Position Paper

On European Aviation Safety Agency's
'Prototype' Commission Regulation on Unmanned Aircraft Operations

2016-10-12

Federal Association
for Information Technology,
Telecommunications and
New Media

Marc Bachmann
Head of Aviation and Defense
P +49 30 27576-102
m.bachmann@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Thorsten Dirks

CEO
Dr. Bernhard Rohleder

Bitkom represents more than 2,300 companies in the digital sector, including 1,500 direct members. With more than 700,000 employees, our members generate a domestic turnover of 140 billion Euros a year, exporting high-tech goods and services worth another 50 billion Euros. Comprising 1,000 small and medium-sized businesses as well as 300 start-ups and nearly all global players, Bitkom' members offer a wide range of software technologies, IT-services, and telecommunications or internet services. They produce hardware and consumer electronics or operate in the sectors of digital media and the network industry. 78 percent of the companies' head-quarters are located in Germany with an additional amount of 9 percent in other countries of the EU and 9 percent in the USA as well as 4 percent in other regions. Bitkom supports an innovative economic policy by focusing the modernization of the education sector and a future-oriented network policy.

General Remarks

The general concept of introducing risk- and performance based regulation, as introduced at the Riga Conference and through the European institutions' work with UAS is not easy to recognize in the "open category".
EASA's current proposal calls for four different sets of product requirements, training needs and performance limitations - all for drones weighing below 2 kg, while drones between 2 kg and 25 kg are subject to one set of rules. This appears to be an artificial categorization.

Risk is the sum of consequence and probability. It appears EASA has only taken consequence as a factor when using AIS as a determining factor for drone categories. Probability of incidents in the open category – where a safety distance to people and property is required – is very low. The lack of any grave incidents within the current frameworks around Europe also point in the direction of probability for incidents being very low.

EASA is suggesting to implement:

- Product requirements (performance limitations),
- Registration of operators,
- Mandatory geofencing and UTM in certain areas
- Electronic Identification
- Training of Drone pilots
- Assessment of drones

for even small drones operated for recreational purposes in rural areas. These requirements all seek to fulfil the same objective: ensure safe operations.
Of course, measures should be taken to do this, but implementing all of the above to an industry that is operating very safely is over-regulation.

On the use of AIS: It appears that there are large discrepancies between EASA and FAA's use of AIS as well as the interpretation of the different steps on the scale. We would strongly encourage EASA to ensure that the same understanding is applied on both side of the Atlantic.

Detailed Remarks

Articles 4.4 and 4.5
We support the use of geofencing. In the light of the desire to create a harmonized set of rules for Europe, the open mandate given to Member States to define prohibited or restricted areas is worrying as this could well lead to great discrepancies among Member States.

Article 5.2
The use of subcategories is welcomed, as there are clearly different risks associated with drones of weights between 0 and 25kg. However, the proposed categorization based on AIS seems to create many categories for low weight drones – in all operational scenarios. The principle of using AIS to categorise flights with a defined minimum standard to people seems conflicting as measures have already been taken to keep drones from exposing people to danger.

Article 7.1
Further clarification on safety critical service is desired, as well as an exact clarification between liability of manufacturers, data providers and drone pilots.
Additional information need to be provided what kind of evaluation or certification by what competent authority or lab is requested to comply with the rules.
Currently the best established mechanism for certification of security products is through the Common Criteria (CC, ISO/IEC 15408). It has been implemented in many EU Member States and other countries and benefits from a dedicated European mutual recognition agreement, the SOG-IS MRA.

Article 9.1(a)

For insurance reasons additional information need to be provided about how the documents need to signed/encrypted that those can be proven as being valid.

Article 9.1(h)

For insurance reasons data integrity shall be initiated by the authority that the operator can use this data for insurance reasons ('geofencing data has been received correctly right before the planned flight')

Proposed new text:
"...approve, restrict or prohibit airspace areas or define special zones, and make this information available ***based on secure communication and signed data.****"*

Article 11.1

A further clarification of the process would be desirable as to ensure that industry can weigh in.
To avoid manipulation of UA the Basic Regulation shall define minimum requirements for security and privacy of UA (like the seat belt for cars).

A UAV Trust Label might mark the proper (evaluated) implementation of such requirements.

Article 12

For this to be operational, regard should be given to the sizes and shapes of said areas. Small drones can have limited software performance that will make EU-wide geofencing with a broad variety of shapes very difficult to implement.

EASA should at least produce a long list of areas to be geofenced which Member States can then adhere to. Further, EASA must ensure that geo-data is delivered in a uniform format, including sizes and shapes of prohibited and restricted areas.

Article 12.1(b)

Additional information need to be provided what kind of evaluation or certification by what competent certification authority is requested to comply with the rules of UA robustness.

Article 13.1

UA shall comply with safety AND security regulations. Consequently security requirements for UA need be setup.

Proposed new text:
"EASA and the competent authorities shall collect, analyse and disseminate safety ***and security*** *information concerning UA operations in their territory in accordance with the Basic Regulation and its Commission acts.*

Article 14.3
It does appear optimistic that all consumers will have updated their products by then. Further, it will be very difficult to enforce this requirement.

UAS.OPEN.70 (b)
(applicable to categories A0 and A1 as well)

Altitude limitation is well below what is seen in all EU Member States today as well as what is seen in other areas of the world.

Safety records of drones already flying do not point to altitude being a major issue, as there is limited air traffic in these heights outside airport (which should be geofenced).

UAS.OPEN.80 (c)
These training requirements seem to be too rigorous that they can be fulfilled through any other means than traditional classroom training. This will be an impediment to the positive use of drones and limit the market potential for drones.

UAS. SPEC.90
Proposed new text:

"Where required in the operational authorisation, the operator shall ensure that, as a minimum, records of completion of preflight or postflight checks, time in service, and of defects and repairs with regard to the UAS are retained in the form of a logbook, or equivalent. ***The logbook shall be treated like personal data according to the GDPR****."*

UAS. SPEC.100
Additional information need to be provided what kind of evaluation or certification by what competent certification authority is requested to comply with the **rules related to security.**

UAS.LUC.20 (b)
As safety requirements are not sufficient in a connected UA. Like in other connected IoT devices security also needs to be taken into account seriously. The security manager shall take the responsibility to avoid manipulation of the UA, data theft, data integrity, etc.. He might ask third party experts for support.

Proposed new text:
"The LUC holder shall appoint a safety manager and a ***security manager****."*

UAS.LUC.20 (c)

As safety requirements are not sufficient in a connected UA (IoT device) security also need to be taken into account. The security board shall take the responsibility to avoid manipulation of the UA, data theft, data integrity, etc.

Proposed new text:
"For organisations having a workforce of more than 20 full-time equivalents (FTEs) involved in the UA operations and maintenance, a safety board ***and a security board*** *shall be established."*

UAS.LUC.30 (c)

Additional information need to be provided what kind of evaluation or certification by what competent certification authority is requested to comply with the rules.

Proposed new text:
"Records shall be stored in a manner ***using state-of-the-art security features*** *that ensures protection from unauthorised access, damage, alteration and theft."*

Appendix I.3 a-b and Appendix I.4 a-b

No drone manufacturer of drones this size has height limitation that is accurate towards ground level – therefore any limit in this respect will be practically impossible to adhere to.

Based on drone operations until now there is no benefit or evidence pointing towards a 50m limit, why it appears to be an overly conservative height.

Appendix I.6.a

We strongly encourage EASA to keep focus on the operators role in connection with drone operations. This article seems to be shifting much responsibility towards manufacturers and other service providers. We believe it is vital to keep the pilot as the deciding factor for any flight, as technology is not yet mature enough to ensure this safely.

Appendix I.6.c

Electronic Identification should be defined in a broader sense as there are many possible solutions, but only very limited what is actually functional at this stage.

Appendix I.6.d

This is a legal requirement for a technology that is not even developed yet! Several UTM initiatives are under development around the world, but prescribing this by law is not the way to ensure innovation and development. The potential harm from introducing such systems should be carefully considered, as they may outweigh potential gains.
In line with geofencing requirements it is vital that EASA will play a role in where such systems can made mandatory.