Submission 87 – uAvionix Australia

Response to"Remote Identification (Remote ID) Discussion Paper June 2023

uAvionix Australia welcomes the opportunity to provide comment on the Remote ID paper.

1. General Comments

a) The discussion surrounding remote ID does not make clear the problem to be addressed. Rather it notes a system which exists and discusses how it could be used.

b) The nature of the proposed devices proposes particular problems :

i. The FAA standard use F3411 defines the purpose as follows : "The objective is to increase UAS remote **pilot accountability by removing anonymity** ……" – the uses proposed in the discussion paper take the proposed use much much further which we don't think appropriate.

ii. The FAA standard ASTM F3411 further says : "This specification is applicable to UAS that **operate at very low level (VLL) airspace**" meaning below 500 feet. The discussion paper does not make this clear and whether in Australia you propose limiting to below 500 feet.

iii. BRID : Is very limited range and using unprotected frequencies not suitable for safety of life applications

iv. NRID : Acceptable range from fixed sites may be possible but is unusable for air-air use without involvement of 3rd party systems which would require demanding aviation standards of reliability, latency, availability

v. NRID : Not available in the majority of airspace countrywide especially at lower levels when obstructed by terrain.

vi. Use of satellite communication from devices will destroy the cost/benefit argument. The satellite frequency band would need to be "weather proof" – bringing larger antennas and larger transmission power.

vii. Positional data of these devices does not have any effective integrity checks (like used in ADS-B) and latency and reliability requirements are a concern.

viii. Appendix 3 makes it clear that it is not suitable for DAA, with which we concur

2. Comments on Applications of Remode ID:

The following provides our response to the potential uses of Remote ID

a) Helping track illegal or noncompliant drone use and report potentially suspicious drone activity to relevant authorities for further action.

uAvionix Australia :

Unlikely to succeed because bad actors can easily disable transmissions (eg shielding with foil).

BRID does not operate on a protected frequency and spoofing is likely. Eg see https://github.com/jjshoots/RemoteIDSpoofer

b) Helping educate the community around local laws and regulations relating to drone use.

uAvionix Australia : Surely it is at best a miniscule byproduct following the expense of fitment

c) Gathering of data which will form an evidence-base to support future regulatory and policy development.

uAvionix Australia : The lack of knowledge about the numbers of manned VFR aircraft and drones is a major issue and uAvionix is supportive of means to address this problem. The VFR component is slowly being addressed as VFR aircraft fit with ADS-B or EC devices but more needs to be done. uAvionix supports proposals that increase our joint knowledge of aviation risks in all parts of the country. However, we doubt that this application alone would justify remote ID.

Knowledge of aircraft density in network supported areas could be improved by NRID. However, the majority of the country has poor network support. BRID provides almost no such support except at very small isolated points.

d) Facilitate faster, more efficient, and/or automated approvals to operate in airspace for which drones may need permissions.

uAvionix Australia : This depends on the airspace and conditions so we discuss each separately below:

i. ***Controlled airspace**: If a drone needs to operate in controlled airspace and be **separated** from other VH registered aircraft then the expectation of other airspace users and ATC is that it be fitted with adequate communications, naviagation and surveillance equipment for the separation standard used. Small separation distances requires high integrity/availability and update interval with low latency surveillance and coms.*

But BRID has low transmit power and range making it almost useless for ATM management system use.

NRID may have adequate range between aircraft and network connect point but both BRID & NRID are unlikely to have adequate aviation performance particularly integrity, latency and guaranteed reliability (MTBF) for delivery of a separation service.

Situational awareness visibility can clearly assist ATC. However, with the increase in the number of targets if all drones are so equipped – it is unlikely that the ATC paradigm will be able to operate as it does today. Even today, ATC has not yet enabled the display of situational awareness EC devices onto ATC screens.

In the event that FIMS or another system is used this could change.

In any case BRID will be unable to provide that capability due to its range limitation but NRID could provide some service for situational awareness in areas with adequate network coverage. Situational awareness is further discussd discussed below in Class G sections below.

ii. ***Class G : (Above or outside FIM Airspace) Aircaft operating in class G depend on see and avoid. ie: a form of air-air surveillance.***

No UTM or FIMS can de-risk conflict between drone & VFR aircraft because VFR aircraft are not required to file flight plans nor use surveillance equipment. Some VFR operations even have no radio! Hence a UTM or FIMS may not even know about these aircraft.

uAvionix Australia : BRID will not serve air-air situational awareness because the reliable detection range is too small and because the frequency is not protected.

NRID would have difficulty providing air-air situational awareness because

- *it relies on multiple air-ground radio communication links (aircraft 1 to ground – central processing and then – ground to aircraft 2) bringing latency and performance issues*
- *there is no NRID receiver in non-drone VFR and IFR aircraft operating in this space. Fitment of certified NRID devices in conventional aircraft will bring significant new issues into play.*
- *However, if the NRID display device is a smart phone one needs coverage plus resolution of safety issue of pilots managing mobile devices whilst in command of an aircraft (MMI issues.)*

There is no suggestion that NRID transmitters or displays be provided or required for VFR aircraft so they aren't "part of the system". However, a combined ADS-B NRID picture could be sent to a smart phone – with the current weakness that VFR aircraft aren't yet all equipped wih ADS-B.

The consultation paper does not discuss the critical requirement to manage conventional aircraft operating in the same airspace as drones. *A drone only solution is not appropriate unless it applies to UTM or FIMS airspace or drone only airspace.*

A better solution to solve the interoperability between conventional aircraft and drones is to require all drones operating outside drone only airspace to have ADS-B sense and avoid, whilst at the same time requiring the VFR aircraft without ADS-B/EC to have EC devices. Further details can be provided if required.

iii. Class G : (Below or inside FIM Airspace) Aircaft operating in class G depend on see and avoid. ie: a form of air-air surveillance.

uAvionix Australia :The paper provides no clarity on the operation below 400 feet / inside FIM airspace so it is difficult to comment.

We can agree that NRID could be useful to monitor compliance of UAVs to approved flight trajectories and automatically generate alerts.The safety requirements when manned aircraft operate in this airspace is unclear to us.

If this is the target airspace to use NRID then that should be made clear.

e) Support management of, and response to, other drone related issues such as noise, privacy, and environmental concerns.

uAvionix Australia : No comment

f) Support management of, and response to, other drone related issues such including through adjacent technologies such as the future UTM.

uAvionix Australia : Any UTM / FIMS will likely operate on approved operations in tunnels of airspace and operate in a different paradigm to existing ATC. NRID may provide good support (when networks exist) for ensuring drones comply with approved operations. BRID is unlikely to support a UTM given the limited range of these devices.

3. <u>Comments on para 2 "Background :</u>

a) The growth in drone numbers is putting pressure on existing systems and could impact aviation and public safety if no action is taken. ***uAvionix Australia : Agree***

b) Will be a critical element of future air traffic management systems (including the uncrewed traffic management (UTM) system) that will integrate crewed ***uAvionix : Disagree for reasons above***

4. <u>Comments on para 4 "How does Remote ID work?</u>

Broadcast (BRID) : *This form could maybe be useful for security and enforcement. It is equivalent to a car numberplate in the sky,. It is NOT suitable for ATC surveillance (OK) and is not suitable for aircraft-to aircraft surveillance because of the limited transmit power and hence limited range/reliability. It may be suitable for drone-drone surveillance. It will do nothing to support safety from general aviation, regional aviation or any fast moving drones.*

Network based (NRID). : *This form is also useful for security and enforcement. However, once again it is not suitable for aircraft-to aircraft surveillance because*

- *Large parts of Australia do not have network coverage*
- *Unlike ATC surveillance there is no way to ensure adequate latency or accuracy/integrity. It is unlikely that such devices will have integrity algorithms like Avaition standard RAIM as exists today for aviation navigation and ADS-B products*
- *There is no way to ensure the reliability required for air-air or air-ground because of the numerous players involved in such a network. Reliability engineering , design and ongoing management to ensure those standards are met would be essential.*

It will do nothing to support safety from general aviation, regional aviation unless these players also equip. An equipage program of the whole Australian aviation fleet following on from the ADS-B program seems unlikely to be justified.

International standards are only suitable if the application defined in the standard is the same as proposed in Australia. If the proposed application is for enforcement purposes overseas, it would be inappropriate for Australia to use those standards for other applications unless CASA were convinced of the safety of doing so.

5. <u>Comments on para 6 "Challenges"</u>

a. Regarding "data availability will vary in different locations and contexts"

   uAvionix Australia : Agreed. The impact on conventional aircraft is not adequately discussed.

b. Regarding : Interoperability with other systems, including a Flight Information Management System (FIMS) and the UTM ecosystem.

   uAvionix Australia : Clarity is required regarding the impact or not of these systems on the VFR fleet operations is required before one can adequately discuss the tools to be used – potentially including Remote ID.

   Significant challenges may also exist to ensure that reibaility, integrity, availability are met and maintained.

c. Regarding : End user experience, including how information collected by Remote ID systems is presented and viewed.

   uAvionix Australia : For adequate discussion we need to know exactly who the end users are and the role of those users. This includes IFR & VFR aircraft, ATC, and FIMS/UTM system operators as well as the drone community

d. Regarding : Privacy and cyber security safeguards as Remote ID systems may collect, store and transfer private, personal, and commercial information.

uAvionix Australia : A broadcast system like ADS-B does not have these issues because "broadcast" is for the use of all receivers. Safety systems should not be reliant on the use of private information.

6. Annex 1 NRID challenges

a. Regarding : Satellite could be a bearer of NRID in these locations, however this may be cost prohibitive.

uAvionix Australia : More than cost is involved. For a satellite transmission in "weather" L band frequencies are needed for reliable communication. This requires adequate transmit power and increased antenna size.

7. Annex 1 ADS-B

uAvionix Australia : ADS-B is used to manage the nations IFR aviation fleet with thousands of Australian passengers at any instant being separated from other aircraft using this technology. It is being used worldwide.

The discussion paper says ADS-B is not suitable for drones (not carrying people) this application because of lack of encryption and security issues but it is OK for all the people in airlines. ***Clearly this is false.***

However, uAvionix agrees that ADS-B should not be transmitted by most drones – for other reasons.

uAvionix Australia argues that ADS-B IN should be fitted to all drones operating in airspace with VFR traffic so that they can take action to avoid VFR aircraft.

8. Annex 2 International standards

uAvionix Australia : The FAA standard use F3411 defines the purpose as follows : "The objective is to increase UAS remote ***pilot accountability by removing anonymity*** *……" – the uses proposed in the discussion paper take the proposed use much much further which we don't think appropriate.*

The FAA standard ASTM F3411 further says : "This specification is applicable to UAS that operate at very low level (VLL) airspace" meaning below 500 feet. The discussion paper does not make this clear and whether in Australia this is limited to below 500 feet.

9. QUESTIONS

9.1 Data and access questions

1. Who should have access to Remote ID data and to what information?

   uAvionix Australia : It depends on what application it is used for.
   All UAS operators.

2. Should there be a data collection standard?

   uAvionix Australia : No comment

3. What is the best method of providing Remote ID data to relevant stakeholders?

uAvionix Australia : It depends on what application it is used for.

4. What types of drone operators should be required to carry Remote ID equipment to operate drones? What should be exempt and why?

   uAvionix Australia : Any aircraft transmitting ADS-B should be exempt because they are already known "to the system"

5. How can Remote ID privacy issues be managed?

   uAvionix Australia : What privacy issues?. ADS-B has few, and they could be managed in a similar way for other users.

9.2 Technology questions

6. Is Remote ID (BRID, NRID or both) an appropriate solution for Australia? Are different typesof Remote ID more fit-for-purpose in different contexts or applications? Are there other types (or variations of types) of Remote ID that should be considered?

   uAvionix Australia : It depends on what application it is used for. BRID is suitable for compliance perhaps. NRID may be able to provide flight plath compliance for UTA/FIM systems in some areas

7. What factors should Remote ID mandates be based on, e.g. location, airspace related, other?

   uAvionix Australia : It depends on what application it is used for.

8. What technical requirements, standards and governance arrangements should be considered in the introduction of Remote ID to position for integration with adjacent systems, including the development of the UTM ecosystem?

   uAvionix Australia : It depends on what application it is used for.
   If used in ATM/UTM systems it would be best to standardise using Asterix surveillance standards defined by Eurocontrol

9. What features does Remote ID require to ensure tamper resistance and to mitigate security issues (including cyber risks)?

   uAvionix Australia : Impossible. It is not always possible. Aluminium foil can always mask the signal. The bigger risk is spoofing given the wide availability of transmitters/receivers.

Usage questions

10. What impacts could mandatory equipage have on drone operators?

    uAvionix Australia :no comment

11. Should mandatory equipage be rolled out to all drone operators, or phased through types of operators and/or operations?

    uAvionix Australia :ADS-B equipped drones/aircraft should be exempt and consideration of ADS-B IN "sense and avoid" mandates should be considered.

12. Are there existing standards that should be considered/adopted to facilitate Remote ID uptake in Australia?

    uAvionix Australia :no comment

13. Who should we be engaging with, particularly outside of the aviation industry (e.g. tel

    uAvionix Australia : AAUS, AOPA, RAAA, RAAus etc