Acceptable Means of Compliance and Guidance Material to Regulation (EU) 2021/664 on a regulatory framework for the U-space

Issue 1

16 December 2022[1]

[1] For the date of entry into force of Issue 1, please refer to ED Decision 2022/022/R at the Official Publication of EASA.

TABLE OF CONTENTS

AMC AND GM TO REGULATION (EU) 2021/664 ON A REGULATORY FRAMEWORK FOR THE U-SPACE (THE U-SPACE FRAMEWORK)

GM1 Article 1(1) Subject matter and scope

SCOPE — MILITARY AND STATE AIRCRAFT

(a) Although military and State aircraft operations are in principle excluded from the scope of Regulation (EU) 2018/1139[2] and its implementing and delegated acts, the safety of such operations is paramount when conducted in airspace that is subject to EU aviation safety regulations. In this context, the safe separation between military and State aircraft also in the U-space airspace is always expected during all stages of flight.

(b) It is recalled that when defining UAS geographical zones in accordance with Article 15 of Regulation (EU) 2019/947[3], Member States should also consider other aspects than safety, such as security aspects. Indeed, a Member State could designate a U-space airspace in critical areas for security and/or defence reasons, including military and State aircraft operations.

(c) In this context, military and State aircraft authorities are partners in the decision-making process of the coordination mechanism (as per Article 18(f) of Regulation (EU) 2021/664[4]) for the designation of U-space to cover the safety and security aspects in a U-space airspace, from the initial 'airspace risk assessment' until the U-space is implemented and monitored.

(d) The involvement of military authorities in relation to U-space is considered key to guaranteeing the level of safety and security in the U-space airspace from both a ground and an air risk perspective.

(e) For example, military and State aircraft that conduct short-notice off-airfield landings while carrying out their assigned operations may require portions of the U-space to be adjusted or possibly deactivated. In this case, air traffic control units should apply the dynamic reconfiguration of the U-space airspace at short notice, if/when required by military and State aircraft, as necessary, in accordance with the principles of Article 4 of Regulation (EU) 2021/664.

---

2 Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (OJ L 212, 22.8.2018, p. 1) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1139&qid=1670245547063).

3 Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft (OJ L 152, 11.6.2019, p. 45) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0947&qid=1670245620396).

4 Commission Implementing Regulation (EU) 2021/664 of 22 April 2021 on a regulatory framework for the U-space (OJ L 139, 23.4.2021, p. 161) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0664&qid=1670245701371).

GM2 Article 1(1) Subject matter and scope

SCOPE — SUPPORT TO PASSENGER OPERATIONS

At this stage of the implementation, the U-space is not foreseen to support passenger operations, which are today carried out with manned VTOL-capable aircraft and which ultimately could be autonomously performed with e-VTOL UAS.

Indeed, the U-space system is intended to ensure the segregation of manned aircraft subject to air traffic control or the remain-well-clear spacing of manned aircraft not subject to air traffic control, including manned VTOL-capable aircraft. UAS operations currently foreseen in urban environments are UAS carrying payload or goods, but not humans. Therefore, today, the U-space regulatory framework has been designed and relies on the overall assumption that drone-to-drone collisions will ultimately have limited consequences.

The integration of UAS passenger-carrying operations will require the reassessment of the whole U-space framework, with particular focus on:

(a) the acceptable level of safety (ALS) that will have to be strengthened in maintaining appropriate safety levels for manned aviation (i.e. to mitigate the risk of human casualties);

(b) complementary enablers/prerequisites that may be required to support the safety of such operations (e.g. additional mandatory U-space services and on-board functionalities).

GM1 Article 1(3) Subject matter and scope

APPLICABILITY

(a) The scope of Regulation (EU) 2021/664 is limited to unmanned aircraft, as well as to natural and legal persons involved in their operation; in the context of this Regulation: UAS operators, U-space service providers (USSPs), and common information services (CIS).

(b) Therefore, the requirements on ATS providers or the requirements related to manned aircraft operations are not included in this Regulation. Instead, the provisions pertaining to ATS providers are included in a dedicated amendment to Regulation (EU) 2017/373[5] through Regulation (EU) 2021/665. The provisions related to manned aircraft are included in a dedicated amendment to Regulation (EU) No 923/2012[6] (the SERA Regulation) through Regulation (EU) 2021/666 on implementing acts as regards air operations as well as the use of airspace and the design of airspace structures respectively.

---

[5] Commission Implementing Regulation (EU) 2017/373 of 1 March 2017 laying down common requirements for providers of air traffic management/air navigation services and other air traffic management network functions and their oversight, repealing Regulation (EC) No 482/2008, Implementing Regulations (EU) No 1034/2011, (EU) No 1035/2011 and (EU) 2016/1377 and amending Regulation (EU) No 677/2011 (OJ L 62, 8.3.2017, p. 1) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R0373&qid=1670245893943).

[6] Commission Implementing Regulation (EU) No 923/2012 of 26 September 2012 laying down the common rules of the air and operational provisions regarding services and procedures in air navigation and amending Implementing Regulation (EU) No 1035/2011 and Regulations (EC) No 1265/2007, (EC) No 1794/2006, (EC) No 730/2006, (EC) No 1033/2006 and (EU) No 255/2010 (OJ L 281, 13.10.2012, p. 1) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32012R0923&qid=1670245971615).

(c) Regulation (EU) 2021/664 does not apply to the following UAS operations for the following reasons:

(1) model aircraft operating in the framework of model aircraft clubs and associations that have received an authorisation in accordance with Article 16 of Regulation (EU) 2019/947 have demonstrated a good level of safety in clubs and associations, which allows to keep the seamless transition from the different national systems to the new Union regulatory framework provided for by Regulation (EU) 2019/947 is maintained;

(2) unmanned aircraft of a maximum take-off mass (MTOM) of less than 250 g when used in subcategory A1 of the 'open' category do not represent a significant safety risk in case of collision; this includes privately built unmanned aircraft of a MTOM of less than 250 g, as well as class C0 UAS as defined in Regulation (EU) 2019/945[7], including those that are toys in the meaning of Directive 2009/48/EC[8];

(3) UAS flying according to instrument flight rules (IFR) in accordance with the current standardised European rules of the air (SERA); they benefit from the provision of air traffic service (ATS), as summarised in Appendix 4 to Regulation (EU) No 923/2012; this does not exclude certified UAS from flying in U-space airspace with the support of U-space services; and

(d) Finally, it is recalled that Regulation (EU) 2021/665 does not apply to UAS that carry out military, customs, police, search and rescue, firefighting, border control and coastguard or similar activities and services undertaken in the public interest, by virtue of the scope defined in Article 2(3)(a) of Regulation (EU) 2018/1139.

GM2 Article 1(3) Subject matter and scope

MAXIMUM CEILING OF U-SPACE AIRSPACE

To ensure an additional strategic layer of mitigation as regards separation between manned and unmanned aircraft, Member States may consider limiting the U-space airspace to a 150 m (500 ft) height above the ground or water, in particular when the U-space airspace is designated in uncontrolled airspace.

Considering the novelty of the U-space and the lack of experience with its implementation, this limitation is deemed desirable to ensure safety of operations in the U-space airspace across the EU.

In this context, Member States may nevertheless decide to designate U-space airspace with a height greater than 150 m (500 ft) above the ground or water in controlled or uncontrolled airspace provided that there are additional services and means available to ensure a common reference altitude system between UAS and manned traffic, as well as additional U-space services and performance requirements for the services derived from the airspace risk assessment.

---

[7] Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems (OJ L 152, 11.6.2019, p. 1) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0945&qid=1670246132139).

[8] Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys (OJ L 170, 30.6.2009, p. 1) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32009L0048&qid=1670245459524).

GM1 Article 2(6) Definitions

DYNAMIC AIRSPACE RECONFIGURATION — SHORT-TERM CHANGES

Under the definition of 'dynamic airspace reconfiguration', the phrase 'short-term changes in manned traffic demand' may cover various cases ranging from clearing the path of an aircraft in emergency or distress, to accommodating unexpected traffic demand due to any contingency situation or allowing a shorter route for an individual flight, as well as potential U-space airspace restrictions to enable military and State operations. But the objective is to keep these cases exceptional when establishing the U-space airspace, for the sake of safety and efficiency of the aviation system.

GM1 Article 3 U-space airspace

GENRAL

(a) Member States have complete and exclusive sovereignty over the airspace above their territory and, therefore, have full authority over the designation of the U-space airspace.

(b) The designation of the U-space airspace is driven by safety, security, privacy or environmental considerations.

(c) For the designation of the U-space airspace, Member States are expected to assess numerous safety-significant factors, including, among others:

(1) the type, density, and complexity of existing and planned unmanned traffic, including UAS operations taking place in the context of authorised model aircraft clubs and associations;

(2) the type, density, and complexity of existing and planned manned traffic, including air sports activities;

(3) the operational capacity of the designated ATS providers to interface with the CIS provider and USSPs in the designated U-space airspace;

(4) the operational capacity of USSPs and, when relevant, the single CIS provider;

(5) the complexity of the airspace structure;

(6) the availability of safe and secure communication mechanisms to enable UAS operators and USSPs to exchange digital information;

(7) the classification of the airspace and the services provided to instrument flight rule (IFR) and visual flight rule (VFR) aircraft;

(8) existing UAS geographical zones defined in accordance with Article 15 of Regulation (EU) 2019/947; and

(9) the topographical environment and prevalent meteorological conditions.

(d) Conversely, when a Member State considers issuing a new authorisation to model aircraft clubs and associations or when defining new UAS geographical zones, already designated U-space airspace should be considered.

(e) Initial designations of U-space airspace are expected to take place at low-level altitude, e.g. below 500 ft, and where there is very little expected manned traffic.

(f) Besides the four mandatory U-space services, Member States may decide that additional U-space services are needed to support the safe, secure, and efficient conduct of UAS operations in specific volumes of U-space airspace.

(g) The regular reassessment of the U-space airspace is expected to be conducted by the Member States to evaluate its effectiveness in supporting the safe, secure, and efficient conduct of UAS operations.

AMC1 Article 3(1) U-space airspace

AIRSPACE RISK ASSESSMENT

The designation of the U-space airspace is intended to enable the safe management of a large number of UAS operations, while ensuring safety continuum as regards manned aviation:

(a) The airspace risk assessment should primarily consider the air risk and the related ground risk as a collateral effect of UAS mid-air collisions, and should ensure that the related hazards are adequately addressed.

(b) The airspace risk assessment should cover, as a minimum:

(1) hazard identification, including safety, security, privacy and environmental hazards;

(2) risk analysis, meaning the evaluation of the likelihood and severity of harmful effects induced by the identified hazards;

(3) based on the previous analysis, the definition of mitigation actions that should be taken when necessary to ensure an acceptable risk level.

(c) The airspace risk assessment should further allow to derive the U-space airspace design, performance requirements, constraints, etc., required to enable safe operations.

(d) The reassessment of the U-space airspace should be conducted to:

(1) support the introduction of major changes to the designated U-space airspace; and

(2) dynamically evaluate its adequacy and adjust its definition based on the experience gained from operations and major evolutions that may occur in its environment (e.g. emergence of critical ground infrastructures, extension of populated areas).

(e) The airspace risk assessment process should consider the coordination mechanism laid down in Article 18(f) of Regulation (EU) 2021/664.

GM1 Article 3(1) U-space airspace

REASONS FOR THE DESIGNATION OF U-SPACE AIRSPACE

The U-space airspace may be designated for several reasons; for example:

(a) Safety

(1) Having the need to share a common volume of airspace between manned and unmanned aircraft;

(2) To improve the visibility (e.g. by means of electronic conspicuity) of (un)manned aircraft, thus enabling a known traffic environment;

(3) To decrease the risk on ground in the case of multiple UAS flying over an assembly of people in urban areas or over highly populated areas (in combination with other means such as the certification of unmanned aircraft, UAS operators, etc.); and

(4) In the case of high UAS density, there could be a specific need to reduce the risk of UAS mid-air collision by organising the traffic through the introduction of certain UAS route structures. U-space services, such as geo-awareness, may provide support in that respect.

(b) Economy

(1) To ensure a fair and efficient sharing of the airspace volume between manned and unmanned aircraft, and between manned aircraft;

(2) To enable more complex and denser UAS operations; and

(3) To support the development of the drone sector and the provision of associated services to the public.

(c) Security

(1) To improve the visibility of unmanned aircraft by having most of the airspace users identified;

(2) To support the enforcement of local regulations and rules (e.g. prohibition of flights over sensitive sites, limited schedules, specific performance requirements) where there are too frequent violations, if the availability of the related UAS geographical zones is not sufficient to ensure the effective application of flight constraints to support UAS operations. This may notably concern the protection of critical infrastructures and no-fly zones;

(3) To support Member States' authorities in identifying, responding to, and investigating the use of UAS for malicious or unlawful purposes; and

(4) To support the protection of services that are critical to the proper functioning of the Member States, the economies and the societies from the use of UAS for malicious or unlawful purposes.

(d) Privacy

To support the enforcement of particular conditions for certain or all UAS operations for privacy reasons. Flying over some specific areas could be restricted to some users or to some slots (as it is the case for restricted areas for manned aviation).

(e) Environment

(1) To define environmental requirements for UAS operations (noise could be limited, a minimum height could be required);

(2) To distribute traffic density to an acceptable level of disturbance over environmentally sensitive sites;

(3) Enabling a diverse set of UAS operations (e.g. commercial and residential areas etc.), while respecting environmentally protected areas.

(4) To minimise CO_2 emissions, especially in urban environments.

GM2 Article 3(1) U-space airspace

AIRSPACE RISK ASSESSMENT — GENERAL

(a) An airspace risk assessment involves making use of information to determine possible relevant air and ground risks posed by unmanned aircraft flying in the airspace volume assessed, and regulate the conditions on privacy, security and environmental protection for all parties involved, including the citizens.

(b) An airspace risk assessment is a combination of qualitative and quantitative analysis ensuring that safety and performance criteria are defined, and that assumptions and enablers are consistent with the current airspace design and procedures. The methodology used in this process needs to contain a clear set of objectives and a realistic view of the operations conducted in a given airspace volume.

(c) Different formats are recognised (formal to less formal) for the approach to the analytical aspects of an airspace risk assessment. For some hazards, the number of variables and the availability of both suitable data and mathematical models may lead to credible results with sole quantitative methods (requiring mathematical analysis of specific data). However, few hazards in aviation lend themselves to credible analysis solely through quantitative methods. Typically, these analyses are supplemented qualitatively through critical and logical analysis of the known facts and their relationships.

(d) When available, appropriate tools for the quantitative analysis of the ground and air risk assessment may be used for the substantiation of the airspace risk assessment.

(e) In the case of UAS operators that intend to operate within a specific category under an operational authorisation or a light UAS operator certificate (LUC), the risk assessment referred to in Article 5(2) of Regulation (EU) 2019/947 should consider the outputs of the airspace risk assessment.

(f) The objective of the methodology applied should be to define a means for providing assurance that the U-space is acceptably safe, secure, and that privacy and environmental concerns are duly considered, covering at least the definition phase of the life cycle, and leading to the designation of the U-space airspace. Furthermore, the deployment of an operational U-space airspace requires an iterative process, through its development life cycle, from initial system definition to transition into service and finally to operations. The iterative process could make use of different tools and methods, such as fault-tree analyses, event-tree analyses, common-cause analyses, data collection, tests and validations, or documentation of the evidence, among others. During this process, the original airspace risk assessment could be modified through a feedback loop if necessary.

(g) An airspace risk assessment should be revised when the operational, regulatory and technology deployment context significantly evolves, or when the criteria too upon which the airspace has been designed significantly evolve. The operational context includes incident and accident reports, traffic density, new procedures, and new stakeholders. The frequency of the reassessment depends on local conditions, and is expected to be performed in conjunction with the activities of the coordination mechanism in Article 18(f) of Regulation (EU) 2021/664.

GM3 Article 3(1) U-space airspace

AIRSPACE RISK ASSESSMENT — PROCESS PHASES

(a) An airspace risk assessment is a process composed of different phases that can be represented as detailed below:

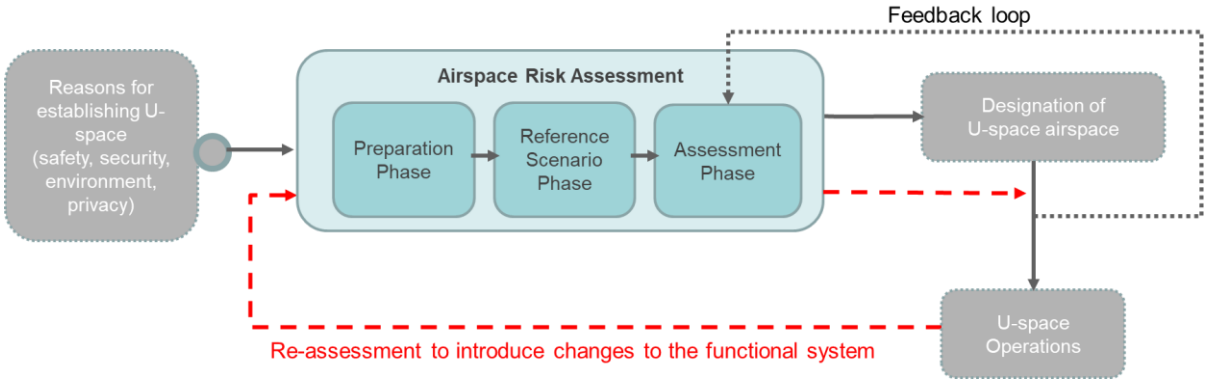

Figure 1: Airspace risk assessment process

(1) ***The preparation phase*** begins with defining the airspace in the scope of the assessment, including operational, procedural and infrastructure design requirements from all involved stakeholders, as well as defining any assumptions and constraints. An assessment team needs to be created to ensure that no area is left unexamined.

(2) ***The reference scenario phase*** concerns only the analysis of the use of the airspace assessed before changes are introduced. An important step in this phase is conducting interviews with stakeholders (including non-aviation entities), assessing ground

infrastructure, identifying technical support infrastructure, and collecting the necessary data in a common data format. This would ensure a harmonised approach for all entities involved.

(3) ***The assessment phase*** includes hazard identification, risk analysis and mitigation planning. These processes should be applied separately to safety, security, privacy, and environmental hazards, and their associated risks. As the nature of hazards, risks, and mitigation measures are specific to each of these four areas, the methodologies employed by Member States to identify hazards, assess risks, and plan appropriate mitigation measures should fit the specific needs of the area assessed, and of each Member State. Nevertheless, the assessment should guarantee that the risk is acceptable or tolerable while identifying the requirements that are to be met in that perspective. Ultimately, the appropriate mitigation measures from each assessment should be compatible with each other and they should not adversely impact on the other areas.

GM4 Article 3(1) U-space airspace

AIRSPACE RISK ASSESSMENT — SAFETY PART

(a) The assessment phase considers the following items when approaching safety:

(1) Important aspects to include in the assessment are related to traffic density, mapping information related to population density and obstacles, in-depth assessment of encounters with manned aviation, consequences of mid-air collision between unmanned aircraft, and meteorological information, among others.

(2) It is expected that the assessment phase includes a description of the safety activities to be conducted during its life cycle (e.g. in a safety plan). The aim is to specify the detailed safety assessment activities to be undertaken for a given airspace. This preparatory process identifies the main safety issues associated with the airspace under assessment as soon as possible.

(3) It is recommended that the following safety assessment activities, at a minimum, be performed at safety planning level:

(A) Description of the key properties of the operational environment that are relevant to the safety assessment.

(B) Initial identification of the hazards in the airspace under assessment.

(C) Derivation of suitable safety criteria for the airspace under assessment.

(D) Determination of the operational activities relevant to the airspace under assessment.

(4) The safety assessment methodology describes the following elements:

(A) Identification of hazards and definition of the safety criteria.

(B) To satisfy the safety criteria, definition of the airspace safety specification at operational level in normal, abnormal, and emergency conditions.

(C) Definition of the airspace safety requirements describing the high-level design characteristics of the functional system to ensure that the system operates as specified.

(5) Such requirements may be allocated to different stakeholders (e.g. USSPs, UAS operators, etc.)

(b) Safety hazards

(1) Currently, in Regulation (EU) 2017/373, the term 'hazard' means 'any condition, event, or circumstance which could induce a harmful effect'. This definition is maintained in the context of the U-space airspace risk assessment.

(2) This definition relates to a broader understanding of what a hazard is. It addresses two types of hazards: (i) hazards inherent to aviation, which the functional system will have to mitigate; and (ii) 'system-generated' hazards, which are created by the potential failure of the functional system.

(3) In an airspace risk assessment associated to UAS operations, both types of hazards (i.e. existing and system-generated hazards) need to be considered, analysed and mitigated.

(4) By definition, hazards inherent to aviation are hazards which exist in the operational environment before any form of deconfliction has taken place. These hazards are the base for the definition of the safety criteria. Two examples of these hazards inherent to aviation, regarding air risk and ground risk respectively, could be:

(A) a situation where the intended trajectories of two or more aircraft are in conflict;

(B) a situation where the intended trajectory of an aircraft conflicts with the terrain or an obstacle.

(5) System-generated hazards are hazards generated by the possible failure/malfunction of the functional system. Possible examples of system-generated hazards may be:

(A) unmanned aircraft entering controlled airspace;

(B) failure in separating two aircraft.

For the identified system-generated hazards, there is a need to provide:

(A) the assessed immediate operational effect(s);

(B) the possible mitigation means in terms of measures to be implemented to protect against the risk-bearing hazards;

(C) the assessed severity of the mitigated effect(s), in accordance with a severity classification scheme defined for the U-space airspace;

(D) the airspace safety specification elements, to limit the tolerable frequency with which the system-generated hazard could be allowed to occur.

(c) It is recommended that safety assurance activities be documented to present sufficient evidence that the actions taken have been adequate and complete in identifying and mitigating the risks (e.g. safety assessment report).

GM5 Article 3(1) U-space airspace

AIRSPACE RISK ASSESSMENT — CHECKLIST TEMPLATE

For the purpose of conducting an airspace risk assessment, Member States may wish to use a checklist for different types of environments for which hazards and impacts may be considered when performing an airspace risk assessment (the following list is not exhaustive):

Ground risks	
• Critical aerodrome areas ○ ILS critical and sensitive areas, radar, etc.	
Populated areas	
• Boundaries of population density areas ○ cities and suburbs	
• Boundaries of dynamic population density areas ○ Recurring or one-off events and gatherings (concerts, stadiums, beaches, etc.)	
• Schools, hospitals, and other public buildings	
Physical infrastructure	
• Governmental/military installations	
• Prisons	
• Bridges and dams	
• Telecommunication and data centres	
• High-tension power lines and substations	
• Nuclear and conventional power stations	
• Chemical industry sites	
• Laboratories	
• Main roads, railway lines	
• Ports, harbours and waterways	

• Water treatment plants	
• Restricted, prohibited and danger areas	
• Summits and VIP protection	
Locations that could cause interference to a UAS flight	
• Electromagnetic wave emitting sites ○ mobile phone base stations ○ ground telecommunication sites ○ TV and radio broadcast sites ○ surveillance equipment sites	
• Solar panel and wind farms	
• Water jets, geysers, etc.	
• Areas prone to inclement weather	

Air risks	
Generic airspace restrictions	
• ATS routes ○ aerodrome traffic zone (ATZ);	
• Aerodrome areas ○ control zones (CTR) ○ terminal control areas (TMA)	
• Manned-aviation restricted areas ○ temporary reserved area (TRA) ○ temporary segregated airspace (TSA) ○ cross-border area (CBA) ○ radio mandatory zone (RMZ) ○ transponder mandatory zone (TMZ)	
Restricted airspace and no-drone zones	
Nature reserves and other noise-sensitive areas or environmentally sensitive areas	
Aerodrome operating hours, dimensions, and location	
Manned aircraft operations, locations, and most common routes	

Unmanned aircraft operations, locations, and most common routes	
Heliports and aerodromes	
IFR operations	
• Arrival and departure routes	
• Transit routes	
• Radar vectoring areas	
• Altitudes	
VFR operations	
• VFR common routes and altitudes	
• Operations below 150 m (500 ft)	
• Low-altitude military operations	
Generic operations	
• High probability of manned or unmanned traffic (HEMS, etc.)	
• Gliders, microlights	
• Model aircraft and rocket model activities	
• Balloons	
• Seasonal or permanent recreational activities	
• Base jump, wing suits, kitesurfing, parachuting, parasailing, hang-gliders, paragliders, etc.	
State-specific operations	
• Police	

• Customs, border control	
• Firefighting	
• Military	
• Search and rescue	
• Maritime and fisheries surveillance	
• Operators of essential services	

Communication, navigation and surveillance (CNS) — the advance identification of specific locations may be helpful to address potential CNS issues on UAS operations	
Communication	
• COM — VFR requirements, frequencies, radio, transaction expiration time (TET)	
• COMSEC — UAS COM interference, USSP–UAS link, USSP–RP, RP–USSP, e-conspicuity system	
• UAS COM and uncontrolled manned aircraft traffic (e-conspicuity) frequency availability, including coverage of 3/4/5G network	
Navigation	
• Navigation requirements and/or limitations (for U-space)	
• GNSS performance including outage reports and augmentation (GBAS, SBAS, etc.) availability	
Surveillance	
• Critical surveillance areas (coverage, etc.)	
• Available means of surveillance (ADS-B Out, SRD 860, mobile telephony (e.g. GNSS-LTE), etc.)	

Non-exhaustive list of possible stakeholders involved in the airspace risk assessment process (in no restrictive order):

National/State entities	Organisation	Contact Person
Competent authorities		
ATM/ANS service providers (ANSPs)		
Air traffic controllers (ATCOs)		
Police and State security		
State defence/military		
Customs		
Aviation entities	Organisation	Contact Person
En-route flight information service (ATS providers)		
Aerodrome operators		
Airlines		
Pilots (GA, IFR, emergency services)		
Flight schools		
UAS operators/pilots		
U-space service providers (USSPs)		
UAS manufacturers		
Model aircraft clubs, airsports associations and aviation-related associations		
General aviation representatives (VFR)		
Non-aviation entities	Organisation	Contact Person
Critical infrastructure (nuclear stations, etc.)		
Industry		
Local government		
Hospitals		
Education/schools		
Road and rail transport		
Ports and the maritime sector		
Telecommunications and others that emit electromagnetic waves		
Forestry and environmental protection (including non-governmental organisations (NGOs))		
Others		

GM6 Article 3(1) U-space airspace

AIRSPACE RISK ASSESSMENT — ACCEPTABLE LEVEL OF SAFETY (ALS)

(a) One of the main objectives of the implementation of the U-space is to increase the level of safety of the introduction of UAS operations to an acceptable level. In aviation, the acceptable level of safety is generally defined in terms of the probability of an aircraft accident occurring and the consequences being acceptable to the society, i.e. the society is ready to accept or be subjected to the risk that the event might involve. The role of Member States in this regard is to translate the societal perception into qualitative or quantitative criteria addressing the probability and consequences of occurrences.

(b) The acceptable level of safety is defined by Member States, which should consider the inputs from UAS operators and USSPs regarding their needs and capacities. In order to set acceptable levels of safety for the U-space airspace, it is proposed to set safety criteria as per Regulation (EU) 2017/373 considering the singularities and specificities of the different types of risks posed by unmanned traffic in the U-space.

(c) The defined set of safety criteria should cover all possible identified risks. Each criterion should be verifiable and expressed in terms of an explicit level of safety risk or another measure that relates to a specific safety risk. In the absence of sufficient data related to U-space operations to take as a reference to determine the safety criteria, safety indicators from manned aviation operations may be used.

(d) It is worth remarking that when setting safety criteria for the U-space airspace, the goal is to maintain at least the safety levels attained over years of experience in manned aviation. However, considering the specificities of UAS operations in the U-space, this might mean a higher rate of mid-air collisions than for manned aviation. Nevertheless, considering the mitigation means that ensure separation between manned and unmanned aircraft, the mid-air collision between two unmanned aircraft will not result in casualties in the air. The ground risk is likely to be higher in populated areas, particularly when comparing high density of unmanned operations with traditional manned aviation. The definition of safety criteria should take these factors into account, as well as the presence of critical infrastructures in the vicinity which could be negatively impacted by UAS operations.

(e) With reference to units of measurement, the most common unit of measurement applied to manage aviation risks is generally the reference to ‘aircraft per flight hours’. Nevertheless, there are other units that could be used in the framework of an airspace risk assessment. In general, it is considered that the most appropriate unit of measurement to assess U-space safety risks refers to ‘per flight hour’ for en-route phases of flight, while for the take-off, approach and landing phases of flight, reference to ‘per movement’ over a period of time (e.g. ‘per year’) is the most convenient.

(f) The airspace safety specification at operational level will define what must happen at operational level in the airspace for the specified acceptable level of safety to be met. Different factors can be adjusted, like for instance the type of traffic, aircraft and system performance, equipment, procedures, aircraft speed, type of operation, maximum capacity, the number of

people overflown (population density), among others, to comply with the airspace safety specification at operational level. Once the U-space is operational, comparative approaches to determine the appropriate level of safety to be attained by the changes in the functional system (reassessments) may be useful. In these cases, the rationale of 'maintaining or improving' the current safety level of operations in the U-space may be used to define the new safety criteria associated to the changes made to the functional system. Such an approach is convenient for the consolidation of the U-space where incremental improvements are applied, while planning safety in the long term in terms of procedures and system design can produce additional quantitative figures.

(g) Finally, the acceptable level of safety should be materialised through the definition of the U-space airspace safety requirements, such as the set of U-space services, performance requirements, as well as the operational conditions and constraints, describing the high-level design characteristics of the functional system to ensure that the system operates as specified, thus satisfying the airspace safety specification at operational level.

GM7 Article 3(1) U-space airspace

AIRSPACE RISK ASSESSMENT — QUANTITATIVE SAFETY FIGURES

At this early stage of the implementation of the U-space regulatory framework, the limited experience with assessing the safety of UAS operations and the uncertainty on the related level of risk acceptable to the society do not permit to define sensible and harmonised quantitative safety figures. This may require to use simplified assumptions and approximations to establish quantitative values.

In the future, when more operational experience will have been gained, numerical examples to propose an acceptable level of safety could be provided with the appropriate accuracy.

GM8 Article 3(1) U-space airspace

OTHER RISKS

During the assessment phase, the following guidance regarding the associated security, privacy, and environmental risks may support the Member States.

Security

(a) The implementation of the European regulatory framework for the protection of critical infrastructure as well as cybersecurity may lead to risk assessments that are relevant to the airspace considered. These risk assessments may be considered as components of the airspace risk assessment if they are reviewed to take into consideration the possible designation of a U-space airspace.

(b) It is recommended that a security risk assessment be conducted to assess the security risks of an organisation which emerge from intentional, unauthorised electronic interaction. The necessary process steps and methodologies to conduct the security risk assessment will vary depending on the particular security risk assessment process that has been adopted.

(c) The methodology used to assess cybersecurity risks is very similar to the one used for physical security risks and, therefore, recommended to use it during the assessment phase. The process for the risk assessment and for the sharing of information security risks is illustrated in Figure 2 on the next page. This comprises several activities that need to be performed for each risk assessment.

(d) There are fixed inputs (marked with the letters A, B, C, D) that should be common to all risk assessments conducted by an organisation. These would be established as part of the overall corporate risk management process. The activities described may be conducted in a different order depending on the particular methodology used, and the activities and fixed inputs may have different names as well. Risk sharing can happen at any life cycle stage and should be dependent on agreed thresholds for reporting.

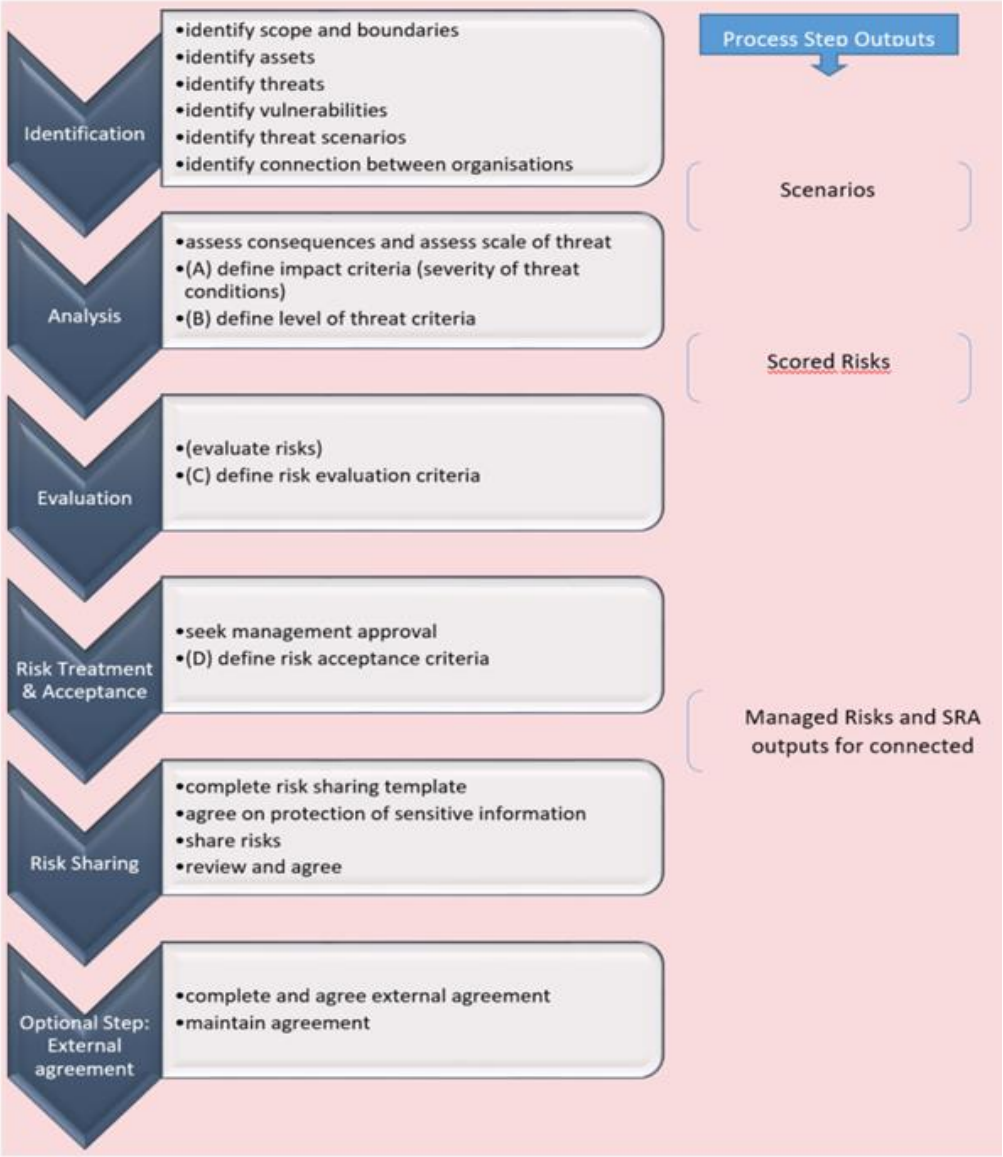

Figure 2: Risk assessment and sharing of information according to EUROCAE ED-201A

(e) To ensure comparability and compatibility between the different security assessment methodologies and definitions of risk, it is recommended that the parties involved should have a common method for categorising risks and different classes of risks. The use of different methods may produce incomparable outputs that are unusable between the parties involved.

(f) The following principles may be used for risk sharing outputs where there is a safety impact identified between connected organisations and ecosystems using the same risk assessment method:

(1) Assurance that the outputs of the assessments produce results which are comparable internally and externally.

(2) Agreement upon common definitions for the connected interfaces (e.g. risk classes, vulnerabilities).

(3) Sharing information on assessed risks that have a potential safety impact on their partners, which relate to connecting networks, to sharing information, and to using third-party products.

(4) The use of different risk assessment matrices should be used according to the type of impact that is being assessed and shared (e.g. safety, capacity).

(5) An organisation may only compare and use the severity of same-type impacts, i.e. a safety impact with a safety impact; a safety impact cannot be compared with an organisational impact.

(6) Security protection

(i) The general type of protection (e.g. type of encryption standard).

(ii) The attribute being protected is important as it may be the case that one organisation protects availability, but the receiving organisation is concerned with protecting integrity.

(iii) The assurance of security protection which represents the quality it has been designed to operate. If the assurance level of the protection measures of the connected organisation is not broadly equivalent, then each connected system will either have to agree to share and manage the risk to an acceptable level for both organisations or individually manage the risk to an acceptable level.

Privacy

(g) A risk assessment on privacy is aimed at assessing the privacy risks to third parties emerging from intentional or accidental visualisation, capture and/or retention of personal images or information through (close) overflight or hovering. The necessary process steps and methodologies to conduct the privacy risk assessment will vary depending on the particular privacy risk assessment process that has been adopted.

(h) The main legal reference regarding privacy risk assessment is Regulation (EU) 2016/679[9] (the General Data Protection Regulation (GDPR)). However, the GDPR only applies to 'personal data' as defined in its Article 4(1), not to commercial information, which will generally be covered by national laws. A privacy risk assessment is conducted to additionally ensure the security of third-party commercial data.

(i) Article 35 of the GDPR provides for the conduct of a data protection impact assessment (DPIA), where the processing of any personal data obtained is likely to result in a high risk to the rights and freedoms of the subjects of that data. This DPIA must describe the characteristics of the data treatment, the risks identified, and the mitigation measures adopted. A DPIA may be used to support the airspace risk assessment.

Environmental

(j) An environmental risk assessment should assess the risks to people, wildlife and the natural environment which emerge from flights near built-up areas, especially schools and hospitals, protected landscape, natural reserves, along known wildlife migratory routes, or over lakes, rivers, and other bodies of water. The necessary process steps and methodologies to conduct an environmental risk assessment will vary depending on the particular environmental risk assessment process that has been adopted.

(k) Environmental risk assessments for UAS operations should ensure compliance with plans and programmes for which such environmental assessments have been carried out.

Noise

(l) Regulations (EU) 2019/945 and 2019/947 lay down provisions as regards noise limitation of small UAS. They require manufacturers to minimise noise, and operators to follow the guidelines for reducing noise during operations. The assessment and management of environmental noise of small UAS should take these provisions into account. Directive 2002/49/EC[10] relating to the assessment and management of environmental noise remains applicable, and the action plans required in paragraphs 5 to 7 of its Article 8 should be updated to include noise from UAS used in the 'specific' and 'certified' category. In effect, environmental airspace risk assessments ensure that UAS operations comply with these action plans regarding environmental noise.

(m) Many regulations on aircraft noise include airports, for example Regulation (EU) No 598/2014 on the establishment of rules and procedures with regard to the introduction of noise-related operating restrictions at Union airports within a Balanced Approach[11].

---

[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679&qid=1670338209397).

[10] Directive 2002/49/EC of the European Parliament and of the Council of 25 June 2002 relating to the assessment and management of environmental noise - Declaration by the Commission in the Conciliation Committee on the Directive relating to the assessment and management of environmental noise (OJ L 189, 18.7.2002, p. 12) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32002L0049&qid=1670450666651).

[11] Regulation (EU) No 598/2014 of the European Parliament and of the Council of 16 April 2014 on the establishment of rules and procedures with regard to the introduction of noise-related operating restrictions at Union airports within a

Air quality

(n) Directive 2008/50/EC[12], implementing a common approach to ambient air quality and cleaner air for Europe, applies to the management of local air quality at and around airports. Assessments should determine whether drones whose lift and propulsion do not come solely from electric sources comply with this Directive.

Protection of wildlife and the natural environment

(o) Concerns regarding aviation and wildlife generally focus on strikes against aircraft, mostly by birds. This is also a problem for unmanned aircraft. Such strikes could cause the unmanned aircraft to become uncontrollable, presenting a danger to people and property on the ground. Assessments should ensure that UAS operations avoid known wildlife migratory routes.

Assessments should ensure that local laws on the protection of wild birds, notably through Directive 2009/147/EC[13] on the conservation of wild birds, are respected. They should also ensure that Directive 92/43/EEC[14] on the conservation of natural habitats and of wild fauna and flora, and in particular of *Natura 2000* sites and other areas of special scientific interest and of outstanding natural beauty, is observed.

GM9 Article 3(1) U-space airspace

AIRSPACE RISK ASSESSMENT — COORDINATION WITH THE U-SPACE STAKEHOLDERS

In conjunction with Article 18(f) of Regulation (EU) 2021/664, for Member States to ensure a viable and effective designation of the U-space airspace, it is recommended as best practice to:

(a) exchange on best practices with other Members States and/or the Agency to ensure consistency and interoperability across the European Union — for instance, in seeking harmonisation on safety criteria and performance requirements;

(b) coordinate with the providers of common information, the single CIS provider (when relevant) and USSPs to evaluate:

(1) the availability of the required capabilities and performance requirements;

(2) the operational capacity according to the volume of operations expected in the U-space airspace;

(3) the operational capacity to interface with ATS providers;

(4) the procedures supporting the dynamic airspace reconfiguration in controlled airspace;

Balanced Approach and repealing Directive 2002/30/EC (OJ L 173, 12.6.2014, p. 65) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0598&qid=1670450907343).

[12] Directive 2008/50/EC of the European Parliament and of the Council of 21 May 2008 on ambient air quality and cleaner air for Europe (OJ L 152, 11.6.2008, p. 1) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008L0050&qid=1670451158754).

[13] Directive 2009/147/EC of the European Parliament and of the Council of 30 November 2009 on the conservation of wild birds (Codified version) (OJ L 20, 26.1.2010, p. 7) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32009L0147&qid=1670451516653).

[14] Council Directive 92/43/EEC of 21 May 1992 on the conservation of natural habitats and of wild fauna and flora (OJ L 206, 22.7.1992, p. 7) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31992L0043&qid=1670451799785).

(5) the availability of a common secure interoperable open communication protocol to enable digital information exchange between the U-space airspace actors;

(c) coordinate with the relevant ATS providers to evaluate the particularities or constraints of the controlled airspace to be considered during the designation of the U-space airspace;

(d) coordinate with UAS manufacturers to evaluate that UAS satisfy the required capabilities and performance requirements;

(e) coordinate with UAS operators to gain understanding of the intended operations and evaluate the service performance required, the practicability of the operational constraints, as well as the planned contingency and emergency procedures.

GM10 Article 3(1) U-space airspace

AIRSPACE RISK ASSESSMENT — COORDINATION AT LOCAL LEVEL

The public consultation (hearing process), as addressed in the AMC and GM to Article 18(f) of Regulation (EU) 2021/664, is intended to further elaborate the U-space airspace risk assessment with regard to the following:

(a) evaluating the soundness of the risk assessment (technical aspects) and potentially enriching it with complementary risks that may be indicated during the public consultation;

(b) integrating the considerations from to the public impacted by the establishment of the U-space airspace, and refining its design accordingly (e.g. to cater for local well-being needs as per GM1 and GM3 to Article 18(f));

(c) ultimately evaluating, and supporting as necessary, the social acceptance of the U-space airspace deployment.

AMC1 Article 3(4) U-space airspace requirements

U-SPACE AIRSPACE — DESIGN, OPERATIONAL CONDITIONS AND CONSTRAINTS

Considering Annex I to Regulation (EU) 2021/664, Member States should establish and provide the U-space airspace definition, encompassing:

(a) the geographical limits of the area where the U-space airspace is designated;

(b) the internal airspace structure (e.g. airspace blocks with their maximum and minimum size, subject to activation/deactivation);

(c) the UAS geographical zones defined in Article 15 of Regulation (EU) 2019/947, which could be encompassed within the U-space airspace.

Furthermore, Member States should define the U-space airspace operational conditions and constraints:

(a) for U-space airspace designated in controlled airspace, the means and procedures to disseminate information regarding dynamic airspace reconfiguration;

(b) the potential pre-established contingency or emergency procedures;

(c) the weather limitations, in terms of maxima or minima for important meteorological parameters (e.g. maximum gust, and visibility minimum, temperature minimum);

(d) the maximum simultaneous UAS operations, and the maximum density of UAS flights allowed within the designated U-space airspace;

(e) the minimum safety distance (spacing) to be maintained between manned and unmanned aircraft in airspace where manned aircraft operations are not subject to air traffic control;

(f) the residual airspace risk class (ARC) to support the specific operations risk assessment (SORA) as defined in Regulation (EU) 2019/947;

(g) any other operational conditions and constraints derived from the airspace risk assessment (e.g. mitigation of specific hazards identified during the assessment).

AMC2 Article 3(4) U-space airspace requirements

U-SPACE AIRSPACE — PERFORMANCE REQUIREMENTS

Considering Annex I to Regulation (EU) 2021/664, and derived from the airspace risk assessment, Member States should establish the following:

(a) The U-space services' performance requirements and operational constraints:

(1) the 'geographic proximity' to UAS operators at which the UAS remote identification has to be acquired and provided to support the network information service;

(2) the maximum data 'latency' and 'frequency' at which the traffic information needs to be provided to UAS operators to ensure the proper functioning of the traffic information service;

(3) the 'proximity' to the UAS position, and the associated definition of the surveillance volume at/within which the traffic information should be provided to UAS operators;

(4) the 'deviation thresholds', meant to be the maximum acceptable deviation from the intended UAS flight path, to be considered by the USSP when processing a flight authorisation or to generate a non-conformance alert to the UAS operator;

(5) flight authorisation constraints that may be defined to ensure fair and efficient access to the U-space airspace;

(6) the data quality requirements for weather data, when relevant;

(7) the minimum coverage (e.g. horizontal and vertical range within and, when required, also outside the U-space airspace) for the receipt of information from electronically conspicuous manned aircraft that are not subject to air traffic control, considering the means of compliance as defined in AMC1 to point SERA.6005(c) of Regulation (EU) No 932/2012, and complementary information about manned aircraft traffic potentially shared by the relevant air traffic service units.

(b) The required UAS capabilities and performance requirements.

For the determination of the performance requirements, the contribution of the U-space actors (layers) should be taken into account including, when relevant, the single CIS provider, the USSP, and UAS operators (e.g. reaction time).

GM1 Article 3(4) U-space airspace

U-SPACE AIRSPACE — RESULTS OF THE AIRSPACE RISK ASSESSMENT

The acceptable level of safety is supported by a comprehensive set of performance requirements, operational constraints and limitations that are to be subsequently considered and/or satisfied by the U-space actors (e.g. USSPs, UAS operators, UAS manufacturers). These performance requirements and operational constraints and limitations are intended to be established throughout the risk assessment, be performance based, and commensurate with the level of risk that needs to be mitigated in the U-space airspace.

GM2 Article 3(4) U-space airspace

U-SPACE AIRSPACE — STRUCTURE

The design of the U-space airspace could be organised into a set of airspace components that can be a basic set of airspace blocks which can be combined/deactivated in changing combinations/configurations to meet the actual manned aviation requirements. It can also be a more sophisticated mathematical grid, the geometry of which can vary depending on the complexity and density of the operations (e.g. triangles to allow for straight 'areas' boundaries). An efficient strategic approach to the design of the U-space airspace is therefore important, also taking into account the need to manage the complexity of the dynamic airspace reconfiguration procedure, which might be progressively increased at the later stage of the U-space implementation.

GM3 Article 3(4) U-space airspace

U-SPACE AIRSPACE — INTERNAL GEOGRAPHICAL ZONES

The U-space airspace may encompass sub-geographical zones as defined in Article 15 of Regulation (EU) 2019/947 and in the related AMC and GM:

(a) zones limited in place and time (e.g. operations allowed only at certain periods and in certain areas);

(b) zones restricted to UAS operations that fulfil a specific set of conditions and specific authorisations;

(c) zones of exclusion where UAS operations are prohibited (e.g. no-fly zones).

GM4 Article 3(4) U-space airspace

U-SPACE AIRSPACE — AIR RISK CLASS (ARC) — APPLICATION OF THE SPECIFIC OPERATIONS RISK ASSESSMENT (SORA) FOR UAS OPERATIONS IN THE 'SPECIFIC' CATEGORY

While it is considered that the initial ARC of UAS operations in the 'specific' category is established taking into account the airspace classification and type of complexity of the airspace (e.g. height, danger area, etc.) for the purpose of a harmonised U-space airspace implementation, it is recommended to apply the residual ARC as follows (after having applied all the strategical and pre-tactical and tactical means that support the implementation of the U-space airspace, and having ensured the proper utilisation of the required U-space services):

It is recommended to apply residual 'ARC-b' for U-space in both controlled and uncontrolled airspace (or in airspace where both controlled and uncontrolled manned aircraft may operate simultaneously), relying on the provision of tactical information through the 'traffic information service' and the U-space segregation principle (e.g. dynamic airspace reconfiguration) to maintain safe separation from manned aircraft, while still accounting for a certain level of air risk for manned aircraft.

The demonstration by UAS operators of the relevant tactical mitigations performance requirements (TMPR) to their competent authority that has provided the operational authorisation is still required. In the context of U-space, additional requirements complementing the defined SORA/TMPR in Regulation (EU) 2019/947 may be established by the Member State through the definition of the U-space performance requirements.

GM5 Article 3(4) U-space airspace

U-SPACE AIRSPACE — PERFORMANCE REQUIREMENTS FOR U-SPACE SERVICES

The performance requirements are related to the provision of services and to Regulation (EU) 2021/664 as follows:

(a) The maximum data 'latency' is related to the 'traffic information service' (Articles 5(2) and 8(1) of Regulation (EU) 2021/664);

(b) The 'proximity' to the UAS position is related to the 'network information service' (Article 8(1) of Regulation (EU) 2021/664);

(c) 'Deviation thresholds' are related to the 'flight authorisation service' (Article 10(2)(c) of Regulation (EU) 2021/664), and the 'conformance service' (Article 13(1) of Regulation (EU) 2021/664);

(d) The 'proximity' to the UAS position and the definition of the surveillance volume are related to the 'traffic information service' (Article 11(1) of Regulation (EU) 2021/664);

(e) The 'frequency' at which the information needs to be provided to the UAS operator is related to the 'traffic information service' (Article 11(1) of Regulation (EU) 2021/664);

(f) The data quality requirements for weather data are related to the 'weather information service' (Article 12 of Regulation (EU) 2021/664).

GM6 Article 3(4) U-space airspace

U-SPACE AIRSPACE — SAFETY AND SECURITY OBJECTIVES

To ensure that the acceptable level of safety is achieved, safety objectives may be specified in terms of required levels of integrity and reliability, and be allocated to the U-space actors. Similarly, security objectives aligned with the safety objectives, type of operation and level of threats may be also defined to ensure assurance in the security measures.

While the objectives are meant to be commensurate with those existing today for manned aviation, the practicality of the implementation may limit the approach (e.g. difficulty in applying a relevant software assurance level (SWAL) approach).

GM7 Article 3(4) U-space airspace

U-SPACE AIRSPACE — FLIGHT AUTHORISATION CONSTRAINTS

Linked to specific airspace, and to ensure efficiency as well as fairness as regards access to the U-space airspace, Member States may constrain:

(a) the minimum and maximum time (size of time window) before scheduled take-off time at which flight activation is requested;

(b) the maximum time a flight authorisation request may be sent in advance to ensure the effective implementation of the ‘first in, first serve’ principle and prevent undue occupation of the U-space airspace.

GM8 Article 3(4) U-space airspace

U-SPACE AIRSPACE — FLIGHT AUTHORISATION DEVIATION THRESHOLDS

It is expected that the acceptable level of safety may be achieved by having UAS flight authorisation for 4D trajectories that do not intersect and contain their flights for 95 % of the time.

The UAS flight authorisation describes the flight trajectory as a series of one or more 4D volumes expressed in height (base, ceiling), longitudinal and lateral limits, and duration (entry and exit times). Each dimension includes the uncertainty of the flight, considering the UAS operational performance, and the assumptions on the operator proficiency and weather conditions.

It is recommended as best practice that these uncertainties be capped in the given probability of 95 %. The resulting deviation threshold defines an additional 4D volume around each planned 4D volume for a flight. The dimensions may be specified to balance the needs of safety with the efficient use of the airspace, and refine them over time for the U-space airspace under consideration based on the observed usage of the U-space airspace, the performance (and conformance) of the UAS flights in the airspace, and other factors.

GM9 Article 3(4) U-space airspace

U-SPACE AIRSPACE — TRAFFIC INFORMATION AND SURVEILLANCE VOLUME

Proximity is understood as the distance between two aircraft. In the context of traffic information service, its value should be determined in such a way to allow UAS operators enough time to take appropriate action to avoid collision hazards. Proximity values may vary depending on the geography of the U-space airspace and the type of expected operations (e.g. BVLOS/VLOS), and also on the type and performance of manned aircraft that operate in or cross through the U-space airspace.

The constraints in terms of situational awareness, and thus the proximity values, may differ for manned and unmanned aircraft. Manned aircraft are usually much faster than unmanned aircraft. Due to their higher velocity, and due to the fact that manned aircraft induce wake turbulence, UAS operators may need to ensure situational awareness at a much wider scale to effectively assess incoming traffic and take appropriate action to maintain sufficient spacing.

For instance, to enable a 10-minute reaction time for the UAS operator, and considering a manned traffic velocity of 120 kt (≈240 km), a wider volume of 20 NM (≈37 km) and 5 000 ft (≈1 500 m) may be taken as reference to adequately monitor manned traffic patterns.

These factors are to be considered by Member States to ultimately specify the appropriate ‘surveillance volume’. In addition, considering such constraints, and to safely enable operations close to the geographical borders of the U-space airspace, the ‘surveillance volume’ should include the adjacent airspace beyond the strict geographical limit of the U-space airspace.

GM10 Article 3(4) U-space airspace

U-SPACE AIRSPACE — RECEIPT OF TRAFFIC INFORMATION FROM UNCONTROLLED MANNED AIRCRAFT

Traffic information may be complemented by information about manned aircraft traffic shared by the relevant air traffic service units. This may include information from primary and secondary surveillance radars, multilateration surveillance systems and other surveillance or tracking systems already used by air traffic service units.

The complementary traffic information about manned aircraft traffic should be considered as one of the inputs to the airspace risk assessment referred to in Article 3(1) of Regulation (EU) 2021/664.

The complementary traffic information may, in exceptional cases and subject to deriving positive results from the airspace risk assessment referred to in Article 3(1) of Regulation (EU) 2021/664, alleviate the need for the deployment of new ground infrastructure necessary for the continuous receipt of information from manned aircraft that make themselves electronically conspicuous in accordance with AMC1 to point SERA.6005(c) of Regulation (EU) No 932/2012. This is to be considered especially in situations where the deployment of new ground infrastructure could constitute a disproportionate burden on USSPs when compared to the existing requirement for manned aircraft that operate in airspace which is being considered for designation as U-space airspace by the Member States.

GM11 Article 3(4) U-space airspace

U-SPACE AIRSPACE — TIMELINESS AND LATENCY

The maximum latency values may vary depending on the geography of the U-space airspace and the type of the expected operations.

In general, information will be handled by multiple parties, and a maximum latency would have to be subdivided into fractions, and latency budgets would have to be allocated to individual parties, while at the same time the number of re-transfers would have to be limited in order to protect the maximum overall latency.

GM12 Article 3(4) U-space airspace

UAS CAPABILITIES AND PERFORMANCE REQUIREMENTS

Depending on the U-space airspace design and constraints, not all UAS types are capable of being safely operated within the U-space airspace. The UAS capabilities and performance requirements may be expressed in terms of expected:

(a) climb/descent rates or vertical speed, horizontal speed, autonomy/range/endurance,

(b) noise levels,

(c) connectivity,

(d) required navigation equipment,

(e) flight data accuracy, integrity and latencies (refresh rate),

(f) availability and integrity of the command-and-control link,

(g) resilience to environmental conditions (e.g. as applicable: wind, icing, electrical interference),

(h) resilience to cyberthreats and related security measures.

GM1 Article 4 Dynamic airspace reconfiguration

GENERAL

(a) Article 4 introduces the concept of dynamic reconfiguration of the U-space airspace and requires Member States to ensure that this concept is effectively put in place to avoid proximity between manned and unmanned aircraft within the U-space airspace.

(b) The dynamic reconfiguration of the U-space airspace is an important element of the overall safety argument for safe operations in the U-space airspace. It applies to a U-space airspace that is established in controlled airspace and allows manned aircraft to fly clear of the U-space airspace whilst ensuring the containment of the U-space traffic. Dynamic reconfiguration is carried out by the ATC unit in response to variable manned traffic patterns, which demand short-term U-space airspace adaptations.

GENERAL UNDERSTANDING OF THE OPERATIONAL CONCEPT

(c) Initially, at least, the number of instances where dynamic airspace reconfiguration would be required should be limited. In addition, certain strategic measures could be taken to limit the extent of the dynamic airspace reconfiguration through, for example, the design of the U-space airspace itself. The better the airspace is designed, the easier it will be for ATC units to segregate manned from unmanned aircraft in the U-space airspace.

(d) Operationally, the ATC unit will inform USSPs that, depending on the U-space airspace design, certain portions of the U-space airspace (or its entirety) are (is) not eligible for flight authorisation, activation, and utilisation by the UAS. When these portions of the U-space airspace are dynamically deactivated, for tactical, short-term changes in manned traffic demand, USSPs should not grant flight authorisation/activation and should request the UAS operator that already flies into the deactivated portion of the U-space airspace to either exit it or land.

(e) The time margins (time within which, after deactivation, it is expected that the UAS that occupies the relevant portions of the U-space airspace will exit them or will have to land) for these operations may be established on a case-by-case basis, based on different factors, such as the proximity of the ATC route to the U-space airspace, including standard instrument departure / standard instrument arrival (SID/STAR), typical performance of manned aircraft in that particular airspace, constraints in the controlled airspace, or unexpected situations (e.g. non-standard go-around, emergency).

OPERATIONAL SCENARIO

(f) When the ATC unit intends to issue a clearance to a manned aircraft to enter the U-space airspace, it will initiate a dynamic airspace reconfiguration procedure. The ATC unit will preliminarily alert, through its respective USSPs, UAS operators about the imminent deactivation of the entirety, or the relevant portions, of the U-space airspace to let them anticipate and engage the appropriate manoeuvres. The ATC unit will then publish a temporary U-space airspace restriction for UAS as part of the CIS for that U-space airspace. USSPs that are active in that U-space airspace will adhere to this newly published restriction and provide the

corresponding information to all UAS operators connected to their services through the geo-awareness service. In addition, they will check authorised UAS flights against the newly published restriction and cancel or amend flight authorisations accordingly.

(g) The UAS operators concerned will be notified through the UAS flight authorisation service and will need to either discontinue their flights or conform with the amended UAS flight authorisations, as applicable. USSPs will notify the ATC unit once the restricted portion of the U-space airspace is clear of UAS traffic as UAS will have exited the restricted portion of the U-space airspace.

(h) The ATC unit will clear manned aircraft to enter the U-space airspace once it is ensured that the segregation from UAS traffic has been achieved.

(i) Upon completion of the manned flight through the U-space airspace, the ATC unit will complete the dynamic airspace reconfiguration procedure, by lifting the dynamic restriction, and USSPs will be allowed again to activate UAS flight authorisations or provide UAS new flight authorisations for UAS operators accordingly.

AMC1 Article 4 Dynamic airspace reconfiguration

SEGREGATION ASSURANCE

(a) Protection buffers should be applied internally in the design phase, when assessing the volume of airspace to be designated as U-space airspace, so that flight authorisations are only granted to a specified vertical/horizontal distance from the U-space airspace limits.

(b) The values of the protection buffers should be taken into account and should be consistent with the UAS performance requirements for a given U-space airspace, specifically those requirements related to the lateral and vertical navigation performance or containment criteria.

AMC2 Article 4 Dynamic airspace reconfiguration

PRELIMINARY ALERT TO UAS OPERATORS

When the location where UAS operations take place is to become deactivated, a preliminary alert should be issued soon enough by the USSPs to UAS operators to allow them to revise the UAS flight authorisations, or enable safe landing, before the restriction becomes active.

AMC3 Article 4 Dynamic airspace reconfiguration

ACKNOWLEDGEMENT OF IMPLEMENTATION

Once the U-space airspace, or parts of it, are clear of UAS traffic (i.e. UAS have been redirected to portions of the U-space airspace that remain active or have landed), the implementation of the dynamic airspace reconfiguration should be acknowledged to the ATC unit.

GM2 Article 4 Dynamic airspace reconfiguration

SEGREGATION ASSURANCE

(a) The segregation effectiveness and assurance are highly dependent on the amount of time given to UAS operators to react according to the performance of the UAS they operate. As per GM2 to point ATS.TR.237 of Regulation (EU) 2017/373 amended by Regulation (EU) 2021/665, the ATC unit is expected to raise an alert as soon as practicable and ensure a recommended time window of 10 minutes before the implementation, plus 2 minutes once the restriction becomes active.

(b) To ensure that manned aircraft that operate in controlled airspace within a U-space airspace are segregated from UAS that operate in that U-space airspace, there is a need for:

(1) performance standards for UAS (those for manned aircraft being already widely established) to make reasonably sure that UAS will have the capability to stay within the defined airspace volume, with reference to both position accuracy and horizontal/vertical speed, and to exit the deactivated U-space airspace or land within a reasonable time;

(2) criteria (e.g. applicable buffer) to determine the airspace volume required to consider that segregation has been reasonably assured.

(c) According to Article 3(4)(a) of Regulation (EU) 2021/664, UAS capabilities and performance requirements are determined by Member States for each U-space airspace, based on the related airspace risk assessment.

GM3 Article 4 Dynamic airspace reconfiguration

SEGREGATION ASSURANCE

According to the GM to point ATS.TR.237 of Regulation (EU) 2017/373 amended by Regulation (EU) 2021/665, it is recommended as best practice that the ATC unit raise an advisory alert to UAS operators either 10 minutes or 5 times the anticipation time before the U-space airspace becomes deactivated. This ‘anticipation time’ is suggested to be a minimum of 2 minutes.

GM1 Article 5 Common information services

U-SPACE ARCHITECTURE

(a) Article 5 of Regulation (EU) 2021/664 defines the content and organises the distribution of 'common information' — that is, the necessary information that needs to be shared between the relevant operational stakeholders for the safe operation of UAS in the U-space airspace.

(b) Common information is a collection of data that originates mainly from three different sources:

(1) the Members States responsible for the design of the U-space airspace, including its dimensions, performance requirements, and static or dynamic restrictions;

(2) the ATS providers responsible for the transmission of manned traffic information as laid down in point ATS.OR.127 of Regulation (EU) 2017/373 amended by Regulation (EU) 2021/665, and the ATS units when applying the dynamic reconfiguration of the U-space airspace;

(3) the USSPs, through the terms and conditions as regards access to their services.

(c) Member States may decide to designate a dedicated entity to provide CIS on an exclusive basis in a given U-space airspace. Such 'single common information service provider' (single CIS provider) would make the relevant information available to all relevant operational stakeholders. The single CIS provider would need to be certified for the services it provides. The designation of a single CIS provider would need to be notified to other Member States as well as to the Agency.

(d) In the absence of a single CIS provider, common information is directly exchanged between the relevant operational stakeholders in a distributed communication architecture, whereby each data provider communicates directly with another USSP for sharing information. Each USSP needs to communicate with other data providers. A clear allocation of common information elements between Member States, ATS providers and USSPs would allow data users to find target data quickly and efficiently. In the absence of a single CIS provider, there is no need for additional certification; the provision of common information elements by ATS providers and USSPs will be covered by their respective certificate and the provisions of Regulation (EU) 2021/664 and Regulation (EU) 2021/665 amending Regulation (EU) 2017/373.

(e) Members States may decide to designate different single CIS providers for different U-space airspace volumes, or designate a single CIS provider for some of their designated U-space airspace volumes only, otherwise opting for a distributed model of exchange of common information.

(f) To achieve a high level of data exchange and interoperability between the CIS and State services (law enforcement and potentially military authorities), the CIS may need to comply with the national security and defence requirements.

GM2 Article 5 Common information services

STAKEHOLDERS

(a) As regards information and data provided to or by the CIS provider, a variety of different stakeholders may be involved. Member States may consider taking the needs and requirements of the stakeholders listed below into consideration.

(b) Stakeholders to provide information to, and retrieve information from, the CIS provider:

(1) competent authorities;

(2) ANSPs/ATSPs;

(3) military authorities (e.g. when being also ATSPs);

(4) USSPs;

(5) single CIS provider, when relevant;

(6) other relevant authorities or organisations (e.g. State agencies, municipalities, nature protection authorities, law enforcement authorities, rescue coordination centres, GNSS services, aerodrome/heliport/vertiport operators, meteorological authorities).

GM3 Article 5 Common information services

DEFINITIONS

For the purposes of Regulation (EU) 2021/664:

(a) 'common information services' (CIS) refers to the digital environment (network or platform) in which the common information elements (data) that support the implementation and proper functioning of the U-space airspace are provided/exchanged.

(b) 'providers of common information' refers to entities/organisations that provide common information elements (data) to the common information services (CIS).

(c) 'single CIS provider' refers to a certified organisation that ensures the interface and exchange between the 'providers of common information' and the USSPs. There is one 'single CIS provider' per U-space airspace. On the principles, the single CIS provider supports the provision of U-space services by providing common information to USSPs, but does not have active operational roles and responsibilities. For instance, it should not take part in the flight authorisation, which is the sole responsibility of the USSP.

(d) 'distributed model' or 'decentralised model' refers to a U-space architecture without a 'single CIS provider' where each 'provider of common information' makes common information elements (data) directly available to the other operational stakeholders (e.g. USSPs).

(e) 'centralised model' refers to a U-space architecture with a 'single CIS provider' which collects common information elements (data) from 'providers of common information' and makes them available to all operational stakeholders (e.g. USSPs).

AMC1 Article 5(1) Common information services

FORMAT OF AIRSPACE INFORMATION

The format of airspace information, including geographical zones, static and dynamic airspace restrictions, adjacent U-space airspace, and the horizontal and vertical limits of the U-space airspace should be as described in Chapter VIII 'UAS geographical zone data model' of and Appendix 2 to the ED-269 'MINIMUM OPERATIONAL PERFORMANCE STANDARD FOR GEOFENCING' standard in the version published in June 2020.

AMC2 Article 5(1) Common information services

INTERFACES

Member States or, when designated, the single CIS provider should provide and document all information required by the users to identify and implement interfaces to support access to the CIS.

GM1 Article 5(1)(b) Common information services

GEO-ZONE DATA FORMAT

Members States may define a format and data model to support the electronic sharing of information. They may use the JSON format (rfc7159) defined in EUROCAE ED-269. To support interoperability, Members States are encouraged to refer to standards and ensure consistency as regards the naming convention.

AMC1 Article 5(1)(f) Common information services

TIMELINESS

Information on static and dynamic airspace restrictions should be made available within 30 and 5 seconds respectively for at least 99 % of the time.

GM1 Article 5(1)(f) Common information services

COMPLEMENTARY AIRSPACE RESTRICTION

Relevant NOTAMs, airspace use plans (AUPs) / updated airspace use plans (UUPs) and navigation warnings are to be considered airspace information and should be made available online as part of the CIS, in accordance with Annex II to Regulation (EU) 2021/664.

AMC1 Article 5(2) Common information services

TIMELINESS

Traffic information should be made available with a latency that is lower than that necessary for the proper functioning of the traffic information service, as determined by the U-space airspace risk assessment, for at least 99 % of the time.

GM1 Article 5(4)(a) Common information services

FEEDBACK ON CIS DATA QUALITY

The providers of common information may suggest categories of anomalies that USSPs or, when designated, the single CIS provider, may use to categorise the type of feedback they share. Those categories may be inspired by data quality requirements such as accuracy, timeliness, or completeness, and offer specific tags for user comments or requests.

AMC1 Article 5(5) U-space service providers

INSTRUCTIONS TO CIS USERS

The necessary information to get access and exchange data through the CIS (e.g. service descriptions, interfaces) should be made available to the public, and should encompass:

(a) the point of contact of the CIS administrator and the procedures to access the CIS (e.g. to obtain the required credentials);

(b) the instructions on how to configure the user interfaces/system to properly support the exchange;

(c) the instructions to ensure the security of the exchange.

AMC1 Article 5(6) U-space service providers

INSTRUCTIONS TO USSPs

The single CIS provider should develop and provide USSPs with instructions to:

(a) configure their interfaces and systems to properly support the provision of services;

(b) ensure the security of the exchange.

GM1 Article 5(6) U-space service providers

ARRANGEMENT BETWEEN THE CIS STAKEHOLDERS

The single CIS provider may need to make a formal arrangement with CIS providers. To allow for flexibility, the formal form of the arrangement is left to the discretion of the parties involved, but may encompass the following items:

(a) The arrangement may:

(1) make reference to service ownership, accountability, roles and responsibilities;

(2) contain a description of the provision of data, information or services;

(3) match the expected service provision with the actual service support and delivery.

(b) The arrangement may establish:

(1) the subject matter, which may cover:

(i) the U-space airspace serviced (one arrangement may cover several U-space airspace volumes);

(ii) the coordination between stakeholders (may be covered in the same arrangement);

(2) the governance model, which may contain:

(i) points of contact for process coordination and system maintenance contacts;

(ii) a coordination process involving representatives from the stakeholders involved; the arrangement may cover procedures to organise meetings;

(iii) provision on dispute resolution;

(3) the data- and information-sharing attributes and constraints:

(i) the scope of data and information to be shared will depend on whether the U-space is designed in controlled or uncontrolled airspace, or in airspace where both controlled and uncontrolled manned aircraft may operate simultaneously (i.e. ICAO airspace class E);

(ii) a data- and information-sharing plan may cover the following:

(A) the data and information shared;

(B) compliance with applicable data protection legislation;

(C) data processing;

(D) data quality;

(E) data subjects' rights;

(F) data retention and deletion;

(G) security and training;

(H) security breaches and reporting procedures;

(I) responsibilities for providing data and services.

GM2 Article 5(6) U-space service providers

ARRANGEMENT BETWEEN THE SINGLE CIS PROVIDER AND THE AIR TRAFFIC SERVICE PROVIDER (ATSP)

Similarly to USSPs, specific arrangements may be necessary between the single CIS provider and the relevant ATSP.

The arrangement may be established according to the example presented in GM1 to Article 5(6) of Regulation (EU) 2021/664 and in Annex V to this Regulation to ensure the adequate exchange of relevant operational data and information.

AMC1 Article 5(7) U-space service providers

MONITORING OF THE AVAILABILITY OF CIS PROVIDERS AND REPORTING OF DATA QUALITY ISSUES

The single CIS provider should monitor the availability of services of the providers of common information, as well as the quality of the exchange and data received. The single CIS provider should inform the providers of common information as soon as practically possible about any detected availability or quality issues with regard to the data received.

AMC2 Article 5(7) U-space service providers

CIS DEGRADATION

The single CIS provider should inform USSPs without undue delay about CIS degradation.

AMC3 Article 5(7) Common information services

PRESERVATION OF DATA INTEGRITY AND QUALITY

The single CIS provider should ensure for the data it collects and distributes that:

(a) it does not alter the information, and preserves the integrity of the information received;

(b) it takes the appropriate measures to maintain the completeness, accuracy, resolution, traceability, timeliness, and logical consistency of the data.

GM1 Article 5(7) U-space service providers

CIS DEGRADATION

It is recommended that the single CIS provider inform USSPs about CIS degradation within 30 seconds.

GM1 Article 6 UAS operators

OBLIGATIONS WHEN OPERATING IN U-SPACE AIRSPACE

(a) Article 6 covers the obligations for UAS operators when they operate in U-space airspace. Apart from making use of the required U-space services, UAS operators would need to ensure in advance that the UAS intended to be operated comply with the applicable capabilities and performance requirements, as well as with the relevant operational conditions and airspace constraints.

(b) To adequately make use of the U-space services, UAS operators may conclude a contract with an active certified USSP of their choice that provides the required set of U-space services in a given U-space airspace.

(c) UAS operators should submit their UAS flight authorisation request to the USSP and comply with the terms and conditions of the UAS flight authorisation once it is granted by the USSP. Certain conditions need to be met prior to the flight. UAS operators are not allowed to commence a flight until they have sent an activation request of the UAS flight authorisation to the USSP. They should ensure compliance with the terms and conditions associated with the UAS operation in the particular U-space airspace. In case they cannot comply with the UAS flight authorisation, UAS operators should amend their original request.

AMC1 Article 6(1)(a) UAS operators

UAS CAPABILITIES AND PERFORMANCE REQUIREMENTS

UAS operators should select UAS of a type that is appropriate to satisfy the UAS capabilities and performance requirements specified for the U-space airspace.

In accepting the 'terms and conditions' of the flight authorisation provided by their USSPs, UAS operators confirm that they have selected the appropriate UAS type that satisfies the required U-space performance requirements.

GM1 Article 6(1)(a) UAS operators

UAS CAPABILITIES AND PERFORMANCE REQUIREMENTS

Depending on the UAS capabilities and performance requirements specified for the U-space airspace, not all UAS types are eligible to be operated. Technical support (e.g. providing technical characteristics of their products) provided by UAS manufacturers may be necessary in the evaluation of the UAS capabilities and performance requirements.

AMC1 Article 6(1)(b) UAS operators

MONITORING OF U-SPACE SERVICES

UAS operators should monitor, through a UAS flight, the availability of U-space services, and the information that may affect safety, such as:

(a) changes in the U-space airspace (e.g. dynamic airspace restriction or reconfiguration);

(b) changes to the flight authorisation (e.g. withdrawal, modification);

(c) traffic information, and especially traffic which may represent a collision hazard;

(d) non-conformance, when provided.

Accordingly, UAS operators should take appropriate action according to operational procedures and planned contingency measures.

AMC2 Article 6(1)(b) UAS operators

COMPLIANCE OF THE UAS FLIGHT

UAS operators should ensure consistency of the UAS configuration with the accepted flight authorisation, and should conduct the UAS flight to stay within the authorised planned 4D volume for 95 % of the time.

AMC3 Article 6(1)(b) UAS operators

ACKNOWLEDGEMENT OF NON-CONFORMANCE

When relevant, and as per Article 13(2) of Regulation (EU) 2021/664, UAS operators should acknowledge receipt of the notification that they are non-conforming by using the means provided by their USSPs.

AMC4 Article 6(1)(b) UAS operators

U-SPACE SERVICES — UAS OPERATORS' INTERFACE

When UAS operators intend to develop their own user interface upon the technical means that may be provided by the USSP (e.g. application programming interface (API)), they should ensure that the implementation of the proprietary user interface continues to satisfy the U-space performance requirements to which they contribute.

In such case, UAS operators should liaise with their competent authority to ensure that the overall acceptable level of safety (ALS) is not compromised by the complementary development activities. Even if, as per Regulation (EU) 2021/664, UAS operators are not directly subject to certification, they should consider Article 15(1)(a) and (b) of that Regulation and the related AMC and GM for the parts which may affect the safe provision of the required

GM1 Article 6(1)(b) UAS operators

U-SPACE SERVICES — GUARANTEE AS REGARDS THE LEVEL OF PERFORMANCE

It is necessary for the UAS operator to be able to demonstrate that the required level of U-space service performance can be achieved for the entire duration of the flight. This may take the form of a service level agreement (SLA) or any formal arrangement made between a service provider and the applicant on the relevant aspects of the U-space services to be provided (including quality, availability, and responsibilities).

GM2 Article 6(1)(b) UAS operators

USE OF U-SPACE SERVICES

Except for compensating for unavailability or degradation of U-space services, for the purpose of data consistency and the provision of safe support to operations, it is recommended as best practice that UAS operators keep using the bundle of services of the same USSP throughout an activated UAS flight.

GM3 Article 6(1)(b) UAS operators

CONNECTIVITY

The UAS operator should establish a digital connection to the USSP whenever the provision of U-space services is required to support operations in U-space airspace.

GM4 Article 6(1)(b) UAS operators

MONITORING OF U-SPACE SERVICES

While it is assumed that the priority for UAS operators is to ensure the safe conduct of a flight, safety of operations relies on the capability of UAS operators to maintain their situational awareness. The information provided by U-space services is meant to reach an acceptable level of safety within the U-space airspace, and needs to be adequately integrated throughout the operations.

A loss of link with the USSP is a safety issue per se as it disconnects the UAS operator from the U-space airspace, prevents it from maintaining situational awareness and eventually negatively impacts on the necessary decision-making to safely react to events that may dynamically happen.

The necessary monitoring procedure (e.g. degree, regularity, etc.) may vary depending on the operational constraints, and the roles and responsibilities of UAS operators (e.g. ‘hands-on’, ‘hands-off’), controls mock-up, etc.).

U-space services and information to the operator in charge of controlling or monitoring the UAS.

GM5 Article 6(1)(b) UAS operators

U-SPACE SERVICES — UAS OPERATORS' INTERFACE

The inadequate implementation of the interfaces with, or the improper use of, the U-space services may impair (e.g. by introducing latencies) the overall performance to an extent which may ultimately compromise the safety of operations within the U-space airspace. It is expected that the user interface that could be privately developed by UAS operators guarantee the satisfaction of the performance requirements defined for the U-space airspace (i.e. do not alter the performance) and the provision of U-space service information, down to the human operator in charge of operating the UAS.

Nevertheless, the responsibility of UAS operators is:

(a) limited to the continued satisfaction of the U-space performance requirements to which they contribute, according to the intended system and UAS operators' user interface implementation;

(b) commensurate with the level of risk that may be introduced locally.

The technical assessment could be conducted and completed through the specified activities in order to comply with Regulation (EU) 2019/947.

AMC1 Article 6(1)(c) UAS operators

OPERATING INSTRUCTIONS

UAS operators should handle the operation of the UAS flight as per the operating instructions established for the U-space airspace and provided by the USSP.

AMC2 Article 6(1)(c) UAS operators

EMERGENCY SITUATION

UAS operators should use the means at their disposal (e.g. built in the UAS and/or provided by the USSP) to declare an emergency when the UAS flight becomes non-compliant with the applicable U-space airspace operational conditions or constraints, or facing an event, to an extent which may result in hazards to other operations performed in the U-space airspace.

GM1 Article 6(1)(c) UAS operators

OPERATING INSTRUCTIONS

The operating instructions originate from the operational conditions and airspace constraints specified for the U-space airspace, and further refined and complemented by the procedures elaborated by the other U-space stakeholders (USSPs, ATS providers, etc.).

GM2 Article 6(1)(c) UAS operators

UAS EMERGENCY STATUS

UAS operators may support the alternative proposed in GM1 to Article 8(2)(f) of Regulation (EU) 2021/664 to compensate for the potential lack of automatic transmission of the UAS emergency status.

GM1 Article 6(3) UAS operators

UAS OPERATORS — SORA AND AIR RISK CLASS

Even if operations are intended to be performed in U-space airspace, the specific operations risk assessment (SORA) should still be carried out as per Regulation (EU) 2019/947. Regarding the evaluation of the air risk, UAS operators are entitled to take credit for their SORA of the residual air risk class (ARC) determined through the U-space airspace risk assessment as per AMC1 to Article 3(4) of Regulation (EU) 2021/664.

The Member State that designates the U-space airspace may define additional, more demanding performance requirements than the tactical mitigations performance requirements (TMPR), otherwise the U-space airspace performance requirements are less demanding and UAS operators should consider whichever is the most stringent. The UAS operator should demonstrate to the competent authority with sufficient evidence that it fulfils the U-space performance requirements or the required TMPR as per the SORA application, whichever is the most demanding.

GM2 Article 6(3) UAS operators

UAS OPERATIONS IN RESTRICTED GEOGRAPHICAL ZONES

UAS operators may operate in restricted UAS geographical zones (as per Article 15(3) of Regulation (EU) 2019/947) provided they have obtained a specific authorisation. In accepting the 'terms and conditions' of the flight authorisation provided by their USSP, UAS operators confirm that they have been authorised to perform operations within restricted UAS geographical zones.

AMC1 Article 6(5) UAS operators

UAS FLIGHT AUTHORISATION

The UAS operator should activate the UAS flight authorisation before the take-off, and end it as soon as possible after landing.

In case of operations that involve multiple take-offs and landings, the UAS flight authorisation should be activated once before the first take-off, and should be ended only after the last landing.

GM1 Article 6(5) UAS operators

ACTIVATION OF THE UAS FLIGHT AUTHORISATION

The UAS operator is expected to start the operation without undue delay after receiving the activation confirmation from the USSP. Time constraints for the specific airspace used may be established by the Member Sate that designates the U-space airspace.

AMC1 Article 6(7) UAS operators

FLIGHT AUTHORISATION PLANNING AND DEVIATION THRESHOLD

UAS operators should plan the UAS flight to stay within a planned 4D volume. Flying outside the planned 4D volume is to be an exceptional event for less than 5 % of the time. The size of the volume should allow for gusts of wind and other likely sources that could cause deviation.

When UAS operators do not consider it possible to appropriately perform the flight within the authorised, planned 4D volume, including the deviation threshold, for 95 % of the time (e.g. based on degraded environmental conditions, or operational constraints), they should replan their flight accordingly (e.g. extended boundaries) and request a new UAS flight authorisation.

AMC1 Article 6(8) UAS operators

CONTINGENCY MEASURES AND PROCEDURES

UAS operators should describe their contingency measures and procedures within the contractual agreement with the USSPs.

In addition, UAS operators should detail for each flight in their flight authorisation requests the planned contingency measures (e.g. alternative routes, emergency landing sites).

AMC2 Article 6(8) UAS operators

CONTINGENCY IN CASE OF DEGRADATION OR A LOSS OF THE USSP SERVICES

To prevent risking safety in case of degradation or a loss of the USSP services during the operations, UAS operators should safely end any active UAS flight as soon as possible, except when they have duly demonstrated to their competent authority that the continuation of the operation will not pose a hazard to the other operations performed in the U-space airspace.

GM1 Article 6(8) UAS operators

CONTINGENCY MEASURES AND PROCEDURES

The contingency measures and procedures may be derived from those specified in point (6)(d) of Appendix 5 to the Annex to Regulation (EU) 2019/947. They may also address the following conditions:

(a) sudden, total or partial unavailability of the U-space airspace,

(b) restriction or revocation of the UAS flight authorisation,

(c) unlawful interference,

(d) engine failure,

(e) loss of signal,

(f) loss of control,

(g) loss of payload,

(h) loss of power,

(i) loss of energy reserves,

(j) adverse weather conditions,

(k) foreign object debris (FOD),

(l) unidentified aircraft entering protected volume around the UAS,

(m) unavailability of landing area.

GM2 Article 6(8) UAS operators

CONTINGENCY IN CASE OF DEGRADATION OR A LOSS OF THE USSP SERVICES

UAS operators may evaluate the degradation or the loss of the USSP services in the context of their operations in the U-space airspace and establish appropriate contingency measures against the resulting hazards.

A hazard assessment should consider:

(a) the impact and severity of the hazards on own operations;

(b) the impact and severity of the hazards on other nearby operations;

(c) the operational environment;

(d) other additional operational mitigation measures, if applicable.

UAS operators should provide USSPs with actions to be taken in the event of a loss or degradation of the U-space services which could result in an overall reduction of safety or pose a risk to nearby U-space operations, and action would be required to be taken by another UAS operator. These actions may be contained within an operator's contingency plan. UAS operators should ensure the effective coverage of the contingency measures in case of degradation or loss of USSP services, especially for services used in flight such as:

(e) the inability to receive information on dynamic airspace reconfiguration and/or modifications to the UAS flight authorisation;

(f) a loss of availability of traffic information data;

(g) sharing of contingencies (as applicable).

GM1 Article 7 U-space service providers

GENERAL REQUIREMENTS

(a) A U-space service provider (USSP) is a new entity established by this Regulation. It refers to an organisation that is certified by a competent authority to provide U-space services in the U-space airspace.

(b) USSPs are responsible for implementing and providing the bundle of U-space services required by the Member State that designates the U-space airspace.

(c) Entities that are not willing to deliver all required U-space services may act as subcontractors to a USSP that provides all required U-space services.

(d) A USSP may subcontract the provision of some or all U-space services to other entities if they remain under its management control. There can also be associations between USSPs or equivalent mechanisms, if it is clear that there is a single certified entity responsible for providing the required bundle of U-space services to UAS operators. When required, the USSP should ensure that the competent authority is given access to any subcontracted organisation and data relevant to support the USSP certification.

(e) USSPs ensure coordination with CIS providers or, when designated, the single CIS provider.

(f) USSPs ensure operational coordination with other USSPs that are active in the same U-space airspace and the relevant ATSPs. Only some specific information is expected to be sent back to the relevant ATC unit.

(g) USSPs support the dissemination and acknowledgment of notification on dynamic airspace reconfiguration, in accordance with Article 4 of Regulation (EU) 2021/664.

(h) USSPs support the competent authority in recording and making operational data available to support the conduct of safe operations in the U-space airspace, as laid out in the AMC and GM to Article 18(f) and (h) of Regulation (EU) 2021/664.

AMC1 Article 7(2) U-space service providers

BUNDLE OF U-SPACE SERVICES

The set of U-space services required to be provided by the USSP to UAS operators is defined by the Member State for each designated U-space airspace. To facilitate the provision of U-space services to UAS operators, a USSP should provide the U-space services required in the U-space airspace served in a form of bundle, which may encompass:

(a) four services as per Article 3(2) of Regulation (EU) 2021/664;

(b) five or six services when considering the provisions of Article 3(3) of Regulation (EU) 2021/664.

AMC2 Article 7(2) U-space service providers

USSP–UAS OPERATOR INTERFACES

The USSP should provide UAS operators with interfaces, together with the U-space services. The interfaces and functionalities should at least allow UAS operators to:

(a) properly use the U-space services;

(b) be provided with the operational instructions applying to the U-space airspace;

(c) get access to the UAS operator's operational records;

(d) declare a contingency or an emergency;

(e) acknowledge any non-conformance, when the conformance monitoring service is required, as per Article 13(2) of Regulation (EU) 2021/664.

AMC3 Article 7(2) U-space service providers

UAS OPERATOR SITUATIONAL AWARENESS

The USSP should ensure that the information that may affect safety is efficiently conveyed transmitted to UAS operators, allowing them to take the necessary, appropriate actions to ensure safety in a timely manner.

Accordingly, the USSP should:

(a) identify the information that supports safety, and requires immediate UAS operator awareness;

(b) reduce the risk of missing the information that supports safety by deploying means to ensure that the attention of UAS operators will be appropriately attracted.

AMC4 Article 7(2) U-space service providers

DEGRADATION OF USSP SERVICES

The USSP should inform without undue delay its UAS operators, other USSPs within the same U-space airspace, and ATSPs when necessary, about the degradation of its services (including degradation that results from the unavailability of CIS providers or ATSPs).

The degradation of USSP services should be supported by procedures or contingency measures to be jointly established with UAS operators.

AMC5 Article 7(2) U-space service providers

U-SPACE AIRSPACE OPERATING INSTRUCTIONS

The USSP should develop and provide UAS operators with instructions on how to conduct operations within the U-space airspace. The operating instructions should encompass:

(a) the transcription of the operational conditions and airspace constraints that originate from the U-space airspace risk assessment;

(b) a user guide documenting how UAS operators should configure and use USSP services;

(c) when the services are provided through an API, the user guide should also contain the technical instructions and requirements to the UAS operators to ensure the continued satisfaction of the performance requirements and overall safety;

(d) recommendations ensuring the security of the exchange;

(e) the normal, contingency, and emergency procedures related to U-space services, to be applied by UAS operators.

GM1 Article 7(2) U-space service providers

CONNECTIVITY

Regulation (EU) 2021/664 assumes that the U-space is a connected environment. A connected environment refers to any digital connection that meets the requirements established by the USSP for the provision of the U-space services in question. A connected environment is not restricted to internet-based connectivity, although the vast majority of connections between a USSP and a UAS operator are expected to be internet based.

Therefore:

(a) U-space information is exchanged in a machine-readable format to support the necessary exchange of data among the U-space actors concerned; and

(b) operations in the U-space airspace require the UAS operator to establish a connection to a USSP.

GM2 Article 7(2) U-space service providers

USSP–UAS OPERATOR INTERFACES

The USSP may have various means to develop and provide UAS interfaces, such as interfaces relying on mobile, web or PC applications, and/or application programming interfaces (API). The solution retained is expected to ensure that the performance requirements are met, and the availability of the services is ensured.

GM3 Article 7(2) U-space service providers

CONDITIONS THAT REQUIRE IMMEDIATE AWARENESS

Safety-critical information, which may require the UAS operators' immediate awareness, may concern the following:

(a) degradation of services;

(b) changes in the configuration of the U-space airspace (e.g. dynamic airspace restriction or reconfiguration);

(c) changes in the flight authorisation;

(d) new emergency in the proximity of the UAS flight;

(e) non-conformance, when relevant for the U-space airspace;

(f) incoming manned traffic which may eventually result in a conflict with the UAS flight trajectory;

(g) infringement of the UAS flight authorisation;

(h) detection of rogue traffic in the proximity or within the volume where the UAS flight is performed.

GM4 Article 7(2) U-space service providers

ALERTING MEANS

Safety relies on the timely reaction of UAS operators to situational changes that may dynamically occur in the U-space airspace throughout the UAS flight. Inappropriate UAS operator reaction due to a lack of sufficient awareness may ultimately compromise safety. Moreover, UAS operations require UAS operators to additionally manage operational information than just strict UAS flight data. In some conditions, especially where high workload is involved, UAS operators may have limited capability to focus their attention on monitoring U-space services in order to detect new relevant information.

Regardless of being served by the USSP through a separate user interface/application or through direct application programming interface (API), UAS operators need to be clearly alerted to new, safety-critical information during all phases of flight (flight preparation, preflight, in flight and postflight).

To effectively attract the attention of UAS operators, the USSP may either implement or provide the supporting means of various techniques such as:

(a) visual annunciations (e.g. flashing red),

(b) aural annunciations (e.g. sounds or voice),

(c) telephony voice messages,

(d) telephony text messages, coupled with haptic sense.

To maximise the effectiveness of the attention-getter, it is recommended that the USSP rely on more than one means for raising awareness on safety-critical information that requires immediate attention.

The implementation of the necessary alerting means should ensure the use of appropriate designs that effectively raise the attention of UAS operators while preventing undue nuisance and distraction that could impair the safe conduct of UAS operations.

GM5 Article 7(2) U-space service providers

DEGRADATION OF USSP SERVICES

It is recommended as best practice that the USSP disseminate the information on the degradation of its services within 30 seconds.

GM6 Article 7(2) U-space service providers

UAS OPERATIONAL RECORDS

It is recommended as best practice that USSPs provide UAS operators with a method to access a copy of their data related to the U-space services required by a Member State (e.g. history of the flight authorisations as well as non-normal conditions). Any requested piece or set of data should be electronically exported and provided to the UAS operators in a machine-readable format.

AMC1 Article 7(3) U-space service providers

ARRANGEMENT BETWEEN USSPs AND ATSPs

For U-space airspace established in controlled airspace, the USSP should establish a written agreement with the relevant ATSP covering the coordination of activities, as well as the exchange of relevant operational data and information. The coordination activities between the USSP and the ATSP should cover:

(a) the emergency management plan as per Article 15(2) of Regulation (EU) 2021/664, including contingency and emergency conditions involving manned and unmanned aircraft;

(b) the exchange of relevant operational data and information, if not provided through the CIS, as per point ATS.OR.127 of Regulation (EU) 2017/373 amended by Regulation (EU) 2021/665;

(c) the dynamic airspace reconfiguration procedure, laid down in Article 4 of Regulation (EU) 2021/664, and in accordance with point ATS.TR.237 of Regulation (EU) 2017/373 amended by Regulation (EU) 2021/665, in identifying the means to:

  (1) receive the dynamic airspace reconfiguration requests from the ATC unit;

  (2) notify in a timely manner the ATC unit about the presence of UAS special operations within the designated U-space airspace as per AMC2 to point ATS.TR.237(a) of Regulation (EU) 2017/373 amended by Regulation (EU) 2021/665;

(3) notify the ATC unit once the airspace reconfiguration has been implemented, as per the conditions addressed in the AMC and GM to Article 4 of Regulation (EU) 2021/664;

(4) alert the ATC unit in case of unavailability of the link with the USSP;

(5) alert the ATC unit in case a relevant non-conformance is identified in the U-space airspace, when the conformance monitoring service is required, and as per Article 13(2) of Regulation (EU) 2021/664.

GM1 Article 7(3) U-space service providers

ARRANGEMENT BETWEEN USSPs AND ATSPs

Although the exchange of data and information between USSPs and ATSPs is routed via the CIS in accordance with Article 5 of Regulation (EU) 2021/664, the coordination of activities (such as emergency procedures) will require the direct interaction and coordination between USSPs and ATSPs. Therefore, the following arrangement topics are not suitable to be delegated to a single CIS provider (when one is designated):

(a) normal, contingency and emergency procedures concerning UAS operations;

(b) nominal, non-normal and emergency procedures concerning manned aircraft operations performed in the U-space airspace;

(c) procedures concerning system or service shortages and degraded level of quality of a service;

(d) procedures, roles and responsibilities for both parties, as required by Article 15(2) of Regulation (EU) 2021/664.

It is recommended that USSPs use GM1 to Article 5(6) of this Regulation to formalise the arrangement with the relevant ATSP.

AMC1 Article 7(5) U-space service providers

ARRANGEMENT AMONG USSPs

For the purpose of ensuring technical interoperability, all USSPs with an interest in the same U-space airspace should adhere to the same arrangement. The arrangement should ensure the compatibility of a USSP system joining the U-space airspace to allow USSPs to add the start/cease of the provision of services in the agreement or remove the start/cease of the provision of services from it.

AMC2 Article 7(5) U-space service providers

MONITORING OF THE AVAILABILITY OF CIS AND ATSPs

The USSP should monitor the availability of, and quality of the exchange with, the provider of common information, or the single CIS provider (if designated), and ATSPs.

AMC3 Article 7(5) U-space service providers

PRESERVATION OF DATA INTEGRITY AND QUALITY

USSPs should ensure for the data they are required to collect and distribute that:

(a) they do not alter the information, and preserve the integrity of the information received;

(b) they take appropriate measures to maintain the completeness, accuracy, resolution, traceability, timeliness, and logical consistency of the data.

AMC4 Article 7(5) U-space service providers

REPORTING OF DATA QUALITY ISSUES

USSPs should inform the providers of common information, the single CIS provider (if designated) and other USSPs that operate in the same U-space airspace as soon as practically possible of any detected availability or quality issues with the data received.

AMC5 Article 7(5) U-space service providers

EXCHANGE OF INFORMATION AMONG USSPs

A USSP should exchange and consolidate the following information with other USSPs that share the same U-space airspace:

(a) UAS remote identification, through the network information service, to support the continuous consolidation of traffic information.

(b) The status of the UAS flight authorisations to ensure the continuous synchronisation of the authorisations within the U-space airspace and adequate deconfliction.

(c) Traffic information, including e-conspicuous manned aircraft, as per point SERA.6005(c) of Regulation (EU) No 932/2012, when duly agreed among the USSPs.

(d) Non-conformance alerts trigged by their UAS operators.

(e) Notification of the degradation of their services.

(f) Contingencies and emergencies of their UAS operators.

(g) Other information as required by the Member State and/or as agreed among the USSPs, which may be necessary to ensure interoperability in the U-space airspace.

AMC6 Article 7(5) U-space service providers

EXCHANGE OF INFORMATION AMONG USSPs — INTERFACES

(a) The exchange of information described in point (c) among the USSPs should conform to the requirements of Annex A to EUROCONTROL 'Specification for SWIM Technical Infrastructure (TI) Yellow Profile', edition 1.1, published on 5 July 2020.

(b) USSPs should document the services that facilitate the exchange of information referred to in Article 3(2) and (3) of Regulation (EU) 2021/664, as well as the related services regarding the safe provision of services, and should adhere to EUROCONTROL 'Specification for SWIM Service Description (SD)', edition 2.0, published on 15 March 2022.

(c) The documentation of services defined in point (b) should be made available to the public (e.g. service descriptions, interfaces).

(d) Compliance with points (a) and (b) should be directly measured against the requirements listed in the respective documents.

GM1 Article 7(5) U-space service providers

ARRANGEMENT AMONG USSPs AND THE MASTER AGREEMENT

USSPs may use a common contract (the master agreement) that defines the technical indicators associated with the provision of services, acceptable and unacceptable service levels, parameters for data-sharing among USSPs, as well as dispute resolution procedures and actions to be taken in specific circumstances.

GM2 Article 7(5) U-space service providers

MONITORING OF THE AVAILABILITY OF CIS AND ATSPs

The frequency at which CIS providers and ATSPs are monitored is commensurate with the level of risk the lack of information may induce. Indeed, while the unavailability of communication with the ATSP may represent a short-term threat to safety, the lack of availability of the UAS operator's registration databases would only represent an issue in case of unresponsiveness to a query.

GM3 Article 7(5) U-space service providers

EXCHANGE OF INFORMATION ON E-CONSPICUOUS MANNED TRAFFIC

The receipt of information on e-conspicuous manned traffic, as per point SERA.6005(c) of Regulation (EU) No 932/2012, may rely on ground infrastructure (e.g. antennas) in the U-space airspace privately deployed by the USSPs. In order not to create an unfavourable situation and unfair treatment among the USSPs, the exchange of information on e-conspicuous manned traffic is subject to a specific agreement made among the USSPs.

GM4 Article 7(5) U-space service providers

EXCHANGE OF INFORMATION — INFORMATION MODEL

(a) U-space services may be provided concurrently by multiple USSPs in the same airspace. This requires the exchange of information and coordination among those USSPs, as well as between USSPs and other entities (such as UAS operators, ATSPs and CIS providers). Such exchange of information is expected to be based on open protocols and formats, using public, IP-based networks as transport layers.

(b) The exchange of information (and its models) should be described in a technology-agnostic way (e.g. in the Unified Modelling Language (UML)). The aim is to document the key aspects of a dedicated information exchange service at conceptual level.

(1) Operational and business context of the service:

(i) service requirements (e.g. information exchange, constraints, validation rules);

(ii) stakeholders that provide/use the service;

(iii) operational activities supported by the service (e.g. flight planning, flight execution, etc.);

(iv) relation of the service to other services.

(2) Service description:

(i) interfaces (e.g. based on request/response or publish/subscribe);

(ii) interface operations (methods to interact with the service, e.g. request a flight authorisation);

(iii) payload definition;

(iv) features (e.g. a flight authorisation object);

(v) properties/attributes (e.g. the identifier within a flight authorisation object);

(vi) data types (e.g. defining the identifier within a flight authorisation record as a list of characters and numbers);

(vii) associations (e.g. the relation of a flight authorisation to a registered UAS);

(viii) dynamic behaviour (and life cycle) description.

(3) Service performance level and validation aspects.

(c) The information exchange services described in point (b) may be realised in different technical implementation levels enabling an architectural approach based on one concept, allowing for multiple potential solutions.

(d) Consequently, different types of data frames might be in use to carry payload. A standard data encoding may be used to provide the service (JSON or ASTERIX on the example of traffic information).

(e) The data encoding should be mapped to the definition of the service payload. Furthermore, the service that provided the information on this data encoding should be mapped in relevant technical details as well, e.g. in the service interfaces and operations. EUROCAE ED-269, which establishes a conceptual definition and its implementation in a standard data encoding, may be used as an example.

(f) Provision of safe services

(1) In addition to the operational information exchanged among the respective USSPs, further information on the respective service's performance (e.g. degradation of services) may be collected and made available to ensure the provision of safe services. Sufficient monitoring may support technical operations to be performed under controlled conditions. This includes ensuring compliance with the related data quality, latency and data protection requirements set out in Annex III to Regulation (EU) 2021/664.

(2) The provision and exchange of any safety-relevant information should follow processes that are comparable to established standards (e.g. ISO 9001 series). Additional information that originates from these processes should be exchanged as well. This includes but is not limited to:

(i) service availability (planned or unplanned downtime, points of contact for technical and operational matters, etc.);

(ii) service limitations (degraded operations, regional constraints, known issues);

(iii) service integrity (security/safety incidents).

(3) Both operational and service performance information should be protected; technical and operational measures should be taken by the USSPs to ensure the necessary information protection.

(g) Protocol

Any information exchange should be based on a common open communication protocol, such as the transmission control protocol (TCP). As a minimum, the requirements documented in the SWIM Technical Infrastructure (TI) Yellow Profile, edition 1.1, published on 5 July 2020, should be met.

(h) Extension of information exchange services

(1) Information exchange services may be extended by the entities described in point (a).

(2) The extension of information exchange services, by changing their description (as described in point (b)(2)), should not jeopardise their semantic interoperability and standardisation across the Member States.

(3) The extension of the payload definition can be usually managed by:

(i) adding additional properties/attributes to the features;

(i) adding new features.

(4) The extension points for additional properties/attributes could be already foreseen in the payload definition, such as free text or a custom enumeration.

(5) If custom features are added by an extension, the association between the default and the additional features should always be managed in the additional feature.

(6) The description of the extended service should introduce optional elements (interfaces, operations, features, attributes/properties, data types, etc.) only.

For instance, if additional information regarding communication infrastructure is provided by an extended flight authorisation service, a new feature called 'communication infrastructure service availability' might be introduced. This new feature might be associated with a flight authorisation feature. The association should be designed without changing the flight authorisation feature, to allow the processing of flight authorisations by services that have no knowledge of the 'communication infrastructure service availability'.

(7) The approach to the service description is laid down in the SWIM Service Description and the EUROCONTROL Specification for SWIM — Information Definition.

(i) Protection of information

The necessary protection level will vary depending on the type of the information exchanged. As a minimum, the requirements documented in the SWIM Technical Infrastructure (TI) Yellow Profile, edition 1.1, published on 5 July 2020, should be met. Additional protection should be put in place where applicable, especially when considering the relevant data privacy regulations (e.g. GDPR).

AMC1 Article 7(6) U-space service providers

CONFIGURATION OF THE PROVISION OF SERVICES

After receiving their certificate, USSPs are entitled to deliver their services in any U-space airspace.

Nevertheless, the result of the U-space airspace risk assessment, and the related performance requirements, operational constraints and digital interfaces may vary between U-space airspace volumes. Therefore, prior to start providing services, the USSP should liaise with the local competent authority to ensure that the provision of services satisfy the performance requirements and constraints established for the U-space airspace where the operations are intended to be conducted.

When the USSP services are inadequate to fulfil the local conditions to an extent which may not ensure the safe provision of services, the USSP should undertake the extension of its certificate to demonstrate its capability to satisfy the complementary U-space airspace requirements and constraints.

AMC2 Article 7(6) U-space service providers

SUPPORTING OPERATIONAL RECORDS

As soon as the operations start and until they are ceased, the USSPs should support the safety of the operations and the competent authority in charge of the U-space airspace, in recording and making available operational data and events that may be encountered. The type of this data and its retention should be agreed with the competent authority, but should be compatible with the dynamic reassessment of the definition of the U-space airspace.

GM1 Article 7(6) U-space service providers

U-SPACE AIRSPACE — ONBOARDING PROCESS

Before reporting the start of operations to the competent authority, and in order to provide services in newly designated U-space airspace, USSPs may have to:

(a) coordinate with the competent authority in charge of the U-space airspace where the operations are intended to be conducted;

(b) coordinate and conclude agreements with the CIS providers (or, when designated, the single CIS provider) in that U-space airspace on data sharing;

(c) coordinate and conclude agreements with other USSPs in that U-space airspace on data sharing;

(d) coordinate and conclude agreements with ATSPs in that U-space airspace;

(e) configure and/or adjust the provision of services:

  (1) to adhere to the common protocol that supports the exchange of information (e.g. among USSPs) in the U-space airspace;

  (2) to satisfy the performance requirements and constraints of the U-space airspace.

GM2 Article 7(6) U-space service providers

CONFIGURATION OF THE PROVISION OF SERVICES

The main items that may vary between U-space airspace volumes are:

(a) the required set of U-space services, which could encompass the provisions of Article 3(3) of Regulation (EU) 2021/664;

(b) the U-space services' performance requirements and constraints, as per Article 3(4) of Regulation (EU) 2021/664;

(c) the common protocol(s) that support the exchange of information with the CIS provider and among the USSPs as per Articles 5(4)(a) and 7(5)(b) of Regulation (EU) 2021/664 and its Annex II.

GM3 Article 7(6) U-space service providers

REPORT TO THE COMPETENT AUTHORITY — TEMPLATE FORM

USSPs may consider using the template form below for the purpose of reporting to the competent authority the start and ceasing of the operations.

Letter to the competent authority

U-space service provider report to the competent authority in accordance with Article 7(6) of Regulation (EU) 2021/664

Report for the start and/or ceasing of the provision of U-space services in accordance with Article 7(6) of Regulation (EU) 2021/664
U-space service provider Name: U-space service provider's certificate number / issue number: Name and contact details of the accountable manager: Member State, or list of Member States, where the U-space service provider intends to start its operations:
Start of operations The U-space service provider hereby confirms that the provision of U-space services will start/restart on: day/month/year
Ceasing of operations The U-space service provider hereby confirms that the provision of U-space services will cease on: day/month/year
The notification of starting/ceasing/restarting operations must be submitted to the competent authority at least 3 months before the effective start/ceasing/restart of operations.
Date, name, and signature of the accountable manager

GM4 Article 7(6) U-space service providers

SUPPORTING OPERATIONAL RECORDS

The operational records are meant to provide data to support the implementation of Article 18(h) of Regulation (EU) 2021/664, and the dynamic reassessment of the definition of the U-space airspace as defined in the AMC and GM to Articles 3(1) and 18(f) of Regulation (EU) 2021/664. The operational data and events that may be of interest to a competent authority are the following:

(a) dynamic airspace reconfiguration or restrictions;

(b) failure to implement dynamic airspace restriction or reconfiguration;

(c) volume of (e-conspicuous) manned aircraft crossing the U-space airspace;

(d) air proximity situation among UAS, and between UAS and manned aircraft;

(e) emergency declared by UAS operators;

(f) deviation (non-conformance) with the flight authorisation;

(g) over-conformance, when the deviation threshold may be too wide and airspace capacity wasted;

(h) detection of rogue UAS, or UAS used for malicious or unlawful purposes.

The information may be provided in terms of:

(i) volume/number of occurrences; and

(j) date, time, and location expressed in WGS 84 coordinate.

It is recommended that the USSP keep the records for a period of 5 years.

GM1 Article 8 Network identification service

GENERAL

(a) The network identification service provides the registration number of a UAS operator, the serial number of an unmanned aircraft, and live flight data of the UAS. It enables the sharing of information with any of the authorised users listed in Article 8(4)(b) of Regulation (EU) 2021/664. Authorised users will be made aware of the geographical position, route course and emergency status, flight level, and type of the UAS, among other data elements. Based on the information provided by the UAS operators, USSPs share and consolidate UAS flight data among themselves and can, therefore, support traffic information when needed.

(b) The network identification service complements the original intent of the direct and network remote identification systems referred to in Regulation (EU) 2019/945. Whereas the remote identification established in Regulation (EU) 2019/945 supports the authorities in aspects related to security and privacy, the network identification service also supports operational needs and the traceability of unmanned aircraft during flight. The responsibility for the provision of the remote identification service lies with different entities. Regulation (EU) 2019/945 lays down the requirements for the design and manufacture of unmanned aircraft systems whereas Regulation (EU) 2021/664 defines the services provided by USSPs.

(c) Detailed and accurate information about the latency necessary for the proper functioning of the traffic information service may be assessed and defined during the U-space airspace risk assessment.

AMC1 Article 8(1) Network identification service

PROVISION OF AGGREGATED UAS REMOTE IDENTIFICATION

USSPs should provide the UAS network remote identification in the geographic proximity of UAS operations that are supported by the provision of their services.

USSPs should exchange network remote identification data with all the service providers that share the same U-space airspace. The resulting aggregated data should cover all available network remote identification data in the U-space airspace concerned.

AMC2 Article 8(1) Network identification service

CONTINUOUS PROCESSING

USSPs should demonstrate a response time for distributing data received from the UAS, or from other service providers, which is smaller than the latency necessary for the proper functioning of the traffic information service, for at least 99 % of the time.

AMC3 Article 8(1) Network identification service

DURATION OF THE FLIGHT

The network identification service should:

(a) be available throughout the duration of the flight, starting as soon as the flight authorisation is activated;

(b) not be required when the operator ceases the flight, independently of the time limit approved in the flight authorisation.

AMC4 Article 8(1) Network identification service

DATA EXCHANGE INTERFACE

USSPs should use the interface defined in Annex 4 to ASTM F3411-22A 'Standard Specification for Remote ID and Tracking'.

GM1 Article 8(1) Network identification service

GEOGRAPHIC PROXIMITY

Member States may support the definition of 'geographic proximity' by setting a value as part of the performance requirements established for each U-space airspace. Alternatively, the value provided in ASTM F3411-22A which specifies a rectangular area with a diagonal no greater than 7 km as a maximum display area may be used. Establishing a value for a geographic proximity smaller than the size of the U-space airspace limits the sharing of unnecessary data among the USSPs and thus supports the technical and economic efficiency of the network.

GM2 Article 8(1) Network identification service

TESTING INFRASTRUCTURE

To support the satisfaction of the U-space performance requirements as per Article 15(1) of Regulation (EU) 2021/664, a possible testing environment is presented in Annex A2 to ASTM F3411-22A 'Standard Specification for Remote ID and Tracking'.

AMC1 Article 8(2) Network identification service

ACCESS

USSPs should provide the authorised users defined in Article 8(4) of Regulation (EU) 2021/664 with access to aggregated network remote identification data using the communication protocol defined in Annex 4 to ASTM F3411-22A 'Standard Specification for Remote ID and Tracking'.

AMC1 Article 8(2)(c) Network identification service

ALTITUDE ABOVE MEAN SEA LEVEL

USSPs should convert the heights above the WGS 84 ellipsoid exchanged with the ASTM F-3411-22A standard to height above mean sea level (MSL) before providing it to the UAS operators.

GM1 Article 8(2)(c) Network identification service

ALTITUDE ABOVE MEAN SEA LEVEL

Due to the fact that the altitude above mean sea level (AMSL) calculated from the measured value of the barometric sensor and the QNH, cannot be compared to the calculated value of the altitude AMSL using the GNSS systems, it is recommended to exchange the altitude values in relation to the WGS 84 ellipsoid between U-space systems.

Wherever the flight altitude above sea level is required to be determined with the use of GNSS systems, it is recommended to use the EGM2008 or at least the EGM96 geoid models as the definition of mean sea level, as agreed with the competent authority.

GM1 Article 8(2)(f) Network identification service

UAS EMERGENCY STATUS

Certain UAS capabilities may not be available as from 26 January 2023, the date on which Regulation (EU) 2021/664 will become applicable. Regarding the identification of the UAS emergency status as per Article 8(2)(f) of Regulation (EU) 2021/664, and to compensate for the potential lack of automatic transmission of the information, it is considered an acceptable alternative for UAS operators to:

(a) continuously monitor the UAS behaviour, and when implemented, the built-in safety parameters or emergency status;

(b) manually trigger the UAS emergency status toward the USSP.

The proposed alternative is considered acceptable until 1 year after the date of entry into force of Regulation (EU) 2021/664, i.e. 26 January 2024.

GM1 Article 8(3) Network identification service

UPDATE FREQUENCY

Competent authorities may use the value defined in ASTM F3411-22A ‘Standard Specification for Remote ID and Tracking’ as aggregated monthly target for update frequency (no more than 3 seconds for 95 % of the time, and in 1 second for 99 % of the time).

GM1 Article 8(4) Network identification service

ACCESS

USSPs may provide a visual interface to the authorised users to access data in accordance with items 5.5.5.6 to 5.5.5.8 of ASTM F3411-22A 'Standard Specification for Remote ID and Tracking'.

GM1 Article 9 Geo-awareness service

GENERAL

(a) Article 9 contains the requirements for USSPs when providing the geo-awareness service to UAS operators, and should not be confused with the geo-awareness function required by Regulation (EU) 2019/945 for certain UAS classes. In the latter case, geo-awareness is defined as a UAS function that detects a potential breach of the applicable airspace limitations and alerts the remote pilots so that they can take effective and immediate action to prevent that breach from occurring. In the framework of the U-space Regulation, geo-awareness is a USSP service that provides UAS operators with the information about the latest airspace constraints and defined UAS geographical zone information made available as part of the CIS.

(b) This service aims to support UAS operators in fulfilling their obligations, as it provides the necessary information on applicable operational conditions and airspace constraints with the level of accuracy and other performance requirements for which it has been certified.

(c) The geo-awareness service is used by the UAS flight authorisation service as a source of data to inform UAS operators of relevant operational constraints and changes both prior to and during the flight.

AMC1 Article 9(1) Geo-awareness service

INFORMATION

USSPs should ensure the timeliness and availability of the geo-awareness information provided to UAS operators.

AMC1 Article 9(2) Geo-awareness service

TIMELINESS

USSPs should process and make geo-awareness data available to UAS operators based on the data's update cycle and criticality level, but no later than its applicability dates and times.

GM1 Article 9(2) Geo-awareness service

TIMELENESS

The table below illustrates the scenarios and values USSPs may consider for the implementation of the geo-awareness service:

Data type	CIS update cycle	Geo-awareness service update
Static geographical zone	Based on the aeronautical information regulation and control (AIRAC) cycle	Daily
Planned dynamic airspace restriction or limitation	Several times a day	Every 30 minutes
Unplanned dynamic airspace reconfiguration	Upon ATC unit request	Within 5 seconds

GM2 Article 9(2) Geo-awareness service

TIME FORMAT AND VERSION NUMBER

USSPs may use the time format and version number provided in Chapter VIII 'UAS geographical zone data model' of and in Appendix 2 to EUROCAE ED-269 'MINIMUM OPERATIONAL PERFORMANCE STANDARD FOR GEOFENCING' standard in the version published in June 2020.

GM1 Article 10 UAS flight authorisation service

GENERAL

(a) The UAS flight authorisation service provides authorisations to UAS operators for each individual flight based on other notified flight requests that may conflict with other unmanned operations within the same U-space airspace. It is a strategic deconfliction tool. The UAS flight authorisation service is provided to a UAS operator under the condition that it has submitted the UAS flight authorisation request before the flight. The content of this request is detailed in Annex IV to Regulation (EU) 2021/664.

(b) The UAS flight authorisation service should be able to handle flight authorisation requests by UAS operators for single flights and for a number of repetitive flights that are conducted consecutively on the same route.

(c) This service covers the flight authorisation provided according to Article 15(1) of Regulation (EU) 2019/947; however, it does not cover operational authorisations granted by the competent authority as defined in Article 12 of Regulation (EU) 2019/947. The service informs operators of overlaps with any airspace restrictions provided by the geo-awareness service (Article 9). UAS flight authorisations in 4D volume may be used by the conformance monitoring service.

(d) This service is also a way for UAS operators to announce their intent to start their operations by activating their UAS flight authorisation. The activation of a flight initiates the provision of tactical services (like traffic information, network and remote identification or conformance monitoring) when required. The subsequent ending of the flight stops the provision of these services.

(e) This service is mandatory in U-space airspace designated in any airspace (controlled or not) and applies to UAS operators. This service enforces the prioritisation rules. When there is more than one USSP providing U-space services in a U-space airspace, all USSPs should exchange the UAS flight authorisation requests among themselves as well as state the changes to those requests — i.e. ‘Accepted’, ‘Activated’, ‘Withdrawn’, ‘Ended’.

(f) The information required to process a flight authorisation is provided by the UAS operators (flight authorisation request), other USSPs (other accepted flight authorisations, traffic information), and the CIS (e.g. temporary restrictions, manned traffic information). The single CIS provider has no coordination role and no other responsibilities than to ensure the provision of a subset of information that supports the flight authorisation process.

AMC1 Article 10(1) UAS flight authorisation service

FLIGHT AUTHORISATION RECORDS

USSPs should keep records of:

(a) all UAS flight authorisations, including:

(1) the data submitted by the UAS operator;

(2) the time of receipt of the requests;

(3) when accepted, the unique authorisation number, and the associated terms and conditions;

(b) UAS flight authorisation requests that are rejected, including the reason for rejection.

AMC2 Article 10(1) UAS flight authorisation service

TERMS AND CONDITIONS

The USSP should include in the terms and conditions of a flight authorisation:

(a) a reminder clause about the applicable conditions and airspace constraints;

(b) the technical requirements, such as the necessary UAS performance requirements;

(c) when relevant, a list of any permissions that are required for a flight to enter restricted airspace (e.g. limited-access geographical zones);

(d) instructions detailing how to handle the flight authorisation and activation requests and constraints, such as the time frame for flight activation or deactivation.

GM1 Article 10(1) UAS flight authorisation service

RETENTION OF RECORDS

It is recommended that the USSP keep the records for a period of 5 years.

GM1 Article 10(2) UAS flight authorisation service

UAS FLIGHT AUTHORISATION PROCESS

(a) The UAS flight authorisation service is a conflict resolution mechanism and authorises flights that are free of intersection with other flight authorisations.

(b) The UAS flight authorisation request describes the flight trajectory as a series of one or more 4D volumes expressed in height (base, ceiling), longitudinal and lateral limits, and duration (entry and exit times). Each dimension includes the uncertainties of the flight, e.g. earliest possible entry, latest possible exit.

(c) The detection of conflict is performed considering the planned 4D trajectories of the flights with the deviation thresholds added.

(d) The flight authorisation service ensures that the trajectory does not conflict with a no-fly zone and warns if the flight enters a restricted area.

(e) The UAS flight authorisation service describes a 4D trajectory typically in terms of height, length, width, and duration, and ensures that the trajectory does not conflict with a no-fly zone.

(f) The performance required is primarily driven by considering separation assurance and collision avoidance.

AMC1 Article 10(2)(a);(b) UAS flight authorisation service

CHECK OF THE UAS FLIGHT AUTHORISATION REQUEST — COMPLETE, CORRECT, FREE OF INTERSECTION

The USSP should verify that the UAS flight authorisation is complete, correct, and free of intersection, and only accept the UAS flight authorisation request when all the following conditions are satisfied:

(a) When specified by the Member State (as per AMC2 to Article 3(4) of Regulation (EU) 2021/664), the flight authorisation request is made within the allowed time frame.

(b) The maximum capacity and density of UAS flights in the U-space airspace (AMC1 to Article 3(4) of Regulation (EU) 2021/664) is not yet reached.

(c) The UAS registration number provided by the UAS operator can be retrieved and validated from the operator's information provided by the Member States as per Article 3(5) of Regulation (EU) 2021/664.

(d) When available, the UAS registration number can be retrieved and validated from the information provided by the Member States.

(e) The UAS flight is compatible with the U-space airspace restrictions and temporary airspace limitations.

(f) The UAS flight does not intersect with a prohibited (no-fly) geographical zone.

(g) The 4D trajectory of the UAS flight, with the deviation threshold (as specified for U-space airspace as per AMC2 to Article 3(4) of Regulation (EU) 2021/664) added, is free of any intersection with a previously authorised request.

The contingency/emergency measures detailed in the flight authorisation request are free of any intersection with a previously authorised request.

AMC2 Article 10(2)(a);(b) UAS flight authorisation service

UAS FLIGHT — ACCEPTANCE OF FLIGHT PLANNED IN RESTRICTED AREA

A UAS flight planned outside the boundaries of the U-space airspace or planned to enter a geographical zone with restricted access may be a UAS operator error. When a UAS flight is planned outside the boundaries of the U-space airspace or in a restricted access geographical zone, the USSP may accept the flight authorisation but should provide beforehand a clear notification to the UAS operator, and should list in the terms and conditions the related airspace restrictions, specific entry permissions and requirements.

Once the UAS operator confirms it has been granted the relevant permissions to perform its flight, the USSP should accept the flight authorisation request.

AMC1 Article 10(2)(c) UAS flight authorisation service

REASON FOR REJECTION OF A UAS FLIGHT AUTHORISATION

A USSP that rejects a UAS flight authorisation request should indicate the reason(s) for the rejection to the UAS operator concerned.

GM1 Article 10(2)(c) UAS flight authorisation service

UAS FLIGHT AUTHORISATION NOT ACCEPTED

(a) The reasons for which the USSP is unable to grant the authorisation should be detailed and clear enough to allow the UAS operator to properly understand the issue and adjust its flight authorisation request accordingly.

(b) As only warnings will be given regarding airspace access, the UAS operator remains responsible for acquiring any necessary access permission.

GM1 Article 10(2)(d) UAS flight authorisation service

DEVIATION THRESHOLDS

Due to the numerous parameters outside the area of responsibility of the USSPs which are required to establish safe and sensible deviation thresholds (e.g. acceptable level of safety (ALS), density of operations, necessary safety margins, etc.), the deviation thresholds are defined by the Member States during the risk assessment and specified as performance requirements as per the AMC and GM to Article 3(4) of Regulation (EU) 2021/664.

AMC1 Article 10(3) UAS flight authorisation service

WEATHER INFORMATION

The Member State may specify weather maxima or minima for important meteorological parameters as part of the U-space airspace operational conditions and constraints. When weather maxima or minima exist, the weather information service is required for the U-space airspace and the USSP should check the adequacy of the weather forecast with the specified weather maxima or minima when processing UAS flight authorisation and activation requests.

GM1 Article 10(3) UAS flight authorisation service

WEATHER INFORMATION

The USSP cross-checks the weather maxima and minima with the ‘mode of operation’ (point 2 of Annex IV) of the flight authorisation request, such as:

(a) visibility requirements for VLOS or BVLOS with aerial observers;

(b) wind and temperature for all operations.

GM1 Article 10(4) UAS flight authorisation service

UAS FLIGHT AUTHORISATION NOT ACCEPTED

USSPs may support the planning of an acceptable alternative in suggesting the start time or change of path.

AMC1 Article 10(5) UAS flight authorisation service

ACTIVATION OF THE UAS FLIGHT AUTHORISATION

The USSP should make a final check of the flight authorisation and should confirm the UAS flight authorisation activation without delay when the following conditions are satisfied:

(a) The UAS operator has accepted the terms and conditions associated to the flight authorisation.

(b) The UAS flight authorisation is activated within the allowed time frame, when specified.

(c) The U-space airspace is not subject to dynamic airspace reconfiguration, and the UAS flight remains compatible with the U-space airspace restrictions and temporary airspace limitations.

(d) The planned UAS flight is compatible with the current weather maxima or minima, when relevant.

(e) The UAS flight authorisation does not intersect with another UAS flight authorisation that has a higher priority (e.g. UAS conducting special operations).

(f) In the proximity of the UAS flight, there are no:

  (1) manned aircraft in a state of emergency;

  (2) cooperative but non-conforming drones, or non-cooperative drones (when their detection is possible);

  (3) e-conspicuous manned aircraft intersecting the planned UAS trajectory.

When the UAS flight authorisation cannot be activated, the USSP should indicate the reason(s) to the UAS operator and may propose an alternative.

GM1 Article 10(5) UAS flight authorisation service

ACTIVATION REQUEST

(a) It is acknowledged that depending on the implementation of the flight authorisation service and the situation in the U-space airspace, the flight authorisation may have been withdrawn. Nevertheless, a final consolidation and check of the accepted flight authorisation against the U-space airspace constraints, conditions, and environment is expected to be performed to ensure the safety of operations.

(b) The activation request is expected close to the start of the flight mentioned in the UAS flight authorisation.

(c) The activation of the flight authorisation triggers the provision of the network identification and traffic information services and, when applicable, the conformance monitoring service. The activation request should enable the provision of these services.

(d) When the USSP receives the activation request, it rechecks the flight authorisation request. If the flight authorisation request has been withdrawn because it has been found to be in conflict with a higher-priority flight authorisation request or a manned aircraft known or believed to be in a state of emergency, then the USSP should respond negatively to the activation request.

(e) If no activation request is received for a flight, the USSP should withdraw the flight authorisation after the time indicated in the flight authorisation request as the latest possible start time of the flight plus any deviation threshold with units of time. The USSP may warn the UAS operator before doing this.

GM2 Article 10(5) UAS flight authorisation service

ACTIVATION OF THE UAS FLIGHT AUTHORISATION

The minimum and maximum time (size of time window) before take-off at which the activation of the flight authorisation may have been identified by the Member Sate for specific U-space airspace. The USSP may further constrain the minimum and maximum time (size of time window) before take-off at which the activation is requested, due to practical considerations (e.g. efficient acceptance of flight authorisations among the UAS operators).

Those constraints are to be provided to the UAS operators in the terms and conditions of the UAS flight authorisation request.

GM3 Article 10(5) UAS flight authorisation service

UNJUSTIFIED DELAY

A possible interpretation of the expression ‘without unjustified delay’ is provided in ASTM F3548-21 ‘Standard Specification for UAS Service Supplier (USS) Interoperability’, which requires that the activation of flight authorisations be confirmed within 5 seconds for 95 % of the time.

AMC1 Article 10(6) UAS flight authorisation service

UAS FLIGHT AUTHORISATION EXCHANGE AND CONFLICTING REQUESTS

To prevent conflicting UAS flights, the USSP should:

(a) make the necessary arrangements with other USSPs to allow for the rapid, reliable, robust and unequivocal identification of conflicts between any UAS flight authorisation requests;

(b) ensure constant synchronisation of the flight authorisations within the U-space they share, in exchanging the UAS flight authorisation requests among themselves as well as stating changes to those requests — ‘Accepted’, ‘Activated’, ‘Withdrawn’, ‘Ended’.

GM1 Article 10(6) UAS flight authorisation service

ARRANGEMENTS IN CASE OF CONFLICTING UAS FLIGHT AUTHORISATION REQUESTS

(a) To ensure the interoperability of USSPs that provide flight authorisation services and resolve potential conflicts, USSPs may follow ASTM F3548-21 'Standard Specification for UAS Service Supplier (USS) Interoperability'.

(b) When duly demonstrated to the competent authority that the following mechanism can be safely implemented, if during operations any USSP fails entirely and cannot support strategic coordination, the arrangement among the USSPs may establish service levels and allow other USSPs to plan over accepted flights managed by the USSP that has failed. In that regard, the terms and conditions associated with the flight should incorporate provisions to deal with that specific case.

AMC1 Article 10(7) UAS flight authorisation service

AIRSPACE RESTRICTIONS AND LIMITATIONS

The USSP should:

(a) when authorising a flight request, use the set of current airspace restriction data coming from the CIS (and the associated geo-awareness service);

(b) check whether there are any entry permission or technical requirements due to any airspace restrictions relevant to the flight, taking into account the flight's 4D trajectory including any deviation thresholds;

(c) list the airspace restrictions as well as the specific entry permission and technical requirements in the terms and conditions provided with the flight authorisation request, if a flight authorisation requires specific entry permission or should meet specific technical requirements due to any airspace restrictions relevant to the flight and the USSP cannot determine from the information in the flight authorisation request whether these requirements are met.

GM1 Article 10(7) UAS flight authorisation service

AIRSPACE RESTRICTIONS AND LIMITATIONS

(a) When the acceptance of the flight authorisation only depends on the information contained in the flight authorisation request (Annex IV to Regulation (EU) 2021/664), or when an appropriate automatic means to request and obtain permission to enter restricted airspace is implemented for the U-space airspace, the USSP may automatically confirm the technical compliance and approve the flight authorisation request. Conversely, the same process could automatically determine technical non-compliance or the absence of entry permission, hence the USSP could automatically reject the flight authorisation request.

(b) For cases other than that referred to in point (a), there are currently no means in the flight authorisation request (Annex IV to Regulation (EU) 2021/664) for the UAS operator to indicate

that it has already obtained permission to enter any restricted airspace or that the aircraft is appropriately equipped. In these cases, the flight authorisation service should inform the UAS operator whether permission is required or whether there are specific requirements to be satisfied (e.g. technical equipments) by including the requirements in the terms and conditions of the flight authorisation request.

(c) In the case described in point (b), the UAS operator is responsible for obtaining the appropriate permission to enter any restricted airspace and/or for using an aircraft that meets any applicable technical requirements. By activating a flight authorisation, the UAS operator commits to meeting the terms and conditions of that flight authorisation request.

AMC1 Article 10(8) UAS flight authorisation service

SPECIAL OPERATIONS

For the purposes of this AMC, the term 'normal' is used for a UAS flight which does not conduct special operations.

(a) When an authorisation request for a UAS flight which conducts special operations conflicts with a previously authorised normal UAS flight, the USSP should update or withdraw the authorisation of the normal flight, as may be necessary by the circumstances, in order to authorise the flight which conducts special operations.

(b) The USSP should inform the UAS operator concerned about any change to the flight authorisation, as per Article 6(6) of Regulation (EU) 2021/664.

GM1 Article 10(8) UAS flight authorisation service

SPECIAL OPERATIONS

USSPs identify flight authorisation requests intended for special operations by the information given under 'type of flight' (special operations) of the UAS flight authorisation request (see point 3 of Annex IV to Regulation (EU) 2021/664).

AMC1 Article 10(9) UAS flight authorisation service

ORDER OF PROCESSING

(a) USSPs should reject any UAS flight authorisation request that conflicts with an earlier authorisation request of the same priority or higher, in accordance with Article 10(2)(b) of Regulation (EU) 2021/664.

(b) As far as practically possible (through the 'proper arrangements' that meet the requirement of Article 10(6) of Regulation (EU) 2021/664), USSPs should process UAS flight authorisations that have the same priority in the order of time at which the operational intent is submitted.

(c) As part of the recording required by AMC1 to Article 10(1) of Regulation (EU) 2021/664, USSPs should record the time of receipt of the UAS flight authorisation requests.

GM1 Article 10(9) UAS flight authorisation service

PRIORITY

(a) A new flight authorisation request cannot override a previously approved flight authorisation of the same priority. To reduce the number of cases where two conflicting flight authorisation requests arrive before the approval of either of them has finished, the time required to approve a flight authorisation request by means of 'proper arrangements' as per Article 10(6) of Regulation (EU) 2021/664 should be as short as practically possible. When two or more conflicting flight authorisation requests are received so close in time that their processing has not finished when the other(s) is (are) received, then there should be no systematic advantage to a given USSP or a given UAS operator.

The result should be one of the following:

(1) the first flight authorisation request received by any USSP is approved;

(2) neither/none flight authorisation request is approved;

(3) any one flight authorisation request at random is approved.

(b) It is not possible to change an already authorised flight so that it conflicts with another authorised flight of the same priority or higher. Any change causing a conflict will be rejected, and the original, unchanged flight authorisation should remain valid.

AMC1 Article 10(10) UAS flight authorisation service

CONTINUOUS CHECK OF FLIGHT AUTHORISATIONS IN RELATION TO THE PRESENCE OF MANNED AIRCRAFT

In airspace where the operation of manned aircraft not subject to air traffic control by the ANSP takes place, the USSP should consider the presence of electronically conspicuous manned aircraft and should:

(a) update or withdraw the flight authorisations, as may be necessary, if the manned aircraft is or is believed to be in a state of emergency;

(b) suggest to UAS operators the update of the flight authorisation when the manned aircraft trajectory intersects with the planned UAS 4D trajectory to enhance continued separation.

GM1 Article 10(10) UAS flight authorisation service

CONTINUOUS CHECK

(a) The checks should be performed from the moment the flight is authorised until the flight is no longer active (i.e. when the UAS operator signals the flight is no longer active).

(b) 'Continuous' checking is likely to be implemented as periodic checking. For an active UAS flight, the check should deliver relevant information as soon as practically possible, hence the checking should be performed at intervals similar to the time between the updates of the network

information service for a given flight. For a not-yet-active flight, the checking interval may be longer and at the time limit according to the time horizon published by the Member States for the validity and availability of geo-awareness data.

GM2 Article 10(10) UAS flight authorisation service

UPDATE OR WITHDRAWAL OF A FLIGHT AUTHORISATION

(a) USSPs may provide an updated, active UAS flight authorisation at the request of the UAS operator at any time provided that by doing so no new conflicts are produced. For example, a USSP may update a UAS flight authorisation at any point in space to assist in avoiding manoeuvres (e.g. holding or hovering) without the flight being considered non-conforming.

(b) When a USSP becomes aware that an existing flight authorisation is impacted by a new dynamic airspace restriction/limitation or that an existing flight authorisation is considered to be at risk from manned aircraft traffic due to information shared by the relevant air traffic service units, or information incoming from a (non-cooperative) drone detection system, then the USSP should either alert the UAS operator and provide it with an updated UAS flight authorisation to resolve the conflict or withdraw the existing UAS flight authorisation. The USSP should request the UAS operator to acknowledge any change in the UAS flight authorisation.

(c) Ending an active flight is a UAS operator action, and it is not expected to be automatically performed by the USSP. Ending an active flight terminates the provision of 'tactical' services, such as network identification, traffic information, and conformance monitoring services. The USSP should warn a UAS operator if it has not ended the flight and the time limit of the flight authorisation has passed.

(d) The USSP may withdraw a flight authorisation prior to flight activation.

AMC1 Article 10(11) UAS flight authorisation service

UNIQUE AUTHORISATION NUMBER

(a) When authorising a flight, the USSP should issue a flight authorisation number that is unique throughout the duration that the authorisation is expected to be referred to, including after flight. This period should be at least 2 years, and preferably more than 10 years.

(b) Each USSP should ensure that the probability of issuing an authorisation number that is the same with that issued by another USSP within the geographic scope of the U-space implementation is lower than once in 2 years and preferably lower than once in 10 years.

(c) USSPs should agree on, and ensure through dedicated arrangements, the robustness of the mechanism ensuring the uniqueness of flight authorisation numbers.

GM1 Article 10(11) UAS flight authorisation service

UNIQUE AUTHORISATION NUMBER

(a) The purpose of a unique authorisation number is to support the identification of a UAS operation during all its phases, including postflight. It provides an identifier for each UAS flight which is, as far as possible, unique across the U-space implementation and unique in a given time period, for at least 2 years and preferably for more than 10 years.

(b) The UAS operator should refer to the flight by its unique authorisation number in any subsequent communication with the USSP regarding that flight. It might include activation, ending, update, or cancellation. The USSP too should refer to the flight by its unique authorisation number in any communication with the UAS operator, for example in case of authorisation withdrawal.

(c) A Variant 1 Version 4 or Version 5 universally unique identifier (UUID) is considered a sufficiently unique flight authorisation number. In case Version 5 is used, the USSP should have a unique identifier and that identifier should be made known to the competent authority as part of the certification process of the USSP.

(d) Updates to a UAS flight authorisation should not result in a change to the unique authorisation number.

GM1 Article 11 Traffic information service

GENERAL

(a) The traffic information service provides information to UAS operators about other air traffic that is or may be present in close proximity to the position of their UAS and supports situational awareness.

(b) The traffic information service supports UAS operators in avoiding collisions with manned and unmanned traffic.

(c) The traffic information service supports concurrent access to U-space airspace for a large number of UAS by providing UAS operators with useful information for the safe and efficient conduct of their flights.

GM2 Article 11 Traffic information service

RESPONSIBILITY WITH REGARD TO THE PREVENTION OF MID-AIR COLLISION

(a) UAS operators are ultimately responsible for the safety of their flights, for meeting the U-space airspace operational constraints, and for ensuring separation or spacing from other manned and unmanned traffic.

(b) This responsibility cannot be transferred to USSPs nor to ANSPs. Neither is authorised to give instructions such as ‘climb’, ‘hold’, etc., to UAS operators; neither is charged with the responsibility to provide conflict resolution advisories, and neither is charged with the responsibility to separate unmanned aircraft from other traffic, other than the USSPs that provide flight authorisation services and ATC units that implement dynamic airspace reconfiguration.

(c) U-space services support the effective decision-making of UAS operators by providing as soon as possible the relevant traffic information to the relevant UAS operators while protecting the integrity and confidentiality of the data originating from manned or unmanned aircraft.

(d) Traffic information is not common information, and the exchange of traffic information does not involve the single CIS provider — except when ATSPs provide the relevant traffic information regarding manned aircraft in U-space airspace established in controlled airspace, as laid down in point ATS.OR.127 of Regulation (EU) 2017/373 amended by Regulation (EU) 2021/665.

AMC1 Article 11(1) Traffic information service

IDENTIFICATION IN REAL TIME

USSPs should:

(a) identify any known traffic in close proximity to the position or intended route of any active UAS flight under their responsibility, and provide in real time that information to the UAS operator; and

(b) report such traffic to the UAS operator in a timely manner.

GM1 Article 11(1) Traffic information service

OTHER CONSPICUOUS AIR TRAFFIC

From the point of view of a UAS operator, and in specific U-space airspace, other conspicuous air traffic comprises all flights under the control of other UAS operators that share the same U-space airspace and conspicuous manned traffic in the U-space airspace and in its vicinity.

GM2 Article 11(1) Traffic information service

PROXIMITY

Member States may support the definition of 'proximity' by specifying the associated 'surveillance volume' through the establishment of the relevant values (range, height) as part of the performance requirements established for each U-space airspace.

Regarding UAS traffic, a rectangular area with a diagonal of 7 km, may be used according to the value provided in ASTM F3411-22A. For manned traffic, it is recommended to use 3 times this value (i.e. 21 km).

AMC1 Article 11(2) Traffic information service

ELABORATION OF TRAFFIC INFORMATION

Traffic information is composite data that USSPs should elaborate from several sources:

(a) in controlled airspace, from the traffic information provided by the ATSP as per point ATS.OR.127 of Regulation (EU) 2017/373 amended by Regulation (EU) 2021/665, through the CIS or, when relevant, from the single CIS provider;

(b) from electronically conspicuous manned traffic, as specified in point SERA.6005(c) of Regulation (EU) No 932/2012, in airspace where manned aircraft operations are not subject to ATC;

(c) from complementary traffic information about uncontrolled manned aircraft;

(d) from the network identification service, providing the UAS remote identification, including the information from other USSPs;

(e) from other authoritative sources.

AMC2 Article 11(2) Traffic information service

RECEIPT OF TRAFFIC INFORMATION FROM UNCONTROLLED MANNED AIRCRAFT

USSPs that provide traffic information service in U-space airspace where the operation of manned aircraft not subject to ATC takes place should ensure they can acquire the e-conspicuous manned aircraft information through the means specified in AMC1 to point SERA.6005(c) of Regulation (EU) No 923/2012. The information may be acquired from external sources (e.g. other USSPs) or by privately owned means of receipt.

AMC3 Article 11(2) Traffic information service

USSP COMMON PROTOCOL — UNIQUENESS OF TRAFFIC INFORMATION

USSPs should adhere to a common protocol to ensure the uniqueness of traffic information and that it is delivered to each UAS operator exactly once.

AMC1 Article 11(3) Traffic information service

PERFORMANCE OF THE TRAFFIC INFORMATION DISTRIBUTION

USSPs should demonstrate a latency for distributing traffic information that is lower than 5 seconds for at least 99 % of the time.

GM1 Article 11(2) Traffic information service

COMPLEMENTARY RECEIPT OF TRAFFIC INFORMATION FROM UNCONTROLLED MANNED AIRCRAFT

As per the result of the airspace risk assessment referred to in Article 3(1) of Regulation (EU) 2021/664, the need for deployment of additional ground infrastructure, in accordance with AMC1 to point SERA.6005(c) of Regulation (EU) No 923/2012, necessary for the continuous receipt of information from manned aircraft that make themselves electronically conspicuous, may be exceptionally alleviated.

GM2 Article 11(2) Traffic information service

FLOW OF TRAFFIC INFORMATION

Traffic information is originally generated on board manned or unmanned aircraft by systems that compute, for example, own time, position and speed of the aircraft.

(a) Operators of unmanned aircraft in U-space airspace provide traffic information to USSPs by means of network identification service.

(b) Operators of manned aircraft not subject to ATC in U-space airspace provide traffic information to USSPs in accordance with point SERA.6005(c) of Regulation (EU) No 923/2012.

(c) Inside controlled airspace, ATSPs provide traffic information on manned aircraft to USSPs.

(d) USSPs share traffic information among themselves and with UAS operators.

(e) There is no direct flow of traffic information from USSPs to operators of manned aircraft.

GM1 Article 12 Weather information service

GENERAL

(a) The USSP collects the weather information necessary to support UAS operational decisions in a specific U-space airspace and supports the provision of other U-space services, such as the UAS flight authorisation service.

(b) It is recognised that the weather information service intended for UAS operations is different from that provided by today's meteorological service providers, especially when it comes to UAS operations in the 'open' and 'specific' category. UAS may fly near buildings and in areas where current aeronautical meteorological information is not always provided. Therefore, Article 12 of Regulation (EU) 2021/664 specifies the minimum content of weather information to be available for the purpose of UAS operations. It does not exclude the possibility that current aeronautical meteorological service providers may also provide this service.

AMC1 Article 12(1)(a) Weather information service

TRUSTED SOURCES

(a) USSPs should use weather data that comes from authoritative sources.

(b) Where such weather data is not formally available from an authoritative source, but is required by end users, USSPs should use weather data from other (non-authoritative) sources, provided they have been verified and validated by the USSP to conform with the data quality requirements.

(c) USSPs should enable the identification of the source of the weather data in accordance with the contractual arrangements concluded with their UAS operators.

GM1 Article 12(1)(a) Weather information service

TRUSTED SOURCES

(a) An authoritative source may be an organisation that is formally recognised by the Member State to originate and/or publish weather information which meets the data quality requirements as specified by that Member State. An authoritative source may be a meteorological service provider certified in accordance with Regulation (EU) 2017/373.

(b) A non-authoritative source may be an organisation other than that defined in point (a), but which originates and/or publishes weather data derived through data gathering or measuring (e.g. by the USSPs themselves, aircraft operators, or other relevant weather information organisations, or a combination of them), which conforms with the data quality requirements as specified by the Member State.

AMC1 Article 12(2)(f) Weather information service

WEATHER INFORMATION

USSPs should provide weather information that contains:

(a) the location of the observation or forecast using:

(1) the ICAO designator, where available; or

(2) the geographic position expressed in the WGS 84 coordinate;

(b) the validity of the observation or forecast by specifying:

(1) the validity area/volume either via the ICAO designator and, where available, the WGS 84 position or WGS 84 area of validity; and

(2) the time of the observation and/or the validity of the forecast in UTC time.

GM1 Article 12(2)(f) Weather information service

WEATHER REPORTS

Article 12(2) of Regulation (EU) 2021/664 defines the minimum weather information set to be provided by the USSP. In certain cases, USSPs may either display a subset of, or enrich, this weather data set (or additional sources of information) to:

(a) provide the information to the end user for awareness;

(b) complete the weather data set with weather information that is publicly available, such as MET information.

AMC1 Article 12(3) Weather information service

UP-TO-DATE INFORMATION

(a) Upon receipt of updated weather information related to current weather, the USSP should provide it to the UAS operator within maximum 30 seconds.

(b) Upon receipt of an updated weather forecast, the USSP should provide it to the UAS operator within maximum 5 minutes from the time the USSP starts processing the data.

(c) The USSP should inform the end user when the information is not up to date.

RELIABILITY

(d) The USSP should inform the end user of the source of the data at the request of the UAS operator.

(e) The USSP should provide a confidence level of the data being provided, where available, or indicate that the confidence level is unknown.

GM1 Article 12(3) Weather information service

UP-TO-DATE INFORMATION

(a) It is the responsibility of the USSP to ensure that the data being consumed or referred to is the last available data set from the trusted source.

(b) The USSP is not responsible for ensuring that the data being exposed by the trusted source is effectively the last available data. This responsibility lies with the trusted source.

RELIABILITY

(c) The reliability of the data pertains mostly to the security, availability, and status reporting to the end user. USSPs should ensure that the UAS operator is presented with accurate information that has not been tampered with, and with information regarding the confidence level of the data where this is available at the source.

(d) When MET data is provided using the standard MET products (such as METAR or aerodrome local report), the confidence levels are contained within the MET standards that define these products, as specified in ICAO Annex 3 'Meteorological Service for International Air Navigation'.

GM1 Article 13 Conformance monitoring service

GENERAL

(a) Article 13 of Regulation (EU) 2021/664 contains a general description of the objective of the conformance monitoring service, as well as the requirements for the USSPs that provide such service. This service checks the current in-flight information of each UAS with respect to the actual progress of the UAS flight as reported by the UAS operator or obtained from the remote identification service. The monitoring is performed per UAS flight.

(b) When any non-conformance of the UAS flight is detected, the USSP alerts:

(1) the UAS operator of the flight for which the non-conformance is detected;

(2) other air traffic,

(3) other USSPs;

(4) the single CIS provider, where applicable; or

(5) other relevant authorities.

(c) The USSP that detects a non-conformance should:

(1) add the information on deviation in the traffic information message if an unmanned aircraft is non-compliant;

(2) alert the UAS operators whose unmanned aircraft fail to comply with their planned operation; and

(3) monitor all current flight operations of their subscribed UAS operators; all USSPs have collective responsibility to dispatch relevant information to the UAS operators concerned.

GM2 Article 13 Conformance monitoring service

NON-CONFORMANCE — EXAMPLES

A non-conformance may occur when a UAS flight does not comply:

(a) with any of the operational conditions or airspace constraints referred to in Article 3(4)(c) of Regulation (EU) 2021/664;

(b) with any of the terms or conditions of its flight authorisation in accordance with Article 10(1) of Regulation (EU) 2021/664;

(c) with any of the deviation thresholds of its flight authorisation in accordance with Article 10(2)(d) of Regulation (EU) 2021/664.

AMC1 Article 13(1) Conformance monitoring service

DETERMINATION OF CONFORMANCE

The USSP should perform the following sequence:

(a) match the unmanned aircraft with a corresponding flight authorisation(s);

(b) determine whether the unmanned aircraft is subject to an accepted and activated flight authorisation;

(c) determine whether the unmanned aircraft complies with the deviation thresholds of the flight authorisation;

(d) when possible, determine whether the unmanned aircraft complies with the requirements laid down in Article 6(1) of Regulation (EU) 2021/664, and the terms and conditions of the UAS flight authorisation;

When the UAS is detected to be non-conformant, the USSP should provide the details of the non-conformance in the alert.

AMC2 Article 13(1) Conformance monitoring service

NON-CONFORMANCE WITH THE DEVIATION THRESHOLDS

The USSP should consolidate the deviation with the flight authorisation, and should confirm the non-conformance, when the UAS is outside the authorised 4D volume, including the deviation thresholds, for more than 5 % of the time as validated over time.

AMC3 Article 13(1) Conformance monitoring service

NON-CONFORMANCE WITH THE FLIGH ACTIVATION/DEACTIVATION

The USSP should detect a non-conformance when a UAS flight:

(a) is performed without flight authorisation or proper flight activation (i.e. accepted by the USSP);

(b) has not ended, and the time limit of the flight authorisation has passed.

AMC4 Article 13(1) Conformance monitoring service

PERFORMANCE OF THE NON-CONFORMANCE ALERTING

To ensure safety of operations through the timely reaction of UAS operators, the USSP should alert UAS operators within 5 seconds, for 99 % of the time, when a non-conformance is detected.

GM1 Article 13(1) Conformance monitoring service

PRELIMINARY ALERT TO THE INFRINGEMENT OF THE 4D VOLUME

When the UAS flight approaches the boundaries of the authorised 4D volume, a preliminary alert may be generated by the USSP to raise awareness of the UAS operator about the potential for infringement and non-conformance.

GM2 Article 13(1) Conformance monitoring service

NON-CONFORMANCE WITH THE FLIGH ACTIVATION/DEACTIVATION

A flight which remains airborne after the time limit of its flight authorisation has passed may no longer be conflict free, and poses a hazard to other flights which conform with their flight authorisations. Therefore, a flight which has not ended by the time its flight authorisation time limit has passed is non-conformant.

GM3 Article 13(1) Conformance monitoring service

NON-CONFORMANCE NOTIFICATION

The aim of the non-conformance notification is to provide information with regard to the specific position of the unmanned aircraft at the time it became non-conformant with respect to its flight authorisation. The information about a non-conformant unmanned aircraft comprises the time, the position, and the number of non-conformant occurrences, each with an indication of deviation when possible.

AMC1 Article 13(2) Conformance monitoring service

ALERTS TO THE AIR TRAFFIC CONTROL UNIT

The USSP should issue a non-conformance alert to the relevant ATC unit when a non-conformant unmanned aircraft is likely to represent a threat to manned aircraft in controlled airspace, i.e. the unmanned aircraft exits the U-space airspace, or enters an area where the implementation of an airspace restriction or a dynamic reconfiguration is in progress.

GM1 Article 14 Application for a certificate

GENERAL

(a) The provision of U-space services and single CIS is subject to certification by the relevant competent authority.

(b) The competent authority may be:

(1) the national competent authority of the Member States where the USSPs and, when designated, the single CIS providers have their principal place of business;

(2) the Agency for USSPs and single CIS providers from third countries;

(3) the Agency, at the request of the USSPs or the single CIS providers that provide services in more than one Member State, following a coordination process described in Article 64 (at the request of the organisation) or Article 65 (at the request of the national competent authority) of Regulation (EU) 2018/1139.

(c) The certification scheme aims to preserve public interest, most notably in terms of safety. The certificate confirms that the single CIS provider or the USSP meets the requirements of Regulation (EU) 2021/664 as regards the provision of specific U-space services in the U-space airspace, commensurate with the risk associated with the U-space services they provide. The certificate specifies the rights and obligations of the single CIS provider or the USSP, with particular regard to safety.

(d) Annexes VI and VII to Regulation (EU) 2021/664 establish the certificate form templates for the USSP and the single CIS provider respectively. By introducing this single certificate concept, all the privileges of a USSP are to be mentioned in the attachment to the certificate specifying the type of U-space services, and the respective conditions and associated limitations. For the CIS provider, the certificate form does not include an attachment specifying the type of U-space services, conditions and limitations of the certificate because the CIS provider should always provide the required CIS in the U-space airspace for which the CIS provider has been designated.

GM1 Article 14(3) Application for a certificate

OPERATIONAL CONDITIONS AND LIMITATIONS IN THE USSP CERTIFICATE

(a) The ‘Limitations’ section of the certificate may be used to identify the restrictions to be applied in the provision of services and any other particularity of the service(s) provided (e.g. intended usage, type of operations).

(b) Limitations may also relate to some restrictions on the service(s) provided associated with non-compliances with respect to some performance requirements.

(c) The ‘Conditions’ may address actions that require to be accomplished to confirm the validity of the certificate.

(d) The certificate captures the specification of 'services', including the relevant performance requirements addressed in AMC2 to Article 3(4) of Regulation (EU) 2021/664, demonstrated to the competent authority.

GM1 Article 14(6) Application for a certificate

APPLICATION FORM — TEMPLATE

Competent authorities may wish to consider using the following application form template, for the purpose of facilitating the harmonised implementation of Regulation (EU) 2021/664.

Applicant details		
(a)	Legal name of the applicant	
(b)	Name of the USSP or the single CIS provider	
(c)	Address of registry	
(d)	Principal place of business	
(e)	Telephone number	
(f)	Email	
Reason for application		
1.	Initial issue	
2.	Renewal	
Declaration		
(a)	Full name of the accountable manager	
(b)	Signature of the accountable manager	
(c)	Date of application	

GM1 Article 15 Conditions for obtaining a certificate

GENERAL

(a) Article 15 of Regulation (EU) 2021/664 contains the conditions for obtaining a certificate. They are inspired from the requirements that apply for ATM/ANS providers (i.e. those contained in Subpart B of Annex III to Regulation (EU) 2017/373) to obtain and maintain their respective certificates, but tailored to the particularities of the U-space.

(b) USSPs and single CIS providers are organisations that directly contribute to safe UAS operations within the U-space airspace, and it is important that they have a risk-based management system in place. It is, therefore, essential that they comply with an appropriate management system established for that purpose. To apply this management system, taking into account the different types of providers and the performance of the services they provide, Regulation (EU) 2021/664 lays down some management system requirements. The elements of this management system are, therefore, harmonised for all the different types of single CIS providers or USSPs, but their application may be different depending on the different services provided, especially for the USSPs. Therefore, the proposed management system provides for a proportionate application of the requirements for both providers.

(c) USSPs and single CIS providers are also required to implement a security management system based on the requirements laid down in point ATM/ANS.OR.D.010 of Subpart D of Annex III to Regulation (EU) 2017/373. It has to be noted that Opinion No 03/2021 'Management of information security risks'[15] proposes amendments, among others, to Subpart D of Annex III to Regulation (EU) 2017/373, which will become applicable to USSPs and single CIS providers once the related regulation is published.

(d) To become a certified USSP, the applicant should demonstrate its capability to provide at least the four mandatory U-space services referred to in Article 3(2) of Regulation (EU) 2021/664. Whenever required by a Member State as per Article 3(3) of Regulation (EU) 2021/664, the applicant should also demonstrate its capability to provide the additional U-space services.

(e) Once an applicant becomes a certified USSP, it may provide services in any U-space airspace across the European Union. However, before the USSP starts providing services, the competent authority of the U-space airspace where the provision of services is intended to take place may need to validate that the USSP satisfies the local conditions (e.g. performance requirements and constraints).

[15] https://www.easa.europa.eu/en/document-library/opinions/opinion-032021

AMC1 Article 15(1) Conditions for obtaining a certificate

SAFETY SUPPORT ASSESSMENT

The applicant should provide the assurance with sufficient confidence that the provision of services that support the conduct of UAS operations will comply with the required level of performance and constraints via a complete, documented and valid argument that the services will be provided and will continue to be provided only as specified in the specified context. The safety support assessment undertaken by the applicant should encompass any contracted activities or specific arrangements.

For that purpose, the applicant should define its 'functional systems', 'specification of services' and 'safety support requirements'.

AMC2 Article 15(1) Conditions for obtaining a certificate

VERIFICATION OF THE SAFETY SUPPORT ASSESSMENT PROCESS

The applicant should ensure that the verification activities as regards the safety support assessment process ensure the completeness and correctness of the argument and include the verification that:

(a) the risk analysis is complete;

(b) the safety criteria are correct and commensurate with the risk analysis;

(c) all the elements of the 'functional system' or environment of operation are identified;

(d) the specification of the operational context is complete and correct;

(e) that the specification of the way the service behaves is complete and correct;

(f) the specification is analysed in the context in which the services are intended to be provided;

(g) the 'safety support requirements' are correct and complete in relation to the specification;

(h) the design is complete and correct with reference to the 'specification of services' and 'safety support requirements', and correctly addresses the safety criteria;

(i) the design is the one analysed;

(j) the implementation, to the intended degree of confidence, corresponds to the design analysed and behaves only as specified in the given operational context; and

(k) the way the service behaves complies with and does not contradict other applicable requirements.

AMC3 Article 15(1) Conditions for obtaining a certificate

CONCEPT OF OPERATIONS (CONOPS)

The applicant should develop its concept of operations, which is meant to:

(a) increase the competent authority's understanding of the applicant's use case;

(b) define the scope of the functional system submitted for certification;

(c) establish the depth and boundaries of the certification, and ultimately the scope of the certificate;

(d) capture the assumptions on the U-space performance requirements to be satisfied as per Article 3(4) of Regulation (EU) 2021/664.

AMC4 Article 15(1) Conditions for obtaining a certificate

COMPLIANCE MATRIX

The applicant should develop a compliance matrix for the competent authority to ensure the soundness and completeness of the compliance demonstration. The compliance matrix should:

(a) cover all the layers of items to be satisfied (i.e. requirements of Regulation (EU) 2021/664, the related AMC and GM, and applicable industry standards);

(b) capture how each item is intended to be satisfied;

(c) link each item with supporting evidence (e.g. documents, tests, engineering documents).

AMC5 Article 15(1) Conditions for obtaining a certificate

INFORMATION THAT SUPPORTS CERTIFICATION

The applicant should provide all necessary information to the competent authority during the certification activities, especially in presenting its strategy for the purpose of certification and seeking agreement on the scope and depth of the assessment of the certification. The applicant should develop evidence, and make it available to the competent authority for investigation, which demonstrates that its 'functional system' allows for the safe provision of the services.

Additionally, the applicant should report to the competent authority any deficiencies (including those related to information security) and/or errors identified in the functional system, especially those that could lead to an unsafe condition. Such reports should be made in a form and manner acceptable to the competent authority.

GM1 Article 15(1) Conditions for obtaining a certificate

CORRELATION BETWEEN REGULATION (EU) 2017/373 AND THE AMC AND GM TO REGULATION (EU) 2021/664

Subpart B, and some requirements in Subpart A and D of Annex III to Regulation (EU) 2017/373 are also applicable to USSPs and single CIS providers by virtue of the specific applicability references made in Article 15 of Regulation (EU) 2021/664. However, the AMC and GM to Regulation (EU) 2017/373 are naturally not addressed to USSPs or to single CIS providers and are, therefore, not applicable to them to.

To facilitate the reading and implementation of the relevant requirements, the following table contains the correlation between the applicable requirements of Subparts A, B and D of Annex III to Regulation (EU) 2017/373 and the AMC and GM to Article 15 of Regulation (EU) 2021/664. In this context, the table below contains the acceptable means of compliance and guidance material for USSPs and single CIS providers to ensure compliance with the listed requirements of Regulation (EU) 2017/373. For the applicable requirements in Subparts A, B and D of Annex III to Regulation (EU) 2017/373, listed in the table below, for which no AMC and GM are provided, USSPs and single CIS providers may propose their own means to comply with the applicable requirements.

Requirement in Annex III to Regulation (EU) 2017/373	**AMC and GM to Article 15(1) of Regulation (EU) 2021/664**
ATM/ANS.OR.A.065	AMC1 Article 15(1)(d) Conditions for obtaining a certificate OCCURRENCE REPORTING
ATM/ANS.OR.A.065	GM3 Article 15(1) Conditions for obtaining a certificate 'UNSAFE CONDITION' IN THE U-SPACE
ATM/ANS.OR.B.001	AMC1 Article 15(1)(e) Conditions for obtaining a certificate MANAGEMENT SYSTEM — TECHNICAL AND OPERATIONAL CAPACITY
ATM/ANS.OR.B.001	AMC2 Article 15(1)(e) Conditions for obtaining a certificate MANAGEMENT SYSTEM — ISO
ATM/ANS.OR.B.001	GM1 Article 15(1)(e) Conditions for obtaining a certificate MANAGEMENT SYSTEM — ISO
ATM/ANS.OR.B.005(a)(1)	AMC3 Article 15(1)(e) Conditions for obtaining a certificate MANAGEMENT SYSTEM — RESPONSIBILITIES AND ACCOUNTABILITIES
ATM/ANS.OR.B.005(a)(2)	AMC4 Article 15(1)(e) Conditions for obtaining a certificate MANAGEMENT SYSTEM — POLICY

Requirement in Annex III to Regulation (EU) 2017/373	AMC and GM to Article 15(1) of Regulation (EU) 2021/664
ATM/ANS.OR.B.005(a)(3)	AMC5 Article 15(1)(e) Conditions for obtaining a certificate MANAGEMENT SYSTEM — SAFETY PERFORMANCE MONITORING AND MEASUREMENT
ATM/ANS.OR.B.005(a)(3)	AMC6 Article 15(1)(e) Conditions for obtaining a certificate MANAGEMENT SYSTEM — SAFETY ASSESSMENT (OF THE APPLICANT'S SYSTEM)
ATM/ANS.OR.B.005(a)(3)	GM2 Article 15(1)(e) Conditions for obtaining a certificate MANAGEMENT SYSTEM — SAFETY PERFORMANCE MONITORING AND MEASUREMENT
ATM/ANS.OR.B.005(a)(3)	GM3 Article 15(1)(e) Conditions for obtaining a certificate MANAGEMENT SYSTEM — SAFETY ASSESSMENT
ATM/ANS.OR.B.005(a)(4)	AMC7 Article 15(1)(e) Conditions for obtaining a certificate MANAGEMENT SYSTEM — ASSESSMENT OF THE MANAGEMENT SYSTEM
ATM/ANS.OR.B.005(a)(5)	AMC7 Article 15(1)(e) Conditions for obtaining a certificate MANAGEMENT SYSTEM — TRAINING AND COMPETENCY OF PERSONNEL
ATM/ANS.OR.B.005(a)(6)	AMC8 Article 15(1)(e) Conditions for obtaining a certificate MANAGEMENT SYSTEM — TRAINING AND COMPETENCY OF PERSONNEL
ATM/ANS.OR.B.005(a)(7)	AMC9 Article 15(1)(e) Conditions for obtaining a certificate MANAGEMENT SYSTEM — COMMUNICATION RESPONSIBILITIES
ATM/ANS.OR.B.005(b)	AMC10 Article 15(1)(e) Conditions for obtaining a certificate MANAGEMENT SYSTEM — DOCUMENTATION
ATM/ANS.OR.B.005(c)	AMC11 Article 15(1)(e) Conditions for obtaining a certificate MANAGEMENT SYSTEM — COMPLIANCE MONITORING
ATM/ANS.OR.B.005(c)	GM4 Article 15(1)(e) Conditions for obtaining a certificate MANAGEMENT SYSTEM — COMPLIANCE MONITORING

Requirement in Annex III to Regulation (EU) 2017/373	AMC and GM to Article 15(1) of Regulation (EU) 2021/664
ATM/ANS.OR.B.010	GM3 Article 15(1) Conditions for obtaining a certificate 'UNSAFE CONDITION' IN THE CONTEXT OF THE U-SPACE
ATM/ANS.OR.B.010	GM4 Article 15(1) Conditions for obtaining a certificate 'FUNCTIONAL SYSTEM' IN THE CONTEXT OF THE U-SPACE
ATM/ANS.OR.B.010	AMC1 Article 15(1) Conditions for obtaining a certificate SAFETY SUPPORT ASSESSMENT
ATM/ANS.OR.B.010	AMC2 Article 15(1) Conditions for obtaining a certificate VERIFICATION OF THE SAFETY SUPPORT ASSESSMENT PROCESS
ATM/ANS.OR.B.010	AMC3 Article 15(1) Conditions for obtaining a certificate CONCEPT OF OPERATIONS (CONOPS)
ATM/ANS.OR.B.010	GM5 Article 15(1) Conditions for obtaining a certificate SAFETY SUPPORT REQUIREMENTS
ATM/ANS.OR.B.010	GM6 Article 15(1) Conditions for obtaining a certificate SPECIFICATION OF SERVICES
ATM/ANS.OR.B.010	GM8 Article 15(1) Conditions for obtaining a certificate CONTENT OF THE CONOPS
ATM/ANS.OR.B.010	AMC1 Article 15(1)(b) Conditions for obtaining a certificate SOFTWARE ASSURANCE
ATM/ANS.OR.B.010	GM1 Article 15(1)(b) Conditions for obtaining a certificate SOFTWARE ASSURANCE — SOFTWARE ASSURANCE PROCESSES
ATM/ANS.OR.B.010	AMC12 Article 15(1)(e) Conditions for obtaining a certificate MANAGEMENT SYSTEM — FUNCTIONAL CHANGE MANAGEMENT PROCEDURE
ATM/ANS.OR.B.010	AMC13 Article 15(1)(e) Conditions for obtaining a certificate MANAGEMENT SYSTEM — CHANGE MANAGEMENT PROCEDURE
ATM/ANS.OR.B.010(a)	AMC4 Article 15(1) Conditions for obtaining a certificate COMPLIANCE MATRIX
ATM/ANS.OR.B.010(a)	GM9 Article 15(1) Conditions for obtaining a certificate COMPLIANCE MATRIX

Requirement in Annex III to Regulation (EU) 2017/373	AMC and GM to Article 15(1) of Regulation (EU) 2021/664
ATM/ANS.OR.B.015	AMC14 Article 15(1)(e) Conditions for obtaining a certificate MANAGEMENT SYSTEM — CONTRACTED ACTIVITIES
ATM/ANS.OR.B.015	GM5 Article 15(1)(e) Conditions for obtaining a certificate MANAGEMENT SYSTEM — CONTRACTED ACTIVITIES
ATM/ANS.OR.B.030	AMC15 Article 15(1)(e) Conditions for obtaining a certificate MANAGEMENT SYSTEM — RECORD-KEEPING — GENERAL
ATM/ANS.OR.B.035	AMC16 Article 15(1)(e) Conditions for obtaining a certificate MANAGEMENT SYSTEM — OPERATIONS MANUAL
ATM/ANS.OR.B.035	GM6 Article 15(1)(e) Conditions for obtaining a certificate MANAGEMENT SYSTEM — OPERATIONS MANUAL
ATM/ANS.OR.D.010	GM1 Article 15(1)(f) Conditions for obtaining a certificate SECURITY MANAGEMENT SYSTEM
ATM/ANS.OR.D.010	GM2 Article 15(1)(f) Conditions for obtaining a certificate INFORMATION SECURITY THREAT

GM2 Article 15(1) Conditions for obtaining a certificate

'APPLICANT' IN THE CONTEXT OF THE U-SPACE

For the purposes of Articles 14 and 15 of Regulation (EU) 2021/664, 'applicant' means the USSP or the designated single CIS provider that seeks the obtention and approval of a certificate as per Article 14 of Regulation (EU) 2021/664.

GM3 Article 15(1) Conditions for obtaining a certificate

'UNSAFE CONDITION' IN THE CONTEXT OF THE U-SPACE

For the purposes of Regulation (EU) 2021/664, 'unsafe condition' may be considered a situation which, due to data error or data alteration (e.g. in case of malicious interactions), a procedure error, or a system excessive response time or malfunction may result (but is not limited) in the following:

(a) insufficient separation/spacing, or air proximity between manned and unmanned aircraft within the U-space airspace, which may result in mid-air collision;

(b) a lack of separation between unmanned aircraft, which may result in mid-air collision leading to an increase of the ground risk;

(c) an unmanned aircraft exiting the boundaries of the U-space airspace;

(d) an unmanned aircraft entering a prohibited (no-fly zone) or a restricted access geographical zone (as per Article 15 of Regulation (EU) 2022/947), which could be established within the U-space airspace.

GM4 Article 15(1) Conditions for obtaining a certificate

'FUNCTIONAL SYSTEM' IN THE CONTEXT OF THE U-SPACE

For the purposes of Regulation (EU) 2021/664, 'functional system' means a combination of procedures, human resources and equipment, including hardware and software, organised to provide services within the context of the U-space airspace.

GM5 Article 15(1) Conditions for obtaining a certificate

SAFETY SUPPORT REQUIREMENTS

Safety support requirements are the characteristics/items of the functional system to ensure that the service performs as specified. The following non-exhaustive list contains examples of safety support requirements that specify:

(a) for software (and equipment), the complete behaviour in terms of functions, accuracy, timing, order, format, capacity, resource usage, robustness to abnormal conditions, overload tolerance, availability, reliability, confidence and integrity;

(b) for people, their performance in terms of tasks (e.g. accuracy, response times, acceptable workload, resilience to distraction, self-awareness, team-player capacity, adaptability, reliability, confidence, skills, and knowledge in relation to their tasks);

(c) for procedures, the circumstances for their enforcement, the resources needed to perform them (i.e. people and equipment), the sequence of actions to be performed, and the timing and accuracy of the actions; and

(d) interactions between all parts of the system.

GM6 Article 15(1) Conditions for obtaining a certificate

SPECIFICATION OF SERVICES

As per the AMC and GM to Article 3 of Regulation (EU) 2021/664, the acceptable level of safety (ALS) is determined during the airspace risk assessment and materialised upon the U-space airspace definition and the related performance requirements and constraints. These 'high-level design characteristics' of the functional system, complemented with those derived from the applicant's safety assessment form the 'specification of services', which is the baseline applicants should use for their safety support assessments alongside the 'safety support requirements'.

In the absence of established U-space performance requirements and constraints, as per the AMC and GM to Article 3 of Regulation (EU) 2021/664, the applicant should make reasonable assumptions to define a suitable set of performance requirements.

The applicant should demonstrate to the competent authority that the specification is complete and correct with regard to its concept of operations (CONOPS) and safety assessment.

GM7 Article 15(1) Conditions for obtaining a certificate

CERTIFICATION DATA AND EVIDENCE

The data and evidence that support the applicant's certification cover both procedural and technical aspects, and encompass the following items:

(a) concept of operations (CONOPS);

(b) compliance matrix with Regulation (EU) 2021/664, the related AMC and GM, and applicable industry standards;

(c) description of the engineering processes and procedures (e.g. software assurance);

(d) engineering and design documentation;

(e) safety assessment;

(f) security risk assessment;

(g) operational procedures and instructions to other dependent stakeholders (e.g. USSPs, UAS operators);

(h) analyses and tests;

(i) records (e.g. review, configuration and changes, statement of works, quality, etc.);

(j) residual defects and limitations.

Given that certification is a dynamic process, other items may be considered necessary to be documented during the certification activities.

GM8 Article 15(1) Conditions for obtaining a certificate

CONCEPT OF OPERATIONS (CONOPS) — CONTENT

The content of the CONOPS should be agreed with the competent authority, and may cover the following:

(a) For the USSP and the single CIS provider:

(1) description of the applicant's business case;

(2) when known, description of the U-space environment where the service(s) is (are) intended to be provided (e.g. identification of the stakeholders);

(3) whether the provision of services is intended in controlled and/or uncontrolled airspace and/or in airspace where both controlled and uncontrolled manned aircraft operations take place;

(4) description of the infrastructure, and how the availability/continuity of the provision of the service(s) is satisfied;

(5) operational capacity (e.g. number of simultaneous operations supported, growth potential/scalability);

(6) specific arrangements (e.g. service acquired from a third party, or through subcontracted activities);

(7) a description of each of the services provided by the applicant, and the operational functions and design principles that drive the implementation of the services delivered to U-space airspace actors;

(8) description of the applicant's 'functional system';

(9) if any, the targeted level of integrity or reliability of the functional systems;

(10) the technical measures regarding cybersecurity (e.g. authentication means, encryption);

(11) when relevant, description of previous certification/approval experience;

(12) declaration of any additional features which are not required to comply with Regulation (EU) 2021/664 (and thus outside the scope of the certification);

(13) the assumptions on the U-space performance requirements addressed in the AMC and GM to Article 3(4) of Regulation (EU) 2021/664;

(14) any other considerations that may help the competent authority to gain a good understanding of the applicant's use case.

(b) For the single CIS provider:

(1) the type of information collected from the CIS, and from which organisation;

(2) interfaces with USSPs, ATSPs and other relevant entities that are entitled to provide information through the CIS;

(3) a description of the service and information provided to the USSPs.

(c) For the USSP:

(1) whether the provision of services is intended in centralised and/or decentralised CIS;

(2) how the information is intended to be exchanged with other USSPs and, when relevant, with the CIS;

(3) the U-space services provided as per Article 3(2) and (3) of Regulation (EU) 2021/664;

(4) the type of supported operations, such as VLOS/BVLOS, over congested environment;

(5) how the services are intended to be delivered to UAS operators (e.g. API or HMI);

(6) the operational limits of their system, e.g. range, altitude, etc.;

(7) the solution implemented to receive the UAS remote identification.

GM9 Article 15(1) Conditions for obtaining a certificate

COMPLIANCE MATRIX

The applicant is free to select the way of packaging the evidence that supports compliance. The development of the compliance matrix may also be an iterative process, as the evidence may not be fully available or characterised at an initial version of the compliance matrix, and several versions of the compliance matrix may be delivered during the initial certification process and subsequently updated during the continued oversight process.

However, even at an initial version of the compliance matrix, the early identification of the documents that support compliance remains necessary in order to provide an overview of the compliance approach.

GM10 Article 15(1) Conditions for obtaining a certificate

APPROACH TO CERTIFICATION

Based on the presentation of the applicant's CONOPS, strategy for certification, and the associated set of data and evidence, the competent authority defines the scope and depth of the certification investigations and selects the documents, set of data, and activities (e.g. onboarding process, software development, tests, change management procedures, etc.) to be assessed.

The competent authority's investigation comprises two main types of investigation:

(a) Desktop reviews: mostly dedicated to documentation reviews performed remotely, without visiting the applicant's facilities.

(b) Audits: to perform an in-depth and comprehensive assessment/inspection of the applicant's organisation, activities, processes, and evidence. Depending on whether or not a physical inspection is necessary, audits may be performed on-site or remotely considering, for example, the efficiency of the access and the assessment of the items subject to investigation, and access to personnel in charge of the applicant's activities.

AMC1 Article 15(1)(b) Conditions for obtaining a certificate

SOFTWARE ASSURANCE

The applicant should ensure that a documented software assurance process is established to produce evidence and arguments that demonstrate that the provision of services satisfies the required U-space performance requirements.

Accordingly, the applicant should control the development of its software and follow a structured process, including planned and systematic activities (procedures), to substantiate with sufficient confidence that:

(a) development errors (e.g. mistakes made in the determination, design or implementation of the requirements) have been identified, corrected or mitigated, and that the potential residual defects in the implementation are minimised;

(b) the software behaves as intended in the specified context.

When relevant, the applicant should also demonstrate that the implementation of potential additional features, except those required for ensuring the safe provision of services, do not interfere with the safe provision of the required services.

When software assurance relies on credit taken from simulated environments and/or automated activities (e.g. automated verification) the applicant should:

(a) identify the scope and the credit taken from those activities and substantiate their relevance for the arguments that demonstrate that the provision of services satisfies the U-space performance requirements;

(b) demonstrate that the simulated or automated environments:

(1) are representative of, or sufficiency close to, the real operational conditions;

(2) can be trusted, in producing evidence of their proper behaviour and products.

AMC2 Article 15(1)(b) Conditions for obtaining a certificate

INFORMATION SECURITY ASSURANCE

In conjunction with point B of Annex III to Regulation (EU) 2021/664, the applicant should ensure a level of security consistent with the intended UAS operations by evaluating and mitigating the risks induced by potential intentional unauthorised electronic interaction (IUEI) on the components of the functional systems (e.g. including the hardware and software, interfaces with the other U-space airspace stakeholders, e-conspicuity, or Network R-ID receivers).

The applicant should follow a continued risk-based approach as regards the following:

(a) To assess the provision of services against any potential information security threat and vulnerability that could affect the confidentiality, availability and integrity of the provision of services.

(b) The result of this assessment, following the identification of any necessary mitigation means, should be that the provision of services entails no identifiable vulnerabilities, or if any, they cannot be exploited to create a hazard or generate a failure that would have an effect that is considered unacceptable, in particular when they may result in an unsafe condition.

(c) When a risk needs to be mitigated, the applicant should provide evidence that the mitigation means provide sufficient grounds for evaluating that the residual risk is acceptable. Accordingly, the effectiveness and robustness of the mitigation means should be demonstrated through (a potential combination of) security-oriented robustness testing, inspection/analysis, refutation/penetration testing, etc., as agreed with the competent authority.

(d) Once the overall residual risk is considered acceptable, the applicant should develop instructions, for example physical and operational security procedures, auditing and monitoring of the security effectiveness, to ensure a continued and effective protection of the provision of services.

(e) When the mitigation means rely on operational security measures to be fulfilled by a third party (e.g. UAS operator, USSP), they should be properly documented and shared with the relevant stakeholder.

(f) The applicant should dynamically reassess the potential for new vulnerabilities and the level of threat that were not foreseen during previous security risk assessments of the functional systems. If the continued assessment identifies an unacceptable threat condition, the applicant should notify the relevant stakeholders and the competent authority in a timely manner of the need and the means to mitigate the new risk.

This risk assessment is referred to as 'security risk assessment'.

GM1 Article 15(1)(b) Conditions for obtaining a certificate

SOFTWARE ASSURANCE — SOFTWARE ASSURANCE PROCESSES

The software assurance processes should provide evidence and arguments that they support, as a minimum, the following:

(c) The software requirements correctly state what is required by the software in order to meet the 'specification of services' and the 'safety support requirements'. For that purpose, the software requirements should:

(3) be correct, complete and, when available, compliant with upper-level requirements;

(4) specify the functional behaviour in nominal and degraded modes, and in terms of timing performance, capacity, accuracy, resource usage, robustness to abnormal operating conditions and overload tolerance, as appropriate, of the implemented software.

(d) The software implementation does not contain functions that could adversely affect the satisfaction of the service specification and/or does not cause undesirable behaviour that may impair the safe provision of services.

(e) Traceability is addressed in respect of all software requirements as follows:

(1) Traceable to the 'specification of services' or the 'safety support requirements'.

(2) Each software requirement allocated to a component should either be traced to an upper-level requirement, or its need should be justified and assessed that it does not affect the satisfaction of the safety support requirements allocated to the component.

(3) Each software requirement is linked to a verification activity (e.g. analysis and/or tests), granular enough to efficiently demonstrate that the requirements are met.

(f) The functional behaviour, timing performance, capacity, accuracy, resource usage (potentially on the target hardware), robustness to abnormal operating conditions and overload tolerance of the implemented software comply with the software requirements.

(g) The software verification:

(1) is correct and completely verifies the software requirements, with a sufficient level of detail demonstrating that the requirements are fully met (e.g. intent of the test; analysis; clear, expected behaviour; and pass–fail criteria);

(2) confirms that the service behaves as specified in an environment representative of the intended operational environment;

(3) allows to verify all the interfaces and the robustness of the implementation;

(4) is performed through review, analysis and/or testing and/or other equivalent means, as agreed with the competent authority;

(5) generates traceable results, with clear identification of any failed item.

(h) The evidence and arguments produced by the software assurance processes should be traceable to:

(1) a known executable version of the software;

(2) a known range of configuration data; and

(3) a known set of software items and descriptions, including specifications, which have been used in the production of that version, or can be justified as applicable to that version.

(i) The software assurance processes should include the necessary activities to ensure that the software life cycle data can be shown to be under configuration control throughout the software's life cycle, including the possible evolutions due to changes or correction of problems.

The activities should include, as a minimum:

(1) configuration identification, traceability and status-accounting activities, including archiving procedures;

(2) problem reporting, tracking, and management of corrective actions; and

(3) retrieval and release procedures.

(j) Software quality control should be undertaken to assess the conformance of the development of the software with established processes and related procedures, and should be supported by any necessary corrective actions according to the findings. The software quality control should be performed independently from the software development team to ensure impartiality of the control.

GM2 Article 15(1)(b) Conditions for obtaining a certificate

SOFTWARE ASSURANCE — USE OF EXISTING INDUSTRY STANDARDS

The applicant is responsible for defining the software assurance processes. The applicant may directly develop its own method, provided it allows to properly structure the software activities and addresses the key software engineering principles and associated software life cycle data upon which the software process assurance is built:

(a) software specification (requirements and design information);

(b) software verification;

(c) traceability (between items);

(d) configuration and change management;

(e) quality assurance.

Nevertheless, it is recommended that the applicant consider the guidance material contained in existing industry standards for software assurance considerations. It should be considered that not all standards address all aspects required, and the applicant may need to define additional software assurance processes.

Guidance material typically includes:

(a) objectives of the software life cycle processes;

(b) activities to meet the objectives;

(c) description of the evidence, in the form of software life cycle data, which indicates that the objectives have been met;

(d) particular aspects (e.g. previously developed or COTS software) that may be applicable to certain applications.

GM3 Article 15(1)(b) Conditions for obtaining a certificate

SOFTWARE ASSURANCE — TESTING INFRASTRUCTURE

The applicant, and especially the USSPs, may set up a testing infrastructure against which authorised users may test their capability to exchange data. Upon agreement on the retrieval of a set of predefined testing data, the applicant may set up an environment to check at regular intervals its capability to conform with the requirements for providing the services. The same infrastructure may then be used by oversight authorities to audit the applicant.

GM4 Article 15(1)(b) Conditions for obtaining a certificate

SOFTWARE ASSURANCE — MONITORING

The applicant may use feedback of software experience to confirm that the software assurance processes are effective. For that purpose, the effects from software malfunctions (i.e. the inability of a programme to perform a required function correctly) or failures (i.e. the inability of a programme to perform a required function) reported according to the relevant requirements on reporting and assessment of service occurrences should be assessed in comparison with the effects identified for the service concerned as per the service specification demonstration.

Additionally, within the safety support assessment process, the applicant may ensure that the monitoring criteria to be used to demonstrate that the safety support case remains valid during the operation of the functional system (i.e. that the service continues to meet its specification) are identified and documented.

These criteria should be such that:

(a) they indicate that the assumptions made in the safety support case remain valid; and

(b) if the properties being monitored remain within the bounds set by these criteria, the service will behave as specified.

GM5 Article 15(1)(b) Conditions for obtaining a certificate

SECURITY RISK ASSESSMENT

The security risk assessment may cover the following steps and security items:

(a) determination of the operational environment of the functional system;

(b) identification of the digital interfaces and assets (i.e. the items contributing to, or sustaining, cybersecurity);

(c) identification of the attack paths;

(d) considering the usual attack (e.g. DoS), assessment of the consequences and severity of the identified threat on the affected items;

(e) evaluation of the potentiality of a successful exploit, or of the difficulty of performing a successful attack that would have an impact on the typical security attributes: confidentiality, availability, integrity;

(f) an iterative approach to converge on an acceptable level of residual risk:

(1) evaluate the severities in conjunction with the potential for attack (or, inversely, the difficulty of attacking);

(2) the outcome of the evaluation is acceptable and does not need additional or strengthened mitigation means;

(3) the outcome of the evaluation is not acceptable and requires an analysis to identify mitigation means to reach an acceptable level of safety;

(4) evaluation of the effectiveness of the mitigation means with respect to the level of risk (combination of the level of threat and severity of the threat condition).

GM5 Article 15(1)(b) Conditions for obtaining a certificate

INFORMATION SECURITY — DEFINITIONS

For the purposes of Regulation (EU) 2021/664, the following is defined regarding 'information security':

(a) 'vulnerability': a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. [Source: NIST SP800-53, Rev 2]

(b) 'threat': a potential for violation of security, which exists when there is an entity, circumstance, capability, action, or event that could cause harm. [Source: IETF RFC 4949]

(c) 'threat scenario': the specification of intentional unauthorised electronic interaction (IUEI), consisting of the contributing threat source (attacker and attack vector), vulnerabilities, operational conditions, and resulting threat conditions, and events by which the target was attacked. [Source: ED-202A / DO-326A]

(d) 'severity': qualitative indication of the magnitude of the adverse effect of a threat condition [Source: ED-202A / DO-326A]

AMC1 Article 15(1)(d) Conditions for obtaining a certificate

OCCURRENCE REPORTING

The applicant should establish procedures for reporting occurrences to the competent authority and to any other organisation necessary, which should include a description of:

(a) the applicable requirements for reporting;

(b) the reporting mechanism, including reporting forms, means, and deadlines;

(c) the personnel responsible for reporting; and

(d) the mechanism for identifying root causes, and the actions to be taken to prevent similar occurrences in the future, as appropriate.

AMC1 Article 15(1)(e) Conditions for obtaining a certificate

MANAGEMENT SYSTEM — TECHNICAL AND OPERATIONAL CAPACITY

The applicant should ensure that it has sufficient technical and operational capacity, that is, adequate and appropriate resources to perform its tasks and discharge its responsibilities.

AMC2 Article 15(1)(e) Conditions for obtaining a certificate

MANAGEMENT SYSTEM — ISO

An ISO 9001 certificate, issued by an appropriately accredited organisation, addressing the quality management elements should be considered a sufficient means of compliance. In this case, the applicant should accept the disclosure of the documentation related to the certification to the competent authority upon its request.

AMC3 Article 15(1)(e) Conditions for obtaining a certificate

MANAGEMENT SYSTEM — RESPONSIBILITIES AND ACCOUNTABILITIES

The applicant should ensure that senior management defines and communicates the responsibilities and accountabilities within the organisation, and documents them within the management system.

The appointment of an accountable manager who is given the required authority and responsibilities requires that the individual has the necessary attributes to fulfil that role. The accountable manager may have more than one function in the organisation. Nonetheless, the accountable manager's role is to ensure that the management system is properly implemented and maintained through the allocation of resources and tasks.

AMC4 Article 15(1)(e) Conditions for obtaining a certificate

MANAGEMENT SYSTEM — POLICY

The applicant should ensure that the management system policy includes a commitment to:

(a) comply with all applicable requirements and standards, and consider best practices;

(b) continually improve the effectiveness of the management system;

(c) provide appropriate resources; and

(d) enforce the performance of the services required to support the achievement of the highest level of safety in the U-space airspace.

The policy should be signed by the accountable manager of the organisation.

AMC5 Article 15(1)(e) Conditions for obtaining a certificate

MANAGEMENT SYSTEM — SAFETY PERFORMANCE MONITORING AND MEASUREMENT

The applicant should ensure that the safety performance monitoring and measurement process includes:

(a) safety reporting;

(b) safety reviews including trend reviews, which would be conducted, among others, during the introduction and deployment of new technologies, change or implementation of procedures, or in situations of structural changes in the operations; and

(c) safety surveys, examining elements or procedures of a specific operation, such as problem areas or bottlenecks in daily operations, perceptions and opinions of operational personnel, and areas of dissent or confusion.

AMC6 Article 15(1)(e) Conditions for obtaining a certificate

MANAGEMENT SYSTEM — SAFETY ASSESSMENT (OF THE APPLICANT'S SYSTEM)

As per the AMC and GM to Article 3 of Regulation (EU) 2021/664, the acceptable level of safety is established during the airspace risk assessment by defining safety criteria for the U-space airspace concerned. The results of the airspace risk assessment should be considered when conducting the safety assessment of the applicant's U-space services that directly contribute to safety.

The applicant should ensure that the functional system that supports the provision of U-space services is complete and correct with regard to the acceptable level of safety of the U-space airspace (i.e. safety criteria, and high-level design characteristics of the functional system defined throughout the airspace risk assessment). A streamlined safety assessment should be conducted, and should comprise at least the following elements:

(a) the identification of additional hazards that may be induced by the decision as regards the design of the applicant's functional system;

(b) the risk analysis and the related effects;

(c) the risk evaluation and, if required, the risk mitigation;

(d) safety criteria and requirements:

  (1) complementing as necessary those already defined in the airspace risk assessment;

  (2) compliant with, and not contradicting, the high-level design characteristics of the functional system defined in the airspace risk assessment;

(e) the specification of the monitoring criteria necessary to demonstrate that the service delivered by the functional system will continue to meet the safety criteria.

AMC7 Article 15(1)(e) Conditions for obtaining a certificate

MANAGEMENT SYSTEM — ASSESSMENT OF THE MANAGEMENT SYSTEM

The applicant should ensure that:

(a) senior management assesses the service provider's management system, at planned intervals, to ensure its continuous suitability, adequacy, and effectiveness;

(b) the assessment includes evaluating opportunities for improvement and the need for changes to the management system, including the policy and the objectives; and

(c) records of senior management assessments are maintained.

AMC8 Article 15(1)(e) Conditions for obtaining a certificate

MANAGEMENT SYSTEM — PERSONNEL TRAINING AND COMPETENCIES

The applicant should:

(a) determine the necessary competencies for personnel that perform activities which support the provision of services;

(b) where applicable, provide training or take other actions to achieve the necessary competencies;

(c) evaluate the effectiveness of the training or the actions taken;

(d) ensure that personnel are aware of the relevance and importance of their activities and how they contribute to the achievement of the objectives; and

(e) maintain appropriate records of education, training, skills, and experience.

AMC9 Article 15(1)(e) Conditions for obtaining a certificate

MANAGEMENT SYSTEM — COMMUNICATION RESPONSIBILITIES

The applicant should ensure that appropriate communication processes are established, and that communication takes place regarding the effectiveness of the management system.

AMC10 Article 15(1)(e) Conditions for obtaining a certificate

MANAGEMENT SYSTEM — DOCUMENTATION

The applicant should include in its documentation:

(a) a statement signed by the accountable manager confirming that the organisation will continuously work in accordance with the applicable requirements;

(b) the scope of the activities;

(c) the titles and names of the nominated postholders;

(d) the chart showing the lines of responsibility between the nominated postholders;

(e) a general description and location of the facilities;

(f) procedures describing the function and specifying how the organisation monitors and ensures compliance with the applicable requirements; and

(g) the amendment procedure for the management system documentation.

AMC11 Article 15(1)(e) Conditions for obtaining a certificate

MANAGEMENT SYSTEM — COMPLIANCE MONITORING

The applicant should:

(a) specify the basic structure of the compliance monitoring function, structured according to the size of the service provider and the complexity of the activities to be monitored, including those which have been subcontracted;

(b) monitor compliance with the procedures they have designed to ensure that services are provided with the required level of safety and quality, as applicable; in doing so, they should as a minimum, and where appropriate, monitor:

(1) manuals, logs, and records;

(2) training standards; and

(3) management system procedures;

(c) ensure that a staff is responsible for compliance monitoring to ensure that the organisation continues to meet the applicable requirements; the accountable manager should ensure that adequate resources are allocated for compliance monitoring;

(d) ensure that the personnel involved in compliance monitoring have access to all parts of the applicant's management system documentation and, as necessary, of any subcontracted organisation; in the case the person responsible for compliance monitoring also acts as safety manager, the accountable manager, with regard to their direct accountability for safety, should ensure that sufficient resources are allocated to both functions, taking into account the size of the applicant, and the nature and complexity of its activities; the independence of the compliance monitoring function should be established by ensuring that audits and inspections are carried out by personnel not directly involved in the activity being audited;

(e) ensure that the relevant documentation includes relevant part(s) of the applicant's management system documentation; the relevant documentation should also include:

(1) terminology;

(2) a description of the service provider;

(3) allocation of duties and responsibilities;

(4) procedures for ensuring compliance;

(5) the compliance monitoring programme, reflecting:

(i) the schedule of the monitoring programme;

(ii) audit procedures;

(iii) reporting procedures;

(iv) follow-up and corrective action procedures;

(v) the record-keeping system; and

(vi) document control;

(f) ensure that the personnel responsible for managing the compliance monitoring function receive training in this task; such training should cover compliance monitoring requirements, manuals and procedures related to the task, audit techniques, reporting and recording; the allocation of time and resources should be governed by the volume and complexity of the activities concerned.

AMC12 Article 15(1)(e) Conditions for obtaining a certificate

MANAGEMENT SYSTEM — FUNCTIONAL CHANGE MANAGEMENT PROCEDURE

The applicant should ensure that:

(a) the procedures for managing changes cover the complete life cycle of a change from definition to operations, including transition into service;

(b) the roles and responsibilities for the change management processes are identified;

(c) a notification process for changes includes:

(1) the point of contact in charge of the notification of changes;

(2) the means used for the notification;

(d) the change management procedure includes a change identification procedure; this procedure should seek out potential changes, confirm that there is a real intent to implement them and, if so, initiate the notification process; and

(e) as part of the change management procedure, they keep a register of the records of all notified changes, including:

(1) the status of the implementation of the change;

(2) the notification;

(3) a link to the location of the actual record, including a reference to all information passed on to the competent authority; and

(4) the review decision from the competent authority and the records of the change approval, when the changes are selected for review.

AMC13 Article 15(1)(e) Conditions for obtaining a certificate

MANAGEMENT SYSTEM — CHANGE MANAGEMENT PROCEDURE

(a) The applicant should seek prior approval by the competent authority for any changes that affect the scope of its certificate or the terms of approval of its service.

(b) The applicant should:

(1) notify the competent authority before any such changes are implemented; and

(2) provide the competent authority with any relevant documentation.

(c) Changes that require prior approval may only be implemented upon receipt of the formal approval by the competent authority.

(d) The applicant should operate under the conditions prescribed by the competent authority during the implementation of such changes, as applicable.

(e) In order for an applicant to implement changes without prior approval, it should submit a procedure and obtain approval for it by the competent authority, defining the scope of such changes and describing how such changes will be managed and notified.

AMC14 Article 15(1)(e) Conditions for obtaining a certificate

MANAGEMENT SYSTEM — CONTRACTED ACTIVITIES

The applicant should ensure that:

(a) a contract exists with the contracted organisation that defines clearly the contracted activities and the applicable requirements;

(b) the contracted activities, performed by an organisation that is not itself certified in accordance with Regulation (EU) 2021/664 to carry out such activities, are included in its oversight process;

(c) when the contracted organisation is itself certified in accordance with Regulation (EU) 2021/664 to carry out the contracted activities, its compliance monitoring should at least check that the approval effectively covers the contracted activities and that it is still valid;

(d) when not certified to provide the service / carry out the activities itself, it should only contract or purchase the services from a certified organisation when so required by Regulation (EU) 2021/664.

AMC15 Article 15(1)(e) Conditions for obtaining a certificate

MANAGEMENT SYSTEM — RECORD-KEEPING — GENERAL

The applicant should ensure that:

(a) all records are accessible whenever needed; the records should be organised in a way that ensures traceability and retrieval throughout their retention period;

(b) records are kept in paper or in electronic format, or a combination of the two, and should remain legible throughout the required retention period;

(c) paper record-keeping systems use robust material which can withstand normal handling and filing;

(d) computer record-keeping systems have at least one backup system which should be updated within 24 hours of any new entry made; computer record-keeping systems should include safeguards against the probability of unauthorised personnel altering the data;

(e) all computer hardware used to ensure data backup is stored in a different location from that containing the working data and in an environment that ensures it remains in a good condition;

(f) the records are kept for a minimum period of 5 years unless otherwise specified by the competent authority.

AMC16 Article 15(1)(e) Conditions for obtaining a certificate

MANAGEMENT SYSTEM — OPERATIONS MANUAL

The applicant should ensure that the operations manual contains the instructions and information required for the intended operation.

The operations manual should:

(a) be signed by the accountable manager;

(b) be printed or available in electronic format and is easy to revise;

(c) have a system for version control management;

(d) include a description of its amendment and revision process specifying:

(1) the person(s) who may approve amendments or revisions;

(2) the conditions for temporary revisions and/or immediate amendments, or revisions required in the interest of safety; and

(3) the methods and means by which all personnel and organisations are advised on changes to the operations manual.

GM1 Article 15(1)(e) Conditions for obtaining a certificate

MANAGEMENT SYSTEM — ISO CERTIFICATE

An ISO 9001 certificate covers the quality management elements of the management system. Other elements required, which are not covered by the ISO 9001 certificate issued by an appropriately accredited organisation, should be subject to complementary evaluation by the competent authority.

GM2 Article 15(1)(e) Conditions for obtaining a certificate

MANAGEMENT SYSTEM — SAFETY PERFORMANCE MONITORING AND MEASUREMENT

Safety performance monitoring and measurement is the process by which the safety performance is verified in relation to the safety policy and the safety objectives established by the applicant.

A performance indicator (PI) is a type of performance measurement. An organisation may use PIs to evaluate its success, or to evaluate the success of a particular activity in which it is engaged. Sometimes success is defined in terms of making progress towards strategic goals, but often success is simply the repeated, periodic achievement of some level of operational goal (e.g. zero defects). Accordingly, choosing the right PIs relies upon a good understanding of what is important to the organisation. Since there is a need to ensure a relevant assessment, various techniques to assess the present state of the business, and its key activities, are associated with the selection of appropriate PIs. These assessments often lead to the identification of potential improvements, so PIs are routinely

associated with performance improvement initiatives. When PIs have performance targets associated with them, they are known as key performance indicators (KPIs).

GM3 Article 15(1)(e) Conditions for obtaining a certificate

MANAGEMENT SYSTEM — SAFETY ASSESSMENT

(a) A safety assessment is conducted when an applicant initiates the process to be issued with a certificate, and when a change affects a part of the functional system used in the provision of its services.

(b) The safety assessment is usually conducted by the applicant itself. It may also be conducted by another organisation, on its behalf, provided the responsibility with regard to the acceptability of the outcome remains with the applicant.

GM4 Article 15(1)(e) Conditions for obtaining a certificate

MANAGEMENT SYSTEM — COMPLIANCE MONITORING

(a) Compliance monitoring is performed by the compliance monitoring manager who should ensure that the activities of the organisation are monitored for compliance with the applicable regulatory requirements, and that these activities are carried out properly under the supervision of other relevant nominated postholders and line managers.

(b) The compliance monitoring manager is responsible for ensuring that the compliance monitoring programme is properly implemented, maintained, and continually reviewed and improved; to that end, they should be able to demonstrate relevant knowledge of the U-space framework and experience in the services provided, as well as in compliance monitoring.

(c) The compliance monitoring manager may perform all audits and inspections themselves or appoint one or more auditors by choosing personnel that have the related competencies, either from within or outside the service provider. Regardless of the option chosen, the independence of the audit function should not be affected in the case where those that perform the audit or inspection are also responsible for other activities within the organisation.

(d) In the case where compliance audits and inspection tasks are assigned to external personnel, compliance monitoring is performed under the responsibility of the compliance monitoring manager who remains responsible for ensuring that the external personnel have the relevant knowledge, background and experience as appropriate to the activities being audited or inspected, including knowledge of and experience in compliance monitoring.

(e) The organisation retains the ultimate responsibility for the effectiveness of the compliance monitoring function, as well as for the effective implementation and follow-up of all corrective actions.

GM5 Article 15(1)(e) Conditions for obtaining a certificate

MANAGEMENT SYSTEM — CONTRACTED ACTIVITIES

(a) 'Contracted activities' means those activities within the service provision conditions attached to the certificate that are performed by other organisations either themselves certified to perform such activities or, if not certified, working under the service provider's oversight. The scope of the oversight covers the contracted activities performed by the external organisation that is not itself certified in accordance with Regulation (EU) 2021/664.

(b) A contract could take the form of a written agreement, letter of agreement, service level agreement, memorandum of understanding, etc., as appropriate for the contracted activities.

(c) To ensure that the contracted organisation can perform the contracted activities, the applicant should first audit the contracted party. For the purpose of verifying the suitability of contracted organisations, the applicant may refer to appropriate consensus-based industry standards and possible related industry-awarded certifications.

(d) The ultimate responsibility for the services provided by contracted organisations always remains with the contracting organisation.

GM6 Article 15(1)(e) Conditions for obtaining a certificate

MANAGEMENT SYSTEM — OPERATIONS MANUAL

(a) The operations manual is a key document for the applicant as well as for the competent authority. It describes how the infrastructure, facilities, and operational procedures will perform safely.

(b) The principal objective of an operations manual is to show how management will fulfil its safety responsibilities. It sets out the policy and expected standards of performance, and the procedures by which they will be achieved.

(c) The competent authority expects the operations manual to be an accurate reflection of the day-to-day functioning of the management system. It shows how the organisation intends to measure its performance against safety targets and objectives. The operations manual should give a clear statement of how safety is developed, managed, and maintained. All safety policies, operational procedures and instructions should be described.

(d) For many small organisations, the operations manual may be both simple and brief if it covers procedures that are essential for the satisfactory performance of day-to-day operations.

(e) The operations manual is one of the means by which all relevant operating staff can be informed about their duties and responsibilities with regard to safety. It describes the infrastructure, services and facilities, all operating procedures, and any restrictions on service availability.

(f) The operations manual describes how the safety of operations is to be managed. There should never be any doubt in terms of safety accountability for each domain or activity described. It

defines who is accountable, who is responsible, who has the authority, who has the expertise, and who performs the tasks described.

(g) The operations manual may vary in detail according to the complexity of the operation, and the type of services provided. It may be presented in any form, including electronic form. In all cases, its accessibility, usability, and reliability should be assured.

GM1 Article 15(1)(f) Conditions for obtaining a certificate

SECURITY MANAGEMENT SYSTEM

Regarding the security management requirements, reference is made to point ATM/ANS.OR.A.D.010 of Subpart D of Annex III to Regulation (EU) 2017/373. Nevertheless, it has to be noted that Opinion No 03/2021 'Management of information security risks'[16] proposes amendments to both Subpart B and D of Annex III to Regulation (EU) 2017/373.

Therefore, once the related regulation is published, the provisions as regards the management of information security risks (Part-IS) will be applicable to the applicant.

GM2 Article 15(1)(f) Conditions for obtaining a certificate

INFORMATION SECURITY THREAT

A threat to information security may be any circumstance or event with the (accidental, casual or purposeful, intentional or unintentional, mistaken) potential to adversely impact the operation and the functional systems and/or constituents, which results from unauthorised access, use, disclosure, denial, disruption, modification, or destruction of information and/or information system interfaces. This includes usual cyber-related threats (e.g. malware), including those that could come from external systems, but does not include physical threats.

16 https://www.easa.europa.eu/en/document-library/opinions/opinion-032021

AMC1 Article 15(1)(g) Conditions for obtaining a certificate

RETENTION OF OPERATIONAL DATA AND INFORMATION

(a) The applicant should retain operational data and information, as applicable, which consists, as a minimum, of the following:

(1) exchange with the UAS operators on UAS flight authorisation request acceptance/rejection;

(2) requested and granted/rejected UAS flight authorisations;

(3) traffic information, as well as conformance monitoring information, provided to UAS operators;

(4) coordination exchange with ATC units and among USSPs;

(5) flown trajectory by the UAS operators; and

(6) status and level of service of the infrastructure used for the provision of the service.

(b) The retention of operational data and information should ensure that all records are accessible whenever needed, and in particular when so required by the competent authority, subject to privacy requirements. The records should be organised in a way that ensures operational data and information traceability and retrieval throughout the retention period.

AMC1 Article 15(1)(h) Conditions for obtaining a certificate

BUSINESS PLAN

(a) The applicant should present a robust business plan that shows that the service provision costs can be covered with the prices that can be achieved on the market.

(b) The business plan should cover:

(1) market analysis;

(2) information on the implementation of new infrastructure or other developments, and a statement on how they will contribute to improving the performance of their services, including level and quality of services;

(3) the expected short-term financial position and any changes to or impacts on the business plan; and

(4) planning showing how the business will be financially sustainable.

GM1 Article 15(1)(h) Conditions for obtaining a certificate

BUSINESS PLAN — SERVICE CONTINUITY

The business plan is required to show that an applicant is financially able to ensure the provision of services but not necessarily that it will provide such services. Indeed, it is recognised that due to certain operational circumstances (e.g. winter conditions) under which UAS operators would not make

use of the U-space services for a certain period of time, the capability of providing services in a continuous manner for a period of 12 months from the start of operations might not be possible. Therefore, the applicant is expected to ensure that its services are available for 12 months in a continuous manner even if it would not necessarily provide the services during the 12-month period.

AMC1 Article 15(1)(i) Conditions for obtaining a certificate

LIABILITY COVER — INSURANCE

The method employed to provide the insurance cover should be appropriate to the potential loss and damage in question, taking into account the level of commercial insurance cover available.

AMC1 Article 15(1)(k) Conditions for obtaining a certificate

CONTINGENCY PLAN

The contingency plan should include the definition and specification of the measures, the coordination with other actors, and the alternative services needed in case of degradation or interruption of the U-space services or the CIS.

AMC1 Article 15(2) Conditions for obtaining a certificate

EMERGENCY MANAGEMENT PLAN — USSPs

(a) USSPs should develop and maintain an emergency response plan (ERP) that ensures:

  (1) an orderly and safe transition from normal to emergency operations;

  (2) the safe continuation of operations, return to normal operations as soon as practicable, and the modification or cancellation of some or all the operations;

  (3) coordination with the ERPs of other organisations, where appropriate.

(b) The ERP should determine the actions to be taken by USSPs and reflect the nature and complexity of the activities performed by them.

(c) USSPs should ensure that communication systems:

  (1) are established to provide rapid response of the emergency equipment to accidents and incidents; and

  (2) are tested regularly to verify their operability.

(d) A complete and current list of telephone numbers should be available to all authorities and to personnel responsible for the ERP, to ensure the rapid notification of all those concerned in case of emergency.

GM1 Article 16 Validity of the certificate

GENERAL

(a) The certificate has an indefinite duration but only remains valid as long as the competent authority has verified that the USSP and the single CIS provider continue to conform with the relevant requirements. For USSPs, the certificate is issued for a bundle of U-space services plus, where applicable, the supporting U-space services provided to support the four mandatory ones. The competent authority should check the validity of the certificate on a regular basis. To maintain their certificates valid once they have been issued, the USSPs and the single CIS providers must respect the conditions and limitations set out by the competent authority. Such conditions should be objectively justified, non-discriminatory, proportionate, and transparent.

(b) It is considered that when the certificate holder ceases its activities, the competent authority cannot assume that it continues to comply with the relevant requirements to ensure the reliable and safe provision of services.

(c) One task that may be performed by the competent authority is to conduct an operational and financial assessment of the certificate holder to evaluate whether additional conditions should be imposed or, in the worse-case scenario, take a decision affecting the certificate, with the possibility of ultimately revoking it.

AMC1 Article 16(3) Validity of the certificate

CRITERIA FOR THE ASSESSMENT OF THE FINANCIAL PERFORMANCE OF AN APPLICANT

When assessing the operational and financial performance of an applicant, the competent authority or the Agency, as applicable, should ensure that the applicant:

(a) is able to meet its financial obligations, such as fixed and variable operational costs or capital investment costs, and uses an appropriate cost-accounting system; and

(b) demonstrate its ability through balance sheets and accounts, as applicable under their legal statute, and is regularly subject to an independent financial audit.

GM1 Article 17 Capabilities of the competent authorities

RESPONSIBILITIES

The main objective of Article 17 of Regulation (EU) 2021/664 is to ensure that the competent authorities have the technical and operational capacity and expertise to assess the resources needed to effectively perform their certification, oversight and enforcement tasks, and to act accordingly should this not be the case.

GM1 Article 18 Tasks of the competent authorities

CERTIFICATION, OVERSIGHT AND OPERATIONAL RESPONSIBILITIES

(a) Article 18 of Regulation (EU) 2021/664 lays down the requirements for competent authorities that perform certification, oversight and enforcement tasks. It also lists several obligations that are directly related to the functioning of the U-space system.

(b) With a view to ensuring that the requirements are always complied with while ensuring that they can effectively perform their tasks, competent authorities are conferred certain investigatory powers. Those powers should be exercised in accordance with the applicable national rules and procedures, while having due regard to several specific elements that are meant to ensure a fair balance between rights and interests of all the stakeholders concerned.

(c) Competent authorities also need to ensure supporting tasks for the effective implementation of the U-space, such as the establishment of a registration system to record the service providers involved in the U-space, to determine the type of data to be made available to those that need it, and the way this data can be exchanged to guarantee interoperability of the systems.

AMC1 Article 18(f) Tasks of the competent authorities

COORDINATION MECHANISM — ROLES AND RESPONSIBILITIES

Competent authorities should ensure the allocation of clear roles and responsibilities for the implementation of the coordination mechanism so that the interests of all U-space actors are well represented and managed in a non-discriminatory manner.

When establishing the coordination mechanism, competent authorities should ensure that it addresses the coordination requirements for demonstrating multi-party public, institutional and private stakeholder participation, and consultation, as applicable, before reaching a resolution.

In addition, competent authorities should nominate an entity as the 'U-space coordinator' responsible for the coordination mechanism. The U-space coordinator should take the initiative to coordinate with other public and administrative authorities and entities (including private ones), at national, regional, and local level in accordance with the national governance model of a given Member State (e.g. federal States, prefectures, cantons, regions, municipalities).

GM1 Article 18(f) Tasks of the competent authorities

COORDINATION MECHANISM — ROLES AND RESPONSIBILITIES

(a) The competent authority is responsible for establishing the coordination mechanism, and in particular for nominating a U-space coordinator responsible for preparing, performing and completing the coordination process by providing recommendations to the competent authority throughout the life cycle phases of the U-space airspace (planning, execution, review; see GM2 Article 18(f) of Regulation (EU) 2021/664).

(b) It is considered beneficial for the fair and just implementation of the U-space to ensure that the nomination and role of the U-space coordinator remains as impartial and independent as possible.

(c) The phrase 'other authorities and entities, including at local level' of Article 18(f) should be understood to include a variety of public, civil society and private organisations and entities (e.g. ministries, environmental and defence organisations, municipalities, environmental associations, civil society organisations, airspace users, drone operators, etc.) in any given country, and thus, an exhaustive list of them is not practical.

(d) The U-space coordinator should identify, involve, and consult with all these relevant 'other authorities and entities, including at local level'. These authorities or entities may be affected by, or interested in, the deployment of a U-space airspace in some way and therefore should be considered accordingly. The term 'local' refers to public and administrative authorities, and to entities of various types at local and regional level, such as municipalities, metropoles, prefectures, regions, airports and ports in accordance with the multilevel governance models of a given Member State. In addition, relevant local civil society organisations, associations, and private entities should be involved and consulted.

GM2 Article 18(f) Tasks of the competent authorities

COORDINATION MECHANISM — PHASES

(a) The complexity of the U-space airspace should be addressed through its different life cycle phases, namely the *planning*, *execution* and *review* phase (see Figure 1).

(b) The coordination mechanism established by the competent authority should be managed by the nominated U-space coordinator and should address the *planning*, *execution* and *review* phase.

(1) The *planning* phase should include the establishment of a multi-stakeholder collaborative set-up, hereafter referred to as 'U-space observatory' (see Figure 2). The set-up of the U-space observatory should address multi-party engagement and collaboration, information flow and transparency, and the establishment of indicators/KPIs or metrics (covering aviation performance, safety metrics, and sustainable urban mobility) on the national, regional and local level of the U-space deployment. To that end, U-space observatories, and thus U-space coordinators, may be established at national, regional and local level to deal with the multilevel governance required.

(2) The *execution* phase should enable the capability to dynamically respond to exceptional cases. It is clarified that for the purposes of the *execution* phase, the term 'dynamically respond' does not refer to airspace communications/operations (as in Article 4 'Dynamic airspace reconfiguration' of Regulation (EU) 2021/664) but rather to how awareness is raised with regard to ground/urban life incidents in U-space airspace operations, so that the U-space can be modified accordingly if needed (based on Article 4 procedures). The design of a U-space airspace can be changed, temporarily or dynamically, and may need

to be adapted after it is designated. Consequently, several different stakeholders may be necessary to be involved. To that end, responsive practices and public infrastructure investments may be required and deployed, maintained and verified (see Figure 3 and the text on the '*execution* phase' for details under GM3).

(3) The *review* phase should contain the lessons learnt (see stakeholders' involvement and feedback loops in Figure 1) with the aim to improve the U-space deployment. The monitoring of the KPIs (established during the *planning* phase), including evidence from and experience with dealing with exceptional cases (*execution* phase), as well as the need to reassess the designated U-space airspace (e.g. by either further restricting it or expanding it in the future to new urban air mobility (UAM) routes, including e-VTOL) should be the drivers for the *review* phase.

GM3 Article 18(f) Tasks of the competent authorities

COORDINATION MECHANISM — PROCESS

The coordination mechanism is considered a high-level framework (see Figure 1) for managing the coordination and alignment activities throughout the life cycle phases of the U-space deployment. The following topics may be considered during its definition and establishment:

(a) The coordination mechanism could facilitate and safeguard the collection of views, concerns and risks expressed by interested and potentially impacted public and private bodies and wider stakeholders in relation to the deployment of the U-space, but also to respectively consider, address and mitigate them, as required.

(b) The coordination mechanism could deal with topics beyond the safety, security and performance of aviation-related activities, which are typically managed at national level, by encompassing and addressing the relevant requirements and constraints (e.g. with regard to the environment and the society) imposed by regional and local authorities at different time horizons of the U-space deployment.

In other words, the aim of the coordination mechanism is that the designated and deployed U-space airspace fits the regional and local well-being needs, local traffic infrastructure and complements it (e.g. without hindering other traffic users such as pedestrians, cyclists, and means of public transport).

(c) The coordination mechanism could generate a 'result' in getting the 'green', or 'red', light, which is a decision made by the Member States based on the final recommendation of the designated competent authorities, which is based on the recommendations of the U-space coordinators. The recommendation of the latter represents harmonisation with local and regional authorities and other entities (public and private) for the short- and long-term U-space deployment.

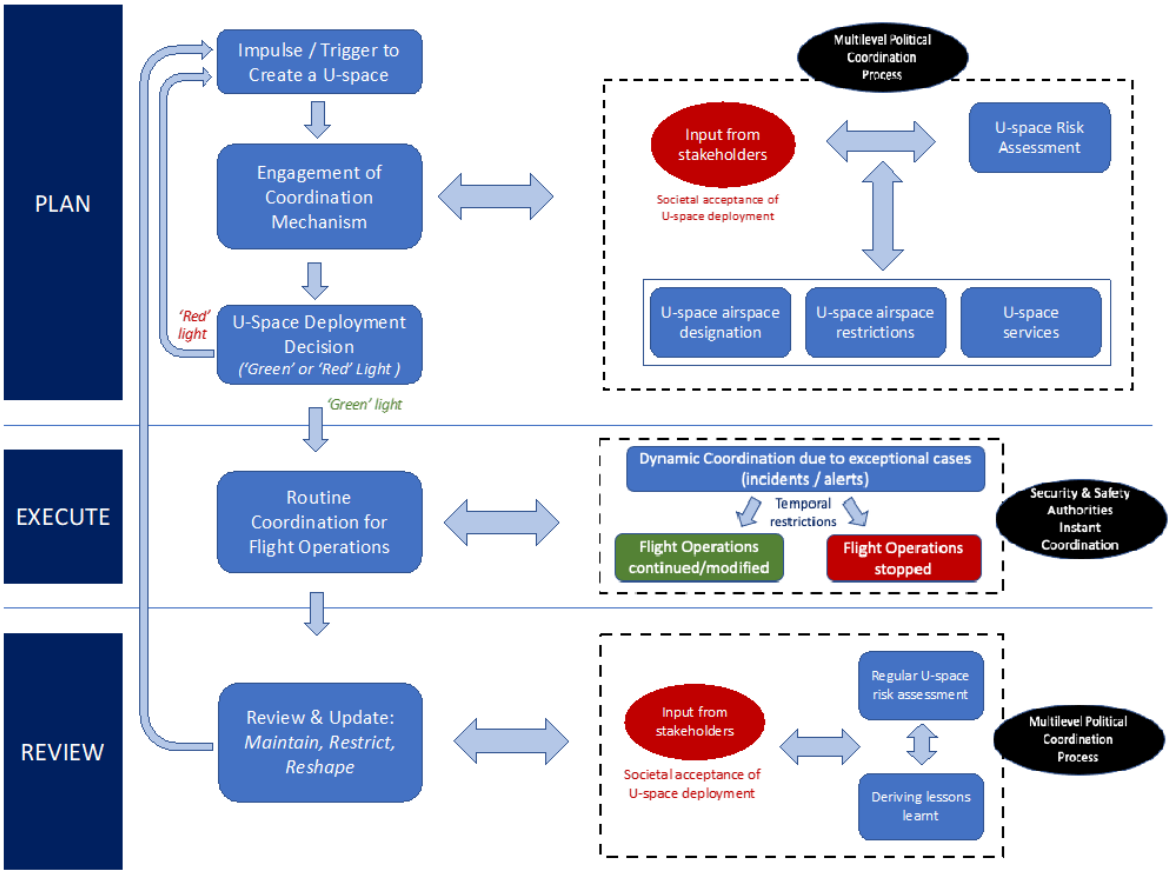

Figure 1: ***Overview of the main tasks that require coordination among stakeholders across the different levels of governance, and of the activities for the* planning*, execution and* review *phase of the U-space deployment***

GM4 Article 18(f) Tasks of the competent authorities

COORDINATION MECHANISM — PLANNING, EXECUTION AND REVIEW PHASE

1. The *planning* phase

The *planning* phase follows a screened trigger, or impulse, to create a U-space (see GM1 to Article 3 for potential triggers) that subsequently engages the coordination mechanism. The engagement of the coordination mechanism should include as a first task the nomination, or confirmation, of U-space coordinators at national, regional and local level, as applicable. This phase starts either due to a submitted U-space designation request (submitted, for example, by USSPs or UAS operators), or due to the need to develop a U-space designation recommendation. In both cases, the competent authority engages the coordination mechanism to deliver a final recommendation to the Member State that makes the final decision on the U-space deployment. In case of approval ('green' light), the U-space is formally designated.

(a) Competent authority: The designated competent authority establishes a coordination mechanism, including the nomination of a U-space coordinator.

(b) U-space coordinator and the hearing process: The U-space coordinator should be introduced to take the lead in managing the hearing process and, hence, have a role in the identification, coordination and alignment process among cross-sectoral stakeholders.

(c) The U-space coordinator should have the proven skills and experience to manage consultations and hearings. Further, knowledge of airspace management or air law could be desirable.

(d) The decision taken during the *planning* phase is based on inputs by all (public and private) stakeholders, and thus takes into consideration not only technical requirements (e.g. aviation safety and security) but also political issues and public policies. Therefore, the legal and practical bases for the involvement of the relevant actors/stakeholders are, in addition to the existing aviation laws, the laws and best practices applicable in each Member State for holding public consultations on infrastructure projects of public interest. The U-space coordinator is responsible for managing the necessary hearing process.

(e) The hearing process aims to ensure inclusion of and consultation with all stakeholders affected by the U-space deployment.

(1) The U-space coordinator should also involve citizens. Public consultation is a necessary step in determining and evaluating the level of the societal acceptance of the planned U-space airspace.

(2) The U-space coordinator should decide the form in which the process itself will take place. Examples could be public hearings and dialogue, or interviews with the affected stakeholders.

(3) A crucial aspect is that the U-space coordinator should state its position on the potential U-space deployment, based on the evidence and knowledge gained through the hearing process. The statement should include the recommendation for the design of the U-space; for example, spatial limits of the designated airspace, specific restrictions regarding areas or types of operation, or required U-space services.

(4) The hearing process should end with the submission of the recommendation from the U-space coordinator to the competent authority, which makes a final recommendation (any deviation from the U-space coordinator has to be justified) to the Member State, which makes the final decision on the U-space airspace designation, establishment of airspace restrictions and determination of the U-space services.

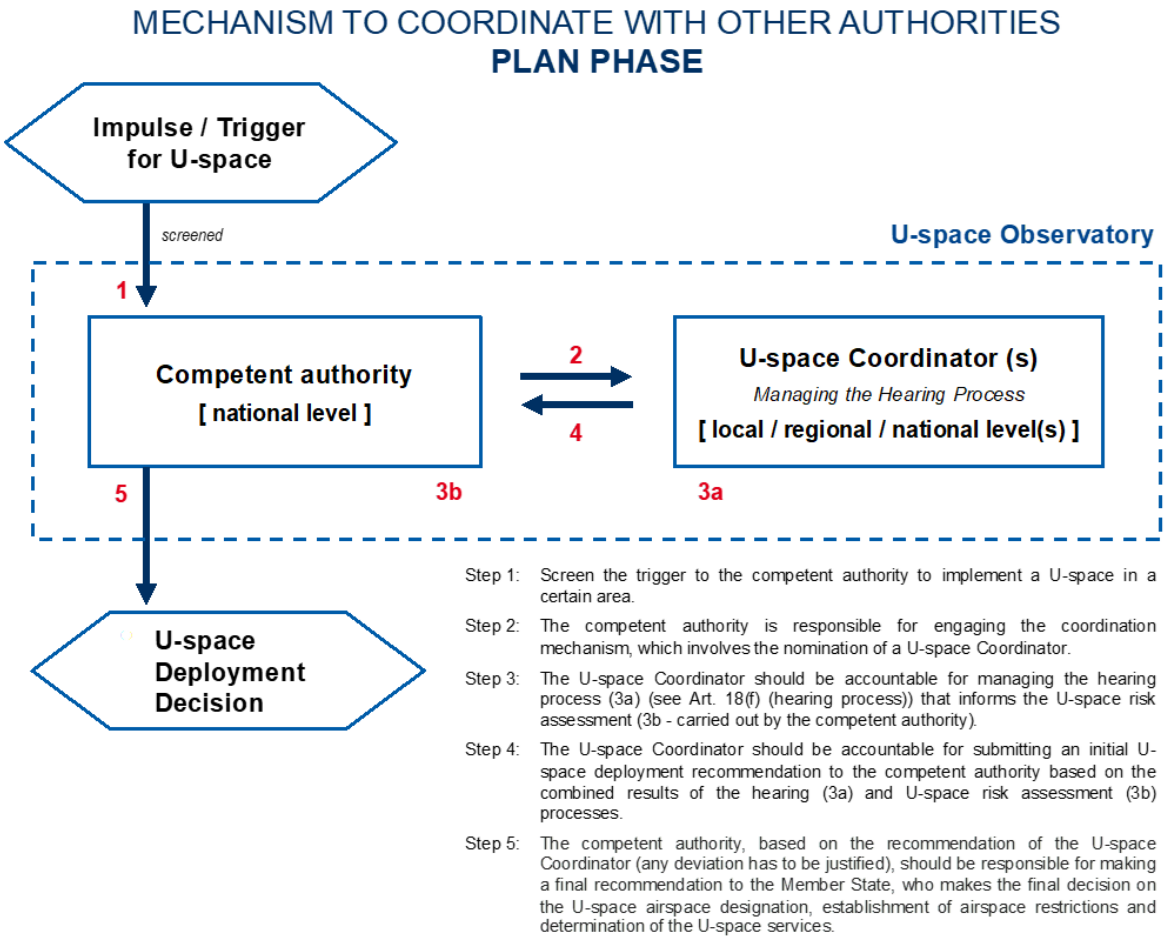

Figure 2: Example of how the coordination mechanism could be implemented. The diagram provides an overview of high-level steps, the stakeholders, and their relationship during the* planning *phase.

(f) U-space observatory: The set-up of a *U-space observatory* may be introduced as a means to promote the systematic coordination at local and regional level while maintaining alignment at national and supra-national level. The dotted lines in Figure 2 are intended to show that the U-space observatory should not necessarily be a separate entity, but rather to emphasise the need for the competent authority, responsible for making a final recommendation to the Member States on the U-space deployment, to coordinate and align with other authorities and entities through a hearing process managed by the nominated U-space coordinator.

(g) In addition to the airspace itself, a U-space airspace also affects portions on the ground of social, cultural and political interest due to the operation of UAS in the lowest parts of the airspace. Therefore, on the one hand, air transport is affected, which is regulated at EU level and requires the application of uniform regulations and rules throughout the Union and, on the other hand, sites of interest on the ground are affected too. Regulatory implementation at Member State level on this matter should be designed to meet the needs of the citizens and the society at local and regional level in a holistic and integrated manner. Therefore, it is considered that the role

of the U-space coordinator should exist at different levels of governance (i.e. national, regional, local) and hence it could be assumed by national, regional and local authorities respectively that will need to coordinate and align on relevant policies, approaches and practices.

(h) The distinction of the competent authority (at national level), as well as of the U-space coordinator (at national level[17]), and the U-space coordinator (at regional/local level) can mitigate the risks posed by the following:

(1) not aligned airspace and ground regulations across the different levels of governance in the Member States;

(2) conflicts of interest among the various public and private actors; and

(3) compromising the liveability of cities and regions.

(i) If multiple local or regional authorities are affected, there may be either one or several U-space coordinators nominated by a competent authority; this is left to the discretion of the given competent authority by evaluating the national governance set-up in conjunction with the capabilities and capacities of the affected authorities.

2. The *execution* phase

(a) The execution phase starts at the time of the actual operations. There is no predetermined end, as long as the U-space is operational.

(b) There may be temporary restrictions or limitations applied to specific U-space airspace:

(1) The competent authority at national level or specific authorities at all levels may request/demand time-critical changes due to safety or security concerns (emergencies). This may trigger, for example, the dynamic airspace reconfiguration by the ATC. The acting authority may be different depending on the kind of the emergency and the organisational structure of the respective Member State.

(2) The temporal restrictions to the U-space are applied only by designating UAS geographical zones according to Article 15 of Regulation (EU) 2019/947 which could be established as:

(i) dynamic geographical zones in terms of time and activated/deactivated without prior announcement; and

(ii) dynamic geographical zones in terms of time and location.

(3) The temporal restrictions applied to the U-space could be introduced by triggering dynamic airspace reconfiguration in accordance with point ATS.TR.237 of Regulation (EU) 2017/373 amended by Regulation (EU) 2021/665.

[17] Depending on the governance model of the respective Member State, the U-space coordinator at national level could be, for example, any authority or entity as described in AMC1 and GM1 to Article 18(f) of Regulation (EU) 2021/664. The choice of a military organisation as U-space coordinator for a U-space where civil operations take place may be done only if the same organisation is not exempted from the application of Regulation (EU) 2018/1139 and its delegated and implementing acts, as well as from Commission decisions.

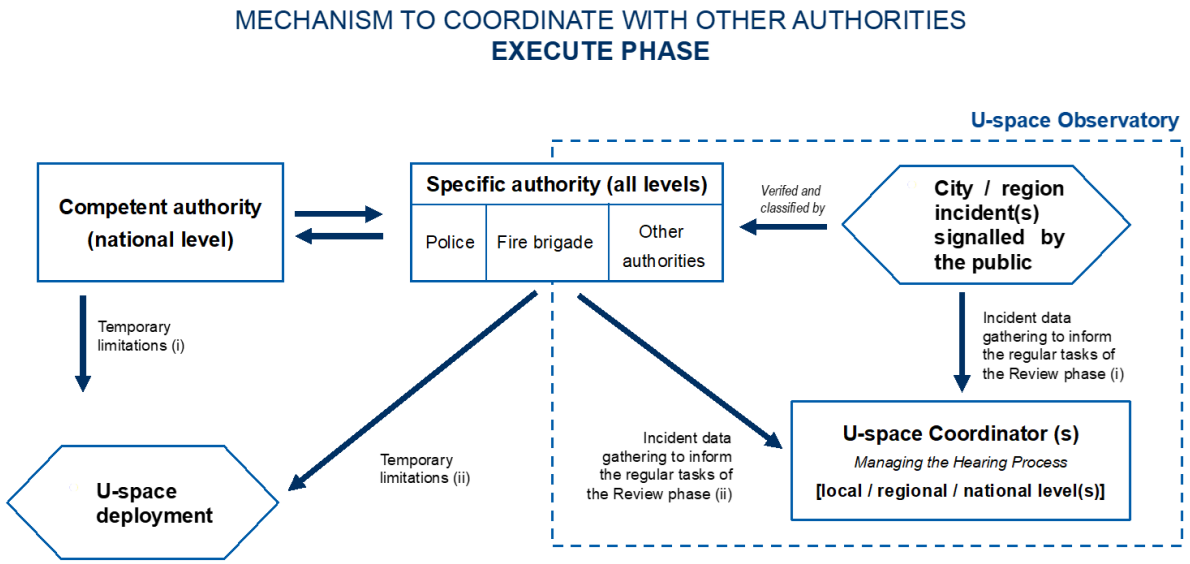

Figure 3: Example of how the coordination mechanism could be implemented. The diagram provides an overview of high-level steps, the stakeholders, and their relationship during the execution phase.

(i) Request by specific authorities (all levels): Emergency response authorities like the police, the fire brigade or civil protection agencies may request temporal restrictions depending on the structure (governance / legal basis) of the respective Member State.

(ii) Temporary limitations in the U-space: Time-critical restrictions for safety and/or security reasons, e.g. in the event of an emergency or a natural disaster. In this case, the competent authority may directly impose, according to national regulations, temporary limitations on the U-space; for example, restricted or prohibited airspace or limitation on the number of UAS in a specific area.

(c) As in manned aviation, the competent authority may always impose temporary limitations (notices to airmen (NOTAMs), airworthiness directives, air exclusion zones) on a UAS operation.

(d) Due to the nature of the U-space (low-altitude flights over populated areas), the dynamic response and reporting (including accident reporting) with regard to incidents, or to exceptional cases, is an important prerequisite to gain social trust and acceptance. To that end, incident detection and verification, as well as a streamlined and visible coordination process between aviation and non-aviation authorities, and among stakeholders, could be facilitated by relevant digital infrastructure (see Figure 3, city/region incident signalled by the public).

(e) U-space coordinator (all levels): During the *execution* phase, the role of the U-space coordinator is to ensure incident data gathering to inform the regular tasks of the *review* phase of the U-space deployment. Established accident reporting mechanisms of cities or regions, or purposefully developed tools for the monitoring of the U-space deployment, may link to the incident data gathering task (see Figure 3).

3. The *review* phase

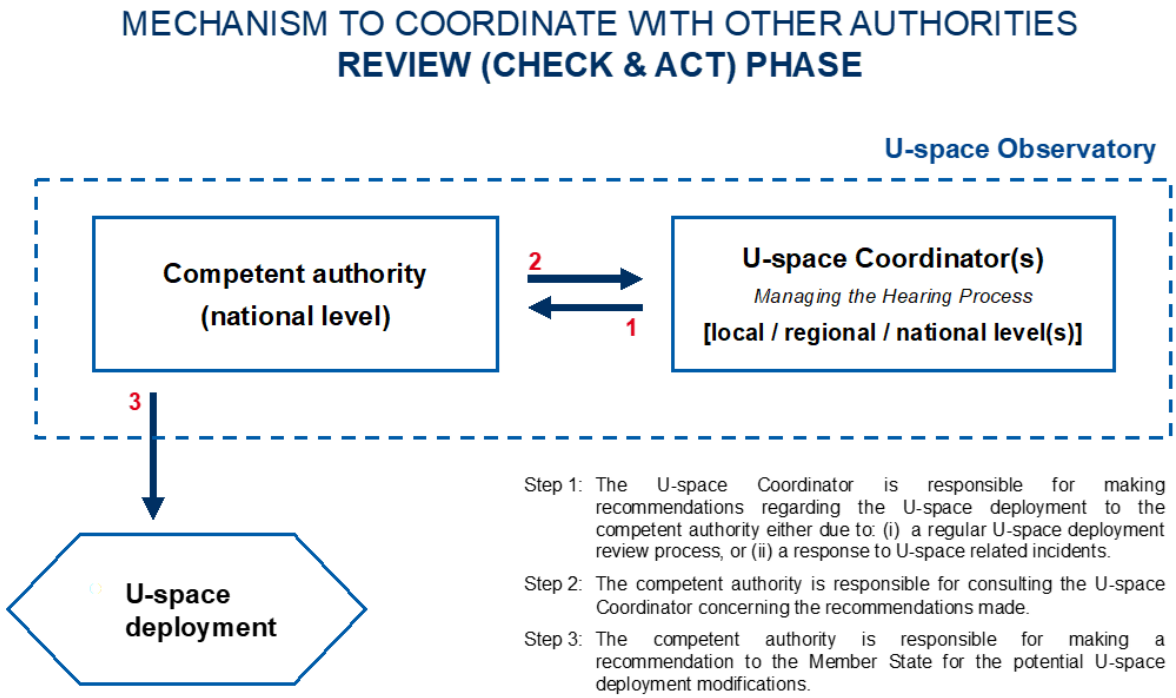

Figure 4: Example of how the coordination mechanism could be implemented. The diagram provides an overview of high-level steps, the stakeholders, and their relationship during the* review *phase.

(a) The *review* phase starts in the form of a regular review (timelines are defined during the *planning* phase) or when a U-space-related incident occurs.

Two types of review are proposed to be carried out:

(1) a technical review, led by the competent authorities in the context of the U-space oversight process (e.g. safety, security, performance indicators, etc.); and

(2) a coordination review, led by the U-space coordinator and involving national, regional, and local authorities together with other stakeholders representing societal, environmental, economic and other areas.

(b) The review process should be initiated and managed by the U-space coordinator in the context of the U-space observatory function (Step 1, Figure 4).

(c) The U-space coordinator should be entitled to make recommendations on maintaining, restricting, or reshaping (expanding or reducing) the U-space deployment. The competent authority should consider the recommendations (Step 2, Figure 4) in view of making recommendations to the Member States to decide on the potential U-space deployment modifications (Step 3, Figure 4). When the competent authority decides to deviate from the U-space coordinator recommendations, the deviations must be justified.

(1) The result of the *review* phase could lead to maintaining or restricting certain operations in the U-space airspace as well as to reshaping the U-space deployment in terms of either opening new opportunities for its expansion or even its decommissioning in case more extreme, negative situations are identified during the *execution* phase.

(2) The *review* phase aims for continuous U-space improvement (*check & act*) through a feedback loop on topics dealt with during the *planning* phase. If the modification creates new concerns, the *planning* phase should start again (see Figure 1).

(d) The *review* phase allows for closing the loop not only in terms of technical and operational performance but also the overall societal acceptance of the U-space deployment with all key stakeholders.

GM5 Article 18(f) Tasks of the competent authorities

COORDINATION MECHANISM — MULTILEVEL GOVERNANCE

(a) The U-space coordinator may be established at three layers (levels). Furthermore, each layer should involve the other layers during the *coordination* process.

(b) The U-space coordinator may involve all layers of governance in the engagement and coordination of public authorities, entities and relevant private stakeholders spreading across the:

(1) national[18] (e.g. ministries, including at federal level, defence authorities);

(2) regional (e.g. prefectures, federal states and cantons, regions); and

(3) local levels of governance (e.g. metropoles, municipalities, airports, ports) and public activity (e.g. civil society organisations, CIS providers, USSPs, UAS operators).

(c) The U-space coordinator should address all three phases of the coordination mechanism. It is an essential element for the U-space to function (technically, operationally and societally) due to its multidimensional impact. While there is a requirement about the spectrum of gathering of opinions, views and risks, and addressing them before the deployment of U-space operations as part of the planning and preparatory activities (*planning* phase), there is also a need for the coordination of tasks among the different public authorities and entities *during* the actual U-space operations (*execution* phase) as well as after their completion (*review* phase).

[18] Where applicable, supranational authorities should also be engaged as necessary; for example, it should be recalled that according to Article 64 or Article 65 of Regulation (EU) 2018/1139 and Article 14(2) of Regulation (EU) 2021/664, EASA may act as the competent authority for USSPs that intend to provide, or provide, U-space services in more than one European Union Member State as well as for USSPs established outside the EU and that intend to provide, or provide, services within its territory.

GM6 Article 18(f) Tasks of the competent authorities

COORDINATION MECHANISM — SCOPE OF TASKS IN THE CONTEXT OF MULTILEVEL GOVERNANCE

Depending on the phase of the U-space deployment, there are different needs as regards the participation of relevant stakeholders referred to in Article 18(f). These different needs and the engagement of different stakeholders may lead to differentiated coordination mechanism set-ups. The scope of the main tasks to be coordinated during each U-space life cycle phase (Plan—Execute—Review), as shown in Figure 1, in conjunction with key stakeholders (who), the timing of their engagement (when), and the coordination activities required (how), are outlined in Table 1 below (the three areas of coordination required by Article 18(f) are shown for each phase).

Table 1: Overview of the who–when–how during the different phases of the U-space coordination mechanism

	Who	When	How	*Remarks*
PLANNING PHASE				
U-space designation	Civil aviation authorities, U-space coordinator, ministries (e.g. environment, culture, interior), the military, ANSPs, regional and local authorities, and other U-space actors (e.g. CIS providers, USSPs, UAS operators).	At the very beginning of the U-space designation process and after the airspace risk assessment (Article 3.1).	By consultation, reiteration and alignment among national, regional and local authorities.	Member States *are the final decision-makers on the U-space designation after collaboration or consultation with relevant stakeholders (e.g. civil aviation and military authorities).*
U-space airspace restrictions	National authorities by defining geo-zones (ref. Article 15 of Regulation (EU) 2019/947). Regional or local authorities for the U-space designation	During the initial U-space designation.	By following the consultation process. Based on the national geo-zones, additional regional and local restrictions may apply.	*U-space is a geo-zone.*
U-space service determination	Key actors: civil aviation authorities Supporting actors: ANSPs, USSPs, UAS operator associations, regional and local authorities, etc.	As part of the U-space designation process.	Coordination only for the optional services through the consultation process.	*Mandatory and optional U-space services should not be confused with commercial or publicly offered UAS services.*
EXECUTION PHASE				
U-space designation	ATSPs (when available), USSPs, U-space coordinator and any other relevant regional/local stakeholders (e.g. emergency medical services, etc.).	Monitored throughout the operations.	Monitored in collecting safety and operational indicators: safety events (accidents, AIRPROX, etc.), occurrences of dynamic configurations, conformance monitoring, rogue drones or rogue UAS operators, etc.	—
U-space airspace restrictions	The authorised actors provide real-time U-space restrictions as part of the CIS. For example, a local authority (e.g. municipal police, fire brigade) and the USSP/ANSP in alignment with the national authorities' policies.	When an emergency is identified and verified by local authorities. ANSPs or USSPs will be notified, and the information will be automatically transferred to the UAS operator.	Automated/real-time triggering of U-space restrictions prompted from verified emergencies by local authorities. Information flow and decision-making to be managed and governed	*These U-space restrictions refer to exceptional cases that result in temporary and/or of a more pseudo-permanent nature.* *Accident reporting mechanisms may link to this task.*

			by U-space standard operations.	
U-space service determination	n/a	n/a	n/a	*Various predetermined and agreed U-space services will be used during a mission. It is expected that more mandatory services will be gradually implemented; in particular, tactical information flow, dynamic geo-fences, etc.*
REVIEW PHASE				
U-space designation	Civil aviation authorities, U-space coordinator, ANSPs and/or CIS providers, USSPs, 'hearing' authority / regional/local actors / authorities, UAS operator associations	As part of regular U-space review exercises. After mitigation of exceptional cases.	Through consideration of U-space KPIs' monitoring and feedback from stakeholders. Through risk assessment, airspace restrictions, U-space services needed.	*Follow-up*
U-space airspace restrictions				*Follow-up*
U-space service determination				*Evaluation of the usability of the U-space services. Considering adding or removing optional services: e.g. by either further restricting or expanding them to new UAM routes (including e-VTOL).*

GM1 Article 18(g) Tasks of the competent authorities

OPERATIONAL PERFORMANCE — FLIGHT AUTHORISATION

Operational performance may be supported in considering the flight authorisation data. The competent authority may monitor or audit authorisation and rejection data to assure equitable access to airspace.

Accordingly, the competent authority may consider the 'propriety' of the arrangements made among the USSPs when granting an operating certificate, and may consider:

(a) the agreement among the USSPs on the use of common protocol and infrastructure;

(b) the performance of the arrangements, such as response time;

(c) that all flight authorisation requests are treated equally.

GM1 Annex IV UAS flight authorisation request referred to in Article 6(4)

CONSTITUENTS

(a) The table below includes clarifications on the information contained in Annex IV to Regulation (EU) 2021/664.

	Information type	Possible examples
1	Unique serial number of the unmanned aircraft or the remote identification add-on	ANSI/CTA-2063-A specified in Regulation (EU) 2019/947
2a	Mode of operation	VLOS, BVLOS
2b	SAIL of the operation	Provision for further potential check
3	Type of flight (special operations)	Article 4(1) of Regulation (EU) No 923/2012 (SERA) (a) police and customs missions; (b) traffic surveillance and pursuit missions; (c) environmental control missions conducted by, or on behalf of, public authorities; (d) search and rescue; (e) medical flights; (f) evacuations; (g) firefighting; (h) exemptions required to ensure the security of flights by heads of State, ministers and comparable State functionaries.
4a	Category of UAS operation	'open', 'specific', 'certified'
4b	UAS aircraft class	C0, C1, C2, C3, C4 C5, C6, < 1 m, < 3 m, < 8 m, ≥ 8 m, Others: can be linked to model aircraft or similar special cases.
4c	UAS type certificate	A UAS subject to certification should comply with the applicable requirements set out in Regulations (EU) No 748/2012, (EU) 2015/640 and (EU) No 1321/2014.
5	4D trajectory	Standardisation of acceptable formats for the storage and distribution of common data models (DTM/DSM/DEM) together with their metadata and timeliness.
6	Identification technology	The technology used for the remote identification (e.g. GNSS-LTE, ADS-B Out)
7	Expected connectivity methods	To be expressed in terms of a standard, when available.
8	Endurance	Maximum endurance (in minutes). Endurance under nominal conditions.

9	Applicable emergency procedure	Emergency procedures will be supplied in a form agreed with the USSP. The information should allow the service provider to anticipate the behaviour of the aircraft in case the link is lost. The emergency procedures contain the planned manoeuvres, change of routes, automatic landing site, etc., which could be performed in case of contingency/emergency, and to be checked free of intersection by the USSP.
10a	Registration number of the UAS operator	AMC1 to Article 14(6) of Regulation (EU) 2019/947
10b	Registration number of the unmanned aircraft	Informally the 'tail number' — for certified aircraft

(b) The 4D trajectory describes a series of one or more 4D volumes, each with entry and exit times. The UAS operator submits this series of volumes, committing to remain within them. The volumes may overlap to express uncertainty in any dimension (for example, time). The conflict detection process is simply the identification of overlapping 4D volumes.

(c) The navigation performance is reflected in the dimensions of the volume. A situation leading to the use of a less precise measurement system (for example, the use of barometric height rather than GNSS) should be reflected in a revision of the dimensions to accommodate the corresponding uncertainty (± 30 m rather than ± 30 cm).

AMC1 Point 2 of Annex V Exchange of relevant operational data and information between U-space service providers and air traffic service providers in accordance with Article 7(3)

EXCHANGE MODEL

(a) The information exchange among the USSPs should consider Annex A to EUROCONTROL 'Specification for SWIM Technical Infrastructure (TI) Yellow Profile', edition 1.1, published on 5 July 2020.

(b) USSPs should document the services that facilitate the information exchange referred to in Article 3(2) and (3) of Regulation (EU) 2021/664 as well as the related services regarding the safe provision of services, and should adhere to EUROCONTROL 'Specification for SWIM Service Description (SD)', edition 2.0, published on 15 March 2022.

(c) The documentation of all services that facilitate information exchange should be made available to the public.

(d) Compliance with points (a) and (b) should be directly measured against the requirements listed in the respective documents (Yellow Profile and published service descriptions).

AMC1 Point 3 of Annex V Exchange of relevant operational data and information between U-space service providers and air traffic service providers in accordance with Article 7(3)

RECOGNISED ENCRYTPION METHOD

To be secure, the exchange of relevant operational data and information between USSPs and ATSPs should comply with the technical considerations of Annex A to the latest version of EUROCONTROL 'Specification for SWIM Technical Infrastructure (TI) Yellow Profile', edition 1.1, published on 5 July 2020.

GM1 Point 3 of Annex V Exchange of relevant operational data and information between U-space service providers and air traffic service providers in accordance with Article 7(3)

ENCRYTPION METHOD — TRANSPORT LAYER SECURITY

To ensure data security and privacy for communication over the internet, transport layer security may be used to encrypt the communication between web applications and servers. USSPs and ATSPs may use the transport layer security 1.2 version of the SWIM Technical Infrastructure (TI) Yellow Profile.

Transport layer security 1.2 compliance covers:

(a) key exchange algorithms (RSA, DH, ECDH, DHE, ECDHE, PSK),

(b) authentication/digital signature algorithm (RSA, ECDSA, DSA),

(c) bulk encryption algorithms (AES, CHACHA20, Camellia, ARIA),

(d) message authentication code algorithms (SHA-256, POLY1305).

AMC1 Point 4 of Annex V Exchange of relevant operational data and information between U-space service providers and air traffic service providers in accordance with Article 7(3)

COMMUNICATION PROTOCOL

The infrastructure that supports the exchange of information between USSPs and ATSPs should comply with the latest version of EUROCONTROL 'Specification for SWIM Technical Infrastructure (TI) Yellow Profile', edition 1.1, published on 5 July 2020.