Traffic Control may direct a pilot to do something, ultimately the decision as to whether to comply resides with the pilot . However, there needs to be assurance that whatever the aircraft is going to do in the apparently wide plethora of possible circumstances, it will always behave as another air-user would expect it to behave.

"The decision for what the aircraft will actually do must reside with the aircraft."

DO-178C Section 2.4.3

Fortunately, DO-178C[4] has at least partially solved the issue of dealing with untrusted functionality (eg AI[5]). At section 2.4.3, Safety Monitoring, "...is a means of protecting against specific failure conditions by directly monitoring a function for failures that would result in a failure condition. Monitoring functions may be implemented in hardware, software, or a combination of hardware and software." The approach is to provide an independent safety monitor that covers the ability to detect system faults at the required integrity level.

Systems Architecture

The systems architecture has to be developed to defend against failure and inaccuracies in sensors; otherwise from the point of view of the software, it's garbage in, garbage out. As noted earlier, many of the systems and material used in UAS are not of manned aviation standards, so failures are more likely. Figure 2 is an overview of a possible systems architecture. Sensors have to cover the spectrum, there has to be sufficient redundancy and this includes off-board data systems such as GPS as well as monitoring on-board systems health. The safety monitor cannot simply block actions, it has to provide an alternative, safe action. This aspect takes a considerable amount of thought and this behaviour has to be accessibly described so that all stakeholders can understand. Although the UAS components may be

[4] The section reference and wording has not changed since the issue of DO-178B in 1992.

[5] Artificial Intelligence (AI) has its place; it is not in safety critical systems without a safety monitor. Indeed, the approach we have in civil aerospace is typically no single point of failure, so why rely upon something that can only ever be around, maybe 95% confident?

built using commodity components, a monitor assured to a manned aircraft standards keeping eye on proceedings provides sufficient protection against failures. However, developing to aviation standards is generally considered expensive and time-consuming.

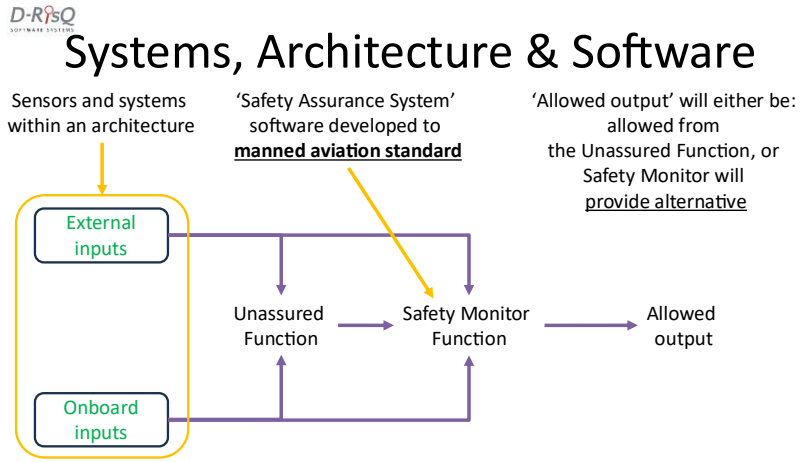


Figure 2 – Safety Monitoring High Level Architecture Overview

Software Development Processes

It is often thought that, in order to develop software to meet aerospace standards, one needs deep pockets. However, the D-RisQ tools have been shown to be highly productive and can dramatically reduce such costs [3]. The software development process is pretty much as usual with the exception that standards compliance includes DO-333, the Formal Methods Supplement to DO-178C. The tools in the process are outlined in Figure 3.

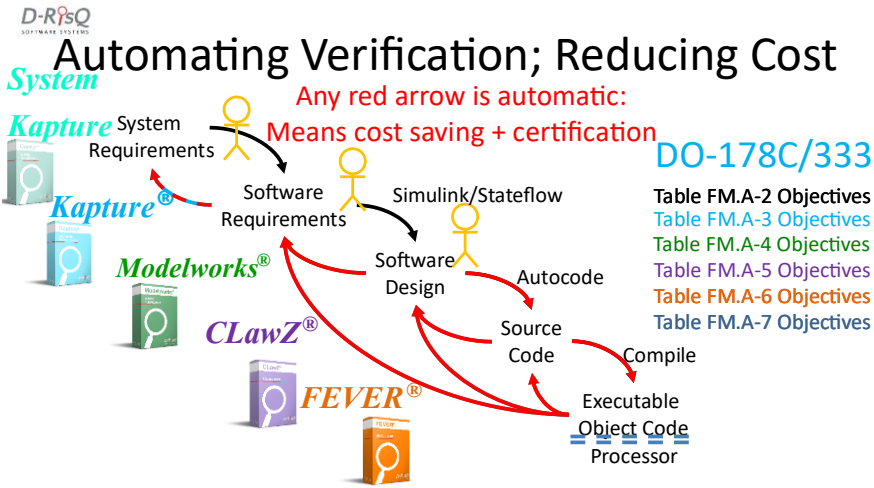


Figure 3 - The D-RisQ Tools in Software Development and Verification

Where is this Happening?



The Digital Tethering project spearheaded by Drone Major Group for Network Rail [4] is exploiting this approach. It has independent safety assurance software developed by D-RisQ with processes designed to meet DO-333. The described behaviour of the aircraft vested in that software assumes that, at some point, the operator will lose communications, have on-board failures, etc and hence we have to build a safety argument that allows safe operation; we have to be able to satisfactorily answer the three questions. All the principles outlined in this article have been implemented and exploits novel navigation and communications systems with redundancy built in, but if things go wrong, the software will continue to behave as described in order to keep the aircraft safe. For example, should the flight control system take the aircraft off track, it will intervene; should one of the navigation systems be insufficiently accurate, the battery be low, the communications be interrupted, etc, the software system will safely intervene.

Conclusion

If the approach for an independent, highly assured safety monitoring system outlined in this article becomes accepted, then there is a potential basis for accepting that drones, in air, land and sea, may be able to operate unsupervised. This supposes that software can be adequately trusted, can be developed at an affordable price and that the many other aspects of systems reliability can also be tackled. This might then provide an impetus to change the law and develop suitable regulation with the resultant impact on insurance premiums for operators and developers alike.

References

[1] EASA, https://www.easa.europa.eu/sites/default/files/dfu/SC-RPAS.1309-01_Iss02.pdf

[2] EASA, https://www.easa.europa.eu/en/document-library/product-certification-consultations/light-uas-2510-01-sail-v-and-vi

[3] D-RisQ, https://www.drisq.com/case-study-steam-boiler-exemplar

[4] Network Rail, https://www.networkrailmediacentre.co.uk/news/network-rail-trials-revolutionary-approach-to-aerial-operations-with-british-drone-companies, accessed April 2025

Image attribution:
ICAO logo: public domain
All other images copyright © Nick Tudor

Nick Tudor, D-RisQ



Following a full career as an RAF Officer Engineer, Nick has been working in software and high integrity systems for the past two decades. As co-Founder of D-RisQ, he has worked in multiple sectors including aerospace, defence, automotive, rail, autonomous systems in air, land, sea, nuclear decommissioning and cyber-security. Perhaps the only claim to fame he might have is as one of the key authors of DO-333, the Formal Methods Supplement to DO-178C (the aerospace software standard).