

# ED-286

## OPERATIONAL SERVICES AND ENVIRONMENT DEFINITION FOR COUNTER-UAS IN CONTROLLED AIRSPACE

### LEGAL NOTICE

This document is the exclusive intellectual and commercial property of EUROCAE. It is presently commercialised by EUROCAE. This electronic copy is delivered to your company/organisation for internal use exclusively. In no case it may be re-sold, hired, lent or exchanged outside your company. It may not be reproduced, in whole or in parts, without prior written permission by EUROCAE.

**MARCH 2021**

## FOREWORD

1. This document was developed jointly by EUROCAE Working Group 115 "Counter UAS" and RTCA SC-238 "Counter Unmanned Aircraft Systems" and was approved by the Council of EUROCAE on 18 March 2021.
2. This document is technically identical to RTCA DO-389.
3. EUROCAE, an international non-profit organisation, is the European leader in the development of worldwide recognised standards for aviation. This is achieved by utilising the expertise from our members and stakeholders across the global aviation community.
4. EUROCAE standards are developed following an open, transparent and consensus-based process, governed by process and quality management principles, which are clearly documented and is in line with the World Trade Organisation (WTO) Technical Barriers to Trade (TBT) Agreement, Annex 3 "Code of Good Practice for the Preparation, Adoption and Application of Standards".
5. EUROCAE standards and other deliverables are recommendations and best industry practices. EUROCAE is not an official body of the European governments. EUROCAE standards are intended to complement and support the regulatory and certification framework.
6. Whilst efforts are made during the standards-development process to avoid the inclusion of proprietary information and material, some of the elements of this document may be the subject of patent, copyright or other proprietary rights. EUROCAE shall not be held responsible for identifying any such rights. Trade names and similar terms used within this document do not constitute an endorsement by EUROCAE thereof.
7. Copies of this document may be obtained from:

EUROCAE

9 – 23 rue Paul Lafargue

93200 Saint-Denis

France

Telephone: +33 1 49 46 19 65

Email: [eurocae@eurocae.net](mailto:eurocae@eurocae.net)

Website: [www.eurocae.net](http://www.eurocae.net)

## TABLE OF CONTENTS

|                                                                        |     |
|------------------------------------------------------------------------|-----|
| FOREWORD .....                                                         | i   |
| TABLE OF FIGURES .....                                                 | iii |
| TABLE OF TABLES .....                                                  | iii |
| CHAPTER 1 PURPOSE AND SCOPE .....                                      | 1   |
| 1.1 Introduction .....                                                 | 1   |
| 1.2 Scope .....                                                        | 3   |
| 1.3 Document structure .....                                           | 3   |
| 1.4 Relation to other Projects .....                                   | 4   |
| 1.5 References .....                                                   | 4   |
| 1.6 Abbreviations .....                                                | 6   |
| 1.7 Definitions .....                                                  | 8   |
| CHAPTER 2 COUNTER-UAS CONCEPT .....                                    | 12  |
| 2.1 The UAS Threat .....                                               | 12  |
| 2.2 Counter UAS .....                                                  | 12  |
| 2.2.1 Existing C-UAS tools and methods .....                           | 12  |
| 2.2.2 C-UAS concept and generic high-level architecture .....          | 13  |
| 2.2.3 Benefits, constraints and other considerations .....             | 15  |
| 2.3 High level legal framework .....                                   | 17  |
| 2.3.1 General issues .....                                             | 17  |
| 2.3.2 Active RF emitters .....                                         | 17  |
| 2.3.3 Privacy laws .....                                               | 18  |
| 2.3.4 Airport regulations .....                                        | 18  |
| CHAPTER 3 OPERATIONAL SERVICES .....                                   | 20  |
| 3.1 Introduction .....                                                 | 20  |
| 3.2 Detection .....                                                    | 21  |
| 3.2.1 Detection, location and tracking .....                           | 21  |
| 3.2.2 Classification and Identification .....                          | 21  |
| 3.2.3 Data Collection .....                                            | 22  |
| 3.2.4 Types of detection technologies .....                            | 22  |
| 3.2.5 Limitations and Possible Impacts of detection technologies ..... | 23  |
| 3.3 Decision Support .....                                             | 24  |
| 3.3.1 Threat Analysis .....                                            | 24  |
| 3.3.2 Alerts .....                                                     | 24  |
| 3.3.3 Incident Response .....                                          | 24  |
| 3.3.4 Neutralization determination .....                               | 25  |
| 3.4 Neutralization .....                                               | 25  |
| 3.5 POST INCIDENT ACTIONS .....                                        | 27  |
| CHAPTER 4 OPERATIONAL ENVIRONMENT .....                                | 29  |
| 4.1 Environment Identification .....                                   | 29  |
| 4.2 Airport and air traffic .....                                      | 29  |

|                 |                                                          |    |
|-----------------|----------------------------------------------------------|----|
| 4.2.1           | Airport type and mix of traffic.....                     | 29 |
| 4.2.2           | Quantity and density of airspace traffic .....           | 30 |
| 4.2.3           | Associated airspace type.....                            | 30 |
| 4.2.4           | Communication, Navigation and Surveillance systems ..... | 30 |
| 4.3             | Traffic Management.....                                  | 31 |
| 4.3.1           | Air Traffic Management .....                             | 31 |
| 4.3.2           | Air Traffic Control Systems.....                         | 31 |
| 4.3.3           | UAS Traffic Management .....                             | 32 |
| 4.4             | Actors.....                                              | 32 |
| 4.5             | Other surroundings and environments .....                | 33 |
| 4.5.1           | The vicinity area .....                                  | 33 |
| 4.5.2           | Electromagnetic interference.....                        | 34 |
| 4.5.3           | Atmospheric conditions .....                             | 34 |
| CHAPTER 5       | TABLETOP EXERCISE SCENARIO DEVELOPMENT.....              | 35 |
| 5.1             | Low Impact Scenario .....                                | 35 |
| 5.2             | Medium Impact Scenario .....                             | 35 |
| 5.3             | High Impact Scenario .....                               | 36 |
| APPENDIX A      | GENERAL OPEN FRAMEWORK FOR C-UAS.....                    | 37 |
| APPENDIX B      | SUMMARY OF REQUIREMENTS .....                            | 41 |
| WG-115 / SC-238 | MEMBERSHIP .....                                         | 45 |
|                 | IMPROVEMENT SUGGESTION FORM .....                        | 50 |

## TABLE OF FIGURES

|             |                                           |    |
|-------------|-------------------------------------------|----|
| Figure 2-1: | Hi-level C-UAS Components .....           | 13 |
| Figure 3.1: | Diagram of the C-UAS layer approach ..... | 21 |
| Figure A-1: | General C-UAS Framework.....              | 39 |

## TABLE OF TABLES

|            |                                                              |     |
|------------|--------------------------------------------------------------|-----|
| Table 1-1: | Abbreviations.....                                           | 6   |
| Table 1-2: | Definitions.....                                             | 8   |
| Table 3-1: | Sample of C-UAS Detection technics .....                     | 22  |
| Table 3-2: | Limitation and impact of C-UAS detection technologies.....   | 23  |
| Table 3-3: | A representative subset of neutralization capabilities ..... | 25  |
| Table A-1: | Definition of Roles.....                                     | 37  |
| Table B-1: | Summary of Requirements .....                                | 41  |
| Table B-2: | Summary of Recommendations .....                             | 413 |
| Table B-3: | Summary of Optional Requirements.....                        | 424 |

## CHAPTER 1

### PURPOSE AND SCOPE

#### 1.1 INTRODUCTION

For many years, nations have recognized the many positive use cases for drones - or unmanned aircraft<sup>1</sup> - and their potential to make many aviation activities safer, greener and quieter. However, there is also a potential for drones to be used carelessly or for malicious purposes, including terrorist and other criminal acts.

Drone sightings, perceived to be hazardous or threatening near airports, have impacted airport and flight operations. In addition, close encounters during takeoff, approach and landing have been reported<sup>2</sup>, with an impact on flight safety. These occurrences have led to the suspension of flight operations with significant impact on the airport, airlines and the public.

During the busy 2018 Christmas travel season, Gatwick Airport near London grounded operations for 33 hours due to recurring drone sightings near the runway. The event resulted in the cancellation of almost 1,000 flights and stranded an estimated 140,000 passengers. The interruption cost the airport nearly £15 million in lost revenue, with the airlines losing as much as £70 million. Local police incurred expenses exceeding £459,000. To date, no suspects have been found. Just 17 months earlier, a drone flying near Gatwick resulted in operations being suspended for a period of 14 minutes. The interruption resulted in flight diversions and delays throughout the night, with some as long as three hours. These incidents serve as a wakeup call to airports - a failure to proactively protect aviation operations from rogue drones could end up being a costly decision.

To prevent such disruptions, the airspace around an airport needs to be protected and unauthorized Unmanned Aircraft System (UAS) activities need to be detected and reported at the earliest possible stage to flight crews, Air Traffic Control, airports and responsible authorities. In accordance with national regulations, neutralization<sup>3</sup> of the UAS, through the Unmanned Aircraft (UA), the Command & Control Datalink (C2 Link), the Remote Pilot Station (RPS) or even the Remote Pilot (RP), could be considered as part of a risk-based response.

In the past, the aviation system has relied mainly on flight crews or airport personnel to detect and report unauthorized UAS activities. This often meant that detection of these operations occurred after they had created a safety hazard. Today, there are only a few technical solutions available for detection of small UAS. There are currently no performance or interface requirements for those technologies.

In addition to the lack of mature detection tools and reporting processes, there is a lack of information to support rapid operational responses to threats or to identify the UAS operator for law enforcement purposes.

There is a need for actions targeting unauthorized UAS operations, such as contingency situations, careless operations, or malicious flight. Authorized UAS operations, especially professional operations, can be expected to follow rules and procedures to ensure safe conduct. This includes registering the UAS or operator, prior authorization for the planned operation (including access to specific airspace), and using proper identification and communication means. The implementation of a UAS Traffic Management (UTM, or U-space in Europe) capability will provide a valuable situational awareness capacity about cooperative UAS, operating in airspaces around airfields or in designated UTM/U-space airspaces.

Many nations have initiated projects to equip some airports (civilian and military) with a Counter UAS (C-UAS) capacity, including UAS detection and/or neutralization

<sup>1</sup> In the context of this document, the words "drone" and "unmanned aircraft" are equivalent. They both refer to the airborne component of a UAS.

<sup>2</sup> Example: [https://www.faa.gov/uas/resources/public\\_records/uas\\_sightings\\_report](https://www.faa.gov/uas/resources/public_records/uas_sightings_report)

<sup>3</sup> In the context of this document, the words "neutralization" and "mitigation" are equivalent. They both refer to the use of technical capabilities to disrupt, disable, seize control of, or destroy a suspect UAS. Further details in following chapters.

capabilities. A non-exhaustive list of European and international actors with an interest or involved in different forms of C-UAS activities is provided here:

- Competent Member State authorities, working independently or on a bi/multilateral basis;
- EU-funded law enforcement networks involving Member State authorities;
- EU-funded projects, including ones funded through Horizon 2020, the Internal Security Fund – Police (ISF-Police), the European Defence Industrial Development Programme (EDIDP), and the Permanent Structured Cooperation (PESCO) arrangement;
- Sectoral and cross-sectoral initiatives launched by individual Directorates-General (DGs) within the European Commission, including critical infrastructure protection (CIP), the protection of public spaces, and protection against chemical, biological, radiological and nuclear (CBRN) threats;
- EU Agencies, including the EU Aviation Safety Agency (EASA), the European Defence Agency (EDA), the European Border and Coast Guard Agency (EBCGA/Frontex), Europol and Cepol<sup>4</sup>;
- The EU Military Staff (EEAS) and relevant Common Security and Defence Policy (CSDP) missions, including civilian ones;
- International organizations, including NATO<sup>5</sup> and NATO-affiliated centres of excellence<sup>6</sup>, INTERPOL<sup>7</sup>, the Hybrid Centre of Excellence in Helsinki; EUROCONTROL.

EASA established in 2019 a Counter Drone Task Force to develop a strategy to improve the situation in Europe. The Task Force proposed an action plan (Ref. 21) including five objectives to provide guidance for Member States to mitigate the threat. These objectives are currently being addressed and partially involve individual working groups:

- Objective #1 – Educate the public to prevent and reduce misuse of drones around aerodromes;
- Objective #2 - Prepare aerodromes to mitigate risks from unauthorized drones use;
- Objective #3 – Support the assessment of the safety risk of drones to manned aircraft;
- Objective #4 – Ensure that C-UAS measures are swiftly considered and implemented from a global safety perspective;
- Objective #5 – Support adequate occurrence reporting.

The Federal Aviation Administration (FAA) recognized in May 2019 (Ref. 24) the airport authorities' safety and security concerns relative to malicious or errant use of UAS and provided information regarding UAS detection systems and the use of countermeasure or mitigation technologies.

In August 2020, consistent with Section 383 of the FAA Reauthorization Act of 2018 (FRA of 2018), the FAA launched the "Airport UAS Detection and Mitigation Research Program" (Ref. 23). This is an effort to test and evaluate technologies and systems that detect and mitigate potential aviation safety risks posed by UAS. The FRA of 2018 requires the FAA to work with the U.S. Department of Defense (DOD), Department of

<sup>4</sup>The Police School in Piła, Poland is responsible for organizing this year's Cepol course on "Unmanned Aerial Vehicles (drones) – threats and opportunities for Law Enforcement". The course was initially scheduled to be held in May 2020 but has since been postponed to the fall. Additional information is available [here](#).

<sup>5</sup>In early 2019, NATO adopted a C-UAS Practical Framework involving a number of different work strands and the creation of a C-UAS Working Group. One of the Practical Framework's priorities is interoperability standards development to be supported by the NATO Communications and Information Agency (NCIA).

<sup>6</sup>The NATO Counter-IED Center of Excellence in Madrid ([link](#)) is engaged in various C-UAS-relevant projects.

<sup>7</sup>Within INTERPOL, there are several different streams with C-UAS relevance, including one aimed at promoting incident reporting and another one focused on guidance-development. As an example, the organization recently published a "Framework for Responding to a Drone Incident for First Responders and Digital Forensics Practitioners".

Homeland Security (DHS) and other agencies to ensure that technologies and systems that are developed, tested, or deployed by federal departments and agencies to detect and mitigate potential risks posed by errant or hostile UAS operations do not adversely impact or interfere with safe airport operations, navigation, air traffic services, or the safe and efficient operation of the National Airspace System (NAS). In addition, the FRA of 2018 requires the FAA to develop a plan for the certification, permitting, authorizing or allowing of UAS detection and mitigation technologies and systems in the NAS. The FRA of 2018 also requires the FAA to take certain actions as part of the plan, including convening an Aviation Rulemaking Committee. Further, the FRA of 2018 requires the FAA to conduct an operational test and evaluation of technologies and systems that detect and mitigate risks posed by UAS at five airports, and directs the FAA to use detection and mitigation technologies and systems to detect and mitigate the unauthorized UAS operation that pose a risk to aviation safety as part of the required test and evaluation.

In August 2020, joint U.S. Government agencies (FAA, Department of Justice (DOJ), Federal Communications Commission (FCC) and DHS) issued an advisory guidance document (Ref. 40) to assist non-federal public and private entities interested in using technical tools, systems, and capabilities to detect and mitigate UAS. The advisory provides an overview of potentially applicable U.S. federal laws and regulations, as well as factors relevant to whether those laws may apply to particular actions or systems.

At its 40th Assembly in fall 2019 (Ref. 1), the International Civil Aviation Organization (ICAO) recognized the strong common message from Airports Council International (ACI), Civil Air Navigation Services Organisation (CANSO), International Federation of Air Traffic Controllers' Association (IFATCA), International Federation of Air Line Pilots' Associations (IFALPA) and International Air Transport Association (IATA) on "The need for standards and guidance to mitigate the risks of, and to improve response to unauthorized UAS operations".

Considering the urgent need by aircraft and airport operators, a C-UAS Working Group was created by EUROCAE in December 2019 with the task to develop the necessary standards specifying minimum performance and interoperability requirements. In February 2020, RTCA decided to create a Special-Committee that will work jointly with EUROCAE on this topic.

## 1.2 SCOPE

In the context recalled in the previous section, the scope of this Operational Services and Environment Definition (OSED) is to introduce the overall capability of a C-UAS System, including the detection capabilities of unauthorized UAS in a protected area of influence around an airport and address the resulting hazard or threat, in a risk-based balanced manner.

While focus is on the protection of airports, associated air traffic and surroundings, similar situations in different environments might also be considered, such as flight operation around critical infrastructure, over urban areas, major events or mass gatherings.

Threats considered in this document are the unauthorized UAS, conducting errant operations (i.e. malfunctions, clueless or careless operators) or malicious operations (i.e., intentional, criminal operators).

The OSED document provides a detailed description of the operational services of a C-UAS system, and the environment in which such a system will operate. It proposes operational requirements and associated assumptions that will be further detailed in the complementary standard documents: Safety and Performance Requirements (SPR) and Interoperability Requirements (INTEROP).

## 1.3 DOCUMENT STRUCTURE

The document is organized as follows:

- Chapter 1 Introduction: includes the intended purpose and scope of the document, a set of applicable and referenced documents, and a list of abbreviations and definitions;

- Chapter 2 Counter UAS Concept: introduces the UAS threat, the Counter UAS principles and the legal framework regarding their use;
- Chapter 3 Operational Services: describes the services, intended capabilities and associated process cycle of a C-UAS system;
- Chapter 4 Operational Environment: a detailed description of the environment in which a C-UAS system is intended to operate;
- Chapter 5 Tabletop Exercise Scenario Development: introduces a set of threat variables when developing UAS exercise scenarios and provides a high level classification of response scenarios;
- Appendix A Proposes a general open framework which allows to correlate available C-UAS capabilities with stakeholder's roles and responsibilities;
- Appendix B Provides a summary of the requirements and recommendations identified in this standard.

Final sections in the document include:

- The list of contributors to the document development;
- An Improvement Suggestion Form.

#### 1.4 RELATION TO OTHER PROJECTS

The following projects were instrumental in providing information of specific interest for the C-UAS OSED deliverable:

- EASA Counter-UAS action Plan;
- ALADDIN - Advanced hoListic Adverse Drone Detection, Identification and Neutralization Project<sup>8</sup>;
- ACI - Drones in the Airport Environment - ConOps & Guidance Material;
- Blue Ribbon Task Force on UAS Mitigation at Airports.

#### 1.5 REFERENCES

Documents listed below were considered as appropriate references:

1. ICAO Assembly 40th Session - Technical Commission A40-WP/196 "The need for standards and guidance to mitigate the risks of, and to improve response to unauthorized UAS operations"
2. ICAO Doc 10019 – "Manual on Remotely Piloted Aircraft Systems (RPAS)"
3. ICAO Annex 14 – Aerodromes, Volume I - Aerodrome Design and Operations & Volume II - Heliports
4. ICAO Annex 17 – Security
5. ICAO Annex 19 – Safety Management
6. ICAO Annex 10 (Draft under RPAS Panel) – Aeronautical Telecommunications Vol 4 Part II on Detect and Avoid
7. ICAO Doc 8973 – Chapter 19 (to be published), Protection of Civil Aviation Infrastructure against Unmanned Aircraft
8. ICAO Doc 9137 – Part 6, Control of Obstacles
9. ICAO Doc 9137 – Part 8, Airport Operational Services
10. ICAO Doc 9859 - Safety Management Manual
11. ICAO Doc 9981 - PANS ADR – Aerodromes
12. ICAO Doc 10084 - Risk Assessment Manual for Civil Aircraft Operations Over or Near Conflict Zones
13. ICAO Doc 10118 - Global Aviation Security Plan
14. ICAO Tool Kit - [Link](#)

---

<sup>8</sup> The ALADDIN project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 740 859

15. Commission Implementing Regulation (EU) 2017/373 laying down common requirements for providers of air traffic management/air navigation services and other air traffic management network functions and their oversight
16. Commission Delegated Regulation (EU) 2019/945 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems
17. Commission Delegated Regulation (EU) 2019/947 on the rules and procedures for the operation of unmanned aircraft
18. Commission Implementing Regulation (EU) 2020/639 amending Implementing Regulation (EU) 2019/947 as regards standard scenarios for operations executed in or beyond the visual line of sight
19. Commission Delegated Regulation (EU) 2020/1058 amending Delegated Regulation (EU) 2019/945 as regards the introduction of two new unmanned aircraft systems classes
20. DHS, Counter-Unmanned Aircraft Systems - Technology Guide, dated Sept 2019
21. EASA Counter-UAS action plan
22. FAA, "Law Enforcement Guidance for Suspected Unauthorized UAS Operations" Version 5 – Issued 8/14/2018
23. FAA, Airport Unmanned Aircraft Systems (UAS) Detection and Mitigation Research Program - [Link](#)
24. FAA, Letter and Attachments, dated May 7, 2019
25. FAA, Public Safety and Law Enforcement publication - [Link](#)
26. FAA, Concept of Use for the Airborne Collision Avoidance System (ACAS) Xu
27. FAA, UAS Remote Identification - [Link](#)
28. FAA, Airport Categories - [Link](#)
29. NATO Industrial Advisory Group SG-170, "The Engagement of Low, Slow and Small Aerial targets by GBAD (ground based aerial defense), 2013
30. A. Holland Michel, Counter-Drone Systems - 2nd edition (December 2019)
31. ACI, Drones in the Airport Environment - ConOps & Guidance Material
32. Blue Ribbon Task Force on UAS Mitigation at Airports – Final Report Oct. 2019
33. C. D. Baker, K. E. Polito, S. Pollack, (2016), Current Counter-Drone Technology Solutions to Shield Airports and Approach and Departure Corridors, University of Massachusetts
34. Unmanned Airspace - Counter-UAS Directory - [Link](#)
35. DHS, Science and Technology Directorate: Countering Unmanned Aircraft Systems 2017-05-03
36. EUROCAE, ED 258 OSED for Detect & Avoid [Traffic] in Class D-G airspace under VFR/IFR
37. EUROCONTROL ATM Lexicon - <https://ext.eurocontrol.int/lexicon>
38. Frequentis, White paper – Integrated counter-UAV solution for airports
39. JAPCC, "A Comprehensive Approach to Countering Unmanned Aircraft Systems" - [Link](#)
40. Joint U.S. Government Agency Advisory Guidance Document on use of systems and capabilities to detect and mitigate UAS, August 2020 - [Link](#)
41. National Urban Security Technology Laboratory (NUSTL), Counter-Unmanned Aircraft Systems Technology Guide, Sep 2019
42. RAND Corporation, Best, K et al., How to Analyze the Cyber Threat from Drones - Background, Analysis Frameworks and Analysis Tools, January 2020 - [Link](#)
43. Wallace, R.J. & Loffi, J.M., Examining Unmanned Aerial System Threats & Defenses: a Conceptual Analysis, International Journal of Aviation, Aeronautics, and Aerospace
44. RTCA, DO-365 MOPS for Detect and Avoid (DAA) Systems.
45. Sandia, UAS Detection, Classification, and Neutralization: Market Survey 2015

46. The MITRE Corporation, Small Unmanned Aircraft: Characterizing the Threat – February 2019
47. G. Markarian, A. Staniforth, "Countermeasures for Aerial Drones", Artech House, 2021

## 1.6

**ABBREVIATIONS****TABLE 1-1: ABBREVIATIONS**

| Abbreviation | Definition                                                                   |
|--------------|------------------------------------------------------------------------------|
| ACI          | Airports Council International                                               |
| ADS-B        | Automatic Dependent Surveillance - Broadcast                                 |
| ALADDIN      | Advanced hoListic Adverse Drone Detection, Identification and Neutralization |
| ANSP         | Air Navigation Service Provider                                              |
| APP          | Approach                                                                     |
| APT          | Airport                                                                      |
| ATC          | Air Traffic Control                                                          |
| ATM          | Air Traffic Management                                                       |
| ATS          | Air Traffic Service                                                          |
| C2 Link      | Command & Control Link (component of a UAS or RPAS)                          |
| CAA          | Civil Aviation Authority                                                     |
| CANSO        | Civil Air Navigation Services Organisation                                   |
| CBRN         | Chemical, Biological, Radiological and Nuclear                               |
| CEPT         | European Conference on Postal and Telecommunications                         |
| CNS          | Communication, Navigation and Surveillance                                   |
| CSDP         | Common Security and Defence Policy                                           |
| C-UAS        | Counter Unmanned Aircraft System                                             |
| DG           | Directorates-General                                                         |
| DHS          | U.S. Department of Homeland Security                                         |
| DOD          | Department of Defense                                                        |
| EASA         | European Union Aviation Safety Agency                                        |
| EBCGA        | European Border and Coast Guard Agency                                       |
| ECC          | Electronic Communications Committee                                          |
| EDA          | European Defence Agency                                                      |
| EDIDP        | European Defence Industrial Development Programme                            |
| EMP          | Electro Magnetic Pulse                                                       |
| EO           | Electro Optical                                                              |
| EU           | European Union                                                               |
| FAA          | Federal Aviation Administration                                              |
| FCC          | Federal Communications Commission                                            |
| GIS          | Graphical Interface System                                                   |
| GNSS         | Global Navigation Satellite System                                           |

|         |                                                                  |
|---------|------------------------------------------------------------------|
| HF      | High Frequency                                                   |
| HMI     | Human Machine Interface                                          |
| IATA    | International Air Transport Association                          |
| ICAO    | International Civil Aviation Organization                        |
| IFALPA  | International Federation of Air Line Pilots' Associations        |
| IFATCA  | International Federation of Air Traffic Controllers' Association |
| IFR     | Instrument Flight Rules                                          |
| INTEROP | Interoperability Requirements                                    |
| IR      | InfraRed                                                         |
| ISF     | Internal Security Fund                                           |
| ITU     | International Telecommunication Union                            |
| LEA     | Law Enforcement Authority                                        |
| LIDAR   | Light/Laser Detection And Ranging                                |
| LOS     | Line Of Sight                                                    |
| NATO    | North Atlantic Treaty Organization                               |
| NCIA    | NATO Communications and Information Agency                       |
| NIAG    | NATO Industrial Advisory Group                                   |
| NTIA    | National Telecommunications and Information Administration       |
| OPT     | Optional Requirement                                             |
| OSD     | Operational Services and Environment Definition                  |
| PESCO   | Permanent Structured Cooperation                                 |
| PD      | Personal Data                                                    |
| PII     | Personally Identifiable Information                              |
| REC     | Recommendation                                                   |
| REQ     | Requirement                                                      |
| RF      | Radio Frequency                                                  |
| RFI     | Radio Frequency Interference                                     |
| RP      | Remote pilot                                                     |
| RPAS    | Remotely Piloted Aircraft System                                 |
| RPS     | Remote Pilot Station                                             |
| SOP     | Standard Operating Procedures                                    |
| SPR     | Safety and Performance Requirements                              |
| TCA     | Terminal Control Area                                            |
| TMA     | Terminal Maneuvering Area                                        |
| TWR     | Tower                                                            |
| UA      | Unmanned Aircraft                                                |
| UAS     | Unmanned Aircraft System                                         |
| UHF     | Ultra-High Frequency                                             |

|     |                                      |
|-----|--------------------------------------|
| UTM | UAS Traffic Management               |
| VFR | Visual Flight Rules                  |
| VHF | Very High Frequency                  |
| WRC | World Radiocommunication Conferences |

## 1.7 DEFINITIONS

**TABLE 1-2: DEFINITIONS**

| Term                | Definition                                                                                                                                                                                                                                                                                                                                                                                                             | Source                                                        |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| Aerodrome           | A defined area on land or water (including any buildings, installations and equipment) intended to be used either wholly or in part for the arrival, departure and surface movement of aircraft                                                                                                                                                                                                                        | ICAO (Ref. 25)                                                |
| Airport             | Airport means an area of land or water that is used or intended to be used for the landing and takeoff of aircraft, and includes its buildings and facilities, if any<br><br>The term airport may imply a certain stature (having satisfied certain certification criteria or regulatory requirements) that an aerodrome may not have. Therefore, whilst all airports are aerodromes, not all aerodromes are airports. | 14 CFR § 1.1<br><br>ACI (Ref. 31)                             |
| Authorized (UAS)    | Any drone activity with authority or permission to operate in the aerodrome environment<br><br>UAS for which operation in the airport airspace is known and approved.                                                                                                                                                                                                                                                  | Adapted from ACI (Ref. 31)<br><br>Developed for this document |
| Counter UAS (C-UAS) | Set of technological and operational tools to monitor, detect, identify, record and enable response to unauthorized UAS activities; C-UAS may also include countermeasures capable to neutralize, or limit, potential risks, in a risk-based balanced manner                                                                                                                                                           | Developed for this document                                   |
| C-UAS process cycle | It represents the end to end processes that make up the C-UAS events, including different operational capabilities such as detection, decision, neutralization and post incident actions<br><br><i>Alternative Terms are considered equivalent such as C-UAS processing chain, C-UAS</i>                                                                                                                               | Developed for this document                                   |
| Classification      | A stage at which a sensor of some sort has sufficient information to sort a target into a certain class                                                                                                                                                                                                                                                                                                                | Adapted from technical literature for this document           |
| Collaborative (UAS) | See Authorized (UAS)<br><br><i>In this document, “collaborative (UAS)” is used similarly to “authorized (UAS)”</i>                                                                                                                                                                                                                                                                                                     | Developed for this document                                   |
| Command and Control | A part of the C-UAS system specialized in commanding and controlling all the C-UAS elements, providing to the operator a real time surveillance picture resulting from processing and fusing all available information. It provides different tools for analyzing and managing detected incursions and threat, including the interaction and cooperation with other systems.                                           | Adapted from technical literature for this document           |

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                              |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| Command and Control (C2) link | The data link between the remotely piloted aircraft and the remote pilot station for the purposes of managing the flight.                                                                                                                                                                                                                                                                                                                          | ICAO (Ref. 2)                                                                |
| Control Unit                  | Means the equipment or system of equipment to control unmanned aircraft remotely as defined in point 32 of Article 3 of the Regulation (EU) 2018/1139, with the exception of any infrastructure supporting the C2 link service, which supports the control or the monitoring of the unmanned aircraft or both during any phase of the flight<br><i>See also Remote Pilot Station</i>                                                               | EU (Ref. 18 and Ref. 19)                                                     |
| Cooperative (UAS)             | UAS equipped with a functioning means of electronic identification (e.g., Mode A/C or S transponder, ADS-B Out or e-Identification) aboard and operating.                                                                                                                                                                                                                                                                                          | Adapted from ICAO (Ref. 6), FAA (Ref. 26), EUROCAE (Ref. 36), RTCA (Ref. 44) |
| Detection                     | 1) Global: Set of capabilities, technologies and procedures used to get the situational awareness in real time about the UAS operating in the airport airspace. Global detection stream includes four stages: detection, tracking, classification, and identification.<br><br>2) Initial: First stage of the global detection stream. Initial detection refers to the capability to recognize the presence of an object in a location or ambiance. | Adapted from technical literature for this document                          |
| Direct remote identification  | Means a system that ensures the local broadcast of information about a UA in operation, including the marking of the UA, so that this information can be obtained without physical access to the UA<br><i>See “e-Identification”</i>                                                                                                                                                                                                               | EU (Ref. 16)                                                                 |
| Disruption of operations      | The interruption of airport ground-based or airborne flight operations, due to an established risk from unauthorized UAS                                                                                                                                                                                                                                                                                                                           | Developed for this document                                                  |
| e-Identification              | The ability of a UAS to provide electronic information about a UA in operation that can be received by other parties.<br><i>In this document, the word “e-Identification” is used similarly to the following terms: Remote Identification and Direct Remote Identification</i>                                                                                                                                                                     | Adapted from existing definitions (ICAO, EU Regulation)                      |
| Hazard                        | 1) A condition or an object with the potential to cause injuries to personnel, damage to equipment or structures, loss of material, or reduction of the ability to perform a prescribed function<br><br>2) A condition or an object with the potential to cause or contribute to an aircraft incident or accident                                                                                                                                  | ICAO (Ref. 10)<br><br>ICAO (Ref. 5)                                          |
| Identification                | An ability to recognize an airborne vehicle sufficiently in order to categorize it and have an ability to assign the contact with a threat level. Available supplemental information can be used to further refine the context of the threat."                                                                                                                                                                                                     | Adapted from technical literature for this document                          |
| Layer                         | Each of the processes that support the C-UAS cyclic sequence (C-UAS process cycle). Layers build upon each other and include some support protocols to achieve a comprehensive C-UAS Operational Services System.                                                                                                                                                                                                                                  | Developed for this document                                                  |

|                                  |                                                                                                                                                                                                                                                                           |                                                                              |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
|                                  | <i>In this document, layer is used similarly to phase</i>                                                                                                                                                                                                                 |                                                                              |
| Malicious                        | Intended to create a hazard                                                                                                                                                                                                                                               | Developed for this document                                                  |
| Mitigation/<br>Mitigate          | Mitigate is often used interchangeably with negate, interdict or neutralize. It describes the methods used to remove or reduce the threat posed by a UAS<br><i>See neutralization</i>                                                                                     | DHS (Ref. 20)                                                                |
| Neutralization                   | Refers to capabilities, technologies, and procedures used to reduce partially or fully the severity of one or multiple unauthorized UAS threat, disrupting or disabling their normal operation<br><i>In this document, neutralization is used similarly to mitigation</i> | Developed for this document                                                  |
| Non-collaborative (UAS)          | See unauthorized (UAS).<br><i>In this document, non-collaborative is used similarly to unauthorized</i>                                                                                                                                                                   | Developed for this document                                                  |
| Non-cooperative (UAS)            | UAS not equipped with an electronic means of identification (e.g., a transponder or ADS-B or e-identification) or not operating such equipment due to malfunction or deliberate action.                                                                                   | Adapted from ICAO (Ref. 6), FAA (Ref. 26), EUROCAE (Ref. 36), RTCA (Ref. 44) |
| Operator                         | 1) A person, organization or enterprise engaged in or offering to engage in an aircraft operation.<br>2) Person who uses/operates the C-UAS equipment.                                                                                                                    | ICAO (Ref. 2)                                                                |
| Phase                            | See layer<br><i>In this document, phase is used similarly to layer</i>                                                                                                                                                                                                    |                                                                              |
| Recognize                        | Be aware that an air vehicle, which may or may not pose a threat, is within the area of interest                                                                                                                                                                          | Adapted from technical literature for this document                          |
| Remote Identification            | Remote Identification (or Remote ID) is the ability of a UAS in flight to provide identification information that can be received by other parties.<br><i>See “e-identification”</i>                                                                                      | FAA (Ref. 27)                                                                |
| Remote Pilot                     | A person charged by the operator with duties essential to the operation of a remotely piloted aircraft and who manipulates the flight controls, as appropriate, during flight time.                                                                                       | ICAO (Ref. 2)                                                                |
| Remotely Piloted Aircraft        | An unmanned aircraft which is piloted from a remote pilot station.                                                                                                                                                                                                        | ICAO (Ref. 2)                                                                |
| Remotely Piloted Aircraft System | A remotely piloted aircraft, its associated remote pilot station(s), the required C2 Link and any other component as specified in the type design.                                                                                                                        | ICAO (Ref. 2)                                                                |
| Remote Pilot Station             | The component of the remotely piloted aircraft system containing the equipment used to pilot the remotely piloted aircraft.<br><i>See also Control Unit</i>                                                                                                               | ICAO (Ref. 2)                                                                |
| Risk                             | The combination of the overall probability or frequency of occurrence of a harmful effect induced by a hazard and the severity of that effect.                                                                                                                            | EU (Ref. 15)                                                                 |
| Safety                           | The state in which risks associated with aviation activities, related to, or in direct support of the                                                                                                                                                                     | ICAO (Ref. 5)                                                                |

|                           |                                                                                                                                                                                                                                                                                                                                                              |                                                     |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|
|                           | operation of aircraft, are reduced and controlled to an acceptable level                                                                                                                                                                                                                                                                                     |                                                     |
| Security                  | Safeguarding civil aviation against acts of unlawful interference. This objective is achieved by a combination of measures and human and material resources.                                                                                                                                                                                                 | ICAO (Ref. 4)                                       |
| Stakeholder               | A person or organization that has a direct or indirect impact related to C-UAS Regulations, Performance, Operational guidance.                                                                                                                                                                                                                               | Adapted from existing literature                    |
| (Drone) Swarm             | A group of behaving entities that together coordinate to produce a significant or desired result or behavior.                                                                                                                                                                                                                                                | Adapted from existing literature                    |
| Threat                    | A man-made occurrence, individual, entity, or action that has, or indicates, the potential to harm life, information, operations, the environment and/or property.                                                                                                                                                                                           | ICAO (Ref. 12)                                      |
| Track                     | An ability to provide an updated geographical reference point in 2 or 3 dimensions and if possible, make a historical trace on a local area map, where any perceived target/threat was first detected and be able to plot its progress                                                                                                                       | Adapted from technical literature for this document |
| Unauthorized (UAS)        | Any UAS with activity in the airport airspace without authority or permission, which could result in safety/security risk and/or have a negative impact on business continuity and/or reputation                                                                                                                                                             | Adapted from ACI (Ref. 31)                          |
| Unmanned Aircraft         | Any aircraft intended to be flown without a pilot on board is an unmanned aircraft. They can be remotely and fully controlled from another place (ground, another aircraft, space) or pre-programmed to conduct its flight without intervention. Unmanned Aircraft classification includes Remotely piloted aircraft, Autonomous aircraft and Model aircraft | ICAO (Ref. 2)<br>ICAO (Ref. 14)                     |
| Unmanned Aircraft Systems | An aircraft and its associated elements which are operated with no pilot on board.                                                                                                                                                                                                                                                                           | ICAO (Ref. 14)                                      |

## CHAPTER 2

### COUNTER-UAS CONCEPT

#### 2.1 THE UAS THREAT

UAS is considered a threat when its operation has, or indicates, the potential to harm life, information, operations, environment and/or property, especially in the case of manned air traffic and airports. Such operation can have negative impact in terms of safety, security, privacy or environment, affecting airspace users, people on the ground, critical infrastructure, etc.

A threat appears when the operation of UAS is performed in a non-collaborative way, meaning the UAS is operated without authorization in a controlled airspace or without information exchange with Air Traffic Control (ATC), or UAS Traffic Management (UTM) services / U-space (if available).

This is particularly true for small UA, as current ATC primary surveillance systems (mainly radar) are not designed to detect this type of aircraft. It is also expected that UAS threats will mostly operate as non-cooperative aircraft, lacking any cooperative devices, such as transponder, ADS-B (or the Remote ID when available), that is considered by ATC secondary surveillance systems.

**NOTE:** *It is not possible to specify a precise quantitative value for “small” related to the detection limits or the associated level of risk. Multiple available UAS classifications exist with different quantitative criteria about “small”, for example, NATO Class I UAS (less than 150Kg), EASA Open category (less than 25Kg), DOD Cat 1 or 2 (less than 55lbs).*

**NOTE:** *UA presents multiple forms of flight characteristics (speed, altitude and maneuvers) and autonomy.*

A threat situation can result from the use of only one to multiple UAS, in coordinated or uncoordinated operations. The use of UAS swarms represents the most complex case.

Multiple factors can influence threat level, such as those related to the threat character or probability. Typically, the higher threat level, the less occurrence probability.

Finally, according to the intent of the operator, an UAS threat can be classified in one of these categories: (1) Malfunctioning or uncontrolled UAS behavior due to external factors (e.g. electromagnetic interference), (2) Clueless operators who are operating without any awareness they are causing a hazard. (3) Careless operators who are operating without regard for potential consequences (4) Criminal operators (including terrorism) who are operating intentionally in a hazardous and malicious way.

#### 2.2 COUNTER UAS

##### 2.2.1 Existing C-UAS tools and methods

Arthur Holland Michel and Dan Gettinger provided an overview of existing C-UAS in their appreciated contribution to the Joint Activity WG-115/SC-238:

*“In a survey conducted in 2015, researchers at the Sandia National Laboratories identified a dozen dedicated C-UAS systems available for acquisition that year. Less than five years later, a 2019 study by the Center for the Study of the Drone at Bard College found more than 500 products on offer. Given the increasing integration of small UAS into modern life, C-UAS is set to become a fundamental aspect of airspace safety and security.*

*Existing C-UAS systems rely on a variety of techniques for detecting and neutralizing UAS, but despite advancements in technology over the past few years, the technical challenge of countering drones has not yet been fully surmounted. No C-UAS system is perfect and the issue is compounded by a lack of standards for the design and use of C-UAS system, as well as reliable test and operational data.*

*Given the intense interest and massive investment in C-UAS in recent years, many of these shortcomings may be addressed in the years ahead. However, UAS technology itself is not standing still, and advances in this area will pose new challenges from a C-UAS perspective.”*

## 2.2.2 C-UAS concept and generic high-level architecture

C-UAS refers to a set of technological and operational tools to monitor, detect, identify, record and enable response to unauthorized UAS activities; C-UAS may also include countermeasures capable to neutralize, or limit, potential risks, in a risk-based, balanced manner.

As a system of systems, a C-UAS system is typically composed of several complementary components, namely command and control, detection sensors and countermeasures, interfaces and protocols to support interaction with other systems and stakeholders involved in the C-UAS stream and tools for information recording and post-analysis.

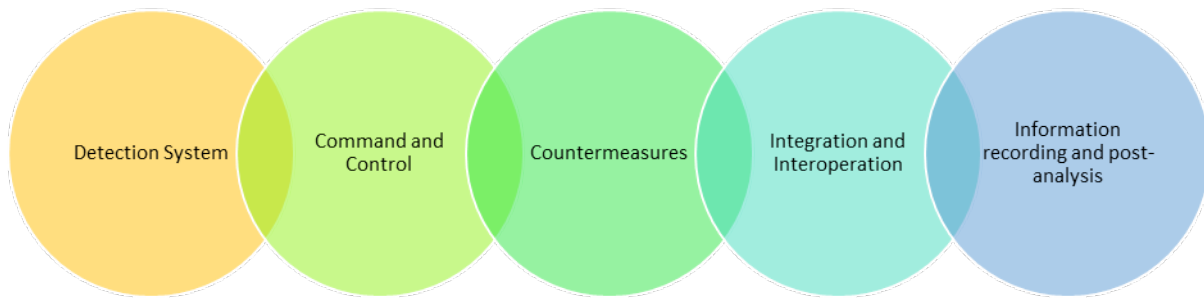


**FIGURE 2-1: HI-LEVEL C-UAS COMPONENTS**

C-UAS system provides protection under two complementary processes in accordance with standard operating procedures:

1. Safety: C-UAS protects from interference with safe aircraft operation during apron operations, taxi, takeoff and landing;
2. Security: C-UAS protects airport infrastructure from unlawful interference and threats to people, property, privacy, etc.

[REQ:1] The C-UAS system shall provide support for both security and safety.

Different types of deployment can be considered: C-UAS system placed in fixed positions (stationary), mounted on vehicles or drones (mobile/non-permanent), or portable (hand-held).

### 2.2.2.1 Detection system

The detection system provides real time situational awareness information to the C-UAS system by monitoring key areas according to the stakeholder needs. Its main goal is to support early and agile detection, location, tracking, classification and identification of unmanned aircraft system(s) based on deployment of one or more sensors of the same or different type operating in a complementary manner. Some technologies, such as RF sensing, can also support the detection of the RPS.

Multiple sensing technologies are available:

- Radar;
- Radiofrequency (RF);
- Electro-optical (EO), considering both infrared (IR) and visible cameras;
- Acoustic;
- E-Identification;
- Etc.

**NOTE:** Human sensing capabilities, like sight and hearing, can also contribute to the detection but they have a highly limited performance.

Sensing technologies can be classified in two groups depending on if they radiate or not:

- Active (for example, radar, LIDAR, ...);
- Passive (for example, radio-frequency sensors, electro-optical, acoustic, passive radar, etc.).