DRONES

IN THE AIRPORT ENVIRONMENT:

CONCEPT OF OPERATIONS & INDUSTRY GUIDANCE

TABLE OF CONTENTS

ANNEXES **51**

FIGURES

INTRODUCTION

1

1. Introduction

Unmanned Aircraft Systems (UAS), Remotely Piloted Aircraft Systems (RPAS) or 'drones[1]' as they are commonly known have seen a rapid technological development in recent years and probably will continue to do so in the future. The number of applications seems endless but some realism has to be applied too, in order to manage expectations. One of these realities is that you cannot fly drones everywhere and anytime. One of the areas where this is obvious is within the vicinity of airports (at airports or within the airport perimeter).

Concerning drones, the main challenge for many airport communities is to find the right balance between business opportunities (advantages) and challenges/risks (disadvantages). Special attention needs to be given to manage the different risks effectively.

In February 2019, the ACI EUROPE Drone Task Force was formed with the aim of discussing drone operations at airports with all relevant stakeholders, not only to exchange information but also to provide guidance on how drone operations could be facilitated, whilst ensuring the necessary safety and security levels at airports. It was agreed that one of the deliverables should be a Concept of Operations (ConOps), designed to provide clarity and recommendations to the airport community (airport operators, air traffic control, surveillance units, drone operators, etc.), as well as the regulation and standardisation bodies (European Commission, EASA, Civil Aviation Authorities, EUROCAE, etc.).

This ConOps is intended to exceed the general concept of operations as it includes background information, a number of recommendations and reference material in the Annex. The idea is that stakeholders involved in airport drone operations can find the most relevant information they would need to get themselves organised, without the need to look elsewhere.

It is the desire of ACI EUROPE that this Concept Document will become the recognised reference material for drone operations in the airport environment, serving multiple stakeholders.

ACI EUROPE also hopes that the principles of operating with drones in the airport environment described in this document will inspire Regulators and Competent Authorities to embrace the ideas and recommendations, and work together with all stakeholders, including standardisation bodies, to develop technical and operational standards across Europe based on this document.

Finally, it is important to recognise that it is essential to inform and educate the general public about the risks posed by operating drones within/near any airport environment, and that the mindset should be, "I should not operate drones near airports". This message needs to be clear, simple and easily available to the general public, including 'do's and don'ts'. [2]

1. The generic term 'drone' will be used in this concept document when feasible to facilitate easy reading.
2. Some useful information/guidelines can be found in the Annex under Regulations and Useful Links.

OBJECTIVES

2

2. Objectives

The aim of this Concept of Operations (ConOps) is to describe how drones could safely be used in the airport environment, taking into account both safety and security aspects (amongst others).

The key element will be to describe which essential items will need to be considered before any drone operations can be conducted, to prevent unauthorised drones operating at/near the airports and what arrangements need to be put in place in order to keep risks at an acceptable level (or mitigate them, as appropriate). In this context, it is essential to have a clear understanding of the differences between cooperative and non-cooperative drones, the roles and responsibilities of the different actors and the actions to be taken in the different scenarios.

The targeted audiences[3] of this Concept Document are:

- Regulators (at both European and national level)
- Airport Operators
- Air Traffic Control organisations (ANSPs[4])
- Law Enforcement Authorities.

Other stakeholders that may have an interest in this Concept Document are:

- Drone Operators
- Aircraft Operators
- Drone Manufacturers (industry)
- Standardisation bodies
- Citizens.

It should be borne in mind that drone technologies are being developed at a rapid pace, with the risk that within 2 years parts of the information described in this document will become outdated and would need an update in order to stay relevant. Therefore, as much as feasible, this document stays away from the technological aspects, but rather concentrates on generic descriptions (conceptual level) and providing best practices/recommendations.

In order to achieve the goals outlined above, this concept document will mainly focus on four essential questions:

WHO?	WHAT?	WHERE?	WHEN?
Identify stakeholders	Scope	Airport environment	Normal Ops
Roles & Responsibilities	Operational Concept	Zones	Abnormal Ops
	Prerequisites		
	Access Request Process		
	Risk Assessment		
	Coordination		
	Communication		
	Use Cases		

3. The focus of this document will be on the actors rather than the generic stakeholder. See Annex H (Glossary and Abbreviations) for description of Actor and Stakeholder.
4. Air Navigation Service Providers.

SCOPE

3

3. Scope

One of the challenges faced with drones is the wide scope of (potential) applications in which they could be used. The list is almost endless ([5]) and we will not endeavour to be comprehensive. A (limited) number of applications will be described in the Standardised Use Case library (see Annex) which should be seen as an 'add-on' to the generic principles outlined in the main document.

Inclusions

- Description of the Roles & Responsibilities
- Description of the Airport Environment
- Description of the Prerequisites
- Description of the Operational Concept
- Safety Management
- Security Management
- Coordination & Communication.

Exclusions

- Drone operations outside the UAS Geographical Zones
- Military and other non-public airports
- Urban air mobility (transport of people to/from urban areas)[6].

The U-Space concept will only be explained briefly. See 'Operational Concept' for more information.

5. https://en.wikipedia.org/wiki/List_of_unmanned_aerial_vehicle_applications
6. It may be included in a future update of this Concept Document, depending on developments.

ROLE & RESPONSIBILITIES

4

4. Roles & Responsibilities[7]

Concerning drone-operations in an airport environment, several key actors might be required to interact in different phases of the process. The following main actors - inter alia - have been identified:

- Competent Authorities
- Law Enforcement Authorities
- Airport Operators
- Air Navigation Service Providers (ANSPs)
- UTM/U-Space Service Provider(s)
- Drone operators
- Drone pilots
- Manned aircraft pilots
- Drone manufacturers
- Citizen(s).

The table below describes their typical roles and responsibilities:

Role	Responsibility
Competent Authority	The competent authority is the recognised authority for approving the safety case of drone operations. The competent authority should address the following domains: • Drone design and drone operation • Aerodrome operation • Air Navigation Service.
Law Enforcement Authority (LEA)	(Generally called police services) is any government agency responsible for the enforcement of the (civil) laws. At civil/military operated airports, this role is typically performed by the military authorities. The responsibilities of the Law Enforcement Authority vary from country to country but in relation to drones typically cover **policing of airports and protection of designated national infrastructure and national security**. Law Enforcement Authorities are responsible to counteract non-cooperative drones and any illegal drone activity, and take appropriate mitigating actions.

7. The Roles and Responsibilities described in this chapter are conceptual and, therefore, generic. It is intended as industry guidance. (Local) regulations and circumstances may need other arrangements.

Airport Operator[8]	The Airport Operator has to ensure the collection of all necessary drone operations approvals (in close consultation with the ANSP). Approval consideration will include – but is not limited to – the following aspects: • Operational need/business case • Type of drone operation • Safety aspects • Security aspects • Capacity impact. The airport operator should also be responsible for the coordination of drone activities with the other actors (ANSP, drone operator). A coordination and communications protocol should be made available to all actors involved. The airport operator can (typically) only be held responsible for activities inside the airport boundaries. For (drone) activities outside the airport perimeter, the responsible entity for that area needs to ensure that appropriate arrangements have been made since the drone activities may fall outside the airport jurisdiction.
Air Navigation Service Provider (ANSP)	The ANSP is the designated provider of air traffic service in a specific area of operation (airspace). The ANSP assesses whether the proposed operation can be safely conducted in the particular airspace that they cover, and what additional arrangements need to be made to obtain authorisation. The ANSP finally authorises the drone operation at a given time (for uncontrolled aerodromes the authorisation will be typically provided by the airport operator). The ANSP is responsible for monitoring drones, and should enable airport operators to keep track as well (by means of appropriate arrangements).
UTM / U-Space Service Provider	UTM/U-Space Service Providers are entities that provide services to support safe and efficient use of airspace. These services may support an operator's compliance with their safety obligation and associated Risk Assessment.[9]

8. At Mil/Civ airports, the (military) airport operator typically will make its own arrangements, assessments and arrange approvals. However, the military are more than welcome to use this ConOps for guidance and make arrangements based on its recommendations.
9. See Annex D 'Risk Assessment' and E (Workflow/Checklist).

Drone Operator	The drone operator is responsible for safe operation of the UAS and hence the safety risk analysis (to be complemented by a safety/risk assessment by the responsible entity giving the drone operations approval). The operator must substantiate the safety of the operation by performing the specific operational and risk assessment. Supporting material for the assessment may be provided by third parties (e.g. the manufacturer of the UAS or equipment, UTM service providers, etc.). Once the requirements are met, the operator obtains an operational authorisation from the Competent Authority. Secondly, the drone operator will need to obtain the operational approval of UAS operations in/near an airport environment (UAS Geographical Zone), which are the responsibility of the airport operator/ANSP involved.
Drone Pilot	The pilot is designated by the drone operator or is the drone owner, as being in command and charged with the safe conduct of the drone flight.
Manned Aircraft Pilot	The pilot is designated by the aircraft operator/owner as being in command and charged with the safe conduct of the flight.
Drone Manufacturer	For the purposes of the SORA,[10] the drone manufacturer is the party that designs and manufactures the UAS. The manufacturer/designer has unique design evidence (e.g. system performance, system architecture, software/hardware development documentation, test/analysis documentation, etc.) that they may choose to make available to one or many drone operator(s) or the competent authority to help substantiate the operator's safety case. Alternatively, a potential UAS manufacturer may utilise the SORA to target design objectives for specific or generalised operations. To obtain airworthiness approval(s), these design objectives could be complemented by use of JARUS[11] Certification Specifications (CS) or industry consensus standards if they are found acceptable by the competent authority.
Citizens (general public)	Citizens should familiarise themselves with the restrictions of drone operations in the airport vicinity. They shall inform the airport operator (or designated party) without any delay if they see (assumed) unauthorised drone operations and help authorities to identify the drone position/movement and its operator/drone pilot.

10. SORA: Specific Operations Risk Assessment (See Annex D).
11. JARUS: Joint Authorities for Rulemaking on Unmanned Systems.

RECOMMENDATIONS

It is highly recommended that the Competent Authority clarify the Roles and Responsibilities of (at least) the following actors:

- Law Enforcement Authority
- Airport operator
- ANSP
- UTM/U-Space Service Provider
- Drone Pilot.

Elements to consider (but not limited to):

- Information sharing
- Approval of procedures
- Risk Assessment process (Safety & Security)
- C-UAS activities
- Coordination
- Communication
- Incident Reporting
- Safety & Security Management.

(All the above for 'good' and 'bad' drone scenarios)

AIRPORT ENVIRONMENT

5

5. Airport Environment[12]

5.1 Area of Responsibility

The airport operator can (typically) only be held responsible for activities inside the airport boundaries. For (drone) activities outside the airport perimeter, the responsible entity for that area needs to ensure that appropriate arrangements have been made since the drone activities may fall outside the airport jurisdiction.[13]

5.2 Dimensions & other characteristics

An **aerodrome** is a location from which flight operations take place such as large commercial airports, small general aviation airfields and military air bases.

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.

For the purpose of this concept document, only **'protected aerodromes'** will be considered and can be one of the following:

- an EASA certified aerodrome ('airport')
- a government aerodrome (i.e. military airfield)
- a national licensed aerodrome (i.e. most smaller 'general aviation' airfields).

In the majority of cases, a 'protected aerodrome' can be readily identified as an aerodrome that has an Aerodrome Traffic Zone (ATZ) established around it.

5.2.1 Aerodrome Traffic Zone (ATZ)

An aerodrome traffic zone (ATZ)[14] is defined as: An airspace of defined dimensions established around an aerodrome for the protection of aerodrome traffic.

The ATZ is intended to protect the aerodrome traffic, i.e. the traffic on the manoeuvring area and the traffic in the immediate vicinity of an aerodrome. This includes, but is not limited to, the aircraft in the aerodrome traffic circuit. There are no worldwide accepted definitions about the size of ATZs in terms of lateral or vertical limits. Generally, the ATZ is considered to be a "small-volume" airspace, usually a cylinder extending from the surface up to a few thousand feet with a radius of a few nautical miles (NMs). The centre of the ATZ may be the aerodrome reference point (ARP), the centre of the (longest) runway, or another suitable point.

12. The Airport Environment described in this chapter is conceptual and therefore generic. It is intended as industry guidance. (Local) regulations and circumstances may need other arrangements.
13. See also Chapter 4, Roles & Responsibilities, Airport operator.
14. https://www.skybrary.aero/index.php/Aerodrome_Traffic_Zone_(ATZ). ICAO Annex 2 is official reference.

The airspace within the ATZ may be either controlled[15] (and served by an aerodrome Control Tower) **or uncontrolled** (in which case e.g. aerodrome flight information service (AFIS) is offered). The precise form and dimensions of the ATZ may vary from country to country, and this information can be found in the appropriate national Aeronautical Information Publication (AIP) published by the Civil Aviation Authority (CAA)[16] of each (ICAO) Member State.

Apart from ATZs, there is a NOTAM[17] system for notifying blocks of airspace where particular limitations are placed on the flight of all aircraft (manned and unmanned). Such areas are typically either Prohibited Areas, Restricted Areas or Danger Areas (military ranges, etc.). Other airspace may have temporary restrictions imposed at specific times, either as a result of a longer term pre-planned event, or in reaction to a short notice occurrence, such as an emergency incident. It is important to note that these restricted areas apply to all aircraft including drones, regardless of weight or height of operation.

Further details can be found in the AIP for a particular country, and are not be elaborated further in this concept document (out of scope).

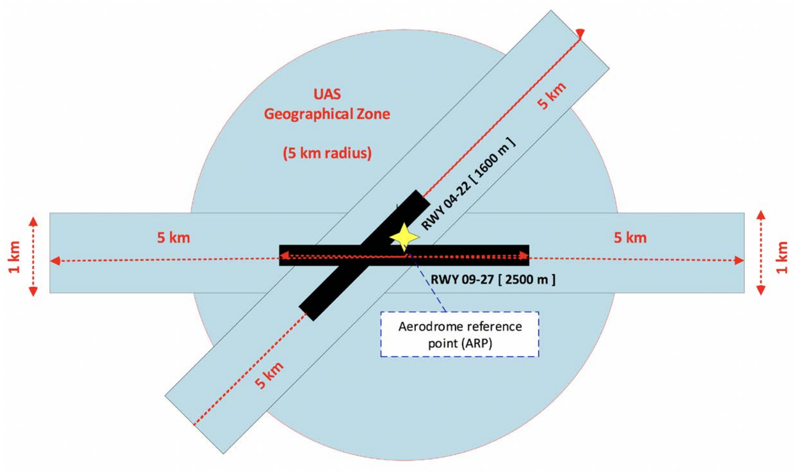
5.2.2 UAS Geographical Zone

Flights of drones around airfields or airports that are highly restricted. It is illegal to fly drones of any size within the UAS Geographical Zone of a protected aerodrome without appropriate prior permission from air traffic control at the airport, and/or from the airport operator.

In the majority of cases (i.e. aerodromes that have an ATZ), the UAS Geographical Zone should primarily consist of two separate zones:

- The ATZ at the aerodrome
- The runway protection zones[18].

FIGURE 1: **UAS GEOGRAPHICAL ZONE WITH AERODROME TRAFFIC ZONE (ATZ) & RUNWAY PROTECTION ZONES**



15. Controlled airports are protected by a Controlled Airspace extending upwards from the surface of the earth to a specified upper limit (ICAO Annex 11 Air Traffic Services).
16. https://www.eurocontrol.int/articles/ais-online
17. NOTAM: Notice to Airmen.
18. The term Runway Protection Zone (RPZ) is also used in the context of airfield design and land-use in the U.S. and should not be confused with the context in this document (protection of airports for unauthorised drones).

The exact shape and dimensions of the UAS Geographical Zone may vary depending on the specific aerodrome that it protects, based on the operational characteristics (complexity, type and volume of traffic, etc.). This should be assessed locally, resulting in an optimal UAS Geographical Zone configuration.

Typically, heliports only comprise the ATZ portion of the Flight Restriction Zone (FRZ) and do not include runway protection zones.

Prior to flight, remote drone pilots should check to ensure that they are operating well outside these areas unless explicitly authorised to operate within the zone(s) mentioned above.

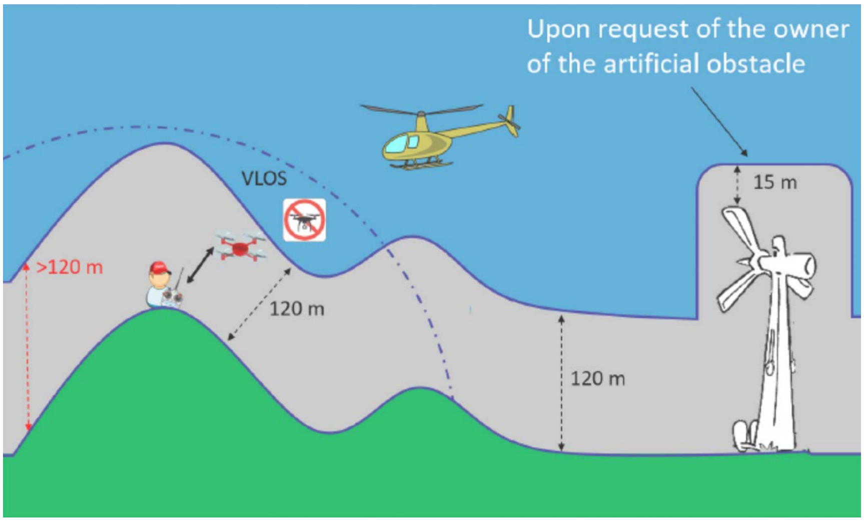
The establishment of No Drone Fly Zones[19] can help in the detection and enforcement of unauthorised drone use (deterrence, establish legal criminalisation basis).

However, No Drone Fly Zones need to be combined with additional mitigation measures in order to cope with potential safety/security hazards and acts of unlawful interference.

120m (400 ft) limitation

Height[20] limitation is intended to contribute to the safety of manned aircraft from the risk of collision with a small unmanned aircraft (drone). With the obvious exception of take-off and landing, the majority of manned aircraft fly at heights greater than 500ft from the surface. While there are some other exceptions where manned aircraft are permitted to fly at 'low level' (such as Police, Air Ambulance and Search and Rescue helicopters, as well as military aircraft), **flying a small unmanned aircraft below 120m (400ft) significantly reduces the likelihood of an encounter with a manned aircraft**. This is reflected in the aviation regulations.

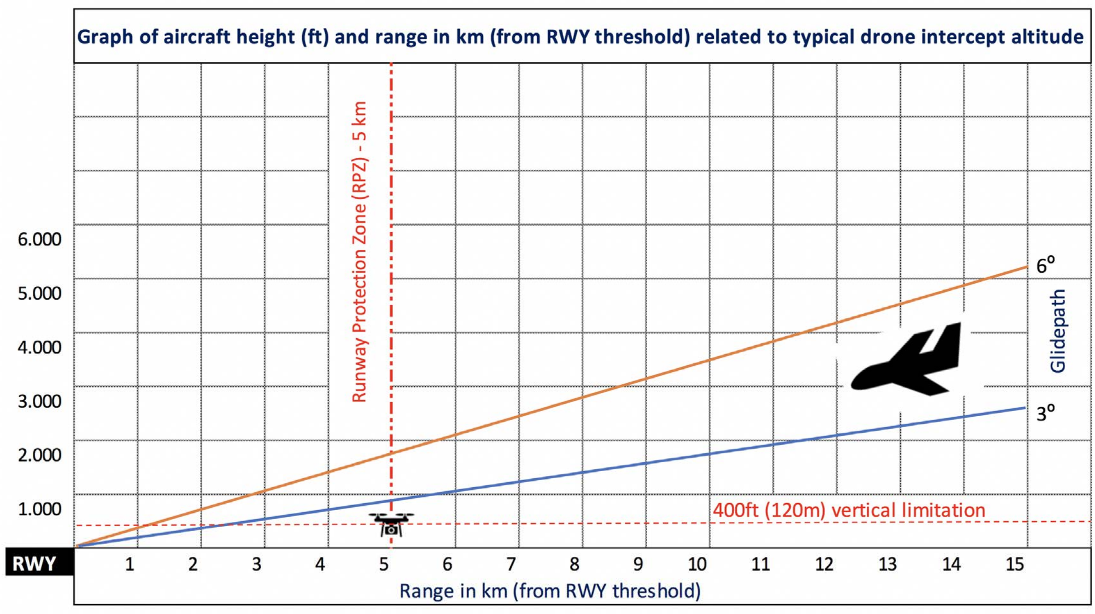
FIGURE 2: **MAXIMUM DRONE HEIGHT (EASA)**



19. See Chapter 6 (No Drone Fly Zones) for more information.
20. In aviation terms, 'height' means the vertical distance from a specified datum (typically Above Ground Level, AGL), or an object like building. Altitude is the height above the reference level (typically Mean Sea Level, MSL).

Please note that the limitation applies to 'heights above/distances from' the surface of the earth (AGL). It does not automatically apply to heights/distances from tall buildings or other structures; in such cases, an additional permission from the Competent Authority will be required, which will invariably also require permission to operate within a congested area.

FIGURE 3: **TYPICAL APPROACH PROFILE MANNED AIRCRAFT**



The above graph (Figure 3) shows an aircraft on a typical 3° ILS glide path to a runway for landing. The UAS geographical zone and runway protection zones protect both **departures** and **arrivals**. It should be kept in mind that aircraft on an approach typically use a 3° glide path, but with departures, the climb gradient may well vary due to performance differences,[21] which can be significant.

A protection zone with a 5km radius from the Aerodrome Reference Point (ARP) is becoming the norm across Europe, but may not be appropriate/feasible everywhere. More protection may be required due to the layout of the airport (e.g. as a result of a multiple runway configuration). It is the responsibility of the Competent Authority to determine and communicate the exact UAS Geographical Zone dimensions (horizontal, vertical), in collaboration/consultation with the airport operator/ANSP involved.

21. E.g. due to aircraft type differences, take-off mass, weather, departure procedures, etc.

RECOMMENDATIONS

Regulators, Competent Authorities and airport operators are strongly recommended to standardise the UAS Geographical Zone as much as possible, keeping the following criteria as a baseline:

Horizontal

- Radius: The Aerodrome Traffic Zone (ATZ) as a minimum or expanded radius when more protection is required due to the layout of the airport (e.g. runway configuration)
- Runway Protection Zones (RPZ): A rectangle extending 5km from the threshold of the runway away from the aerodrome, along the extended runway centreline, and 500m either side
- Airport perimeter: all security relevant airside buildings and areas that are encompassed by the airport perimeter fence, if not already covered by the two criteria above.

Vertical[22]

- The maximum height above ground level (AGL) inside the UAS Geographical Zone should not exceed the maximum of the vertical limit of the ATZ, whereby the maximum height in the Runway Protection Zones should be kept as low as possible (maximum 120m/400ft height from ground level (AGL) as is standard elsewhere
- Airports/ANSPs need to check if any of their IFP (instrument flight procedures) have protected zones which could interfere with the 120m (400ft) vertical limitation and take appropriate action where needed.

Deviations from above recommendation could be possible on a case-by-case basis, only after conducting a safety assessment ensuring the additional risks can be mitigated (e.g. crossing traffic at low altitude).

The UAS Geographical Zones shall be effective regardless of UAS size and weight.

- Competent Authorities are strongly recommended to make the UAS Geographical Zones easily accessible for drone operators and the general public[23] (website, app)[24]
- Competent Authorities are strongly recommended to ensure that software developers can easily download the airport data (KML files, etc.) from the AIS[25] website.

22. Above this height, it is strictly forbidden to operate a drone, unless a prior written approval by the Competent Authority is obtained. A risk assessment and mitigation measures need to be provided as a minimum.
23. Avoid using unnecessary aviation terms (e.g. use km and m instead of NM for lateral and ft for vertical dimensions), or use both.
24. E.g. DroneSafe (UK) website (https://dronesafe.uk/restrictions/) contains an interactive map, which shows all the UAS Geographical Zones. Developers can download the data (KML files, etc.) from NATS' AIS website. Another good example is Norway: https://avinor.no/en/corporate/at-the-airport/droner/choose-airport
25. Aeronautical Information Service.

5.3 Prerequisites

Before any drone operations can be authorised within a UAS Geographical Zone, arrangements need to be made taking into account the following aspects:

PREREQUISITES

- Operator/drone pilot(s) known and registered
- Operator/drone pilot(s) licenced and trained
- Acceptable equipment[26]
- Confirmation of adherence to all applicable EASA and national/local regulatory requirements
- Equipment meeting conspicuity requirements[27]
- Appropriate third party liability insurance arranged for commercial operators
- Operations Manual available and maintained
- Drone pilots must give priority to all (manned) aircraft and stay well clear of their flight path
- Drones must be flown at a safe distance from people and buildings
- Detailed Scenario/Flight plan
- VLOS, daylight only[28]
- Safety assessment for the specified operation (SORA complemented by aerodrome operator and ANSP analysis)
- Airport manager (written) permission
- Civil Aviation Authority permission
- Coordination and communication protocol with ATC (Approach, TWR) and airport operator[29]
- Go/No-Go decision protocol arranged.

The above list should be considered as a baseline. Regardless of the form of the arrangement between the drone operator and ATC/Airport Manager, the roles and responsibilities of the actors during all phases of drone operations should be unambiguously set out.
The above prerequisites are based on the (EASA) regulations mentioned in Annex A, the Approval Process description (Annex C), the SORA risk assessment methodology (Annex D) and other relevant chapters of this document.

→ **See Annex A (Regulations) for generic rules applicable to operation of drones.**
→ **See Annex C for Approval Process.**

26. In this context, "acceptable" means acceptable for the airport operator/ANSP for the operations to be conducted.
27. E.g. by mode-S transponder (used by manned aircraft), or different methods to broadcast the drone's position at close range by Bluetooth or Wi-Fi transmitters, or via a cellular communications network. The options may change as technology evolves. Alternative arrangements are possible, to the satisfaction of airport operator/ANSP.
28. Daylight restriction could be lifted if risks associated with night operations can be mitigated properly and risk assessment guarantees safe and secure operations.
29. A single point of contact/coordination is desirable, when possible.

OPERATIONAL CONCEPT

6

6. Operational Concept

6.1 U-Space

U-space is a set of new services and specific procedures designed to support safe, efficient and secure access to airspace for large numbers of drones. These services rely on a high level of digitalisation and automation of functions, whether they are on board the drone itself, or are part of the ground-based environment. U-space provides an enabling framework to support routine drone operations, as well as a clear and effective interface to manned aviation, ATM/ANS service providers and authorities. U-space is therefore not to be considered as a defined volume of airspace, which is segregated and designated for the sole use of drones. U-space is capable of ensuring the smooth operation of drones in all operating environments and in all types of airspace (in particular but not limited to very low level airspace). It addresses the need to support all types of missions and may concern all drone users and categories of drones.

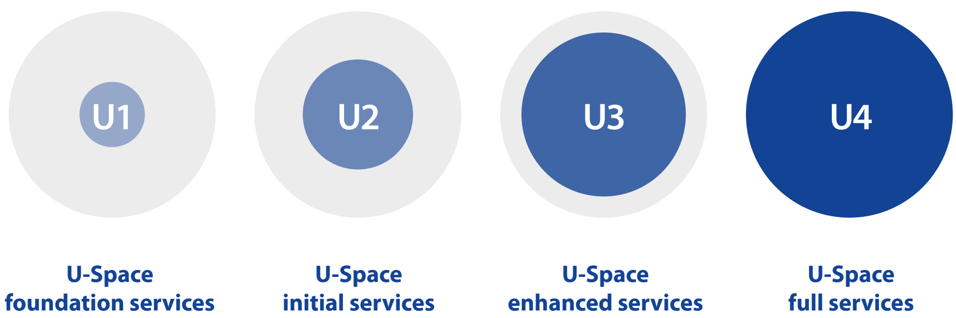
The U-space framework comprises an extensive and scalable range of services relying on agreed EU standards and delivered by service providers. **These services do not replicate the function of ATC, as known in ATM, but deliver key services to organise the safe and efficient operation of drones and ensure a proper interface with manned aviation** (especially where U-Space and controlled airspace meet or overlap), **ATC and relevant authorities**. They may include the provision of data, supporting services for drone operators, such as flight planning assistance, and more structured services, such as tracking or capacity management.

Three services have already been identified as "foundation services":

- electronic registration of drone and pilot (e-registration)
- electronic identification (e-identification) and
- geofencing/geo-awareness.

Current initiatives envisage that electronic registration is mandatory for drone operators (except operators of drones weighing below 250g), as well as some classes of drones used in the open category, and all drones used in the specific category[30]. Electronic identification will allow authorities to identify a drone flying and link it to information stored in the registry; the identification supports safety and security requirements, as well as law-enforcement procedures.

FIGURE 4: **U-SPACE SERVICE LEVELS (SESAR)**



30. See Annex A (Regulations).

The progressive deployment of U-space is linked to the increasing availability of blocks of services and enabling technologies. Over time, U-space services will evolve as the level of automation of the drone increases, and advanced forms of interaction with the environment are enabled (including manned and unmanned aircraft) mainly through digital information and data exchange.

There are 4 types of services presently envisaged in the U-Space concept:

	U-Space Services	Details
U1	**Foundation**	Provide e-registration, e-identification and geofencing.
U2	**Initial**	Support the management of drone operations and may include flight planning, flight approval, tracking, airspace dynamic information, and procedural interfaces with air traffic control.
U3	**Advanced**	Support complex operations in dense areas and may include capacity management and assistance for conflict detection. Indeed, the availability of automated 'detect and avoid' (DAA) functionalities, in addition to more reliable means of communication, will lead to a significant increase of operations in all environments.
U4	**Full**	Particularly services offering integrated interfaces with manned aviation. They support the full operational capability of U-space and will rely on very high level of automation, connectivity and digitalisation for both the drone and the U-space system.

→ **See Annex H for more information about U-Space (Reference Documents & Useful links / SESAR)**

6.2 Facilitation

Three models of drone facilitation are considered in the concept of operations. These are:

1. Segregated Operations
2. Coordinated Operations
3. Integrated Operations

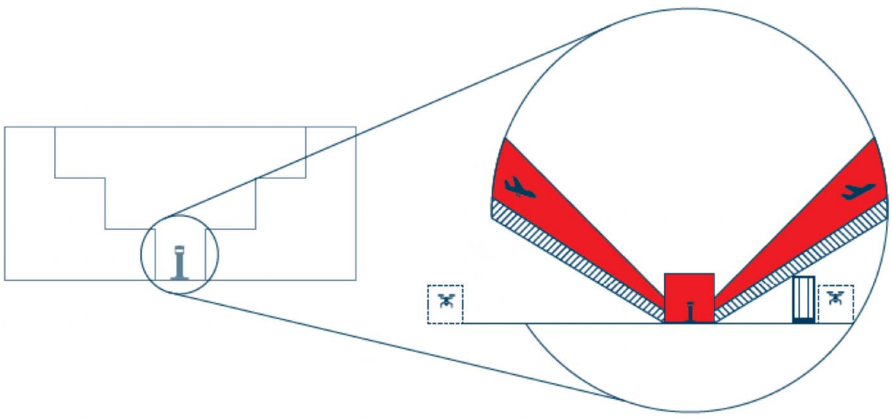
These models will evolve as knowledge, technology and regulations improve, and experience drives efficiencies in processes. Drones can also move between the models as global capability and technology develops.

6.2.1 Segregated Operations

Operations would normally impact on ATC, but the characteristics of the requested location mean that **direct interaction with ATC is not required** and ATC can work independently around the drone(s) operation.

Prohibited/Restricted/Danger (PRD) Areas are the most easily identifiable locations for segregated operations and existing military PRD Areas will be increasingly used for drones operations.
For civil operations, the Competent Authority is responsible for assessing the level of risk and determining if a Temporary PRD Area is required. For drones operations within PRD Areas, existing procedures are utilised by ATC to segregate other airspace users from the PRD Area.

FIGURE 5: **SEGREGATED DRONE OPERATIONS (RPAS OPERATIONAL CONCEPT, AIRSERVICES 2016)**



Drone operations that are planned over a movement area, runway or approach/departure path of a controlled aerodrome but in close proximity to and beneath the height of a nearby terrain feature, or man-made obstacle, may be "shielded" from other airspace users by virtue of the terrain or obstacle. An example is a drone operation below the height of a large structure, which conventional aircraft will fly over. These operations should utilise guidance material provided by the Competent Authority to assess the operation and should be coordinated and approved by the airport operator if inside airport boundaries and by ANSP in other situations.

Non-Critical Specialised Operations

Non-critical specialised operations are those operations that do not include overflight, *even in the event of failures and malfunctions*, of:

- congested areas, gatherings of people, urban agglomerations
- roads, railway lines[31] or waterways
- sensitive infrastructure.

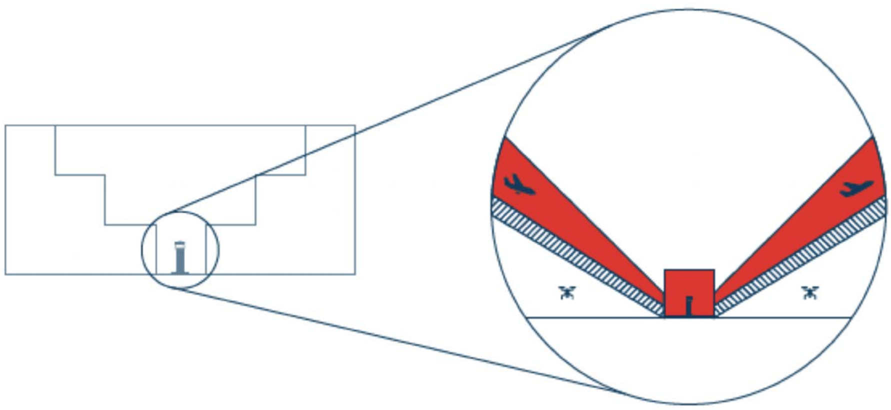
The non-critical operations are conducted in a **volume of space** of **150 meters** and **500 meters radius** and under the following conditions:

- at an adequate horizontal safety distance (and never less than 150m) from congested areas and within ATZs
- at a distance of at least 50m from people and things that are not under the operator's direct control
- in daylight conditions
- in BVLOS conditions
- outside UAS Geographical Zones and areas below take-off and landing trajectories
- at a distance greater than 5km from the airport (Aerodrome Reference Point or geographic coordinates published), where there is no UAS Geographical Zone to protect flight operations
- outside the active regulated zones and the prohibited areas, promulgated in AIP and NOTAMs.

6.2.2 Coordinated Operations

Coordinated Operations refer to drone(s) operations where **interaction with ATC is required**, as determined through assessment of the characteristics of the location and equipment levels and capability of the drone. These operations will need an appropriate risk assessment and may need to have a standard "Drone Buffer" applied in order to provide a proper separation between the drone operations and manned aircraft (in the air and on the ground) to mitigate the risks as much as possible.

FIGURE 6: **COORDINATED DRONE OPERATIONS (RPAS OPERATIONAL CONCEPT, AIRSERVICES 2016)**



31. The railway industry is concerned about the risk presented by drones, particularly to high-speed trains. Therefore, at least high-speed lines could be considered as more critical.

Coordinated drone operations may form the majority of requests received by the Competent Authority, the ANSP and airport operators, and require the greatest development of procedures. At present, most of these operations are within 5km of a protected aerodrome. However, the number of requests for operations above 120m (400ft) Above Ground Level (AGL) is increasing continuously and is expected to expand to more frequent Beyond Visual Line of Sight (BVLOS) operations over time.

The evolving management of Coordinated Operations fits into 3 broad areas:

	Coordinated Operations	Description
1	**Use Cases**	This applies to drones weighing less than 25kg.
2	**Drone Buffers**	This refers to the development of a number of standard buffers for the segregation of manned aircraft.
3	**Individual Assessments**	This refers to the assessment process that the Competent Authority utilises for requests made by drone operators for access to protected aerodromes.

Standardised Use Cases

The aim of the standardised Use Cases is to ensure that drone operations will be conducted in a structured way, with arrangements and mitigation measures appropriate and tailored to the purpose of that operation.

→ **See Annex F for a library of standardised Use Cases**

Drone Buffers

The development of standard buffers enables ATC with a series of tactical options to segregate drone operations from other airspace users. It is envisaged that as this work evolves and as drone operators and ATC become more familiar with the buffers and processes, drone operators will be able to contact ATC directly on the day of operations, similar to other airspace users such as survey flights and parachute operations. This will reduce the work involved in the assessment process and the operation will be approved subject to normal traffic considerations.

As experience with drone operations in controlled airspace expands, it is expected that the buffers constructed in the initial stages will be reviewed and refined.

RECOMMENDATIONS

It is recommended that ANSPs develop standard buffers in order to separate drone operations from manned aircraft movements (in the air and on the ground). These buffers could be incorporated in the Standardised Use Cases, facilitating standard approach to risk mitigation measures at least until effective technologies and protocols are widely available and deployed.

Individual Assessments

Apart from the standardised Use Cases, there may be drone operations that will continue to require Individual Assessment due to the nature and/or the location of the drone operation. It is envisaged that the number of Individual Assessments will decrease over time as the standardised Use Cases will be further developed and drone buffers principles become more mature.

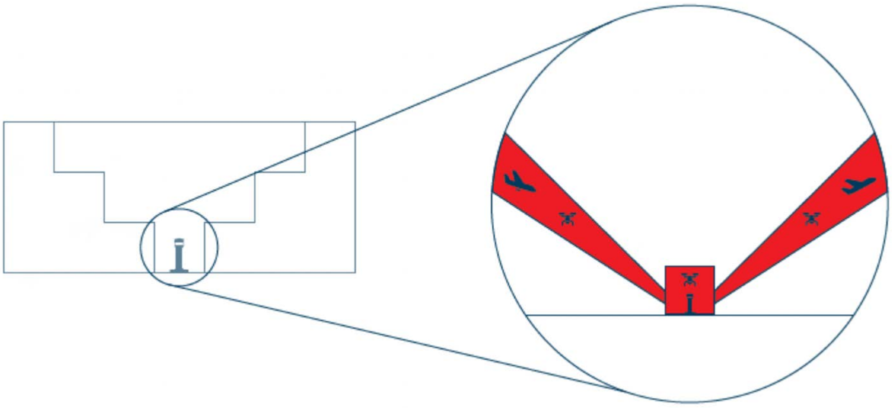
6.2.3 Integrated Operations[32]

Operations where the equipment levels and capability of the drones are highly reflective of conventionally piloted aircraft, and they can be largely managed through (pre-existent) systems and processes.

Integrated Operations are typically capable of presenting real-time navigational information using (conventional) navigation systems and maintain continuous two way communications with ATC. Separation standards are applied and the drone is effectively managed as an IFR aircraft. Where elements of drone performance characteristics are subtly different to conventional aircraft, standards may need to be adapted.

32. Integrated Operations will not typically be associated with the low level airspace surrounding protected aerodromes and the associated FRZs. It would require U3/U4 level of services (U-Space).

FIGURE 7: **INTEGRATED DRONE OPERATIONS (RPAS OPERATIONAL CONCEPT, AIRSERVICES 2016)**



For larger drones that require the use of airport facilities, current ATC technologies and drone sense-and-avoid systems are not yet ready for the establishment of standards for the inclusion of drones in the normal airport traffic patterns.

Due to the technological gap, along with results found in air traffic simulations[33] highlighting the need for extended downwind travel and wake turbulence avoidance, ATC and/or the CAA are likely to keep drones segregated from manned aircraft in the name of flight safety, and a desire not to disrupt normal airport operational capacities. Integration of military drones with manned aircraft in the airport traffic area has been done successfully. These experiences, along with additional tests and trials anticipated at the drones test sites, will provide information that may aid the development of airport operational standards in the future. In the near term, the easiest and safest solution is to keep drones away from the airport pattern.

6.3 Drone Fly Zones (DFZ)

To streamline the airspace access assessment process for drone operations and low-level airspace surrounding protected, aerodromes will be categorised into three zones (Red, Amber and Green) according to how compatible drone operations are with other airspace users in these zones.

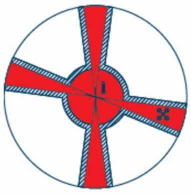
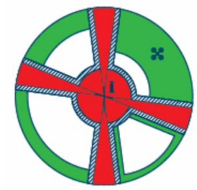
These zones typically relate to drone operations below 120m (400ft) AGL and within 5km of a protected aerodrome that potentially affect operations over the movement area, runway or approach/departure path of that aerodrome.

The Drone Fly Zone (DFZ) concept will improve the information available to drone operators when planning to operate in areas where a specific clearance is required.

The concept of the three fly zones within controlled airspace is designed to provide two primary operational advantages:

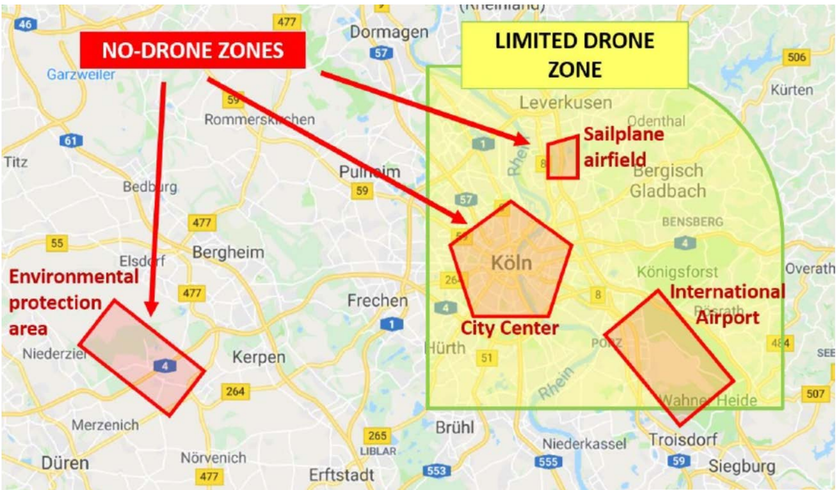
1. Guidance to drone operators on when approval is required from a Competent Authority for an operation and the likelihood of that operation being approved
2. Guidance to ATC when assessing or advising on airspace access applications.

33. FAA (USA).

No Fly Zone	Apply to Fly Zone	Advise and Fly Zone
Red Zone	**Amber Zone**	**Green Zone**
		
An area of operation where **drone operations are not compatible with other airspace users** ATC must perform an assessment to determine if the operation can be facilitated The assessment is complex and approval is not likely If approval is given, it will carry significant conditions or restrictions	An area of operation where **drone operations may be compatible with other airspace users** ATC must perform an assessment to determine if the operation can be facilitated While approval is likely, it might carry some conditions or restrictions	An operational area where **drone operations are compatible with other airspace users** ATC is advised by a drone operator prior to and following an operation

The Amber Zones can be compared with the "Limited Drone Zone" (LDR)[34] as indicated in the picture below:

FIGURE 8: **LIMITED DRONE ZONE (LDZ) AND NO DRONE ZONE (NDZ) - EASA NPA 2015-10**



34. CORUS ConOps for U-Space (https://www.sesarju.eu/node/3411).

RECOMMENDATIONS

The key enabler for the three fly zones is a suite of three dimensional maps that specify the location of the zones for each protected aerodrome. It is recommended that Competent Authorities/ANSPs develop standardised specifications to identify the requirements for the 3 different Drone Fly Zones.

The drone facilitation models and fly zones suggest no changes to existing regulatory requirements or airspace classifications. Rather, they should be considered enhancements to current requirements and processes.

SAFETY & SECURITY

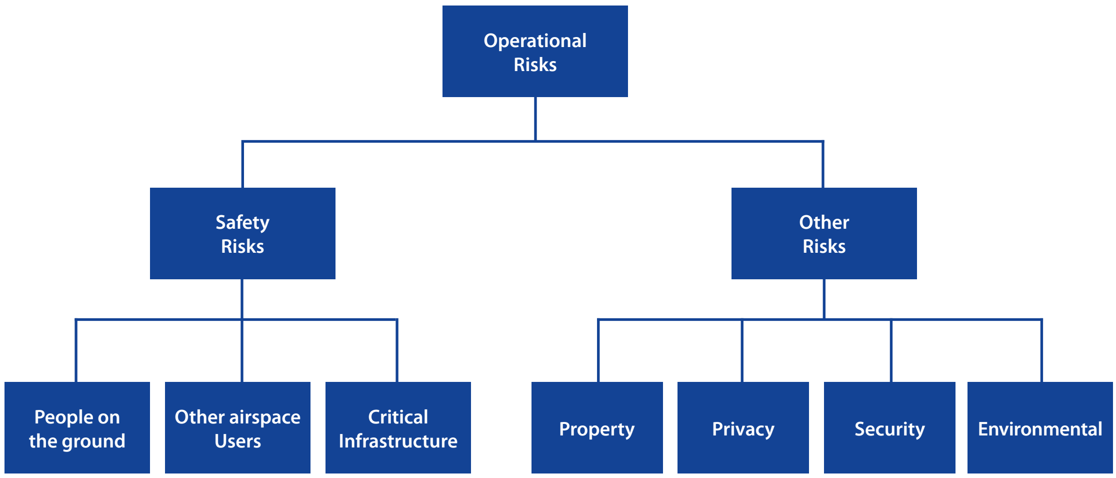
7

7. Safety & Security

7.1 General

Safety and security management aspects for airports encompass all areas within the Flight Restriction Zones (FRZs), including airside and landside areas.[35] It should include cooperative drone operations (e.g. drone runway inspection, drone parcel delivery) and non-cooperative drone operations (e.g. malicious acts). In the latter case, one may also argue that when a drone enters airside in an unauthorised manner, it can first be seen as a security concern (e.g. access control, intrusion in a security restricted area, etc.). This then becomes suddenly a safety issue if that same unauthorised drone reaches the runway in service, as well as a business continuity issue before operations can resume in safe conditions. In many cases the principles apply to both areas. Therefore, a holistic approach to safety, security and operations continuity in relation to drones in the airport environment is necessary.

FIGURE 9: **(FROM JARUS) ILLUSTRATES THE DIFFERENT OPERATIONAL RISKS ASSOCIATED TO DRONE OPERATIONS**



In addition to the regulations laying down rules and requirements for users and manufacturers of drones, the prevention and protection to counter drone technology will also come from the use of technology. Effective mitigation for non-cooperative drones is typically based on four pillars:

1. First line of defence starts with the drone manufacturers and collaboration to include safety/security elements by design features embedded in the drones in line with the Regulation[36]
2. Strict rules for users/operators of drones
3. Intermediate line of defence may include enhanced detection and response capability at aerodromes where the risk level is significant
4. Developing specific mitigation measures and procedures, depending on local security risk assessments.

35. See Annex G (Glossary) for descriptions.
36. EU REG 2019/945

7.1.1 Cooperative vs. Non-Cooperative Drones

From a safety/security perspective, the process to address cooperative and non-cooperative drone operations is different.

For cooperative drone operations, the process is rather straightforward because risk(s) could be clearly identified, evaluated and mitigated despite drone operations being relatively new. **SORA will be used for the drone design and the drone operational part (specific drone category) whereas aerodrome and ATM/ANS safety assessment will be conducted for the Airport and ATS part to verify that such operation is acceptably safe in this airport operational environment**.

Cooperative drone operations include, inter alia, aerodrome movement area inspection/monitoring (e.g. runway pavement inspection, FOD detection, PAPI calibration), wildlife management, ILS calibration, parcel delivery, etc.

For **non-cooperative drone operations**, the process is obviously different, because for such a case it is not possible to define, a priori, the risk(s). Non-cooperative drone characteristics and airspace (ATZ) trajectories are unknown (type of drone, weight, speed, endurance). The only preventive mitigation could be to implement appropriate detection systems informing and locating uncooperative drones in order to prevent any safety/security issue by stopping air operations in all or part of the airport.

RECOMMENDATIONS

The safety/security risk assessment should include identifying sensitive infrastructures and/or areas and consider developing specific procedures for these 'hot spots'.

It should be noted that SORA is not applicable to non-cooperative drone operations.

Non-cooperative drone operations could be split into two families:

1. One relative to drone penetrating the airspace (ATZ) by 'mistake' by 'the reckless and careless' citizens and
2. One relative to malicious acts.

As for the first family, preventive mitigations exist to limit such occurrence by information and training of drone pilots as the current EASA regulation requires.

7.2 Safety Considerations

In relation to drone operations in the airport environment, there are 2 key areas that need to be given proper consideration:

- Safety risks in the air
- Safety risks on the ground.

Once the risks are identified, consideration needs to be given to the consequence of an occurrence that can be designated as a harm of some type. The potential categories of harm are:

- Fatal injuries to third parties on the ground
- Fatal injuries to third parties in the air
- Damage to critical infrastructure
- Damage to property on the ground.

It is acknowledged that the competent authorities, when appropriate, may consider additional categories of harm (e.g. disruption of a community, environmental damage, financial loss, etc.).

Safety starts with design, training, operational approval and actors' adherence to procedures. All of these elements should be addressed for each of the relevant domains (drone operator, aerodrome operator and ANSP). A risk assessment is needed whereby mitigation measures can be identified and timely action taken, where needed. Some examples of mitigation actions are training, tracking of the drone position, licensing, use of geofencing, coordination and communication protocol, phraseology to be used by the drone pilot, etc.

SORA is the risk assessment process for the drone domain (drone design, drone operator and drone pilot) when considering cooperative drone operations and the drone specific category. SORA should be complemented by a risk assessment associated with aerodrome operations and in concert with the ANSP in order to have the complete risk picture associated with this drone operation.

To obtain the complete risk picture, the analysis should address normal, abnormal and faulted conditions, as illustrated in Figure 10. This will assist the identification of the complete list of requirements/mitigations for safe drone operations at the airport.

FIGURE 10: **NORMAL - ABNORMAL - FAULTED CONDITIONS**[37]

To be safe in normal conditions	To be safe considering abnormal conditions	To be safe in normal faulted conditions
Coordination Respecting operational volume Compliance with ATC instructions Adequate CNS, etc.	Severe weather conditions Ionospheric disturbances Interference	Equipment failure Procedure not applied Human error
Functionality and Performance	**Mitigations/Resilience**	**Mitigations/Limit Frequency of occurrence**

37. CNS: Communication, Navigation and Surveillance.

For cooperative drone operations:

- The complete risk picture should be obtained by complementing SORA with the aerodrome and ANSP safety assessment.
- The safety assessment process should consider safety from three points:
  *to be safe in normal conditions
  *to be safe considering abnormal conditions
  *to be safe considering faulted conditions.

For non-cooperative drone operations, the safety of air operations could be endangered, in particular during the take-off and landing phases. It does not mean that ground personnel, vehicle or manned aircraft taxiing or airport infrastructure cannot be endangered by such operations but the risk is lower. This is because the severity associated with a mid-air collision during take-off or landing is higher due to the higher level of energy (higher speeds).

Currently, there are no available standards (e.g. EUROCAE) for the technical solution and its operational use to control these risks properly (See C-UAS section). However, the following high-level principles should apply if the airport decides to deploy C-UAS technology:

- Detecting and monitoring non-cooperative drones
- Understanding the illicit drone activity and determining the level of risk
- Providing an immediate answer when required to "protect" manned aircraft operations at the airport.

For non-cooperative drone operations:

- Safety of air operations in particular during take-off and landing might be endangered by non-cooperative drone operations.
- If the airport decides to deploy C-UAS technology, the risk might be controlled by:
  * detecting and monitoring non-cooperative drones
  * understanding the illicit drone activity and determining the level of risk
  * providing an immediate answer when required to "protect" manned aircraft operation at the airport.

7.3 Security Considerations

States should conduct risk assessments to assess the threat level posed by drones and have a process for informing airport operators, ANSPs and aircraft operators and other relevant stakeholders of the assessed threat level and both the required and recommended actions or mitigations by all stakeholders.

Two important principles should be recognised:

- The risks of drones cannot be eliminated, but managed
- Prohibition of (unauthorised) drones in the vicinity of airports, security intelligence, and aviation security coordinated contingency and response plans jointly constitute the most effective means of countering the drone threat from a security perspective.

Security risks associated with drones fall into two broad categories:

- Use of drones to attack an aircraft in flight, and
- Use of drones as weapons to attack targets on the ground, which may include aviation-related targets (aircraft, airports) or non-aviation targets (crowds, events).

Attacks on aviation targets whether on the ground or airborne are considered "Acts of Unlawful Interference" to civil aviation by ICAO[38].

Aircraft in either arrival or departure phase are vulnerable to attack using a drone. The two most notable scenarios associated with small drones flown deliberately into critical aircraft components (engine, windshield) are:

- Use of drone's mass to cause damage
- Use of a drone with an explosive device attached.

Other scenarios aimed at attacking aviation using drones could include:

- Delivery of a chemical, radiological or biological agent into a public area
- Direct attack on an aircraft on the ground or airport with an explosive device.

Deliberate acts, which may not be considered acts of terrorism or acts of unlawful interference, might include:

- Deliberate disturbance to airport operations (protest, approach/departure path interference)
- Transportation of dangerous items into restricted areas
- Espionage and surveillance of sensitive operations.

38. See ICAO Annex 17 (Sections 4.3 – 4.6).

When an attack is likely (based on intelligence provided by the State, notification of an increased threat level or receipt of a credible threat), additional measures to facilitate early detection could include:

- Increased surveillance for drones (e.g. visual patrolling or identification and tracking assisted by means of technology)
- Airspace closure
- Armed-physical response/assisted by means of C-UAS technology.

Where threats exist, unless otherwise stated, authorities in coordination with airport operators should coordinate with all entities to ensure that security measures (landside and airside) are established to mitigate identified threats of acts of unlawful interference in accordance with a risk assessment carried out and maintained by the relevant authorities in coordination with all relevant stakeholders.

7.3.1 Responsibility for State Security

Law Enforcement Authorities are responsible for State security. The Law Enforcement Agencies should liaise with airport operators, the ANSP, air carriers or any other relevant entity with regard to security arrangements appropriate to the assessed threat to the airside/landside area and communicate relevant security information, as they deem appropriate.

An airport operator shall coordinate and jointly develop, where appropriate, their aerodrome security plan (or make reference in the aerodrome security plan to the required security provisions made in the plan dedicated to the management of drones at the aerodrome).

There is a growing use of drones for different categories: hobby, commercial, crime and terror. Each one of these drone usages creates a different threat:

Drone Operator Category	Threat
Hobby/Private	Unintentional risk to public safety, aviation and personal privacy, mainly due to lack of experience and knowledge of regulation.
Commercial	Uncontrolled usage of low altitude air space with risk to aviation, public safety and intellectual property (IP) theft, mainly due to lack of air traffic control regulation and technology and regulation enforcement capability.
Crime	Using the drone's high availability and capabilities for intentional law breaking, mainly due to lack of enforcement.
Terror	Using the drone's high availability and capabilities to convert it into a weapon.

7.3.2 Drone Threat Levels[39]

An example of a generic threat level classification that could trigger an appropriate response is provided below:

	Level 1	Level 2	Level 3
Threat	Civilian and hobbyist drone operators taking unintentional pictures/videos of the site and uploading them to the internet or social media	Criminal/espionage/ terrorist organisation using drones for intelligence collection from the site	Terrorist organisation attacking the site/site facilities/site personal with drones carrying small bombs or explosive device
Range	Drone 0-100m Operator 50-300m	Drone 50-200m Operator 300-1000m	Drone 0-50m Operator 500-1000m
Probability	High	Medium-High	Low-Medium (and rising)
Damage	Low	Medium	High
Relevancy	All urban sensitive sites (embassies, government, high security, airports)	All urban sensitive sites (embassies, government, high security, airports)	Using the drone's high availability and capabilities for intentional law breaking, mainly due to lack of enforcement

The matrix above is just an example and different models exist. The most important is to realise that there are different kinds of threats with associated different threat levels.

39. Drone Threat and CUAS Technology (Elbit whitepaper).

7.3.3 Threat Analysis

In order to determine what systems and procedures are needed for protecting an aerodrome, a threat analysis should be performed. Elements to consider are:

- Site environment (rural or urban, buildings/offices/terminals (crowds), nearby traffic and public transport, other environment specifics, like WI-FI/cellular/radio critical areas)
- Site size (for airports typically a quite large area)
- Endurance capability of the drone and range
- Altitude to perform the operation (maximum)
- Size, weight and payload of the drone
- Drone speed
- Kinetic energy at impact
- (Loss of) conspicuity (no identification/position/operator information)
- (Loss of) communication
- Degree of complexity to transform a drone as a weapon
- Intent (threat intelligence)
- Drone pilot ability/skills to manoeuvre the drone at (the vicinity of) the airport
- Whether or not the aerodrome already benefits from early detection and response capabilities (means to detect, identify and respond to a risk of drone unauthorised incursion being technological, procedural, or physical).

For certain categories of drones only, risk assessment criteria commonly used for MANPADS can be pertinent and also considered:

- Identify possible launch sites selection (PLS) factors
- How to rate identified PLS given the possible target(s) envisaged, the drone(s) to be used and its characteristics (performance specifications, etc.).

If a drone needs to land at an airport to deliver and/or pick up cargo there needs to be a process in place to verify the clean/unclean status of drone and cargo.[40]

7.3.4 Protecting Against Non-Cooperative Drones (C-UAS)

Protection against non-cooperative drones is known as Counter-UAS (C-UAS).

A detailed description of Counter UAS (C-UAS) measures and regulatory context is outside the scope of this concept document. The definition of the set of specifications is the responsibility of the Regulators (European Commission, EASA and National Law Enforcement Agencies). Therefore, only a summary of the present available technologies are listed in order to provide a generic overview.[41]

In Chapter 8, information can be found about Coordination and Communication in case of non-cooperative drones.

40. See Appendix F (Use Cases): Parcel Delivery & Pickup.
41. This section may need to be updated, depending on technology developments and changes in regulatory requirements.

7.3.5 Main Types of present C-UAS Technologies

C-UAS technologies focus on two main capabilities:

- Detection
- Defeating (neutralising)

There is no single technology that can detect and defeat all drone threats in all the operational scenarios. Therefore, a modular or integrated and scenario-adapted solution is needed. A modular and multi-layered C-UAS system approach that can be customised to the needs of each site and determines which threat scenario is considered the most effective.

Detection/identification	Interception (non-kinetic)	Interception (kinetic)
Radar systems	Spoofing	Net-based solutions
Radio frequency (RF) scanners	Radio frequency (RF) jamming	Directed-energy weapons (DEW), including lasers, high energy microwaves, and electromagnetic pulses
Daylight/thermal (EO/IR) cameras	Global navigation satellite system (GNSS) jamming	Expendable UAS and tactical projectiles
Acoustic sensor		Anti-aircraft weaponry

Apart from the system components, it is necessary to clarify Roles and Responsibilities in relation to C-UAS, and to develop robust coordination arrangements (procedures). In the case of a (suspected) non-cooperative drone, quick response is typically required and no time should be wasted when action is required.

7.4 Safety Management

EASA regulations for aerodromes[42] require that 'the aerodrome operator shall implement and maintain a management system integrating a Safety Management System (SMS)'.
The management system shall include:

1. clearly **defined lines of responsibility and accountability** throughout the aerodrome operator, including a direct accountability for safety on the part of senior management
2. a description of the overall philosophies and principles of the aerodrome operator with regard to safety, referred to as the safety policy, signed by the accountable manager
3. a **formal process that ensures that hazards in operations are identified**
4. a formal process that ensures **analysis, assessment and mitigation of the safety risks** in aerodrome operations
5. the means to verify the **safety performance** of the aerodrome operators organisation with reference to the safety performance indicators and safety performance targets of the safety management system, and to validate the **effectiveness of safety risk controls**
6. a formal process to:
    a. **identify changes within the aerodrome operators organisation**, management system, the aerodrome or its operation, which may affect established processes, procedures and services
    b. describe the arrangements to **ensure safety performance before implementing changes**
    c. **eliminate or modify safety risk controls** that are no longer needed or effective due to changes in the operational environment
7. a formal processes to **review the management system** referred to in the first paragraph, identify the causes of substandard performance of the safety management system, determine the implications of such substandard performance in operations, and eliminate or mitigate such causes
8. a **safety training programme** that ensures that personnel involved in the operation, rescue and firefighting, maintenance and management of the aerodrome are trained and competent to perform the safety management system duties
9. formal means for **safety communication** that ensures that personnel are fully aware of the safety management system, conveys safety critical information, and explains why particular safety actions are taken and why safety procedures are introduced or changed
10. coordination of the safety management system with the **aerodrome emergency response plan**; and coordination of the aerodrome emergency response plan with the emergency response plans of those organisations: it must interface with during the provision of aerodrome services
11. a formal process to ***monitor compliance*** of the organisation with the relevant requirements
12. The aerodrome operator shall **document all management system key processes.**

The management system shall be proportionate to the size of the organisation and its activities, taking into account the hazards and associated risks inherent in these activities.

42. EU REG 139/2014 (ADR.OR.D.005 Management system) – See Annex H (Regulations).

7.4.1 Safety Management System (SMS)

The Safety Management System (SMS) of an aerodrome operator should encompass safety by establishing an organisational structure for the management of safety proportionate and appropriate to the size of the aerodrome operator, and the nature and type of operations. The organisational structure should include a **Safety Review Board (SRB)**, and depending on its organisational complexity and structure, a Safety Services Office to assist the work of the safety manager.

7.4.2 Safety Review Board – Safety Action Group[43]

Safety Review Board

Depending on the size of the organisation, the type and complexity of operations, the responsibilities of the Safety Review Board may be included in other high level committees of the organisation.

Safety Action Group

- A Safety Action Group (SAG) may be established as a standing group, or as an ad hoc group to assist or act on behalf of the Safety Review Board
- More than one safety action group may be established depending on the scope of the task and specific expertise required
- A Safety Action Group should report to, and take strategic direction from the Safety Review Board, and should be comprised of managers, supervisors, and personnel from operational areas
- The Safety Action Group should:
    - monitor operational safety
    - resolve identified risks
    - assess the impact on safety of operational services
    - ensure that safety actions are implemented within agreed timescales.

The Safety Action Group should review the effectiveness of previous safety recommendations and safety promotion.

The SAG typically includes the (safety) managers, supervisors and staff from operational areas (e.g. airport operator, ANSP, airline/pilot representatives).

43. Different titles may also be used for the Safety Services Office, the Safety Review Board, and the Safety Actions Group (e.g. Safety Committee).

7.5 Security Management

Airport Security Programme[44]

Every airport operator shall draw up, apply and maintain an airport security programme. That programme shall describe the methods and procedures that are to be followed by the airport operator in order to comply both with regulations and with the national civil aviation security programme of the Member State in which the airport is located. The programme shall include internal quality control provisions describing how compliance with these methods and procedures is to be monitored by the airport operator.

An Airport Security Officer typically will be designated, responsible for the coordination of all aviation security policies, procedures and preventative measures applied at a designated airport. Like the Safety Action Group, the airport security programme typically involves (security) managers, supervisors and staff from operational areas.

7.6 Incident Reporting

The success and acceptance by the public of expanded drone operations will hinge partly on how safe and secure those in the communities served by airports feel with drones flying above or near them. As drone flight exposure increases, the likelihood of an accident or incident involving a drone will also increase.

Airports are encouraged to use their individual safety/security reporting systems as a means to collect information on drone safety. Such reporting systems are vital parts of an airport SMS. Whether the system involves a telephone hotline, a specific safety email address, or an anonymous means to report concerns, all airports including those that do not currently have drone activity can play important roles in ensuring the safe and successful growth of drone operations.

From the drone operator point of view, active reporting is a crucial aspect of keeping any operation organised and efficient. It is important to log every mission (including date, departure time, arrival time, aircraft, etc.), as well as which pilots and drones are available.

Maintenance and Operations Management (MOM) software is under development. MOM is one of many examples of software tools that allow users to log all important data, as well as to stay organised with a flight calendar and maintenance reminders.

---

44. EU REG 300/2008 - Common rules in the field of civil Aviation Security (11 MAR 2008) - Article 12 (See Annex I (Reference Documents & Useful links) for hyperlink).

7.7 Training[45]

Airport operational personnel should receive initial and regular refresher training on applicable airport policies and procedures regarding the operation of authorised and unauthorised drones.

Training should include (but not be limited to):

- National regulations on drone operations in and around airports
- Types of drones authorised to operate at/or in the vicinity of the airport
- Technology used for drone operations, and tracking and identification procedures
- Coordination procedures with ATC and other state authorities on drone operations
- Risk assessment methodologies on drone operations
- Any specific operating restrictions related to the operation of the drone such as:
    - Permissible time of the day for drone operation and its duration
    - Areas around the airport where drone operations are permitted (including understanding on the vicinity of the airport)
    - Allowable proximity (separation) and altitude/height to be maintained by the drones to other manned aircraft, buildings, people etc.
    - Any pre-requisite NOTAM requirements
    - Contact information of the drone operator, including emergency contact information for both drone and aerodrome operator.

For authorised use of drones at an airport, airport specific training should be provided to drone operators operating for airport related requirements such as security surveillance, wildlife hazard management, calibration of navigational aids, etc. This should be in addition to the operator's licence obtained from regulatory authorities.

7.7.1 Educating UAS Operators and the Public

A goal of organisations serious about using drones for commercial purposes is to ensure unmanned flights are as benign and safe as possible. It benefits drone businesses when those buying and flying small UAS for private purposes are educated on the proper and safe use of these new aircraft. Education will also help gain support and acceptance by members of the public likely to be impacted by drone operations.

45. Source: ACI Drones Policy Paper (2018).

RECOMMENDATIONS

Airport operators are encouraged to develop and maintain a holistic view on safety/security management and include drone operations in their safety and security management system(s).

Airport operators and relevant stakeholders should be made aware of and/or trained on requirements for drone operations at or in the vicinity of their airport(s), including safety/security risks and mitigating actions, coordination arrangements and incident reporting (to include citizens).

COORDINATION & COMMUNICATION

8

8. Coordination & Communication

Coordination and communication are both very important, and appropriate arrangements (including procedures) need to be made, taking into account all actors and stakeholders.

The first thing that needs to be done is to lay down the **Roles and Responsibilities** in relation to (not limited to) coordination and communication. Once that has been agreed upon, coordination and communication procedures need to be laid down for the following process phases:

- Strategic (Approval Request)
- Pre-tactical (D-1; Operational Scenario)
- Tactical (D-0; Day of Operations)
- Post Ops.

For the Day of Operations (D-0) it is of utmost importance to make sound coordination and communication arrangements for the following:

- Normal Operations (for a particular established use case), and
- Contingency Operations.

When making these arrangements, it should be kept in mind that in **case of contingencies there may be little or no time for coordination and decisions may need to be taken quickly** (both from safety and/or security perspective). This may have a significant impact on the Roles and Responsibilities. Therefore, it is recommended that brainstorming begins in terms of "What-if" scenarios and develop/implement Quick Reaction Procedures (QRPs).

Experience shows that contingencies typically have more impact than initially anticipated, and drone contingencies are no exception. Therefore, it is prudent and recommended to incorporate drone contingencies in the airport emergency plans and perform exercises on a regular basis in order to raise awareness and test/amend procedures where necessary.

Frequentis has developed an understanding of KPIs, responsibilities and procedures for Drone Detection and Intervention at airports across all actors (including airports, ANSP, law enforcement). The methodology used is based on 'information stream design', which aims to ensure the highest efficiency in operating procedures, and to derive technical requirements for supporting systems.

A generic workflow ('Information Stream Matrix – Detection & Intervention') can be found in Annex E (Workflow/Checklist) as an example, showing a worst case scenario summarising involved actors, systems, resources, phases and key activities.[46]

46. This scenario and the more detailed version is available online and can be adopted and customized to concrete needs and requirements at airports, including local risk scenarios, available resources, responsibilities, actors, systems, etc. See Annex H (Various/Frequentis) for more information.

RECOMMENDATIONS

- A single point of coordination/contact is desirable, and should be considered in making the coordination/communication arrangements.
- It is strongly recommended that Quick Reaction Procedures (QRPs) are developed in order to react effectively to non-cooperative drones. Training should take place on procedures to ensure all actors will act accordingly.
- Airport operators are advised to include drones in their airport emergency plans, and perform communication/coordination exercises on a regular basis.

ANNEXES

A. Regulations

To ensure the free circulation of drones and a level playing field within the European Union, EASA has developed common European rules.[47] The approach taken is to apply the highest safety standards achieved in manned aviation to drones. The rules are based on an assessment of the risk of operation and aim to strike a balance between the obligations of drone manufacturers and operators, in terms of safety, respect for privacy, the environment, protection against noise, and security.

The new rules ensure that drone operators – whether recreational or professional – will have a clear understanding of what is and is not allowed. They will cover each operation type from those not requiring prior permission, to those involving certified aircraft and operators, as well as minimum remote pilot training requirements.

Operators will be able to operate their drones seamlessly when travelling across the EU or when developing a business involving drones around Europe. Common rules will help foster investment and innovation in this promising sector.

Registration of UAS operators & certified drones becomes mandatory

Starting from 1st July 2020 all drone (UAS) operators shall register themselves before using a drone:

- in the **'Open' category**, with a weight
    - more than 250g or
    - less than 250g when it is not a toy and it is equipped with a sensor able to capture personal data
- in the **'Specific' category**.

All certified drones (operated in high risk operations) must also be registered. The registration number needs to be displayed on the drone and submitted via the e-identification technology.

FIGURE 11: **DRONE CATEGORIES (EASA)**

OPEN category - Low risk NO-PRE APPROVAL LIMITATIONS: 25kg, VLOS, height <120m, system of zones 3 Sub-categories: fly over, close, far from people General public Model Flying Photographers	**SPECIFIC - Increased risk** Authorisation by NAA based on specific operation risk assessment (SORA) Declaration in case of standard scenario; LUC BVLOS operation (Linear inspections, aerial work,...) Transport of goods	**CERTIFIED - Risk as manned aviation** Certification of UAS, approval of the operator and licensed pilot (unless autonomous flight). Air Taxi International IFR (cargo, passengers) Package delivery over people

47. https://www.easa.europa.eu/easa-and-you/civil-drones-rpas

Drone user can start operating in limited 'Open' category. Between June 2020 until June 2022

- Drones with a weight less than 500g may be operated in an area where it is reasonably expected that no uninvolved person is overflown
- Drones with weight up to 2kg may be operated up to 50m horizontal distance from people
- Drones with weight up to 25kg may be operated at 150m horizontal distance of residential, recreational and industrial areas, in a range where it is reasonably expected that no uninvolved person is overflown during the entire time of the operation.

Operations in 'Specific' category may be conducted after the authorisation given by the National Aviation Authority

Based on:

- The risk assessment and procedures defined by the EU Regulation
- Predefined risk assessment published by EASA as an AMC[48].

Regulatory requirements of the OPEN, SPECIFIC and (from 2020/21) on the CERTIFIED categories of UAS operations can be found in (EU) Regulation 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft (articles 4, 5 & 6).

Please note that EU regulations are so far incomplete, and drone operations near an airport may be subject to other national/local regulations. Therefore, your first responsibility should be to check the regulations that apply to your national/local situation.

→ See Annex H for Regulations Reference Documents & Useful Links

48. Alternative Means of Compliance.

B. Operational Characteristics

The nature of drones and their operational characteristics introduce several concepts, which are either new to the ATM domain or sufficiently different from conventionally piloted aircraft operations to warrant further consideration.

Visual Line of Sight (VLOS)

A visual line of sight operation is one in which the remote pilot maintains direct visual contact with the aircraft to manage its flight and meet separation and collision avoidance responsibilities. This is the basis for the majority of operations currently being approved by the Competent Authorities. The requirement to maintain visual contact with the drone allows the delegation of collision avoidance accountability to the remote pilot.

It is anticipated that extension of drone operations beyond the line of sight of the remote pilot may be authorised in cases where a trained observer is able to maintain visual line of sight with the drone and direct communication with the drone pilot (RP[49]). This mode of operation is currently referred to as Extended Visual Line of Sight (EVLOS). Operations which cannot be conducted as VLOS or EVLOS are classified as Beyond Visual Line of Sight (BVLOS).

Detect and Avoid (DAA)

At the time of writing, research and technology developments for drone operations are primarily focused on enabling BVLOS operations through the development of what is termed Detect and Avoid (DAA) technology. This technology once established is cited as the key enabler for drone operations especially those outside segregated airspace.

Detect and Avoid is defined[50] as "the capability to see, sense or detect conflicting traffic or other hazards and take the appropriate action". This capability aims to ensure the safe execution of a drone flight and to enable full integration in all airspace classes with all airspace users.

Lost Link

The loss of command and control link contact with the drone such that the remote pilot can no longer manage the aircraft's flight is a key consideration for all drone operations. Lost link C2[51] procedures must be assessed by the Competent Authority for issuing operational permissions. Common procedures for drones that experience a lost link are return to the point of origin, loiter to (re-) establish C2 link or flight termination at or close to its current position.

When there is a loss of C2 link, the RP cannot intervene in a drone flight trajectory and the drone may be limited to performing automated actions. It is possible in extreme circumstances that a drone may experience what is termed a flyaway, characterised by a fully unrestrained operation. A loss of C2 link should not be equated to a failure of voice communication with ATC.

49. Remote Pilot.
50. ICAO Annex 2.
51. RPAS C2 is the command and control interaction between the drone and the remote pilot (or automated) to ensure the safe and efficient flight of the drone during all phases of operations (see Annex G: Glossary).

First Person View (FPV)

First Person View (FPV) refers to a device that generates and transmits a video image from a remotely piloted aircraft to a ground station providing the remote pilot the illusion of an onboard pilot's perspective. While FPV may be a useful aid to navigation in BVLOS applications, limitations of field of view, depth perception, downlink bandwidth and signal reliability mean it cannot yet be considered as the basis of an acceptable DAA capability.

ATC Communications Paths

Drone communication with ATC should be equivalent to manned aircraft capability for the relevant airspace or operation. However, as the RP is not on board the aircraft and equivalent communication performance may be difficult to achieve, a range of alternative communication architectures may be utilised.

These may include:

- Retransmission through the RPA
- Hand held VHF transceiver
- The use of alternate frequencies
- The use of a mobile phone or Portable Electronic Device (PED) as a contingency or backup solution only.

> The use of a mobile phone/device as a primary means of communication with ATC is generally not acceptable. In rare circumstances where a mobile phone/device is the only achievable means of communication, a safety assessment may need to be considered.

A range of contemporary communication solutions for the drone industry is in development and it is likely that the range of alternate options will expand over time.

Handover[52]

Responsibility for the control of a remotely piloted aircraft may be handed over in-flight between pilots using the same RPS, between different stations at the same site, or between RPS located distant from each other. In some circumstances, handover is achieved by the use of deliberate temporary C2 link disruption. Handover capability may be particularly useful in the case of an RPS failure or maintenance issue, allowing the flight to continue without losing control of the RPA.

52. Not typical for drone operations in protected aerodrome environments. If applicable, the handover procedures, systems and associated risks need to be assessed and mitigation actions arranged as necessary.

C. Approval Process

Introduction

Drone flyers must abide by a large and sometimes confusing set of rules about where they can and cannot fly. Flying near airports and many other types of infrastructure has required a cumbersome process of notification by telephone or manual requests for approval. In recent years, applications like Drone Assist in the UK and LAANC (Low Altitude Authorization and Notification Capability) in the USA have become indispensable tools for planning legal flight paths.

The description of Drone Assist and LAANC below are for illustration purposes only.

Drone Assist[53]

Drone Assist is the drone safety app from NATS, the UK's main air traffic control provider, powered by Altitude Angel. It presents users with an interactive map of airspace used by commercial air traffic so that you can see areas to avoid or in which extreme caution should be exercised, as well as ground hazards that may pose safety, security or privacy risks when you are out flying your drone.

It also contains a 'Fly Now' feature that enables you to share your drone flight location with other app users and the wider drone community, helping to reduce the risk of a drone related incident in the UK's airspace.

LAANC (USA)[54]

LAANC is the Low Altitude Authorization and Notification Capability, a collaboration between FAA (USA) and industry. It directly supports UAS integration into the airspace. LAANC provides:

- Drone pilots with access to controlled airspace at or below 400ft
- Air Traffic Professionals with visibility into where and when drones are operating.

Through the UAS Data Exchange, the capability facilitates the sharing of airspace data between the FAA and companies approved by the FAA to provide LAANC services. The companies are known as UAS Service Suppliers – and the desktop applications and mobile apps to utilise the LAANC capability are provided by the UAS Service Suppliers (USS).

LAANC automates the application and approval process for airspace authorisations. Through automated applications developed by an FAA Approved UAS Service Suppliers (USS), pilots apply for an airspace authorisation.

Requests are checked against multiple airspace data sources in the FAA UAS Data Exchange such as UAS Facility Maps, Special Use Airspace data, Airports and Airspace Classes, as well as Temporary Flight Restrictions (TFRs) and Notices to Airmen (NOTAMs). If approved, pilots can receive their authorisation in near-real time. LAANC provides airspace authorisations only. Currently, some 600 US airports support LAANC, with more being added. The concept behind it might be interesting for Europe as well.

---

53. https://dronesafe.uk/safety-apps/
54. https://www.faa.gov/uas/programs_partnerships/data_exchange/

Approval Process sample

FIGURE 12: **UAS GEOGRAPHICAL ZONE ACCESS PROCESS (HOLOGARDE)**

Approval considerations

Topics to be considered to obtain drone operations approval within the UAS Geographical Zone[55]

Step	Item	Details
1	**Operator Licence**	• Operator registered with contact details and licence to operate • Insurance for 3rd party damage arranged[56].
2	**Approved / Acceptable equipment**	• Registration details • Provide system configuration (e.g. frequency used) • Approved navigation capability • Approved surveillance capability ('transponder')[57] • Approved communication capability (if applicable) • Standards used • Conformance with regulatory requirements (e.g. airworthiness and/or operational requirements issued by the Competent Authority).

55. See Annex E for Process Workflow/Checklist.
56. Regulation (EC) 785/2004 defines the minimum level of coverage per accident depending on the drone's maximum take-off mass, where the minimum is €1,000,000. Most recent drone accidents fall into two categories 'Property damage' and 'Near miss' [DR5 2018].
57. Method to broadcast its position/essential details at close range e.g. by Mode-S transponder, Bluetooth or Wi-Fi transmitters, over a network by cellular communications. Must be compatible with ATC systems.

3	**Operations Manual**[59]	• Indicate the tasks and responsibilities of the organisation's actors (e.g. operator, pilot(s), maintenance, training procedures, etc.) • Specify the list of pilots, with their qualifications, and training procedures • Conditions and procedures envisaged for use, in relation to the type of operation of the area and the airspace concerned • Must contain limitations, normal and emergency procedures for conducting the flight, performance data and any operating limitations[59] • Any measures necessary for the protection of third parties on the ground and up in the air • Establish crew coordination procedures, if applicable, in particular the duties of observers • Establish the controls to be carried out before starting the flight activities, they must include checks to determine the absence of electromagnetic interference and inspections to ensure that the system is in navigable condition • Establish a system of registration of operations, and control of the associated risk • Establish procedures to define the take-off and landing area, and possibly the emergency recovery area • Establish the procedures to insert in the system and check the geographic coordinates of the take-off, landing, limits of the operations and of the possible recovery point • Define security measures, including those to prevent intrusion of unauthorised persons in the area of operations and procedures for stowage of the system • Define the procedures necessary to manage problems and accidents.
4	**Detailed Scenario, Flight plan**	• Purpose of flight • Equipment used • Scenario used • Daylight, VLOS only[60] • Pilot and contact details • Exact location (start/route/area/landing) • Time (start/stop) and flight duration • Checklist • Systems and communications check prior to operation.
5	**Communication protocol**	• Describe communication protocol with ATC and airport operator under both Normal and Contingency operations[61] • Include Go/No Go decision protocol.

58. See https://luftfartstilsynet.no/en/drones/commercial-use-of-drones/about-dronesrpas/ for samples (RO1.03).
59. E.g. Wind limitations, meteorological conditions minimums.
60. Daylight restriction could be lifted if risk assessment guarantees safe and secure operations, and risks associated with night operations can be mitigated properly.
61. E.g. Autopilot return to base in case of loss of link.

6	**Risk Assessment**	• Complete risk assessment form (SORA complemented with aerodrome operator and ANSP analysis) • Sign and send to Competent Authority/ATC/Airport Operator as appropriate.
7	**Airport Operator permission**	• Complete and sign the Letter of Agreement/Compliance as provided by airport operator • Airport operator to indicate who will supervise drone operations for adherence to protocol(s) • Infrastructure inspection after drone operations • Pay fees where applicable.
8	**ATC permission**	• Complete and sign Letter of Agreement/Compliance Agreement as provided by ATC (where applicable).
9	**Law Enforcement/ Police permission**	• Complete and sign letter of agreement/compliance • Agreement as provided by police authorities (sensitive infrastructures, populated area overflight).
10	**Flight Evaluation**	• Keep record of flight (date/time, purpose of flight, scenario used, changes to plan and reasons, evaluation and improvement suggestions/actions).

RECOMMENDATIONS

- It is recommended that airport operators develop a simple procedure for the drone operations approval process, preferably via internet application and/or mobile app.
- It is recommended to include the Risk Assessment form in an easy format, e.g. fillable PDF form, which can be downloaded directly via the website/app.
- It is recommended to include the Letter of Agreement/Compliance in an easy format, e.g. fillable PDF form, which can be downloaded directly via the website/app.
- It is recommended to include the checklist for the drone operator in an easy format, e.g. fillable PDF form, which can be downloaded directly via the website/app. This completed checklist must be submitted by the drone operator prior to obtaining approval.
- It is recommended to allocate a unique 'drone mission identification number' in order to facilitate proper follow-up. Once given approval, the drone mission ID number should be used by the actors (unless other arrangements have been made).

→ **See Annex E for Workflow/Operational Checklist**

D. Risk Assessment – SORA[62]

As mentioned in the Introduction (Chapter 1), special attention needs to be given to manage the different risks properly. Typically, the first mindset may be focused on safety and/or security, but there are more risks that may need to be managed:

Safety	Security	Business Continuity	Reputation

The risk and impact level may vary from one airport to another, depending on local circumstances. Business Continuity and Reputation risks will not be elaborated further, but they will be addressed in a future update of this document.

General

A risk-based approach to drone integration needs to be taken. This should include but not be limited to the following:

- The application of risk management tools and techniques
- Consideration, evaluation and mitigation measures of safety risks
- Consideration, evaluation and mitigation measures of security risks
- Consideration of human factors
- Other risks, as identified for the particular use case.

One methodology towards risk-based approach is known as Specific Risk Operations Assessment (SORA), of which a generic description is provided below. As SORA is the proposed risk assessment methodology for UAS operations by EASA, it should be the methodology of choice in order to facilitate approvals from all relevant entities.

> SORA will be used for the drone design and the drone operational part (specific drone category), whereas aerodrome and ATM/ANS safety assessment will be conducted for the Airport and ATS part to verify that such operation is acceptably safe in this airport operational environment.

SORA

SORA is a **multi-stage process of risk assessment** aiming at risk analysis of certain unmanned aircraft operations, as well as defining necessary mitigations and robustness levels.

62. SORA: Specific Operations Risk Assessment.

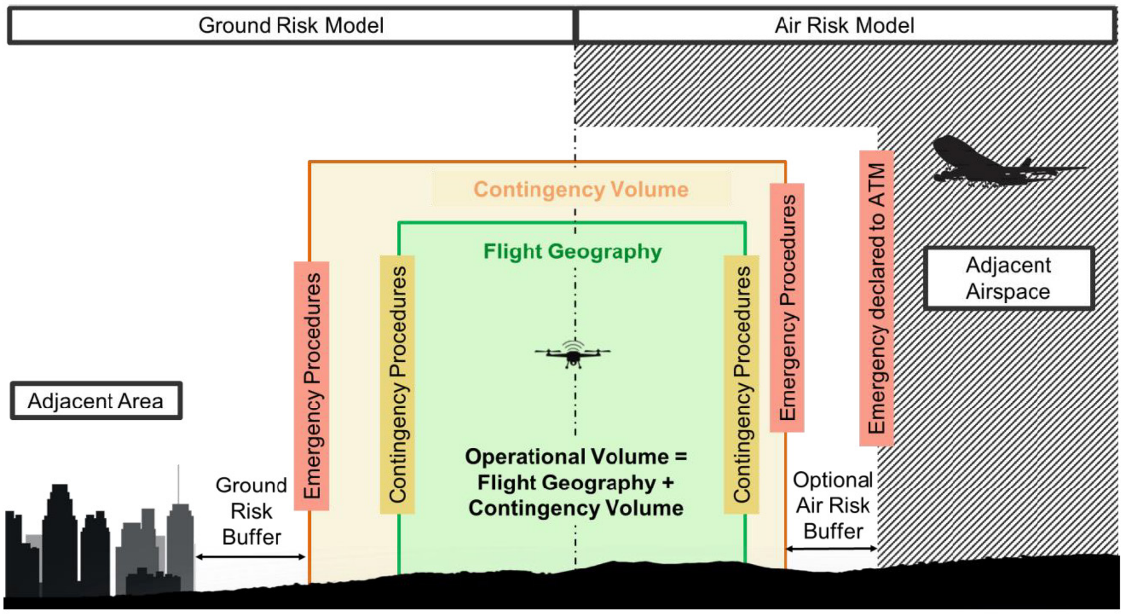
GRC and ARC

SORA focuses on assigning to a UAS-operation two classes of risk:

1. a **Ground Risk Class (GRC)** and
2. an **Air Risk Class (ARC)**

The Specific Operations Risk Assessment (SORA) has been endorsed by the European Union Aviation Safety Agency (EASA) as an Acceptable Means of Compliance (AMC) to fulfil the requirements of the EU Regulations (Basic Regulation, Implementing Act, Delegated Act and Annexes).

FIGURE 13: **GRAPHIC REPRESENTATION OF SORA SEMANTIC MODEL (JARUS)**



The GRC and ARC form the basis to determine the so-called **Specific Assurance and Integrity Levels (SAIL)** for both respectively. The SAIL represent the level of confidence that the UAS operation will stay under control within the boundaries of the intended operation. The SORA allows operators to utilise certain threat barriers and/or mitigating measures to reduce both risk-classes and thereby reduce the SAIL. The final step in the risk assessment is the recommendation of the **Operational Safety Objectives (OSO)** to be met in accordance with the SAIL. The SORA is a method to integrate UAS operations with (commercial) manned aviation independent of the weight of the UA and altitude in the airspace with a certain level of safety.

To facilitate the SORA process, standardised **Use Cases (UCs)** may be developed for certain types of operations, with known hazards and acceptable risk-mitigations. The applicable Use Case[63] may then be used by operators and regulating authorities as a template to reduce the amount of work involved with approving UAS-operations.

63. See Annex F: Use Cases.

Robustness

To properly understand the SORA process, it is important to introduce the key concept of robustness. Any given risk mitigation or operational safety objective can be demonstrated at differing levels of robustness. The SORA proposes three different levels of robustness: Low, Medium and High, commensurate with the risks.

The **robustness** designation is achieved using both

- the **level of integrity** (i.e. safety gain) provided by each mitigation, and
- the **level of assurance** (i.e. method of proof) that the claimed safety gain has been achieved.

These are both risk-based.

Assurance Level	General Guidance
Low	A Low level of assurance is where the applicant simply declares that the required level of integrity has been achieved.
Medium	A Medium level of assurance is one where the applicant provides supporting evidence that the required level of integrity has been achieved. This is typically achieved by means of testing (e.g. for technical mitigations) or by proof of experience (e.g. for human-related mitigations).
High	A High level of assurance is where the achieved integrity has been found acceptable by a competent third party.

FIGURE 14: **DETERMINATION OF ROBUSTNESS LEVEL (SORA)**

	Low Assurance	Medium Assurance	High Assurance
Low Integrity	Low Robustness	Low Robustness	Low Robustness
Medium Integrity	Low Robustness	Medium Robustness	Medium Robustness
High Integrity	Low Robustness	Medium Robustness	High Robustness

For example, if an applicant demonstrates a Medium level of Integrity with a Low level of assurance the overall robustness will be considered as Low. In other words, the robustness will always be equal to the lowest level of either integrity or assurance.

Risk and Harm

Many definitions of the word **"risk"** exist in the literature. One of the easiest and most understandable definitions is provided in the SAE ARP 4754A/EUROCAE ED-79A: "the combination of the frequency (probability) of an occurrence and its associated level of severity". This definition of "risk" is retained in this document. The consequence of an occurrence will be designated as a **harm** of some type.

Many different **categories of harm** arise from any given occurrence. Various authors on this topic have collated these categories of harm as supported by literature. This document will focus on occurrences of harm (e.g. an UAS crash) that are short-lived and usually give rise to near loss of life. Chronic events (e.g. toxic emissions over a period of time) are explicitly excluded from this assessment.

The categories of harm in this document are the potential for causing:

- Fatal injuries to third parties on the ground
- Fatal injuries to third parties in the air
- Damage to critical infrastructure
- Damage to property on the ground.

It is acknowledged that the competent authorities, when appropriate, may consider additional categories of harm (e.g. disruption of a community, environmental damage, financial loss, etc.). This methodology could also be used for those categories of harm.

Several studies have shown that the amount of energy needed to cause fatal injuries in the case of a direct hit are extremely low (i.e. in the region of few dozen Joules). The energy levels of operations addressed within SORA are likely to be significantly higher and therefore the retained harm is the potential for fatal injuries. By application of the methodology, the applicant has the opportunity to claim lower lethality either on a case-by-case basis, or systematically if allowed by the competent authorities (e.g. open category).

Fatal injury is a well-defined condition and, in most countries, known by the authorities. Therefore, the risk of under-reporting fatalities is almost non-existent. The quantification of the associated risk of fatality is straightforward. The usual means to measure fatalities are by the number of deaths within a particular time interval (e.g. fatal accident rate per million flying hours), or the number of deaths for a specified circumstance (e.g. fatal accident rate per number of take-offs).

Damage to critical infrastructure is a more complex condition and different countries may have differing sensitivities to this harm. Therefore, the quantification of the associated risks may be difficult and subject to national specificities.

The likelihood of each category of harm occurring can be broken into its individual component likelihoods as follows:

FIGURE 15: **LIKELIHOOD OF HARM (JARUS)**

Likelihood of fatal injuries to third parties on ground	=	Likelihood of having UAS operation out of control	X	Likelihood of person struck by the UA if the operation is out of control	X	Likelihood that, if struck, person is killed
Likelihood of fatal injuries to third parties in the air	=	Likelihood of having UAS operation out of control	X	Likelihood of other A/C struck by the UA if the operation is out of control	X	Likelihood that, if struck, the other A/C cannot continue a safe flight and landing
Likelihood of damage to critical infrastructure	=	Likelihood of having UAS operation out of control	X	Likelihood of critical infrastructure struck by the UA if the operation is out of control	X	Likelihood that, if struck, the critical infrastructure is damaged

Operational Safety Objectives

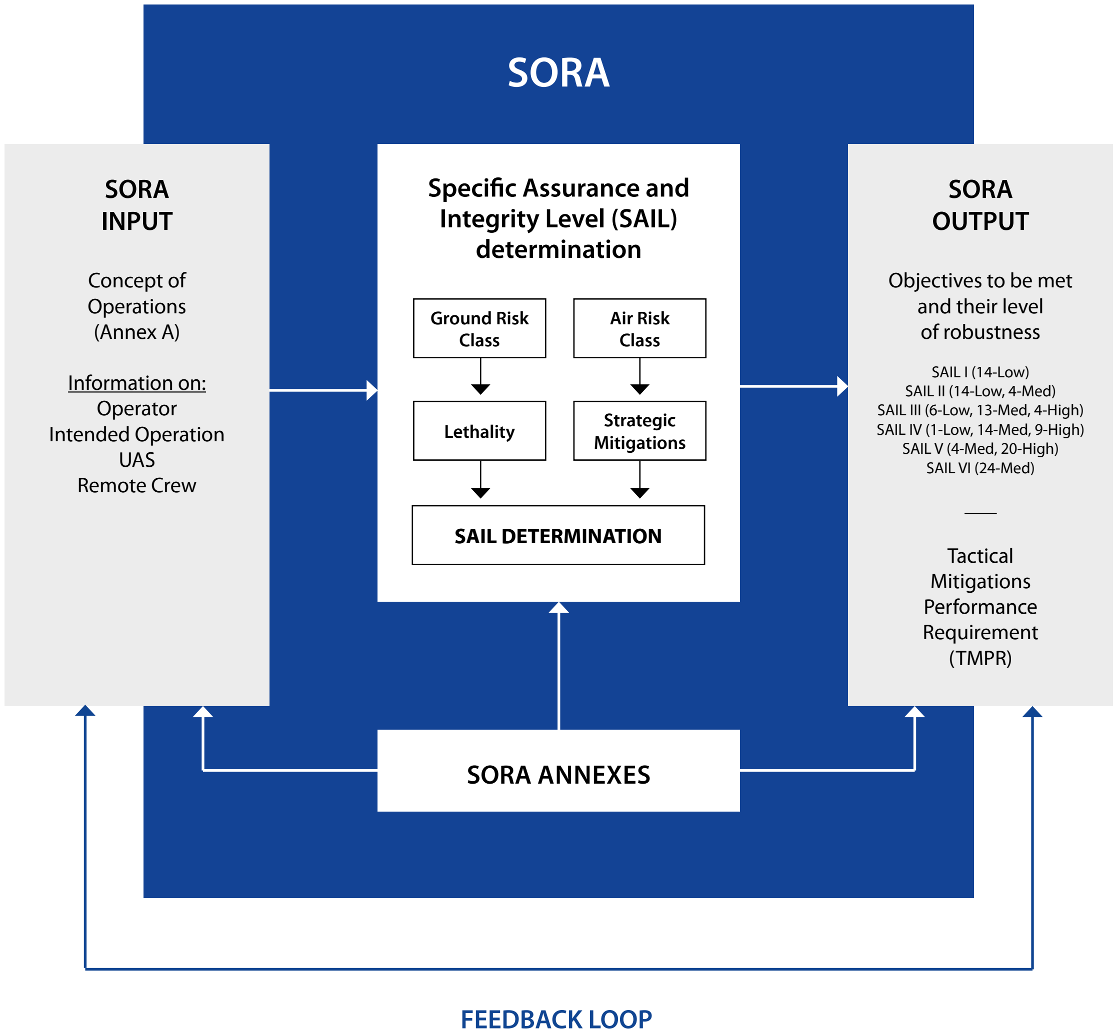
Operational Safety Objectives[64]	
Technical issue with the drone	• Ensure the operator is competent and/or proven • Drone manufactured by competent and/or proven entity • Drone maintained by competent and/or proven entity • Drone developed to authority recognised design standards • Drone is designed considering system safety and reliability • C3 link performance is appropriate for the operation • Inspection of the drone (product inspection) to ensure consistency to the ConOps • Operational procedures are defined, validated and adhered to • Remote crew trained and able to manage the abnormal situation • Safe recovery from technical issue.
Deterioration of external systems supporting UAS operation	• Procedures are in place to handle the deterioration of external systems supporting drone operations • The drone is designed to manage the deterioration of external systems supporting UAS operations • External services supporting drone operations are adequate to the operation.
Human error	• Operational procedures are defined, validated and adhered to • Remote crew trained and able to manage the abnormal situation • Multi crew coordination • Remote crew is fit to operate • Automatic protection of the flight envelope from human error • Safe recovery from human error • A human factors evaluation has been performed and the HMI found appropriate for the mission.
Adverse operating conditions	• Operational procedures are defined, validated and adhered to • The remote crew is trained to identify critical environmental conditions and to avoid them • Environmental conditions for safe operations defined, measurable and adhered to • UAS designed and qualified for adverse environmental conditions.

SORA Process

(a) With a solid understanding of the elements to be evaluated when dealing with risks of specific UAS operations (i.e. threats, harms and their barriers) and armed with a sound knowledge of the main parameters to be estimated, the SORA process can now be established. The entire process is depicted in Figure 16.

64. Source: JARUS guidelines on SORA.

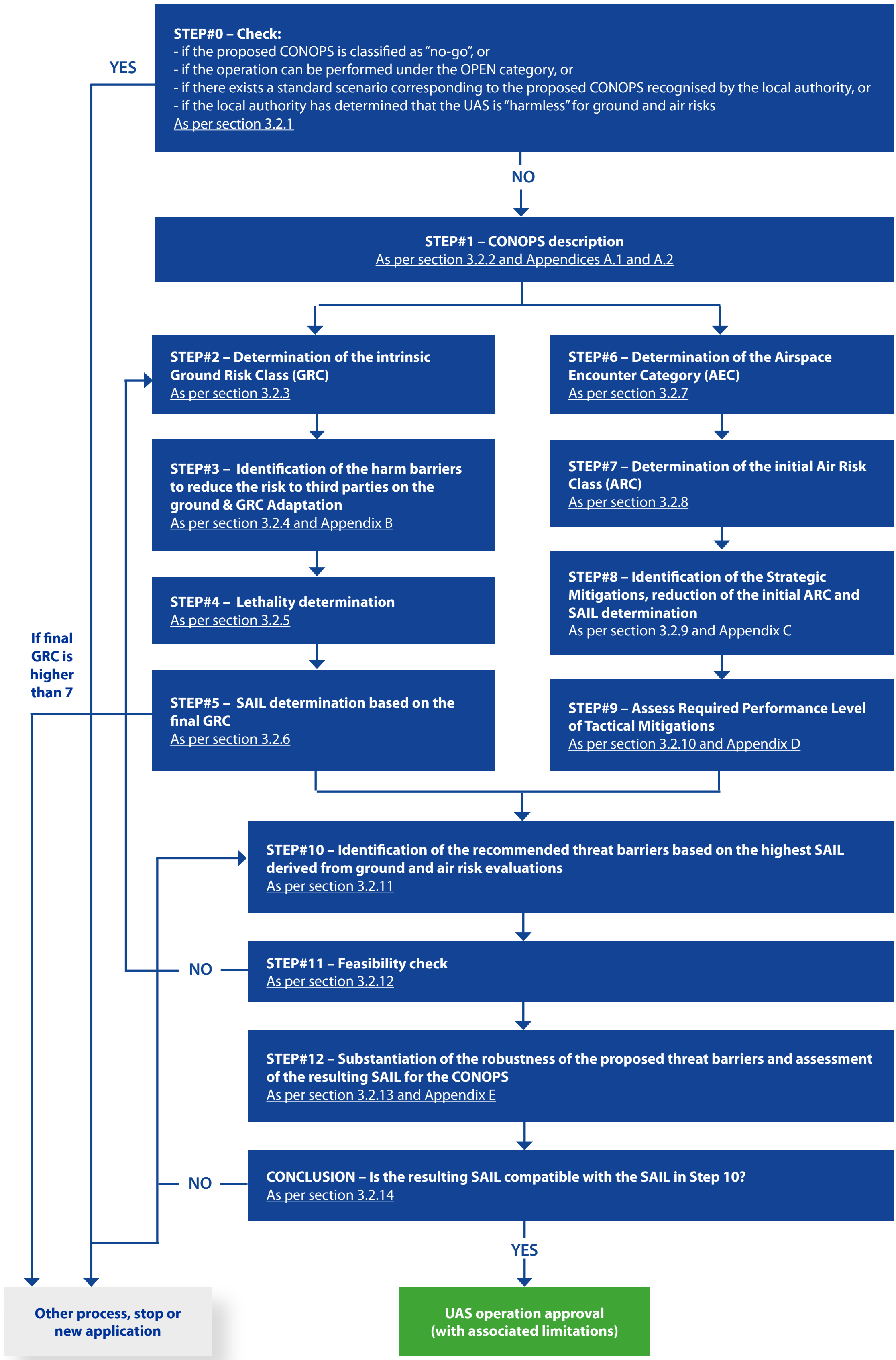
FIGURE 16: **SORA OVERVIEW**



(b) The current SORA focuses on the assessment of ground and air risk. In addition to the SORA, a risk assessment of critical infrastructure should also be performed in cooperation with the responsible organisation for the infrastructure, as they are most knowledgeable of the threats.

(c) The SORA methodology provides a logical process to analyse the proposed ConOps and establish an adequate level of confidence that it can be conducted with an acceptable level of risk. There are essentially fourteen steps supporting the proposed SORA methodology and each of these steps is described in the following paragraphs and further detailed, when necessary, in the relevant appendix.

FIGURE 17: **SORA PROCESS**



→ See Annex A: Regulations > SORA (JARUS, guidelines)

E. Workflow/Checklist (examples)

Workflow[65]

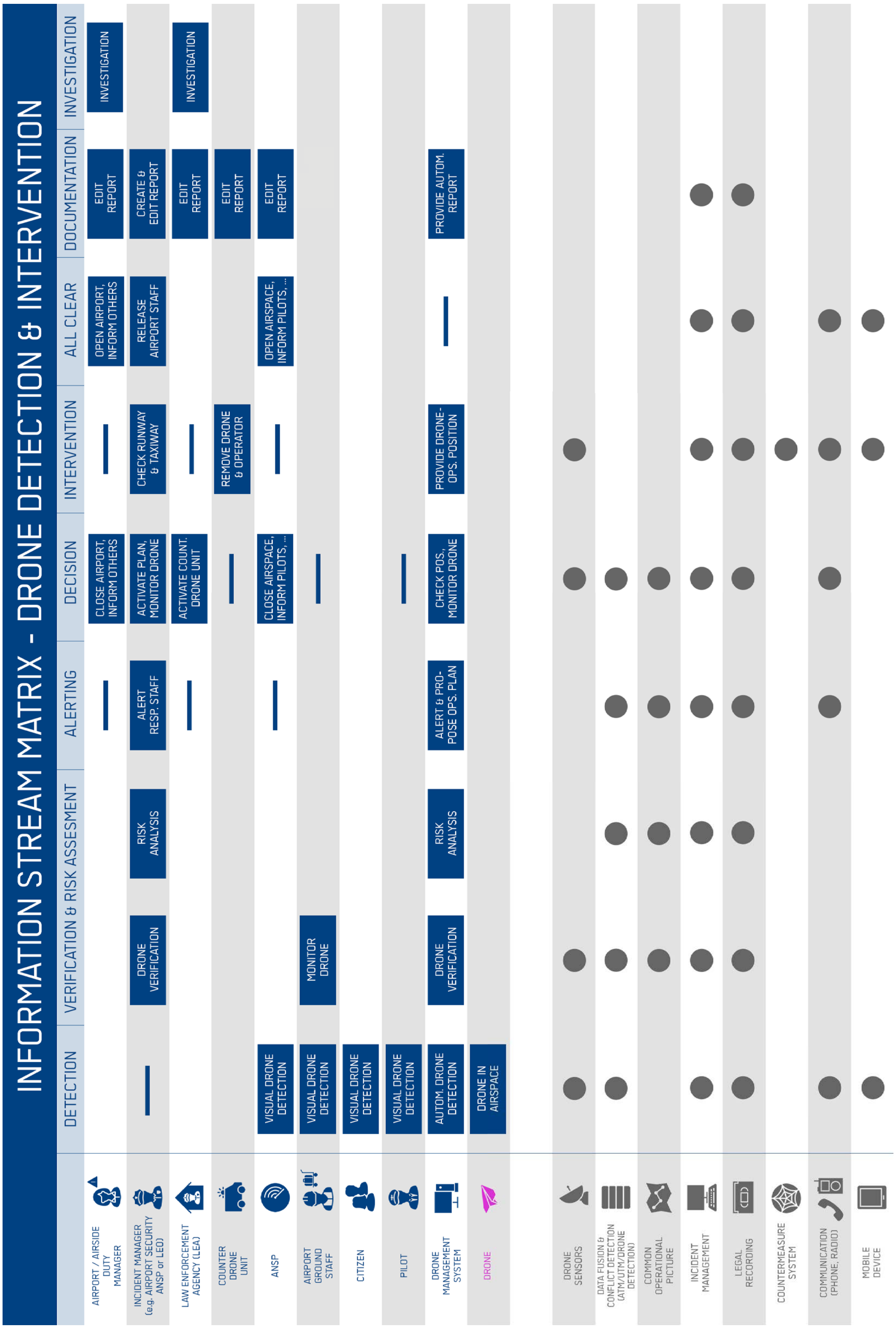
FIGURE 18: **DRONE OPERATIONS PROCESS WORKFLOW**

WHEN	WHAT	HOW	WHO
INITIAL	Obtain Drone Operator Licence	Verify EASA & local requirements	Drone Operator ▼ Competent Authority (CAA)
		Arrange approved equipment	
		Make Operations Manual (use template)	
		Contact Competent Authority (CAA)	
PREPARATION	Elaborate Operational Scenario	Make detailed flightplan	Drone Operator ▼ Airport Operator/ANSP
		Elaborate Risk Assessment (SORA)	
		Elaborate Contingencies	
		Make communications protocol	
PRE-TACTICAL D-1 OR BEFORE	Obtain Airport Operator Approval	Sign Letter of Agreement	
		Arrange applicable fees	
		As per local requirements	
TACTICAL D-0	Execute Operational Scenario	Use checklist(s)	Drone Operator
POST OPS	Report Incident (if applicable)	As required and described in Operations Manual	
	Complete Logbook		
	Evaluate Flight		

65. Airport Operator Approval could also be issued by Air Traffic Control, as per national/local arrangement.

Information Stream Matrix – Detection & Intervention[66]

FIGURE 19: **INFORMATION STREAM MATRIX (FREQUENTIS)**



66. Sample (simplified) matrix provided by Frequentis. A more detailed matrix and more information is available at the Frequentis website – see Annex H (Reference Documents and Useful Information/Various).

F. Standardised Use Cases[67]

The aim of Standardised Use Cases is to ensure the drone operations will be conducted in a structured way, with arrangements appropriate and tailored to the purpose of that operation. It will also be beneficial to manage expectations and explain the roles and responsibilities of each actor in a particular scenario.

Due to the need for a different approach, the Standardised Use Cases can be classified in 2 main groups:

- Good (cooperative) drones
- Bad (non-cooperative) drones.

Good Drones

Inspections Airside

- Flight Aids Inspections - ILS, Papi, Runway Lights, etc.
- Runway/Taxiway/Apron Inspections
- Airside - outside runway strip
- Aircraft - on stand
- Surveying of buildings, runway systems and construction sites.

Inspections Landside

- Airport Perimeter
- Landside - Buildings, parking.

Wildlife Management

Photo & Video

Parcel delivery & pickup

- Note: if a drone needs to land at an airport to drop off/pick up cargo there needs to be a process in place to verify the clean/unclean status of drone & cargo. This needs to be described in the Use Case, and incorporated in various (coordination) checklists.

Bad Drones

Preparation (pre-tactical)

- Define Roles & Responsibilities (all actors)
- Coordination & Communication Arrangements (all actors)
- Risk Assessment.

During Incident (tactical)

- Threat Assessment
- Decision making (activate pre-defined scenario)
- Response procedures.

Post Incident

- Start recovery process
- Resume normal operations
- Documentation and Reporting
- Investigation
- Safety & Security Analysis
- Lessons learned > preparation/communication.

67. More Use Cases will be developed as time progresses, and depending on business cases. See also Annex H for SORA Standard Scenarios (JARUS).

G. Glossary & Abbreviations

Glossary

Terminology	Explanation
Actor[68]	Participant in an action or process. This can be a person or a group of persons representing an organisation (see also stakeholder definition).
Aerodrome Traffic Zone (ATZ)	An airspace of defined dimensions established around an aerodrome for the protection of aerodrome traffic.
Airside	The airside area includes all parts of the airport where aircraft are operated or serviced (runways, taxiways, apron, and aircraft parking stands, de-icing facilities and dedicated maintenance areas).
Arrangement	A (written) agreement between two or more entities.
Beyond Visual Line of Sight (BVLOS)	An operation in which the remote pilot or RPA observer does not use visual reference to the remotely piloted aircraft in the conduct of flight.
Command and Control Link[69]	The data link between the RPS and the RPA, over which the flight is managed, is the Command and Control (C2) link. The C2 link may be direct between the RPS and RPA or relayed through an intermediate vehicle such as a satellite. The C2 link may perform four basic functions: 1. Relay of the remote pilot's instructions to the aircraft over the telecommand or uplink 2. RPA response, status and health reporting over the telemetry or downlink 3. Communication, carrying air-ground or air-air communications between the RP and ATC or other aircraft 4. Payload command and control; uplink, downlink and communications functions specific to the operation of the payload carried by the RPA. No certification standards have yet been established for C2 and various media are utilised,[70] from 3G mobile signals to satellite communications[71]. The robustness of the C2 link, particularly the telecommand and telemetry components is an important consideration for the integration of RPAS (drones) into ATM operations. This is discussed under 'Lost Link' (Operational Characteristics).

68. Definition in Google Dictionary.
69. C2 = Command and Control, C3 = Command, Control & Communication.
70. ICAO Doc 10019, Manual on Remotely Piloted Aircraft Systems (RPAS).
71. See http://jarus-rpas.org/publications JAR doc 02 - RPAS C2 Link RCP.

Congested Areas	Areas or agglomerations used as residential, industrial, commercial, sporting areas, and in general areas where there may be gatherings, even temporary, of people.
Contingency	Something that might possibly happen in the future, usually causing problems or making further arrangements necessary.
Controlled Airspace	Controlled Airspace is a generic term, which covers ATS airspace classes A, B, C, D, & E and includes Control Areas, Terminal Control Areas, Airways and Control Zones.
Detect and Avoid (DAA)	The capability to see, sense or detect conflicting traffic or other hazards and take the appropriate action.
Entity	A person, partnership, organisation, or business that has a legal and separately identifiable existence.
Extended Visual Line of Sight (EVLOS)	Operations conducted in areas whose dimensions exceed the limits of VLOS conditions and for which the requirements of VLOS are satisfied with the use of alternative methods.
Flight Termination System	A Flight Termination System allows for the deliberate, safe and controlled termination of flight in the event of an emergency. The system may be initiated by the remote pilot or automatically based on a programmed series of failures or events. A primary consideration in determining the appropriate mode of termination will be to minimise the possibility of harm to other persons, property or aircraft on the ground or in the air.
Hand-over	Procedure for transferring commands from one pilot (or air traffic controller) to another.
Harm	The consequence of an occurrence: categories of harm considered in SORA are: • Fatal injuries to third parties on the ground • Fatal injuries to third parties in the air • Damage to critical infrastructure.
Landside	The landside an area where passenger transit from and to the airside is conducted. In this context, landside includes the terminal buildings (check-in, security, border control, passenger gates, etc.) as well as access facilities to the airport (e.g. car parking areas, trains, access roads, etc.).
Remote Pilot (RP)	The remote pilot (RP) is located external to the aircraft and maintains control of the RPA through a remote pilot station. Remote pilots may be assisted by other crew members but it is the RP who has direct responsibility for the safe conduct of the aircraft throughout its flight. It is the presence of a remote pilot within the system which distinguishes drone operations from other unmanned aerial systems.

Remote Piloting Aircraft (RPA)	Remotely piloted aircraft ('drones') are unmanned aircraft which are controlled by a remote pilot through a remote pilot station located external to the aircraft. Some functions of the RPAS (drones) may be automated but, in normal operation, there always remains an element of manual intervention and control present.
Remote Piloting Aircraft System (RPAS)	System consisting of an aircraft (remote piloted aircraft) without persons on board, used for purposes other than for recreational and sports, and by the related components necessary for control and command (station of control) by a remote pilot.
RPAS C2	RPAS C2 is the aggregation of the airborne and ground-based functions executed between the drone and the remote pilot as commanded by the drone pilot or automated to achieve the interactions required to ensure the safe and efficient flight of the drone during all phases of operations.
Remote Pilot Station (RPS)	Any device through which the RP controls an RPA is considered a RPS. These vary in sophistication from smartphones to complex control suites, sometimes with multiple displays intentionally designed to replicate an aircraft flight deck.
Risk[72]	The combination of the frequency (probability) of an occurrence and its associated level of severity.
Segregated Airspace	Controlled or uncontrolled airspace expressly identified in dimensions, volumes and time windows of use for specific purposes and expressly authorised by the responsible ATC unit through the issue of a NOTAM.
Stakeholder	'Operational stakeholders' means the civil and military airspace users, civil and military air navigation service providers, airport operators, airport slot coordinators and operating organisations and any additional stakeholder groups considered relevant for the individual functions (see also Actor definition).
Unauthorised Drone	Any drone activity (in the aerodrome environment) without authority or permission, and could result in safety/security risk and/or have a negative impact on Business Continuity and/or Reputation.
Unmanned Aerial System (UAS)	UAS means an unmanned aircraft and the equipment to control it remotely.
Unmanned Aircraft (UA)	UA means any aircraft operating or designed to operate autonomously or to be piloted remotely without a pilot on board.

72. Definition by SAE ARP 4754A/EUROCAE ED-79A.

UAS Geographical Zone	'UAS geographical zone' means a portion of airspace established by the competent authority that facilitates, restricts or excludes UAS operations in order to address risks pertaining to safety, privacy, protection of personal data, security or the environment, arising from UAS operations. The UAS Geographical Zone typically consists of Aerodrome Traffic Zone (ATZ) and Runway Protection Zones at protected aerodromes.
U-Space	The U-space framework comprises an extensive and scalable range of services relying on agreed EU standards and delivered by service providers. These services do not replicate the function of ATC, as known in ATM, but deliver key services to organise the safe and efficient operation of drones and ensure a proper interface with manned aviation, ATC and relevant authorities. They may include the provision of data, supporting services for drone operators, for example, flight planning assistance and more structured services, such as tracking or capacity management.
Uncontrolled airspace	Operating volume for which an Air Traffic Control Service is not provided. It is generally associated with at least one Flight Information Service that provides traffic or weather information at the request of the pilot.
Visual Line of Sight (VLOS)	Operations conducted within a distance, both horizontally and vertically, so that the remote pilot is able to maintain continuous visual contact with the plane, without the aid of tools to increase sight, such as to allow him a direct control of the means to manage the flight, keep the separations and avoid collisions.

Abbreviations

Abbreviation	Meaning
AFIS	Aerodrome Flight Information Service
AGL	Above Ground Level (height)
AIP	Aeronautical Information Publication
AIS	Aeronautical Information Service
AMC	Alternative Means of Compliance
ANSP	Air Navigation Service Provider (ATC)
ARC	Air Risk Class (SORA)
ASP	Airport Security Programme
ATC	Air Traffic Control
ATZ	Aerodrome Traffic Zone
BVLOS	Beyond Visual Line of Sight
C2	Command and Control Link
C3	Command, Control and Communication
CAA	Civil Aviation Authority
CNS	Communication, Navigation and Surveillance
CS	Certification Specification
CTR	Control Area (around airports with ATC Tower)
C-UAS	Counter-Unmanned Aircraft System
DAA	Detect and Avoid
DFZ	Drone Fly Zone
EASA	European Union Aviation Safety Agency
EVLOS	Extended Visual Line of Sight
FAA	Federal Aviation Agency (USA)
FPV	First Person View
GM	Guidance Material
GRC	Ground Risk Class (SORA)
IFP	Instrument Flight Procedures
IFR	Instrument Flight Rules
JARUS	Joint Authorities for Rulemaking on Unmanned Systems

LAANC	Low Altitude Authorization and Notification Capability (USA)
LoA	Letter of Agreement
LDR	Limited Drone Zone
LEA	Law Enforcement Authority
LUC	Light UAS Operator Certificate (EASA, Part-UAS)
MOM	Maintenance and Operations Management
NDZ	No Drone Zone
NM	Nautical Mile (1,852 km)
NOTAM	Notice to Airmen
OSO	Operational Safety Objective (SORA)
PLS	Possible Launch Site
PRD	Prohibited, Restricted & Danger (areas)
RCP	Required Communication Performance (JARUS)
RP	Remote Pilot (‘drone pilot’)
RPA	Remotely Piloting Aircraft
RPAS	Remotely Piloted Aircraft System (‘drone’)
RPS	Remote Pilot Station
RPZ	Runway Protection Zone
SAG	Safety Action Group
SAIL	Specific Assurance and Integrity Levels (SORA)
SC	Safety Committee
SMS	Safety Management System
SORA	Specific Operations Risk Assessment
SRB	Safety Review Board (SMS)
STS	Standard Scenario
UA	Unmanned Aircraft
UAS	Unmanned Aircraft System (‘drone’)
UAV	Unmanned Aircraft/Aerial Vehicle
UC	Use Case
UTM	U-Space Traffic Management
VFR	Visual Flight Regulations
VLOS	Visual Line of Sight

H. Reference Documents & Useful Links[73]

REGULATIONS
Common Rules for Drones (EASA)[74] https://www.easa.europa.eu/easa-and-you/civil-drones-rpas
(EU) REG 2019/947 on the Rules & Procedures for the operation of unmanned aircraft (24/5/2019) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0947&from=EN
AMC and GM to (EU) REG 2019/947 https://www.easa.europa.eu/acceptable-means-compliance-and-guidance-material-group/amc-gm-implementing-regulation-eu-2019947
AMC and GM to Part-UAS (UAS operations in the 'open' and 'specific' categories) https://www.easa.europa.eu/document-library/acceptable-means-of-compliance-and-guidance-materials/amc-gm-part-uas-%E2%80%94-issue-1
(EU) REG 139/2014 – Rules for Aerodromes https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2014:044:0001:0034:EN:PDF
(EU) REG 300/2008 on Common Rules in the field of Civil Aviation Security (01/02/20109) https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32008R0300
Development of UAS Regulation (ICAO) https://www.icao.int/safety/UA/UASToolkit/Pages/Narrative-Regulation.aspx
Manual on Remotely Piloted Aircraft Systems (RPAS) - ICAO Doc 10019 https://skybrary.aero/bookshelf/books/4053.pdf
SORA – (JAR Doc 06; JARUS) http://jarus-rpas.org/publications
UAS Operational Categorisation (JAR Doc 09; JARUS) http://jarus-rpas.org/publications
SORA Standard Scenarios (JARUS) https://www.easa.europa.eu/newsroom-and-events/news/easa-publishes-opinion-%E2%80%9Cstandard-scenarios-uas-operations-%E2%80%98specific%E2%80%99
Drone Rules EU http://dronerules.eu/en/professional
FAA Small Unmanned Aircraft Regulations (Part 107) https://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=20516

73. The list with Reference Documents and Useful Links is not intended to be complete and exhaustive, and cannot be. The reader has to realise and accept the drone development is evolving quickly and information may be found out of date even soon after publication of this document. Therefore it is recommended to check if there are updates of new information which supersedes the information given in this section.
74. With download links for: (a) 'Flying a Drone, do's and don'ts' for C0…C4 class of drones (b) 'Safe operations of drones in Europe'. Recommended reading.

SESAR (Research & Development)

U-Space blueprint
https://www.sesarju.eu/U-space

CONOPS European UTM systems
https://www.eurocontrol.int/project/concept-operations-european-utm-systems

Initial UAS Traffic Management (PODIUM)
https://www.eurocontrol.int/project/proving-operations-drones-initial-uas-traffic-management

TECHNOLOGY

Drone Technology – ACI EUROPE Position Paper (2018)
https://www.aci-europe.org/component/attachments/attachments.html?id=255

C-UAS (legal/technical)
https://www.governmenteuropa.eu/legal-technical-drone-technologies/88149/

C-UAS (whitepaper on airport drone protection)
https://www.mydefence.dk/2019/02/mydefence-publishes-white-paper-on-airport-drone-protection/

VARIOUS

ACI Drones Policy Paper (2018)
https://aci.aero/wp-content/uploads/2018/08/ACIPolicyPaper_Drones_2018-1.pdf

ICAO UAS Toolkit (incl request for Authorisation Form)
https://www.icao.int/safety/UA/UASToolkit/Pages/default.aspx

Managing Unmanned Aircraft Systems in the Vicinity of Airports (ACRP Report 144, Project 03-42)
https://www.nap.edu/catalog/21907/unmanned-aircraft-systems-uas-at-airports-a-primer

Airports and UAS (ACRP Report 0342)
https://apps.trb.org/cmsfeed/TRBNetProjectDisplay.asp?ProjectID=4240

Current Landscape of Unmanned Aircraft Systems at Airports, 2019 (ACRP Synthesis 104)
https://www.nap.edu/download/25659

SORA (ECA)
https://www.eurocockpit.be/positions-publications/specific-operations-risk-assessment-sora

Dronesafe (UK)
https://dronesafe.uk/

Guidance for Small Unmanned Aircraft users (CAP 1763, UK CAA)
https://publicapps.caa.co.uk/docs/33/CAP1763%20New%20UAS%20guidance%20Feb%202019.pdf

Guidance on the UAS application process (UK CAA)
https://www.caa.co.uk/Commercial-industry/Aircraft/Unmanned-aircraft/Small-drones/Applications-for-unmanned-aircraft-operational-authorisations/

Drone Guide, Maps, Rules (Avinor, Norway)
https://avinor.no/en/corporate/at-the-airport/droner/choose-airport

Commercial use of drones (Avinor, Norway)[76]
https://luftfartstilsynet.no/en/drones/commercial-use-of-drones/about-dronesrpas/

Regulations and general questions relating to drones (FOCA, Switzerland)
https://www.bazl.admin.ch/bazl/en/home/good-to-know/drones-and-aircraft-models/allgemeine-fragen-zu-drohnen.html

D-Flight map Rome-Fiumicino (ENAV, Italy) – geo-awareness & drone registration service
https://www.d-flight.it/web-app/

Drone Preflight checklist sample (Heliguy)
https://www.heliguy.com/blog/2017/08/10/heliguy-pre-flight-checklist/

Drone Rules PRO Pre-flight checklist (privacy and data protection)
https://safetyculture.com/checklists/drone-preflight/

Drone threat and CUAS Technology - White Paper (Elbit Systems)
https://aviation.report/whitepapers/drone-threat-and-cuas-technology/5730

Drone detection and intervention - Airport, ANSP and law enforcement (Frequentis)
http://www.frequentis.com/drones

At the time of publication, the hyperlinks were valid, but they may have changed since then.

76. Including RPAS Operators Declaration Form, RPAS Operations Manual samples etc. Recommended reading.

I. Summary of Recommendations

Chapter	Topic	Recommendation(s)
4	**Roles & Responsibilities**	It is strongly recommended that the Competent Authority clarify the Roles and Responsibilities of (at least) the following actors: • Law Enforcement Authority • Airport Operator • ANSP • UTM/U-Space Service Provider • Drone Pilot. Elements to consider (but not limited to): • Information Sharing • Approval of Procedures • Risk Assessment process (Safety & Security) • C-UAS Activities • Coordination • Communication • Incident Reporting • Safety & Security Management. (All above for 'good' and 'bad' drone scenarios)
5	**UAS Geographical Zone**	Regulators, Competent Authorities and Airport Operators are strongly recommended to standardise the UAS Geographical Zone as much as possible, keeping the following criteria as a baseline: Horizontal: • Radius: The Aerodrome Traffic Zone (ATZ) as a minimum or expanded radius when more protection is required due to the layout of the airport (e.g. runway configuration). • Runway Protection Zones (RPZ): A rectangle extending 5km from the threshold of the runway away from the aerodrome, along the extended runway centreline, and 500m either side. • Airport perimeter: all security relevant airside buildings and areas that are encompassed by the airport perimeter fence, if not already covered by the two criteria above. Vertical: • The maximum height above ground level (AGL) inside the UAS Geographical Zone should not exceed the maximum of the vertical limit of the ATZ, whereby the maximum height in the Runway Protection Zones should be kept as low as possible (maximum 120m/400ft height from ground level (AGL) as is standard elsewhere). • Airports/ANSPs need to check if any of their IFP (instrument flight procedures) have protected zones that could interfere with the 120m (400ft) vertical limitation and take appropriate action where needed. Deviations from above recommendation could be possible on a case-by-case basis, only after conducting a safety assessment ensuring the additional risks can be mitigated (e.g. crossing traffic at low altitude). The UAS Geographical Zones shall be effective regardless of UAS size and weight.

5	**UAS Geographical Zone**	• Competent Authorities are strongly recommended to make the UAS Geographical Zones easily accessible for drone operator and the general public (website, app). • Competent Authorities are strongly recommended to facilitate software developers to be able to easily download the airport data (KML files etc.) from the AIS website.
6	**Drone Buffers**	• It is recommended that ANSPs develop standard buffers in order to separate drone operations from manned aircraft movements (in the air and on the ground). These buffers could be incorporated in the Standardised Use Cases, facilitating a standard approach to risk mitigation measures at least until effective technologies and protocols are widely available and deployed.
6	**Drone Fly Zones**	• The key enabler for the three fly zones is a suite of three dimensional maps that specify the location of the zones for each protected aerodrome. Competent Authorities/ANSPs are recommended to develop standardised specifications to identify the requirements for the 3 different Drone Fly Zones.
7	**Safety/ Security Risk Assessment**	• The safety/security risk assessment should include identifying sensitive infrastructures and/or areas and consider developing specific procedures for these 'hot spots'.
7	**Safety & Security Management**	• Airport operators are encouraged to develop and maintain a holistic view on safety/security management and include drone operations in their safety and security management system(s). • Airport operators and relevant stakeholders should be made aware of and/or trained on requirements for drone operations at or in the vicinity of their airport(s), including safety/security risks and mitigating actions, coordination arrangements and incident reporting (to include citizens).
8	**Coordination & Communication**	• A single point of coordination/contact is desirable, and should be considered in the coordination/communication arrangements. • It is strongly recommended to develop Quick Reaction Procedures (QRPs) in order to react effectively to non-cooperative drones. • These procedures should be trained to ensure all actors will act accordingly. • Airport operators are advised to include drones in their airport emergency plans, and perform communication/coordination exercises on a regular basis.
Annex C	**Approval Considerations**	• It is recommended to include the checklist for the drone operator in an easy format, e.g. fillable PDF form, which can be downloaded directly via the website/app. This completed checklist must be submitted by the drone operator prior to obtaining approval. • It is recommended to allocate a unique 'drone mission identification number' in order to facilitate proper follow-up. Once given approval, the drone mission ID number should be used by the actors (unless other arrangements have been made).

ACI EUROPE is the European region of Airports Council International (ACI), the only worldwide professional association of airport operators. ACI EUROPE represents over **500 airports** in 46 European countries. Our members facilitate over 90% of commercial air traffic in Europe: **2.3 billion passengers**, **21.2 million tonnes of freight** and **25.7 million aircraft movements** in 2018. In response to the Climate Emergency, in June 2019 our members committed to achieve **Net Zero** carbon emissions for operations under their control **by 2050**, without offsetting.

EVERY FLIGHT BEGINS AT THE AIRPORT.

www.aci-europe.org
Twitter: @ACI_EUROPE

Produced by ACI EUROPE
Designed by Caroline Terrée