# WG-115 / SC-238 – Counter UAS

## 2 April – 4 April 2024 – Plenary Session #22

### 1. Welcome, Introductions, Administrative Remarks by Committee Leadership

Meeting attendees (in part or whole)

| | |
|---|---|
| Akiko Kohmura | ENRI |
| Alex Milns | EUROCAE (WG-115 TPM) |
| Amaury Neyron de St Julien | Groupe ADP |
| Benjamin Lajos Magocs | Mosaic ATM |
| Bianka Karoly | HungaroControl |
| Brandi Teel | RTCA (SC-238 PD) |
| Carlos Barbas | Ineco |
| Charles Sheehe | NASA |
| Christos Skliros | Hellenic Drones |
| Declan Collins | Dublin Airport |
| Isaac Diakite | EDA |
| Henrik | Weibel Doppler Radars |
| Javier Ceballos Gutierrez | EUROCONTROL |
| Juan Vincente Balbastre | Universitat Polytecnica de Valencia |
| Julia Sanchez | EUROCONTROL |
| Kevin Maney | NATCA |
| Lee Gratz | SAAB |
| Lee Nguyen | NUAIR Alliance |
| Max Minev | ERA |
| Mark Reed | ALPA |
| Marianne Iverson | Copenhagen Airport |
| Mel Davis | NATCA |
| Niv Siva | UK CAA |
| Pavel Soukup | Eldis |
| Pavol Serbin | R-SYS |
| Philipp Rudnik | DLR |
| Scott Brenton | NUAIR Alliance |
| Talwyn Haley | FAA |
| Thomas Oster | EASA |
| Tom Haritos | KSU |
| Tony Militello | DoD PBFA |
| Tricia Fantinato | FAA |

Meeting opened 08h00 EDT / 14h00 CEST.

Alex Milns acted as meeting chair in the absence of WG-115 and SC-238 chairs.

Members in-person and on-line introduced themselves.

## 2. RTCA/EUROCAE Opening Policy Material

Alex and Brandi introduced the EUROCAE and RTCA policy slides (IPR, membership, GDPR, recording).

## 3. Review Agenda

Agenda Version 2 as distributed in the Calling Notice was agreed.

The meeting was reminded the purpose for the next 3 days was to commence a review of ED-286 / DO-389 OSED for Counter-UAS in Controlled Airspace.

## 4. Review minutes from Plenary #21 (January 30-February 1)

Alex introduced the draft minutes from meeting #21. Minutes were reviewed and adopted as written.

## 5. Election of WG-115 Co-Chair

Alex called for nominations for the co-chair position. Julia Sanchez nominated Javier Ceballos Gutierrez. Alex advised that Javier had indicated a willingness to support the WG in this role and provided a brief biography of Javier to the meeting. The WG-115 unanimously elected Javier Ceballos Gutierrez to the role of WG-115 co-chair. Javier was unable to be present on 2nd April, but joined for the other 2 afternoons.

Additionally, Brandi advised that the RTCA SC-238 Chair had resigned (as the organisation was no longer a member of RTCA) and that a task was underway to identify an new SC-238 Chair.

## 6. Election of WG-115 / SC-238 Secretary

Following earlier emails and the recent Calls for Participation, Alex and Brandi advised there had been no prior nominations for the Secretary position. No nominations were proposed within the meeting. The secretary position was not filled.

## 7. Consider the implications on SC/WG Terms of Reference and future tasking following publication of:
**a. Advisory and Rulemaking Committees – UAS Detection and Mitigation Systems Aviation Rulemaking Committee Final Report (faa.gov) and**
**b. Handbook on UAS protection of critical infrastructure and public space : a five phase approach for C-UAS stakeholders.**

A briefing was provided on the above ARC report by Tricia Fantinato and Mel Davis. It was noted that the ARC comprises individuals outside the FAA and is intended to advise the FAA; a response from the FAA to the report is currently being developed.

Discussion on the second document was limited in the absence of specific member insight into the report. However, it remains an important reference document for the development of the updated OSED (ED-286A / DO-389A)

## 6. Working Sessions for review and update of ED-286 / DO-389.

Taking as a baseline from the minutes of Meeting #21 **Appendix 1 Topics for OSED Update,** working group members added content and structure to the document, with the end result provided as **Appendix 1** to these minutes, and also available in the ED-286A Document Project Workspace here. Additionally, a scope statement for the updated OSED was drafted by Julia Sanchez with input from Lee Gratz and discussed during the meeting – also available at the previous link.

As the means of progressing the document review, the below work streams and task leaders were identified.  Folders for each work stream were created in the EUROCAE Document Project Workspace, with edit permissions assigned to task leaders as well as any members who expressed interest in working on each area.

| Topic Area | Point of contact/task leader |
|---|---|
| Scenarios and Use Cases | Julia Sanchez - julia.sanchez@eurocontrol.int |
| UAS operations (links closely to the above) | Benjamin Lajos Magocs - lmagocs@mosaicatm.com |
| C-UAS Decision Support | Amaury Neyron de Saint Julien - amaury.neyrondesaintjulien@adp.fr |
| Supporting Documentation | TBA – Amaury Neyron de Saint Julien - amaury.neyrondesaintjulien@adp.fr |
| Architecture | Isaac Diakite - isaac.diakite@eda.europa.eu |
| Sensors, Dataflows and Interoperability | Max Minev -  m.minev@era.aero Amaury Neyron de Saint Julien - amaury.neyrondesaintjulien@adp.fr |
| Safety/Risk/Security considerations | TBA – Amaury Neyron de Saint Julien - amaury.neyrondesaintjulien@adp.fr |

## 7. Review Actions

Alex to notify WG-115 / SC-238 members of meeting outcomes and invite contribution to the above workstreams.

Julia to identify candidates to lead:

- Scenarios and Use Cases, in partnership with Julia.
- Safety/Risk/Security considerations, in partnership with Amaury.

## 8. Any Other Business

None.

## 9. Set Future Meetings

Plenary Meeting #23:  2 July 2024 – Webex.

## 10. Adjourn

Brandi and Alex thanked the members who joined the meeting and look forward to reviewing progress at the next meeting in July.

Meeting closed at 17h10 CEST / 11h10 EDT 4 April.

Minutes prepared by Alex Milns – WG-115 TPM and Brandi Teel – SC-238 PD

## Appendix 1: Topics for OSED Update
### Updates during WG/SC meeting 2-4 April 2024
### Working notes only

**Scenarios and Use Cases**

Large Airports

Medium Airports

Small Airports

Vertiports, Heliports

Different operational scenarios within the airports and approaches

> Aircraft moving vs Infrastructure (building, CNS, fuel farm, electrical power)
>
> Aircraft flying vs on-ground (DG Home categories – parked/taxying, landing, takeoff)
>
> Off site CNS systems

Define how the C-UAS will be used, to support system design. Define the operational services. The intent being to avoid 'bespoke' systems, without being restrictive?

Update the notion of the "Counter-UAS Cycle"

Could automated interfaces be used to notify threat mitigation to other C-UAS operators?

> An obvious scenario is a 'dual use' Civil/Military airport, but consider also adjacent environments such as mass gatherings, prisons, critical infrastructure

Consider multiple airport/airspace users or external actors who may deploy C-UAS in areas near airports etc – coordination efforts to complement operations? What level of consideration is needed for the OSED? Is this proposing a sharing/integrating of surveillance data (or not sharing data), and fusing data between systems, or mitigation coordination being needed? Temporary deployments not to interfere.

UTM/U-Space integration (coordination of legitimate operations). Supported by cooperative surveillance (e.g. remote ID, ADS-B etc…).

Spectrum allocation considerations (control/influence of aviation authorities on 'external C-UAS') – process in place by FAA/FCC (Tal Haley's team) – also need to consider EU side

Julia Sanchez, and to identify second candidate in this area.

**UAS Operations – tie closely into the above scenarios**

Loss of control of (authorised) drones (is this just a case of drone in the wrong place?) and not necessarily a specific use case?

Accidental vs deliberate actions – different use cases/solutions?

Violation of UAS Geographical Zones (banned areas, containment areas), operating outside approved area, operating not in compliance with procedures/equipage

Management of different sizes of drones (detection (high level statement), responses) and different types, operating characteristics (e.g. multi rotor, fixed wing etc). High performance vs reaction time

Evolution of drones needs to be considered.

Consider UAS Swarm as a use case. Also consider a 'coordinated attack' Swarming vs Saturation

Management of operations transiently in/out of C-UAS protected areas.

Maintenance of a 360 degree capability even in case of intrusions from one direction – e.g. coordinated attacks from multiple directions.

Maintaining capability in case of multiple attacks.

Consider incremental engagement of mitigation efforts – e.g. talk to operator, if no outcome then engage RF/kinetic effectors.

ARC discussions – in civil environment perhaps mitigation is 'less desireable' – more emphasis on detection than mitigation.

3 areas – detection area, 1st stage response (e.g. talk to operator), mitigation zone.  C-UAS should have an escalation response protocol.

Consider that authorized drones still need to be monitored incase they operate in an unauthorized way.

Vacant at this stage, possibly to consider as part of the Scenario Descriptions. Benjamin Lajos Magocs can assist (background in swarming)

## C-UAS Decision Support
How is classification done?  Drone or not, authorized or not, UTM/U-space integration, characteristics of drone and area of operation (yellow/orange/red areas), is apparent effort to 'hide' a classification criteria?
Time/speed vs distance for alerting (e.g., 19m/sec = 1km per minute),
    Buffer zones for alerting and coverage
    High speed, low altitude drones
Cooperative Information (Remote ID, USSP data, ATM data) – how to make use of it?
Command and Control – more details, review SP/IR The SP/IR did not address the next step after threat identification
Consider potential launching sites both close to and far from airport/area of interest.
Who knows what and when?

Consider the use of a 'whitelist'/friendly drones and/or known 'bad' drones.  Issues around accurate maintenance of these databases….

Noting the document focuses on the technical aspects, discussion of the below points should be limited and 'high level':
An assumption in ARC that the air traffic controller would have knowledge of what is happening in 'C-UAS environment'.  Information flow of both data and decision-making to ATC?

As an example in CDG – ATC does not have all knowledge – only in 'red' area, other detections not notified.  To manage ATC workload.  LEA will have more data on drone operations than ATC.

OSED to consider these variations in approach, consider where ATC sits in the decision support framework.  C-UAS is a security tool, not an ATM function.

Link to scenarios to consider the above and type of threats, threat assessments.

OSED to consider guiding principles for the design of C-UAS protected areas (red/orange/yellow), actual sizes may not be appropriate for OSED, but guidelines certainly.  Also consider in light of emerging drone technology (speed, type, manouvreability).

Amaury Neyron de Saint Julien

## Documentation – high level only

Aviation and Non-aviation regulatory requirements

Spectrum requirements

Radiation Hazard exclusion areas

EU General Data Protection Regulation, privacy considerations (e.g. for optical sensors)

References to other material establishing the overall operational context for C-UAS deployment and operation.

Reference to SP/IR Ch3 for probability/vulnerabilities/threats/severity for consistent use of terminology.

How does mitigation fit in here?

Tricia Fantinato – to confirm, Amaury Neyron de Saint Julien

## Architecture

Building on the 'black box' as described in the current SP/IR, update the OSED (existing model has evolved since first edition), build on the details to be aligned with SP/IR.

Detect, Identify, Classify, C2, Mitigate, Assess.    Anything missing = not effective C-UAS

Isaac Diakite

## Document review (ICAO, EASA, FAA etc)

Review published docs for relevant content and reporting this to WG co-chair and topic leaders.

Julia Sanchez

## Sensors, Dataflows and Interoperability

Coordination of effort across jurisdictions to maximise coverage, reduce costs by unnecessary duplication.

Sensor Classification (Level 1 – 3 sensor capabilities) – topic for further discussions

- e.g. Level 1 – Using Remote ID sensors e.g. Aeroscope
  - Level 2 – Techniques such as MLAT on UAS - pilot data comms, RF, cameras
  - Level 3 – Fully non-cooperative e.g. radars
- SPR defines performance requirements (for non-cooperative targets)

OSED to outline range of sensor types (build on Table 3-2?).  Limitations of e-Identification (not available or switched off)

Clarity around dataflows now we have a specific functional block for DTI

Consider integration of C-UAS into other systems (maybe covered in INTEROP)

Using C-UAS to inform other authorities with capabilities beyond the C-UAS itself (e.g.4G/5G interruptions/jamming??)

Surveillance 'levels' aligned to 'confidence levels' for decision making?

      Surveillance levels = ability to detect

      Confidence – level 1 has good confidence in the accuracy of detection data, but not confidence in the extent of surveillance of the environment

Completeness of the picture?

- Remote ID surveillance – partial picture
- Radar/non-cooperative sensor / camera etc (together or not with ID)– more comprehensive picture

Consider spoofing, not encrypted Remote ID data – can create false remote ID ->false mitigation response.

Explore the C2 architecture

      Max Minev, Amaury Neyron de Saint Julien

**Safety/Risk/Security considerations**

Confidence in data ->threat level assessment.

Safety and risk considerations of mitigation/countermeasure actions – high level…..

Jamming of C-UAS, remote ID spoofing, GNSS RFI

Cybersecurity as one aspect

Data exchange to/from C2 – protect the C2 (DMZ) from virus.  Can C-UAS system be exposed to Internet?

Does C-UAS need same levels of IT security as ATM systems?

Interface between C-UAS and UTM/U-space.

Consider broad cybersecurity practices/standards – e.g. ED-201, ED-205, IR 664/2021

      Julia Sanchez to identify candidate

      Amaury Neyron de Saint Julien

**Define and describe the overall scope of the OSED.  First step.**

## Chapter 1

Scope review

Methodology that the principles being applied in this document can be used in other operational environments.

Definitions - Taxonomy review

Vertiport, Heliport

## Chapter 2

2.1 - consider risk vs threat (precise definitions)

Overall context - prevention/education - maybe not for EUROCAE doc but reference to other material (e.g EASA).

2.2 review

2.3.2 - Include RadHaz here (protective clothing for portable emitter guns?)

Consider mitigation impacts on the environment (e.g. RFI from jammers impacting legitimate operations).

2.3.5 - Other regulatory requirements - non-aviation, spectrum, RadHaz etc (also ref to 2.3.2)

## Chapter 3

Reviewing Classification methods. Consistency with SP/IR. Develop detail around classification and identification (type, authorised or not,). Data flows from UTM/U-Space to permit understanding whether a drone operation is authorised (also 2.2.2).

Cooperative Information (Remote ID, USSP data, ATM data) – how to make use of it?

Figure 3.1 to be reviewed to align with SP/IR. Ensure C2 component functions are aligned.

## Chapter 4

Building up use cases

Use cases into Appendix, airports, vertiports (are unmanned operations different in risk profile to manned?), heliports

Small airports may be uncontrolled (consider this as a sub-use case?)

Development of alerting zones for each use case (general statements)