

RTCA, Inc.
1150 18th Street NW, Suite 910
Washington, DC 20036
USA

Operational Services and Environment Definition (OSED) for Counter-UAS in Controlled Airspace

RTCA Paper No. 0-2-21/PMC-2118

RTCA DO-389
March 18, 2021

Prepared by: SC-238
© 2021 RTCA, Inc.

Copies of this document may be obtained from
RTCA, Inc.
Telephone: 202-833-9339
Facsimile: 202-833-9334
Internet: www.rtca.org

Please visit the RTCA Online Store for document pricing and ordering information.

FOREWORD

This document was prepared by Special Committee 238 (SC-238) jointly with EUROCAE WG-115 and approved by the RTCA Program Management Committee (PMC) and the EUROCAE Council on March 18, 2021.

RTCA, Incorporated is a not-for-profit corporation formed to advance the art and science of aviation and aviation electronic systems for the benefit of the public. The organization functions as a Standards Development Organization and develops consensus-based recommendations on contemporary aviation issues. RTCA's objectives include but are not limited to:

- coalescing aviation system user and provider technical requirements in a manner that helps government and industry meet their mutual objectives and responsibilities;
- analyzing and recommending solutions to the system technical issues that aviation faces as it continues to pursue increased safety, system capacity and efficiency;
- developing consensus on the application of pertinent technology to fulfill user and provider requirements, including development of minimum operational performance standards for electronic systems and equipment that support aviation; and
- assisting in developing the appropriate technical material upon which positions for the International Civil Aviation Organization and the International Telecommunication Union and other appropriate international organizations can be based.

The organization's recommendations are often used as the basis for government and private sector decisions as well as the foundation for many Federal Aviation Administration Technical Standard Orders and advisory circulars.

Since RTCA is not an official agency of the United States Government, its recommendations may not be regarded as statements of official government policy unless so enunciated by the U.S. government organization or agency having statutory jurisdiction over any matters to which the recommendations relate.

DISCLAIMER

This publication is based on material submitted by various participants during the SC approval process. Neither the SC nor RTCA has made any determination whether these materials could be subject to valid claims of patent, copyright or other proprietary rights by third parties, and no representation or warranty, expressed or implied is made in this regard. Any use of or reliance on this document shall constitute an acceptance thereof "as is" and be subject to this disclaimer.

This Page Intentionally Left Blank

TABLE OF CONTENTS

1	PURPOSE AND SCOPE.....	1
1.1	Introduction.....	1
1.2	Scope.....	4
1.3	Document structure.....	4
1.4	Relation to other Projects.....	5
1.5	References.....	5
1.6	Abbreviations.....	7
1.7	Definitions.....	10
2	COUNTER-UAS CONCEPT.....	15
2.1	The UAS Threat.....	15
2.2	Counter UAS.....	16
2.2.1	Existing C-UAS tools and methods.....	16
2.2.2	C-UAS concept and generic high-level architecture.....	16
2.2.2.1	Detection system.....	17
2.2.2.2	Command & Control System.....	18
2.2.2.3	Countermeasures System.....	19
2.2.2.4	Integration and Interoperation.....	19
2.2.2.5	Information recording and post-analysis.....	20
2.2.3	Benefits, constraints and other considerations.....	20
2.2.3.1	Benefits.....	20
2.2.3.2	Constraints.....	20
2.2.3.3	Other considerations.....	21
2.3	High level legal framework.....	22
2.3.1	General issues.....	22
2.3.2	Active RF emitters.....	22
2.3.3	Privacy laws.....	23
2.3.4	Airport regulations.....	23
2.3.4.1	RF Interference.....	24
2.3.4.2	Personnel Safety.....	24
2.3.4.3	Obstacle Clearance.....	24
3	OPERATIONAL SERVICES.....	25
3.1	Introduction.....	25
3.2	Detection.....	26
3.2.1	Detection, location and tracking.....	27
3.2.2	Classification and Identification.....	27
3.2.3	Data Collection.....	28
3.2.4	Types of detection technologies.....	28
3.2.5	Limitations and Possible Impacts of detection technologies.....	29
3.3	Decision Support.....	30
3.3.1	Threat Analysis.....	30
3.3.2	Alerts.....	31
3.3.3	Incident Response.....	31
3.3.4	Neutralization determination.....	31

3.4	Neutralization.....	32
3.5	POST INCIDENT ACTIONS.....	33
4	OPERATIONAL ENVIRONMENT	37
4.1	Environment Identification	37
4.2	Airport and air traffic	37
4.2.1	Airport type and mix of traffic.....	37
4.2.2	Quantity and density of airspace traffic	38
4.2.3	Associated airspace type	38
4.2.4	Communication, Navigation and Surveillance systems.....	39
4.3	Traffic Management.....	40
4.3.1	Air Traffic Management	40
4.3.2	Air Traffic Control Systems.....	40
4.3.3	UAS Traffic Management.....	41
4.4	Actors	41
4.5	Other surroundings and environments	42
4.5.1	The vicinity area	43
4.5.2	Electromagnetic interference	43
4.5.3	Atmospheric conditions	43
5	TABLETOP EXERCISE SCENARIO DEVELOPMENT.....	44
5.1	LOW IMPACT SCENARIO	45
5.2	medium impact scenario	45
5.3	high impact scenario	45
6	MEMBERSHIP	46
	APPENDIX A GENERAL OPEN FRAMEWORK FOR C-UAS.....	A-1
	APPENDIX B SUMMARY OF REQUIREMENTS.....	B-1

TABLE OF FIGURES

Figure 2-1:	Hi-level C-UAS COMPONENTS.....	16
Figure 3-1:	Diagram of the C-UAS tower approach.....	26
Figure A-1	General C-UAS Framework.....	A-4

TABLE OF TABLES

Table 1-1:	Abbreviations	7
Table 1-2:	Definition	10
Table 3-1:	Sample of C-UAS Detection technics	28
Table 3-2:	Limitation and impact of C-UAS detection technologies.....	29
Table 3-3:	representative subset of neutralization capabilities	32
Table A-1:	Definition of Roles	A-1
Table A-2:	Template For C-Uas Roles And Responsibilities.....	A-2
Table B-1:	Summary of Requirements	B-1
Table B-2:	Summary of Recommendations.....	B-3
Table B-4:	Summary of Optional Requirements	B-4

1 PURPOSE AND SCOPE

1.1 INTRODUCTION

For many years, nations have recognized the many positive use cases for drones - or unmanned aircraft¹ - 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 reported², 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 45 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, neutralization³ of the UAS, through the Unmanned Aircraft (UAS) 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.

¹ In the context of this document, the words “drone” and “unmanned aircraft” are equivalent. They both refer to the airborne component of a UAS.

² Example: https://www.faa.gov/uas/resources/public_records/uas_sightings_report

³ 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.