



EUR 055-20 / WG115-05
RTCA



Saint-Denis, 02nd March 2020

EUROCAE WG-115 “C-UAS”

Meeting #2 Minutes

<i>Date</i>	<i>23rd January 2020</i>
<i>Place</i>	<i>Webex</i>
<i>Venue</i>	<i>Webex</i>
<i>Hosted by</i>	<i>EUROCAE</i>

1. Welcome and Tour de Table

Jorge Munir El Malek Vázquez [JM] welcomed the participants to the 2nd meeting of the Joint Activity EUROCAE WG-115 and RTCA SC-238, As announced and planned WG-115 and SC-238 will develop their activity jointly.

Then the proposed agenda was agreed:

0. Welcome and Tour de Table
1. RTCA and EUROCAE Statements review
2. Approval of Kick Off Meeting Minutes
3. Updates about Joint activity WG115 SC238
4. Presentation and discussion about WorkPlan (update draft)
5. Presentation and discussion about OSED Table of contents
6. Date/Scope of next meeting
7. AOB
8. Close

After agreeing the agenda and considering this meeting was the first joint meeting, a tour de table was open which allowed all participants to introduce themselves and to provide a short introduction to their organisation and expertise in the field of C-UAS. Additionally, [JM] explains some colleagues have not been able to attend, apologizing in advance and sharing feedback for supporting the meeting. ATTACHMENT A include “WG-115 and SC-238 Meeting 2 Attendance”.

2. RTCA and EUROCAE Statements review

Al Secen [AS] presented the standard announcements regarding RTCA Anti-Trust policy, Proprietary policy, RTCA Committee Participation Membership Policy and the Workspace tool available for RTCA members.

Sergiu Marzac [SM] presented the standard announcements regarding EUROCAE membership-based status, IPR policy and the Communication & Privacy policy, including the Workspace tool available for EUROCAE members.

3. Approval of Kick Off Meeting Minutes

After confirming neither additional comments nor changes were required, final draft of the Kickoff Meeting Minutes were approved.

4. Updates about Joint activity WG115-SC238

Brief update focused on the joint activity between WG-115 and SC-238. [JM] explained the kickoff of the SC-238 took place on January 15th 2020. The chairman of the new SC is Max Fenkell.

5. Presentation and discussion about WorkPlan (update draft)

[JM] presented an update of the WorkPlan providing additional information about the 3rd meeting which will take place on March 12th March by Webex from 15:00 until 18:00 (CET). During the same timeslot, those EUROCAE WG-115 and RTCA SC-238 members who will be in Madrid will have the F2F option for attending this meeting. Indra at their Headquarters will host the optional F2F. *(Update after meeting: check section 7 of these meeting minutes for getting more information about the F2F option).*

Nancy Ford [NF] highlights RTCA Symposium will take place in June 16th and 17th in Washington, considering some members of the WG115-SC238 Joint Activity will attend, it would be interesting to have in consideration the same week for planning a F2F meeting.

Patrick Garnier [PG] suggested that considering the closeness between March and April meeting, the April meeting could be delayed a little. *(Update after meeting: considering the demanding objectives established by the TOR, the lead team considered useful to preserve the April meeting, though delaying it until the last week of April or first week of May, the new proposal will be shared on March 12th during the 3rd meeting.)*

6. Presentation and discussion about OSED Table of contents

[JM] reminded the group that a Call for Editor and Contributors was still open, [JM] explained the main Editor's responsibilities.

[JM] exposed several volunteers presented their interest in contributing, particularly:

- Julia Sánchez – EUROCONTROL
- Nancy Ford – Security101
- Martin Lanni – Quantum Aviation
- Ludmila Lapteva and Benoit Samiez – Hologarde – Group ADP

[JM] explained several comments about OSED draft were received days before the meeting: (1) Christer-Matterson Brown (DG HOME) who apologized in advanced for his absence from the meeting, (2) Nancy Ford (Security 101). See ATTACHMENT B.

[JM] explained that once the contributors' team for OSED is clearly defined, the lead team aligned with contributors would plan the next weeks and established the how-to-do to interact and collaborate among them.

After this introduction, [JM] proposed to open the OSED draft and review step by step the proposed Table of Contents and the high level description of each chapter and section, following some good praxis such as: (1) Balanced discussion, avoiding detail by detail analysis, (2) Time efficient contributions.

Throughout this review, the members shared multiple comments and fruitful discussions, such as:

- Chapter 1
 - 1.1. Introduction
 - [NF] suggested the rule to have any acronym spelt in full in its first occurrence of the document and then use of the acronym in the rest of the document. *(Update after meeting: this praxis will be followed by default).*
 - [NF] include under consideration "critical infrastructures" as other environments where C-UAS capability could be extended. Andy Cebula [AC] agreed with the importance to consider urban areas, critical infrastructures, highlighting these

- cases are the next in relevance after airports in USA.
 - [JM] shared his view about extending the number of environments, reminding current Terms of Reference (TOR) established “around the airfield” as first and main environment. At the same time TOR could support the possibility to extend “... to operations to other environments”. At that moment (beginning of the activity) group should be focused on the airfield environment. The group could consider additional ones in the future, mainly those considered “similar environments” and finding an effort balance compatible with the proposed timeline, the group should not cover every rogue use of UAS.
 - It was suggested some representative of U.S. Customs and Border Protection (CBP) or Department of Homeland Security (DHS) should be involved in the joint activity.
 - Katsuyuki Nakatsubo [KN] considered important to have all the involved stakeholders in the group (such as DHS).
 - Additionally, it is suggested to take into account traffic density in the SPR and INTEROP which impacts in the C-UAS domain.
 - After multiple comments, the group agreed about the suitability of having representation of multiple stakeholders, including final users and, particularly, U.S. DHS, [AS] stated that having representation from those agencies would be very beneficial and reminded they had been invited several times.
 - 1.2 Scope
 - An error was identified in the description: “existing” instead of “exiting” (error). The next version of OSED will include this fix.
 - Some comments were shared about operational aspects (such as to consider both cases Line-of-Sight and Beyond-Line-of-Sight, etc). Aligned with Markus Wolf's [MW] suggestion, chapter 4 “Operational Environment” would provide room for this type of content, the discussion about operational aspects moved to that chapter.
 - 1.6.2 Definitions
 - [JM] pointed out the EUROCAE's criteria: “Wherever possible, abbreviations and definitions used in EUROCAE documents should be identical to those used in other international standards, such as ICAO Standards and Recommended Practices (SARPS)”.
 - [AC] suggested the importance to have a clear definition of “Collaborative drone”.
 - [NF] provided several considerations for definitions not yet listed (see Attachment B).
 - Others comments
 - [PG] identified an error in the Introduction description, according to current TOR, SPR was acronym of “System Performance Requirements”. According to this issue there was a discussion about System or Security. *(Update after meeting: according to TOR, the deliverable is named System Performance Requirements. Officially, there is no safety high-level requirements from the regulatory, due to this context, it could be challenging to work on this topic, trying to identify detailed safety requirements on the Sensors/Detection, indeed C-UAS has not really an impact in safety of aircraft as we do have for CNS systems. Anyway, if during the work on SPR the WG finds interesting ideas and valuable requirements, WG can take them into account and provide some guidance.*
- Chapter 2
 - The discussion of the group identified as important short-term task to provide a clear definition of collaborative and non-collaborative drones, as well as collaborative and non-collaborative.
 - Some comments were focused on the drone categories to be consider in the scope of the OSED. [AS] clarified the activity of the group should not be necessarily limited to just small UAS (supported by Rule Part 107 of FAA), but optionally piloted vehicles, larger vehicles can be considered. Some comments pointed out the importance to focus

on specific categories (particularly, those drones supported by existing regulation, such as small UAS (Part 107)), taking into account performance or interoperability requirements would be conditioned by their characteristics and if there were multiple categories, the documents (OSD, SPR, INTEROP) would be very extensive. [AS] answered the lead team would analyze and consider this info and will give feedback. *(Update after meeting: WG-115<:SC-238 has the objective of proposing minimum requirements so no need to address specific types of drones, this can also provide more flexibility).*

- Ian Bradley [IB], contributed with his view about the definition of collaborative and non-collaborative concepts. [IB] pointed out the definition should consider several factors, beyond RF “emission” or “non-emission”, a drone without emitting information does not mean it is a non-collaborative drone, it can operate autonomously in a collaborative way.
 - Regarding 2.1.2 – Threat definition: [JM] reminded an example provided by [AS] in the RTCA kickoff about threat: those objects, which current systems cannot detect. One member of the group highlighted that depending of that definition the scope of this section could change notably. [AS] proposed to get visualization of Gatwick and Heathrow last December, “that is what we want to solve, the law breakers. There are no rules to cover them”.
 - Regarding the Benefits section, [MM] pointed out from IATA they had done a study about consequences of C-UAS systems. He can be share it with the lead team for taking info for this section.
- Chapter 3
 - [AS] pointed out section 3.3.6 (Airspace Closure) and 3.3.7 (Runway Closure) were out of the scope of this WG.
 - [MM] told there was a tool in Europe, inside EUROCONTROL, for continuous monitoring, 3.3.5. EUROCONTROL can be involved in this section.
 - It was confirmed the intention to cover all detection modalities (radar, acoustic, RF, ...) in the Operational Capabilities section.
 - Lead Team pointed out defeat and recovery means were out of scope of the WG work. However, they had to be considered in order to define the interoperability requirements according to TOR (“Interoperability of the defeat capabilities with the airport and ANSP systems will be addressed”).
 - Additional comments:
 - The name of the WG (C-UAS) was confusing about counter capabilities, considering the focus was mainly on Airspace Awareness Detection.
 - Difference between Detection and Identification. [PG] reminded the importance of clarifying those terms.
 - Julia Sánchez [JS] highlighted the importance to specify the meaning of the term “threat”, that definition impacted on the different C-UAS stages (locating, tracking, verifying, identifying, classifying, neutralizing).
 - Chapter 4
 - Some suggestions for taking into account in this chapter:
 - Consider airspace authority.
 - Classification of the airspace.
 - Type of aircrafts in that airspace.
 - Types of operations occurring when weather is good or not.
 - Impact on the airspace if a drone comes in.
 - What happen in the visual environment (good or bad weather).
 - According to the experience in Europe, for example Frankfurt airport, [MM] commented typical drone ban zones in Europe had different ranges (1.5, 5 and up to 8Km),.
 - Regarding the impact of rogue drones on air operations and airport activities, issues not included in the current TOR, [PG] suggested these important considerations be accounted somewhere (list of out-of-scope topics), for example, another forum, another WG, or even to consider the idea to extend the mandate and create a sub-group. EUROCAE staff can also advise if any other WG already addresses these issues (impact of malicious drones (rule breakers) on airport activities (flights – landing, take offs – taxing, planes and passengers’ security, etc.).
 - Considering there were other groups such 105 and its subgroups, [MM] asked Jorge to share the list with EUROCAE team to check if that list of “out of scope” issues were cover by existing initiatives.

- *(Update after meeting: No other WGs cover those “out of scope” issues. Impact of rogue drones is an important topic but out of scope for the joint activity of WG-115/SC-238).*
-

Additional Remarks

- There was a suggestion to include a Legal Framework section as a reminder that all drone detection and surveillance systems will have to comply with the regulations in force in the place of operation. *(Update after meeting: A high-level legal framework can be of interest and OSED should be the document which could include it. Lead Team proposes to consider it as an attachment or section, requesting volunteers for contributing to its content).*

Final Remarks:

- [MM] Manfred thanked for the hard work done so far and reminded if anybody had an additional idea could come back to the team. The TAC wanted to help as Committee representing all involved stakeholders (airlines, airports, industry, etc). Additionally, the WG needed somebody who could take care of the document as editor. Any volunteer for contributing was asked to report to the leadership.
- [JM] proposed to take into consideration the remarks that were made during the review and to modify or add elements in the OSED to address these remarks.
- [JM] reminded the need to get contributors and editor either for full sections or for parts of the documents. These potential contributors are welcome to liaise with the leadership team.

7. Date/Scope of next meeting

Joint Meeting 3 Calling Notice

Date	12 March 2020 15:00 – 18:00 (CET)
Place	Webex
Venue	Webex – see attachement
Hosted by	EUROCAE
(Optional F2F) Place	Indra HQ, Avenida de Bruselas 35, 28108, Alcobendas Madrid, Spain
(Optional F2F) Venue	Meeting room #4, semi-basement level (Any doubt, ask in the reception)
Hosted by	Indra Sistemas

Finally, If planning to attend in Madrid for the optional F2F, please, send us an email to me (jmel@indra.es) and Patrick Garnier (patrick.garnier@c-s.fr) to facilitate the organization.

Action items

The meeting reviewed the action list and updated the following list:

Number	Action	Responsible	Due By	Status
1	Correct errors detected in the OSED draft and provide new version	<i>Lead Team</i>	1 st week March	
2	Define multiple key terms to get clarity and alignment (terms such as collaborative and non-collaborative drones, threat, detection, identification,)	<i>Lead Team and Contributors</i>	First weeks of OSED draft	
3	Review and provide clarifications about SPR comments	<i>Lead Team</i>	3 rd meeting	Include "update after meeting" in the draft meeting minutes
4	Evaluate feedback about focusing on specific drone categories	<i>Lead Team</i>	3 rd meeting	Include "update after meeting" in the draft meeting minutes
5	Share with the lead team the IATA document	<i>Manfred Mohr</i>	February 20206	DONE
6	Create list of out-of-scope topics and check with EUROCAE team what alternative groups, subgroups or forums	<i>Lead Team, EUROCAE team</i>	3 rd meeting	Include "update after meeting" in the draft meeting minutes
7	Evaluate the suggestion about including Legal Framework section in the OSED scope	<i>Lead Team</i>	3 rd meeting	Include "update after meeting" in the draft meeting minutes

ATTACHMENT A**WG-115 and SC-238 Meeting 2 Attendance**

Organisation	First name	Last name
AIA Aerospace	Max	Fenkell
Aircraft Owners and Pilots Association (AOPA)	Christopher	Cooper
Airlines for America	Andy	Cebula
Aveillant	Collin	Rogers
Aveillant	Tim	Quilter
Blighter Surveillance Systems Ltd.	Mark	Radford
Collins Aerospace	Garry	Sissons
CS Group	Patrick	Garnier
DLR GfR mbH	Jan	Gebhardt
DroneShield	Mark	Ayerks
EUROCAE	Sebastian	Reschenhofer
EUROCAE	Sergiu	Marzac
EUROCONTROL	Javier	Ceballos Gutierrez
Everis Aerospace and Defense	Jorge	Estévez García
Federal Aviation Administration	Sheila	Mariano
Federal Aviation Administration	Diane	McClatchy
Federal Aviation Administration	Lee	Nguyen
Groupe ADP and Hologarde	Ludmila	Lapteva
Hensoldt Sensors GmbH	Markus	Wolf
Hensoldt UK	Andy	---
Honeywell International, Inc.	William	Sanchez
Hungaro Control	Bianka	Karoly
IATA	Manfred	Mohr
Indra	Jorge Munir	El Malek Vazquez
Japan Radio Air Navigation Systems Association	Katsuyuki	Nakatsubo
JHW Unmanned Solutions LLC	Jim	Williams
National Air Traffic Controllers	Tony	Walsh
Northeast UAS Airspace Integration Research Alliance (NUAIR)	Andy	Thurling
One-ATM	Ray	Young
OpenWorks Engineering	Ian	Rodley
Raytheon	James	Johnson
RETIA, a. s.	Pavel	Sedivy

Rohde&Schwarz GmbH Co. KG	Goetz	Mayser
RTCA	Al	Secen
SAVE SpA	Federico	Cezarotti
SAVE SpA	Gianni	Pezzato
Security101	Nancy	Ford
THALES	Philippe	Juge
Università Telematic	Matteo	Natale
U.S. Air Force	Chritopher	Morrison
WhiteFox Defense	Walter	Stockwell

WG-115 Meeting 2 Apologies

Organisation	First name	Last name
DG Home	Christer-Matteson	Brown
EUROCAE	Alain	Vallée

ATTACHMENT B

Feedback about OSED before 2nd meeting

Feedback from Christer-Matteson Brown

- Introduction and section 4.3:
 - There are certainly grounds to argue that C-UAS capabilities could be extended to semi-urban and rural settings (e.g. prisons/military facilities in the country) as well (besides urban settings, already mentioned in the text). Could the scope of other possible use environments be expanded to reflect this?
 - Regarding the urban setting specifically, it would be useful to include a few lines of very general discussion on how, if at all, the application of countermeasures in this setting might differ from the airport setting.
- Section 2.2:
 - Are there European classifications as well that can be drawn on here?
- Section 2.2.1:
 - There is scope for a more nuanced discussion of the benefits and disadvantages of C-UAS. This is lacking at present.
- Section 3.3:
 - The list of operational services/capabilities bears further consideration. For instance, I wonder if “reaction time from alert” is a value that the “initial detection and identification” might offer. Furthermore, “alert procedures” might be something that accompanies a C-UAS system, informing the behaviour of different stakeholders. In my view, they are not an operational capability in and of themselves, but rather something that supports capabilities, like the decision-making to achieve “airspace closure” or “runway closure”. Finally, “threat detected by other means” is arguably not an operational capability, but rather part of “initial detection and identification”?
- Section 3.3:
 - Obviously, it will be crucial to elaborate clear definitions of terms such as “range”, “detection”, “identification”, etc. in later drafts of the document. For instance, if we take detection/identification as a combined example, will we mean the point at which specific detection/identification data is processed by the sensor system, or the point at which the processed data is made available to the operator? (My understanding is that, in both cases, the difference between the two points in time can in some cases be a matter of several seconds.)
- Section 4.1:
 - Given the range of certain DTI solutions, well beyond airfield perimeters, the “environment identification” might need to be nuanced somewhat.
- Chapter 5 (and related to the comments on urban/semi-/non-urban):
 - The scenarios might include, among others: 1) airport, urban; 2) airport, semi-/non-urban; 3) civilian airport; 4) civ/mil airport.

Feedback from Nancy Ford

General feedback about OSED:

- Section 2.1.2:
 - “Threat Definition and Classification could also include the probability level of a negative event, the frequency and serious impact if an event occurs.”
- Section 2.2:
 - “The concept should influence a layered approach for multiple security measures to mitigate negative impacts. Focus on the concept that one system will not be a silver bullet. Key is first situational awareness, understanding counter measures, etc. but also having process protocols that are measured and tested frequently.”

- Section 3.2:
 - “Defining specific roles and responsibilities... who is the decision maker, who owns risk assessment, who owns recovery, should an event occur? Maybe a RACi model”

Considerations for definitions not yet listed in 1.6.2 Definitions

Term	Definition
Confirmed	Validated by visual site, technology programs, and / or dual authentication. May also include verification of data by experts or leaders with first hand knowledge of a topic
Credible UAS Threat	An identified and confirmed risk that is determined to pose uncontrolled loss, an immediate or near-term negative impact to people, property, or other assets. This may include UAS on a non-registered flight path with or without a payload, and outside established flight path directives.
Detection	Accurate and positive recognition of a UAS in the environment / airspace; Identification of a UAS flight path with intent.; Payload of a UAS; Predictive risk / threat of a non-responsive UAS
Disruption to Operations	A UAS that has the ability to pose risk of interrupting airport ground-based operations or airborne flight operations, due to an established flight path, regardless of intent.
Stakeholder	A person or company that has a direct or indirect impact related to UAS Regulations, performance requirements, Operational guidance of Counter UAS. This includes any persons that have an interest in future UAS rules, to the extent that could possibly impact strategic corporate plans, or pose unreasonable conflicts in innovation vs security risk.
Perceived Threat	Subjective judgement people make about the severity or probability of a risk from UAS operations.
Threat	A verified intent to inflict harm, loss, or the process of taking action of great risk that can have a negative impact to the environment, people, assets, or property.
Unconfirmed	Perceived but not verified, possible threat with uncertain severity or level of probability of materializing