Joint Authorities for Rulemaking of Unmanned Systems

# JARUS guidelines on SORA

## Annex H

## UAS Safety Services Considerations

**DOCUMENT IDENTIFIER : JAR-DEL-WG6-D.04**

| | | |
|---|---|---|
| **Edition Number** | **:** | **2.5** |
| **Edition Date** | **:** | **19.01.2024** |
| **Status** | **:** | **Draft** |
| **Intended for** | **:** | **JARUS External Consultation** |
| **Category** | **:** | **Guidelines** |
| **WG** | **:** | **SRM** |

# CONTENTS

## List of Figures



## List of Tables

# 1 Introduction

## 1.1 Applicability of Annex H

UAS Safety Services offer a breadth of capability to address safety and commercial functions for UAS Operations. This Annex focuses on the safety functions enabled by third-party services, and how competent authorities can be assured that responsibilities are clearly divided between Operators and the Providers of any services they may rely on. Service usage is not limited to any particular airspace or altitude constraint/band/limitation. Therefore, this Annex simply refers to "Service Providers" (SP), recognizing that the competent authority may decide how and where those services may be used (e.g. UTM).

Safety services in Annex H are applied to specific mitigations or objectives identified in the SORA Main Body and supporting Annexes. Services in this Annex must address either a core functionality of calculating and mitigating the intrinsic Ground Risk Class (iGRC) or initial Air Risk Class (iARC); or of fulfilling parts of the Operational Safety Objectives (OSO). ***Version 2.5 of SORA Main Body does not address interactions between multiple UAS, therefore, it is not yet possible to apply this Annex to services that measure or mitigate the resultant risks of these interactions.*** Therefore, there is no provision in Annex H to claim safety credit for services that provide strategic deconfliction between UAS.

The initial version of this Annex envisions three types of services:

- Ground Risk Operations Planning Safety Service, which calculates iGRC in accordance with Step #2 and provides M1(A) mitigation;
- Air Risk Operations Planning Safety Service, which calculates iARC and identifies strategic mitigations; and
- Tactical Conflict Detection and Alerting Safety Service, which fulfills the "detect" and optionally "decide" elements of the Tactical Mitigation Performance Requirements (TMPR).

This Annex does not address details of service provisioning for international UAS flights. However, through its use in deployment of safety services in domestic environments, this Annex may support future bilateral/multilateral agreements on service provisioning.

## 1.2 Division of Responsibilities Within the SORA Process

There are two paths for an Operator to include a Safety Service as part of the SORA Safety Portfolio:

- Absent this Annex, a Safety Portfolio that includes Operator-provisioned safety services;
- Using this Annex, a Safety Portfolio that includes safety services provisioned by a 3rd party and under separate oversight acceptable to the competent authority.

In the first scenario, the Operator may work with a Service Provider to fulfill safety functions, but the Operator ultimately remains responsible for all aspects of the Safety Portfolio. The competent authority's regulatory approval and oversight are exclusively applied to the Operator. A Service Level Agreement (SLA), or comparable document, should need to exist between the Operator

and each Service Provider, but the onus is on the Operator to provide the necessary substantiation of supporting data, analysis, and testing to demonstrate the robustness of the provisioned safety services.[1] The Operator is also responsible for validating the performance of the safety services in the context of the proposed Safety Portfolio.

Using this approach, there is no direct interaction between the Service Provider and the competent authority. However, the Service Provider's roles must be clearly established within the SORA Safety Portfolio, in order to substantiate the robustness of the safety services that are used. The Operator is responsible for having supporting evidence for performance of any externally provided service for safety of the operation. Generally, this is expected to be in the form of an SLA between the Service Provider and the Operator which, at a minimum, documents:

- the service description,
- roles, obligations, and liabilities of each party, and
- the performance, availability, and reliability of the service.

The SLA may make reference to consensus-based industry standards and related mechanisms for verification of conformity.

The second scenario, depicted in Figure 1.1 with expanded detail in Figure 1.2, enables a more defined division of responsibility between the Operator and Service Provider.



[1] OSO #VIII, "External services supporting UAS operations are adequate to the operation", requires that an Operator retains supporting evidence of service performance, through SLA or other official commitment, as part of the Operator's Comprehensive Safety Portfolio to achieve Medium and High levels of assurance.

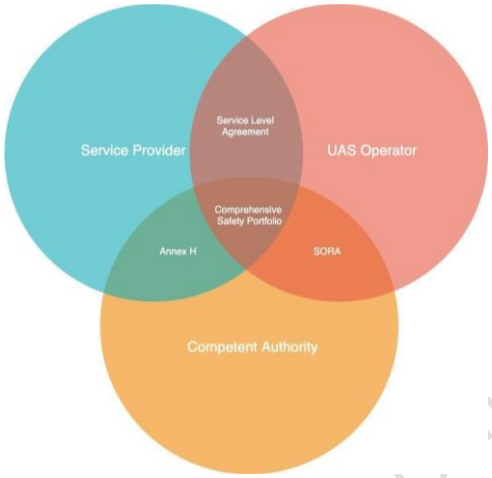


**Figure 1.1**: Division of responsibilites

Figure 1.1 assumes three entities with various responsibilities. The documents that define the relationships between each entity are named in the overlapping shaded regions. The roles of all three entities come together at the center, in the Comprehensive Safety Portfolio that the Operator Provides to the Competent Authority.

Service Providers may be approved by a competent authority, such that the Service Provider and the Operator can share responsibilities in the context of a specific Safety Portfolio. As a first step, the Service Provider should provide a concept of service usage that: 1) describes the capabilities of the service in relation to Annex H-defined services; 2) lists the intended operational usage of the service; 3) indicates any limitations on use of the service by Operators, and 4) documents the specific interface definition (i.e. human factors and digital data). The concept of service usage should substantiate the robustness of the service offerings, and be predicated on data, analysis, and testing, leading to approval from a competent authority. The concept of service usage should include a general (or template) SLA that documents the relationship between the Service Provider and any Operator that uses that provider's safety services. The SLA must, at a minimum, document the roles, obligations, and liabilities of each party, and the expectations of the Operator using the service and Service Provider delivering the service.

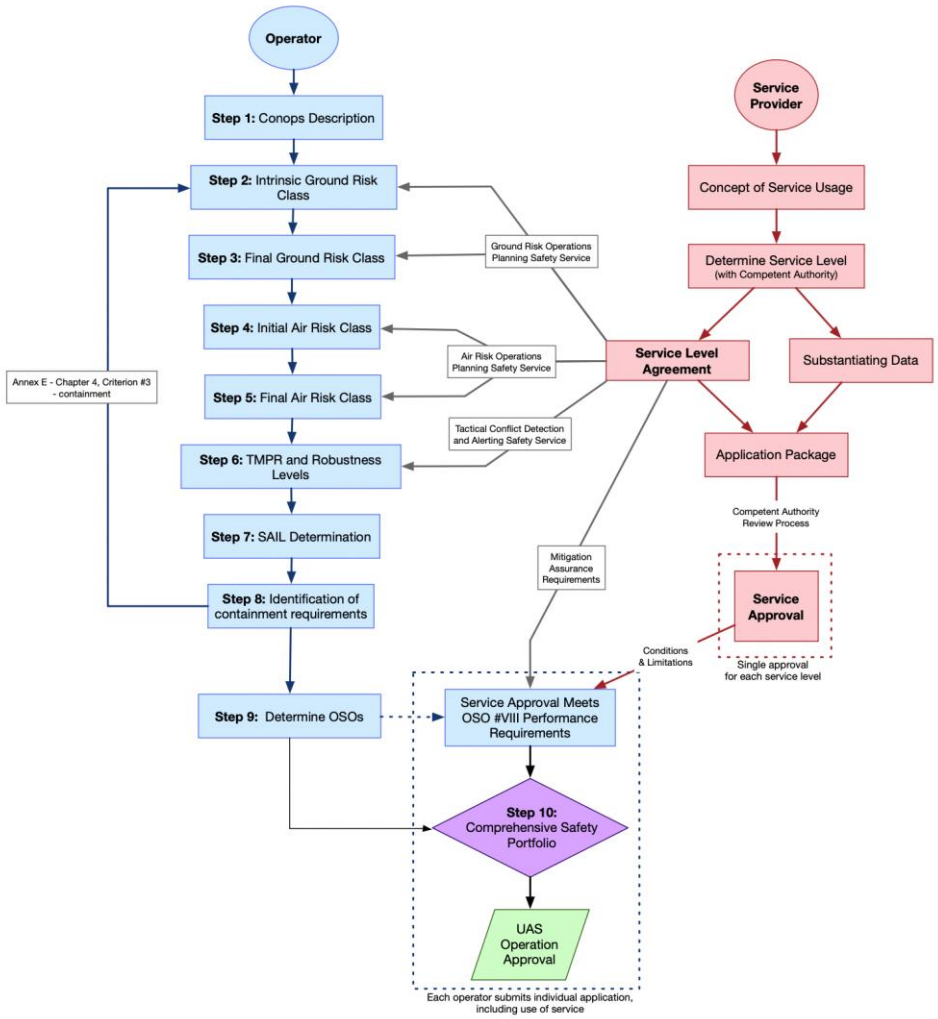


**Figure 1.2:** Adapted SORA workflow under Annex H

Figure 1.2 above associates the familiar SORA steps for the Operator (Main Body v2.5, Figure 3) to the three specific services defined in Annex H, depicting how the service approval process intersects with the development of the Operator's Comprehensive Safety Portfolio (Operator roles are blue, and Service Provider roles are red). The competent authority, possibly crediting industry certifications or standards, works with the Service Provider to determine Service Levels that correspond to different levels of integrity and reliability.

These Service Levels would be reflected in the approval that is issued by the competent authority and would reflect the safety credit that would be allowable for a given service in a Safety Portfolio. An Operator must then show how the safety service is used in the context of their Safety Portfolio, without the need to revisit the substantiation of the service since the competent authority has already provided a service approval. The Operator is still responsible for demonstrating the service is appropriate for the context of their operation. This is indicated by the dashed line flowing from Step 8 in Figure 1.2. The Operator remains responsible for ensuring that the service they pick can satisfy the mission's requirements. This is indicated in OSO #VIII, and highlighted here as a discrete step to emphasize its importance in connecting the Operator and Service Provider responsibilities described in Annex H. The competent authority is responsible for safety oversight of both the UAS Operator, for the given operations covered by the Safety Portfolio; and in parallel of the Service Provider for the provisioned safety service, under the terms of the SLA. For the Service Provider the authority may decide whether a service provider needs to be approved by the competent authority.

## 1.3 Information for Service Providers

The primary audience for Annex H is the Service Providers that seek to qualify services to gain safety credit for an Operator within the SORA framework. Any safety services may be provided from commercial entities or provisioned by a state.

The Annex describes safety services, including function, capability, and levels of performance. It associates details of those functions with levels of robustness (i.e. integrity and assurance) that the Service Provider and Operator are expected to meet. Additionally, it provides a reference framework for how a Service Provider could work with an approving authority to ease an Operator's risk assessment burden.

This Annex provides an alternative workflow to the current SORA process, in which an Operator holds the sole responsibility to assemble all required mitigations, data and documentation in support of a Safety Portfolio. The expectation is that by using a qualified Service Provider acceptable to the competent authority, Operators can follow a parallel, and potentially shorter, process in compiling their Safety Portfolio, leveraging prior documentation, analysis, and approvals by the Service Provider. Additionally, use of approved services may help Operators to more easily identify mitigations that will reduce the overall risks of their missions.

This Annex assumes that, given the option and availability of qualified Service Providers, Operators will choose to use the associated processes described herein because of the savings in time, money and effort. Service Providers have the option to include other features in their service offerings to Operators. Those features may have a safety benefit that is recognized by the Competent Authority separate from SORA, or they may provide an additional benefit that is not measurable against a specific risk or hazard.

## 1.4 Information for Operators

Operators should familiarize themselves with the service levels and capabilities described in this Annex, so that they claim the correct level of mitigation credit in the Safety Portfolio. Note that while some service levels help an Operator gain mitigation credit in accordance with Table 3 in the Main Body, other service levels only assist the Operator in conducting portions of the SORA

process that may otherwise be difficult for the Operator to correctly do unaided. The Operator's Service Provider may be able to help with this process.

Operators should be aware of the terms, limitations and responsibilities defined in the Service Level Agreement (SLA) between them and their Service Provider (see Section 3). A single competent authority's endorsement or approval of a given service offering under this Annex does not mean that the same service is automatically qualified in a different jurisdiction. In meeting OSO #VIII, the Operator must ensure that the services they desire to use are, in fact, qualified or approved by the competent authority for their specific operation.

## 1.5 Information for Competent Authorities

The competent authority has several responsibilities under Annex H, and plays a critical role in ensuring that Service Providers and Operators are correctly using a set of services referenced in this Annex for a given operation and Safety Portfolio.

First, the competent authority must establish a process for assessing Service Provider offerings and determining whether they meet the requirements of a given service description and level in this document.[2] The competent authority or their recognized third party should maintain a record of all available services that have been assessed, the list of consensus-based standards against which the service and the organization of the service provider were evaluated, and how they are classified (for example, approved for a given Service Level and region, or limited to certain vehicles or types of operations, etc). This step is important both for internal auditability and traceability, and also so that Operators can differentiate between various Service Providers and ensure that they subscribe to the appropriate services based on their mission's needs.

Second, the competent authority continues to be responsible for reviewing and approving the Comprehensive Safety Portfolio of the Operator. This role takes on an added dimension within Annex H, since the competent authority should verify that the Operator's Comprehensive Safety Portfolio properly accounts for the usage of a given service. The competent authority (or other entities authorized by delegation) also maintains their role in defining the applicable sources of data to the operators and other airspace users (e.g., airspace restrictions).



[2] It is up to the competent authority to define terminology to be used. Whether a service is "approved," "accepted," "permitted," or "certified" may carry different meanings based on how those terms are codified in applicable regulation.

# 2 Service Provider Provisioned Safety Services

## 2.1 Overview of Service Levels

Service Levels are the mechanism to describe different service capabilities, as well as their contribution to SORA mitigations and their usage in a Safety Portfolio. As a general construct, each safety service in Annex H can be deployed at any of three different service levels, which correspond to Low, Medium and High levels of robustness. Increasing service levels not only add safety features, but also may correspond to use of a service at different phases of flight, and on different time horizons.

Some service level combinations can only be used during development of the Safety Portfolio, on a time horizon that is weeks or months before an actual flight occurs. These services generally provide a more basic level of functionality, and have a minimal ability to mitigate risk because, from an assurance standpoint, the Service Provider self-declares their capability without having to submit to rigorous system testing (Service Level 2) or 3rd party verification of conformity (Service Level 3). Because of the lower qualification burden, these types of services are also expected to be faster and easier for Service Providers to deploy, while providing a benefit to Operators by streamlining the development of their Safety Portfolio.

Services that can be used during preflight carry a greater ability to mitigate risk, and generally rely on more robust (or near-real-time) data sets to support their functionality. Preflight generally encompasses the minutes and hours before a flight, and services may help in making a go/no-go decision, or in refining the flight plan and validating its conformance with what the competent authority has authorized.

Finally, some services can be used inflight, and provide real-time levels of updates and alerts to ensure ongoing adherence to the competent authority's authorizations as conditions change. These services are the most reliant on highly dynamic data sources, and will have the most robust requirements because their failure during a mission may trigger contingency actions on the part of the Operator.

### 2.1.1 General Description of Services:

There are three different services covered in the following sections, including:

- the ground risk Operations Planning Safety Service (OPSS), as described in section 2.3;
- the air risk OPSS, as described in section 2.4;
- the Tactical Conflict Detection and Alerting Safety Service (TCDASS) which is used during flight operations to help Operators detect manned aircraft, and may be incorporated as part of a detect and avoid (DAA) system, as described in Section 2.5.

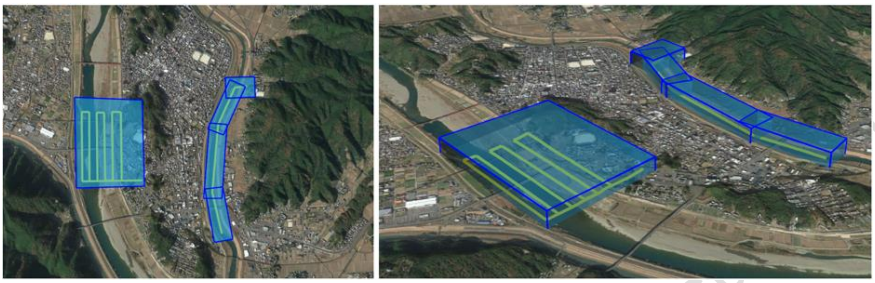

**Figure 2.1**: Notional view of trajectories contained within Operation Plans

Because the three services are independent from each other, Service Providers may choose to implement each service at a different service level.

Prior to the start of flight operations, intentions may be submitted to the Service Provider in the form of an Operational Volume defined in the Main Body section 1.4

The Operational Volume as proposed may be impacted by other planned operations (e.g., overlapping airspace volumes) or other constraints (e.g., airspace restrictions), therefore the Operator should assess all appropriate information affecting the planned operation and make amendments to the plan as applicable.

Operation planning can cover a wide range of tasks, functions, and capabilities, and it is expected that Service Providers will layer or bundle additional capabilities together into their commercial offering, above and beyond the minimum set of capabilities described in the following sections for each Service Level. Safety credit in a SORA Safety Portfolio is considered separately for the air risk and ground risk aspects of the Operations Planning Safety Service, and for the Tactical Conflict Detection and Alerting Safety Service.

Note that under this Annex, the Ground Risk and Air Risk OPSS are not expected to automatically change, modify or revise the Operational Volume the Operator will actually fly based on the various constraints. The expectation is that, given information about various ground and air risks from the OPSS, the Operator will adjust the Operational Volume as needed. Also, the Air Risk OPSS and the Tactical Conflict Detection and Alerting Safety Service are only used to address the risk of encounter between a UAS and a manned aircraft.

### 2.1.2 Service Usage According to Phase of Operations

All service usage, regardless of service level, must be documented in the Comprehensive Safety Portfolio. This is so that the Competent Authority can have assurance that services are being properly leveraged in the context of the Operator's proposed missions, and that appropriate

limitations and contingencies (e.g. for a service failure) are documented. Different service levels may be invoked at different time scales. There is a general alignment between service levels and the level of robustness but that relationship is not always exact and a one-to-one equivalence should not be assumed.

Service Level 1 Ground Risk OPSS and Air Risk OPSS are both intended to be used during the development of the Comprehensive Safety Portfolio, though they may also be used during the preflight phase (minutes or hours before takeoff) as a double-check for the Operator that a specific mission meets the requirements and limitations of the Comprehensive Safety Portfolio. Service Levels 2 and 3 of the Ground Risk OPSS and Air Risk OPSS are both intended for use during the preflight phase. The more robust, granular and dynamic nature of their functions is expected to enable the Operator to fine-tune their specific mission profile to stay within the limitations of the previously approved SORA Safety Portfolio. The Service Level 3 Ground Risk OPSS may also assist during the inflight phase, particularly in terms of being able to alert the Operator to forecast or observed weather conditions that would pose an increased risk, for which the Operator's other mitigations and limitations may not be sufficient (see Section 2.3.3).

All service levels of the Tactical Conflict Detection and Alerting Safety Service operate during the inflight phase, since they partially support the Operator's Tactical Mitigation Performance Requirements. In addition, at all service levels, the Declaration Volume calculations and substantiation are used both in the development of the Comprehensive Safety Portfolio, and as a double-check of the Operator's proposed mission during the preflight phase (see Section 2.5.2).

## 2.2 Ground Risk Operations Planning Safety Service

Fundamental to SORA is the ability to calculate the risk of one's mission in relation to the overflown population. The Ground Risk OPSS helps the Operator determine the intrinsic Ground Risk Class (iGRC), by applying data and performing calculations that may otherwise be difficult for the Operator to achieve on their own.

The Ground Risk OPSS does this by focusing on two specific criteria:

- Applying the Operational Volume Ground Risk Buffer and adjacent area in accordance with Section 2.3.1 and 2.3.2 of the Main Body; and
- Reducing the number of people at risk on the ground through the use of M1(A) strategic mitigations as defined in Annex B, Tables 2 and 4.

Additional iGRC mitigations under M1 (B) and M2 (effects of ground impact are reduced) remain the responsibility of the Operator, and are not addressed by the Ground Risk OPSS.

SORA provides Operators with two mechanisms to determine their iGRC: via the iGRC Table 2 in the Main Body or algorithmically. The tabular version pre-allocates an iGRC based on the Operator's UA dimensions, maximum velocity and maximum population density overflown. Service Providers may choose to calculate iGRC algorithmically, so long as the competent authority agrees with the nominal values for critical areas for platforms (critical area is a representation of the ground impact footprint).[3]

The Operator may reduce the number of people at risk on the ground with flight planning, analysis or inspection of the ground footprint's true population at risk.
The Ground Risk OPSS may support the Operator with this claim through two different services:

1. Applying the Ground Risk Buffer (Section 2.2.1)
2. Reducing the number of people at risk. (Section 2.2.2)

For Item 1, the OPSS will support the applicant in the determination of their risk buffer around the flight geography, for the given altitude, given the desired robustness. Since the determination of this buffer may employ weather data, the Ground Risk OPSS may partially fulfill the requirements of OSO #VII (Section 2.2.3).

For Item 2, the Ground Risk OPSS will either:

1. Apply population density maps mandated by the Competent Authority to complete Step 2 of the SORA process (Service Level 1); or
2. Use the highest resolution static population density maps appropriate to the operation to complete Step 2 of the SORA process (Service Level 1); or
3. Use authoritative population density data that incorporates real time or historical data, or dasymetric mapping techniques with a corresponding level of robustness to substantiate either a 90-percent or 99-percent reduction (Service Level 2) or 99.9-percent reduction (Service Level 3) in the number of people at risk.

[3] Additional details on how to conduct algorithmic computations of iGRC are provided in Annex F.

### 2.2.1 OPSS Req #1: Apply a Ground Risk Buffer

Kommentiert [SB1]: remove Criterion as it is used in Annex B, and mapping in Annex H is not the same,

The ground risk buffer concept is defined in Main Body section 2.3.1 and Annex E Section 4, which should be used as the reference for the implementation of the Ground Risk OPSS. Based on the iGRC, the Ground Risk OPSS can provide a ground risk buffer using two different methods: the 1-to-1 rule and data-informed approach (e.g. UA performance, dynamic population data). The methods rely on increasingly accurate types of data, including dynamic or real-time sources. The ground risk buffer is part of the iGRC footprint, which also includes the Operator's Flight Geography and Contingency Volume.

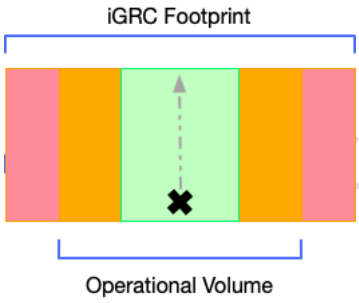


**Figure 2.2:** Schematic view showing the Flight Geography, Contingency Volume and Risk Buffer

**Note**: Flight Geography (green), Contingency Volume (orange), and Risk Buffer (pink)

The Operator is responsible for defining the Operational Volume, which includes the Flight Geography and the Contingency Volume. The method for doing this may be specified in industry standards, or by the competent authority.

The ground risk buffer surrounds the Operational Volume footprint, and the total area is the iGRC footprint. Because the determination of people at risk is based on the size of the iGRC footprint, not just the Operational Volume, Operators may leverage Service Providers that can shrink the size of the Risk Buffer through increasingly robust methods (e.g. increasingly accurate types of population data).
The following two methods defining the Ground Risk buffer:

- **The 1-to-1 Rule**. The ground risk buffer is developed such that the defined ground buffer is equal to or larger than the planned altitude of the operation.
- **Refinement based on UA performance.** Given the knowledge of their aircraft performance, latencies, technical containment performance and behavior during a failure (e.g. ballistic trajectory), an Operator defines an initial buffer. The OPSS then refines that buffer taking into account historical, forecasted and real-time atmospheric conditions, and known system and/or network latencies.

Regardless of which of the two methods used, the outcome of this criterion is a ground risk buffer.

### 2.2.2 OPSS Req #2: Reducing the number of people at risk

As defined in Annex B, M1(A), the operator can claim a one-, two-, or three-order-of-magnitude reduction in the number of people at risk by means of:

- on-site evaluation and appraisal; and/or
- sheltered operational environments; and/or
- use of dynamic density data (e.g. data from service provider) relevant for the proposed area and restricts time of operation (e.g. low population in an industrial area at night).

The Ground Risk OPSS assists an Operator in several possible ways, depending on the Service Level

- Apply population density maps mandated by the competent authority to complete Step 2 of the SORA process (Service Level 1; this cannot be used to claim any order-of-magnitude mitigation credit); or
- Use the highest resolution static population density maps appropriate to the operation to complete Step 2 of the SORA process (Service Level 1; this cannot be used to claim any order-of-magnitude mitigation credit, unless these maps are of a demonstrably higher resolution than what is mandated by the competent authority); or
- Use dynamic population density data that incorporates real time or historical data, or dasymetric mapping techniqueswith a corresponding level of robustness to substantiate either a 90 or 99-percent reduction (Service Level 2) or 99.9-percent (or greater) reduction (Service Level 3) in the number of people at risk.

### 2.2.3 OPSS Req #3: Verification of environmental conditions of Operational Volume

As a means to measure the environmental conditions and ensure that the Operator has sufficient information necessary to adhere to the limits of their operation, the OPSS provides environmental conditions of the Operational Volume prior to departure and during the mission. There are two methods in which environmental conditions can be provided:

- **Method 1: Forecasting Environment Conditions** provides an Operator with near-term predictions of expected conditions based on weather models that utilize historical trends and current measured conditions.
- **Method 2: Real-time Measured Environmental Conditions** provides an Operator with current conditions pre-departure and during a mission to evaluate the impact of environmental conditions on safe operations.

The OPSS provides an Operator with situational awareness as to whether a mission is safe to launch, can support an Operator in monitoring conditions throughout the flight, and can support an Operator in being safely reactive to changing environmental conditions.

### 2.2.4 OPSS Req #4: Defining the adjacent area size and iGRC

The adjacent area represents a reasonably probable ground area where a UA may fly or crash after a flyaway and is defined in the Main Body Section 2.3.2. Based on the Operational Volume, the Ground Risk OPSS can determine the lateral outer limit (with respect to the Operational Volume) of the adjacent area using the maximum cruise speed to determine the probable range after it has left the Operational Volume. The Ground Risk OPSS would define the adjacent area as the ground area between the outer limit of the ground risk buffer (determined from Req #1-#3) and the calculated lateral outer limit.

The Ground Risk OPSS can use the adjacent area to determine the iGRC for the adjacent area based on population density maps (as described in Req #1 and #2) and considerations for non-sheltered assemblies (as described in the Main body Section 2.3.2).

The Operator is responsible for providing the defined Operational Volume and the UA maximum cruise speed to support the Ground Risk OPSS determination of the adjacent area and corresponding iGRC.

### 2.2.5 Ground Risk OPSS Functionality at Each Service Level

The roles and responsibilities of the Operator and Service Provider can be defined by the required tasks needed to support the Ground Risk OPSS and the required data, analysis, and/or testing that is needed to establish a level of assurance. Figures 2.3-2.5 depicts how Req 1-3 of the Ground Risk OPSS relates to the SORA process and the division of responsibilities between the Operator (in blue) and the Service Provider (in red), for each service level.

**Formatiert:** Block

These diagrams show logical process steps, as distinct from engineering sequence diagrams that detail exact information flows. This is an important distinction, since a given service can be implemented successfully in many ways, and it is beyond the scope of this Annex to predefine how a service should be implemented.

In practice, it is expected that the steps to calculate iGRC and refine the ground risk buffer will be iterative within a service. These possible iterations are not shown in the following diagrams.

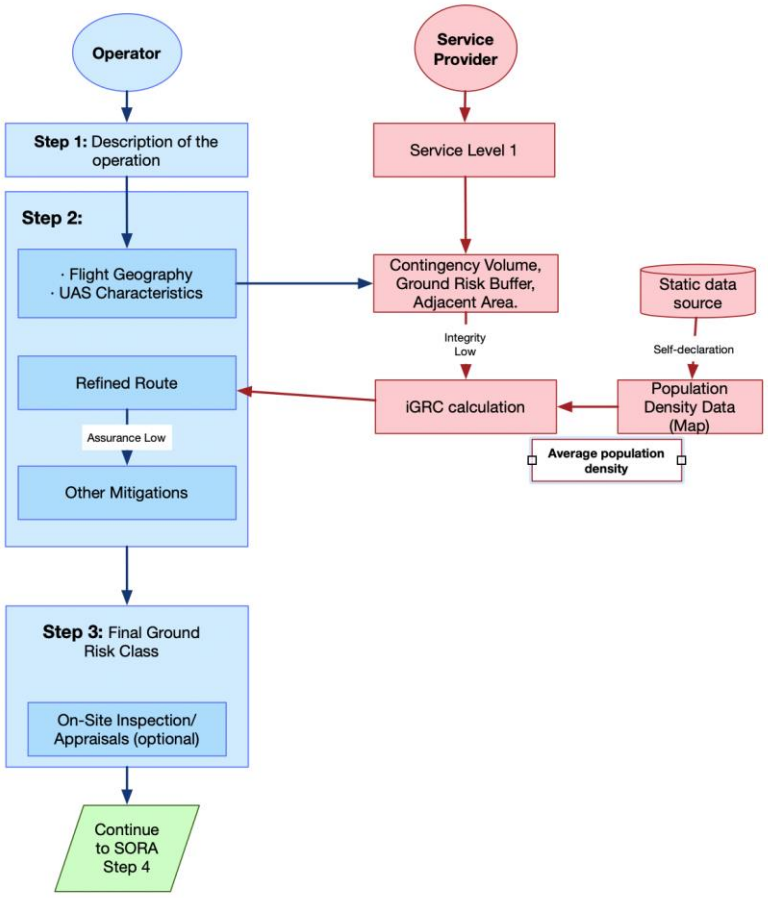


**Figure 2.3:** Operator and Service Provider responsibilities at Service Level 1 (SL1).

**Note**: the only mitigation applied by the service is accounting for VLOS operations. Otherwise, the service assists with SORA Step 2.

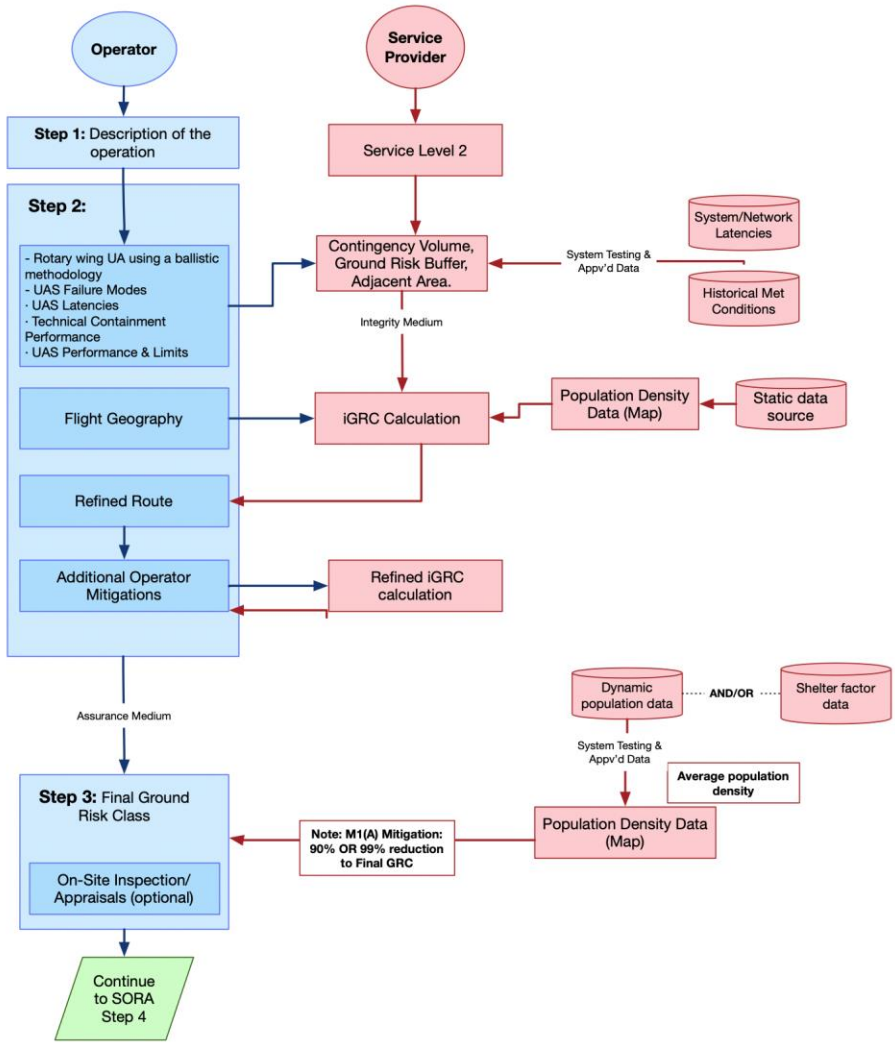


**Figure 2.4**: Operator and Service Provider responsibilities at Service Level 2 (SL2).

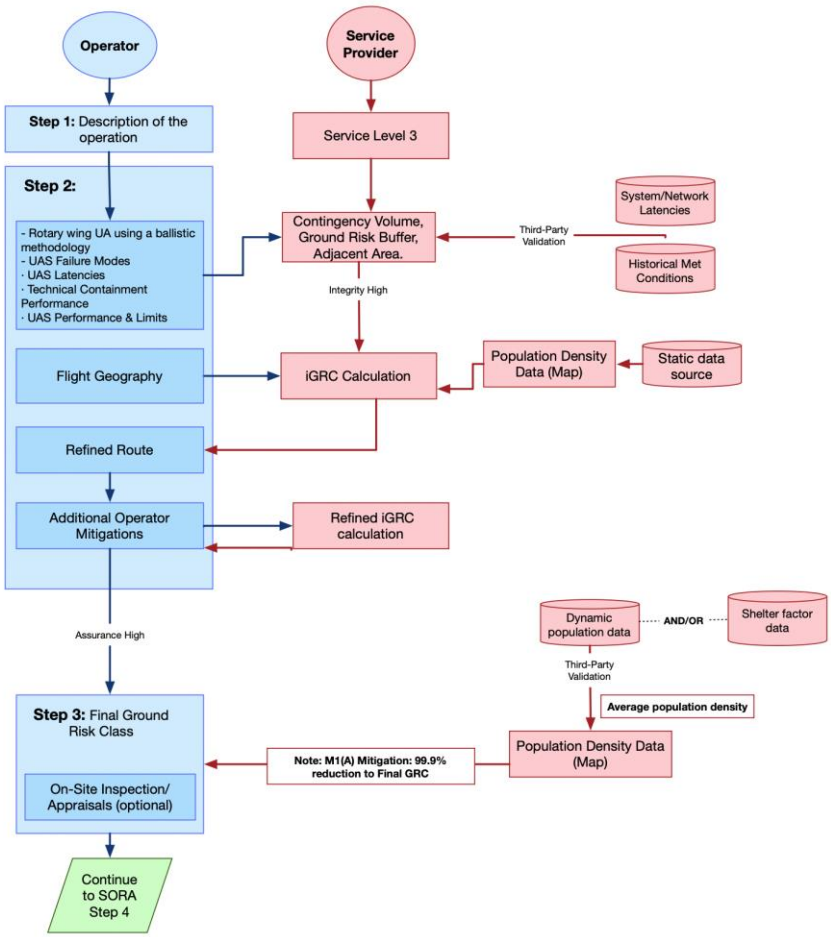


**Figure 2.5:** Operator and Service Provider responsibilities at Service Level 3 (SL3)

The Flight Geography, Operator's specification, and UAS characteristics are provided by the Operator to a Service Provider, who provides a basic population map. The Service Provider supports the Operator's decision of the iGRC. The iGRC is then used to determine the ground risk buffer and the number of people at risk within the Operational Volume to a certain level of integrity. Practically speaking, the steps to calculate iGRC and refine the ground risk buffer may be repeated several times to iterate to the refined route, possibly with Operator involvement during the refinement process. The exact exchange of information should be documented in the SLA.

To achieve a robustness determination necessary to gain a safety reduction on the iGRC, both the Annex B, M1(A) Criterion #1 and #2 must meet the corresponding level of robustness.

### 2.2.6 Division of Responsibility at Each Service Level

To achieve a given Service Level, a Service Provider must satisfactorily fulfill all elements within that service level's column in the Integrity and Assurance tables that follow. Proper usage of the service requires the Operator to fulfill their corresponding responsibilities.

**Table 2.1:** Ground Risk OPSS Integrity, Assurance, and Responsibilities

| | | Service Provider Responsibilities | | Operator Responsibilities | |
|---|---|---|---|---|---|
| | | **Integrity** | **Assurance** | **Integrity** | **Assurance** |
| **OPSS Req #1 Apply a Ground Risk Buffer - Annex E, Chapter 4, Criterion #3** | **Service Level 1 (Low)** | Define a ground risk buffer with at least a 1 to 1 ratio to operating altitude | The Service Provider declares that the required level of integrity is achieved | The Operator provides the Operational Volume. | N/A |
| | **Service Level 2 (Med)** | Define a ground risk buffer that takes into consideration:<br>• Meteorological conditions (e.g. wind)<br>• Communications and surveillance latencies<br>• Operator provided UAS data OR Operator provided initial risk buffer<br>• Rotary wing UA using a ballistic methodology | The Service Provider has supporting evidence that the required level of integrity has been achieved. This is typically done by means of system testing, which may include analysis, simulation, inspection, design review or through operational experience. | Same as low.<br><br>In addition, the Operator provides UAS data or initial risk buffer to Service Provider:<br>• Improbable single malfunctions or failures (including the projection of high energy parts such as rotors and propellers) which would lead to an operation outside of the operational volume,<br>• UAS latencies (e.g. latencies that affect the timely manoeuvrability of the UA),<br>• UA behaviour when activating a technical containment measure,<br>• UA performance | The Operator has supporting evidence to substantiate UAS data or risk buffer given to the Service Provider.<br><br>This is typically done by means of system testing, which may include analysis, simulation, inspection, design review or through operational experience. |
| | **Service Level 3 (High)** | | The claimed level of integrity is validated by a competent third party. | | The claimed level of integrity is validated by a competent third party. |
| **OPSS Req #2, Reducing number of peoplke at risk: Annex B, M1(A) Criterion #1 & 2 (Evaluation of People at Risk and Impact on at risk population. Using a Ground Risk Map)** | **Service Level 1 (Low)** | See Annex B M1(A) Criterion #1<br>AND<br><br>Complete Step 2 of the SORA process by applying population density maps mandated by the Competent Authority;<br><br>**OR**<br><br>Using the highest resolution (Annex F) static population density maps appropriate to the operation. | All mapping products, data sources and processes used to claim lowering the density of population at risk should be accepted/approved by the competent authority.<br><br>The Service Provider has supporting evidence that the required level of integrity is achieved. This is typically done by means of testing, analysis, simulation, inspection, design | The Operator evaluates the area of operations by means of on-site inspections/appraisals to justify lowering the density of people at risk<br><br>(e.g. residential area during daytime when some people may not be present or an industrial area at night time for the same reason). | N/A |

Formatiert: Zentriert, Abstand Nach: 0 Pt., Zeilenabstand: einfach

| | | | | | |
|---|---|---|---|---|---|
| | **Service Level 2 (Med)** | See Annex B M1(A) Criterion #1<br>AND<br><br>Use dynamic population density data that incorporates real time or historical data, or appropriate dasymetric mapping techniques; **AND/OR** uses shelter factor data to substantiate a reduction in people at risk.<br><br>The at-risk population is lowered by at least 1 or 2 iGRC population bands (~ 90% or ~99%) using one or more methods described in the Level of Integrity for Criterion #1 | review or through operational experience. | | |
| | **Service Level 3 (High)** | See Annex B M1(A) Criterion #1<br>AND<br>Use authoritative population density data that incorporates real time or historical data, or dasymetric mapping techniques; **AND/OR** uses shelter factor data to substantiate a **99.9-percent** reduction in the number of people at risk. | All mapping products, data sources and processes used to claim lowering the density of population at risk should be accepted/approved by the competent authority.<br><br>The claimed level of integrity is validated by a competent third party. | | |
| **OPSS Req #3 Environ-mental Condition Verification** | **Service Level 1 (Low)** | N/A | N/A | N/A | N/A |
| | **Service Level 2 (Med)** | Method 1: Forecasting Environment Conditions | The Service Provider has supporting evidence that the required level of integrity has been achieved. This is typically done by means of system testing, which may include analysis, simulation, inspection, design review or through operational experience. | The Operator provides the Operational Volume.<br><br>The Operator defines the UA environmental performance limits. | The Operator has supporting evidence of the vehicle's weather-related performance limits (e.g. maximum winds, min/max operating temperature, precipitation tolerance) |
| | **Service Level 3 (High)** | Method 2: Real-time Measured Environmental Conditions | The claimed level of integrity is validated by a competent third party. | | Weather-related performance limits of the vehicle are validated by a competent third party. |
| Criterion #4 **Adjacent area size and iGRC** | Service Level 1 (Low) | Define the adjacent area size as detailed in Step #2 Section 2.3.2 of the SORA Main Body, where the outer limit is specified by:<br>• Case 1.1 | The Service Provider declares that the required level of integrity is achieved | The Operator provides the Operational Volume, maximum UA cruise speed. | N/A |
| | **Service Level 2** | | The Service Provider has supporting evidence | | |

Formatiert: Abstand Nach: 0 Pt.

| | | | | | |
|---|---|---|---|---|---|
| | **(Med)** | • Case 1.2.1<br>• Case 1.2.2<br>• Case 1.2.3<br>And the inner limit is the outer limit of the risk buffer determined in OPSS Req #1.<br><br>AND<br><br>Determine the iGRC using Table 2 from the Main Body of the adjacent area by calculating the average population density from population density maps and considerations for non-sheltered assemblies. | that the required level of integrity has been achieved. This is typically done by means of system testing, which may include analysis, simulation, inspection, design review or through operational experience. | | |
| | **Service Level 3 (High)** | | The claimed level of integrity is validated by a competent third party. | | |

## 2.3 Air Risk Operational Volume Safety Service

The Air Risk OPSS uses information about the airspace, as well as the Operator's intended operation area, to aid in the calculation of the Initial Air Risk Class (iARC). It may also help to identify time windows and/or locations of operation that can lower the iARC as a means to strategically mitigate and reduce the ARC.

This service further aids the Operator by providing guidance as to the level of Tactical Mitigation Performance Requirements (TMPR), if any, that may need to be fulfilled based on the ARC[4].

The process begins with the assignment of an iARC. Where the competent authority and ANSP have not already established an iARC for an Operational Volume, the SORA may be used to establish one. Using Annex C, the generalized iARC is assigned to a given Operational Volume based on a qualitative classification of the probability that a UAS would encounter a manned aircraft in the Operation Volume (Criterion 1). However, the Operator may observe that the actual risk in the local area differs from the nominal or generalised assessment for the iARC level, defined in Table 1 of Annex C.

Strategic Mitigation consists of procedures and operational restrictions applied prior to takeoff which are intended to reduce the collision risk with manned aircraft (Criterion 2). Given additional data sets provided by the UAS Operator and/or Service Provider, the generalized iARC can be further refined by methods such as airspace characterisation, which better reflect the collision risk of the Operational Volume. At Service Levels 2 and 3, the Service Provider has the responsibility to collect and analyze the data required, and demonstrate their methodology to the competent authority. Expanded details on the key considerations for airspace characterisation and an overview of methodology approaches will be provided in forthcoming Annex G.

As part of their Comprehensive Safety Portfolio, the Operator has the responsibility to coordinate with the local competent authority and/or ANSP to determine the final Residual Risk. However, an Air Risk OPSS can partially support the achievement of this effort via the provision of services that support the fulfillment of Criterion 2. The Residual ARC must be addressed by appropriate Tactical Mitigations as detailed in Annex D.

The Air Risk OPSS only considers encounters between a UAS and a manned aircraft. The scope does not include risk due to wake turbulence. Future versions of the service may address UAS-UAS encounters and associated collision risk.

### 2.3.1 Criterion 1: Calculating the Initial ARC

Criterion 1 helps the Operator gain an understanding of the risk profile by determining the iARC in ways that are consistent with the competent authority's guidance. However, this criterion by itself does not result in a tangible reduction of the risk profile. However, the service is expected to provide a safety and operational benefit, in the form of improved situational awareness and understanding of the airspace for the intended mission. It is also likely that many Service Providers will seek to develop airspace characterisation products in cooperation with the competent authority, to reduce the number of locations where the generalised (and conservative) iARC

[4] The Tactical Conflict Detection and Alerting Surveillance Safety Service may be used to help fulfill the TMPR (Section 2.5).

assessment is in conflict with local conditions. Additional services could draw on the improved quality of the airspace representation to support the Operator in their awareness of adjacent airspace (and its iARC). Finally, the supporting services can make the Operator aware in the flight planning process of their obligations and options for the various mitigation measures needed to maintain safety for a particular ARC.

The difference between Service Levels 1 and 2 is in how the ARC is determined.

At Service Level 1, the Service Provider identifies the values from a suite of qualitative iARC predictors including airspace class, altitude, and the population overflown, given the Operator's proposed Operational Volume. This methodology is described in Section 2.4.2 in the SORA Main Body, where the data used to support the assessment of iARC predictor values includes authoritative and current aeronautical chart data, as determined by the competent authority

At Service Level 2, the Service Provider uses quantitative airspace data and a calculation methodology that is approved by the competent authority to determine the ARC. This may result in an iARC that is higher or lower than the qualitatively derived iARC found using the conventional SORA methodology.

Successful implementation of Service Level 2 requires that the competent authority assess the methodology used, including the type and amount of data used in the quantitative calculations; various considerations in data handling and processing; and the accuracy in determining the ultimate collision risk estimates. Tailoring the underlying data based on time of day, time of year, or other aspects is reserved for Criterion 2.

### 2.3.2 Criterion 2: Constraining the Operational Volume based on air risk

As a means to provide adequate mitigations to limit the collision risk between UAS and manned aircraft, the Air Risk OPSS supports an Operator by strategically constraining the available airspace to help plan an Operational Volume in an area that reduces midair encounter risk. The Air Risk OPSS uses appropriate data sources and methodologies for the airspace. These processes are either defined by the competent authority, or documentation exists to show that they are consistent with the practices recommended in Annex C and forthcoming Annex G.

As an Operator defines an Operational Volume, the OPSS uses authoritative airspace data to support the Operator by determining an iARC based on collision risk estimates. Given the iARC and the Operator-defined Operational Volume, the OPSS will perform an airspace characterization and provide the following methods to make recommendations to the Operator. It is encouraged that the OPSS use a methodology that is consistent with the acceptable methodologies described in forthcoming Annex G. These methods may be combined:

- **Spatial Buffer** constraining the Operational Volume to a geographic area.
- **Temporal Limits** constraining the times of day, days of the week, or months of the year in which the operation is conducted.
- **Applying common airspace structures** (e.g. UAS geozones) and flight rules, which are defined by the Competent Authority

The output of this criterion are the constraints to the Operational Volume by duration, time of execution and/or with an added Spatial Buffer, and the corresponding reduction to the iARC. If no

additional strategic mitigations are applied, then the Operator-accepted recommendations of the OPSS result in the Residual ARC.

### 2.3.3 Division of Responsibility at Each Service Level

To achieve a given Service Level, a Service Provider must satisfactorily fulfill all elements within that service level's column in the Integrity and Assurance tables that follow. Proper usage of the service requires the Operator to fulfill their corresponding responsibilities.

**Table 2.2:** Air Risk OPSS Integrity, Assurance, and Responsibilities

| | | Service Provider Responsibilities | | Operator Responsibilities | |
|---|---|---|---|---|---|
| | | **Integrity** | **Assurance** | **Integrity** | **Assurance** |
| **Criterion #1 (Determine Initial ARC)** | **Service Level 1 (Low)** | The Service Provider determines Initial ARC following SORA qualitative process. | The Service Provider uses authoritative static aeronautical data that is kept current with applicable chart revision cycles. | The Operator provides the Operational Volume | The Operator declares that they are able to maintain their trajectory (or remain within their Operational Volume) consistent with the containment requirements of Step #9. |
| | **Service Level 2 (Med)** | The Service Provider determines Initial ARC following quantitative processes:<br>● Uses georeferenced data based on quantitative methods.<br>● Manned aircraft surveillance data is applicable for the date (e.g month/season), time (e.g. day/night) and location of intended use. | The Service Provider has supporting evidence that the required level of integrity has been achieved. This is typically done by means of system testing, which may include analysis, simulation, inspection, design review or through operational experience. | | The Operator has supporting evidence that they are able to maintain their trajectory (or remain within their Operational Volume) consistent with the containment requirements of Step #9.<br><br>This is typically done by means of system testing, which may include analysis, simulation, inspection, design review or through operational experience. |
| | **Service Level 3 (High)** | Determine Initial ARC following quantitative processes:<br>● Uses an appropriate quantity of georeferenced data based on quantitative methods to assure statistical rigor.<br>● Authoritative manned aircraft surveillance data is applicable for the date, time period and location of intended use. | The proper application of data processing and analysis methods is validated by a competent third party.<br><br>This approval would examine the preprocessing methods for the data sources (resampling, interpolation, cleaning), the techniques used (applied statistics), and the implementation (algorithm, numerical methods and software) of risk calculations. | | A competent third party validates that the Operator is able to maintain their trajectory (or remain within their Operational Volume) consistent with the containment requirements of Step #9. |
| **Criterion #2 (Apply Strategic** | **Service Level 1 (Low)** | N/A | N/A | N/A | N/A |

| | | | | | |
|---|---|---|---|---|---|
| **Mitigations to Reduce the Initial ARC)** | **Service Level 2 (Med)** | The Service Provider:<br>● Applies strategic mitigations either by adjusting the Operational Volume or using any combination of Methods in Annex C.<br>● Determines new lowered Initial ARC<br>● Provides information to the Operator on required steps to adhere to the applied strategic mitigation measures (e.g. equipage requirements, additional operating restrictions). | The Service Provider has supporting evidence that the required level of integrity has been achieved. This is typically done by means of system testing, which may include analysis, simulation, inspection, design review or through operational experience. | The Operator provides the Operational Volume | The Operator has supporting evidence that they are able to maintain their trajectory (or remain within their Operational Volume) consistent with the containment requirements of Step #9. The Operator also has supporting evidence that their internal processes allow them to adhere to the applied strategic mitigations.<br><br>This is typically done by means of system testing, which may include analysis, simulation, inspection, design review or through operational experience. |
| | **Service Level 3 (High)** | | The proper application of mitigation methods, and of guidance/rules, is validated by a competent third party. | | A competent third party validates that the Operator is able to maintain their trajectory (or remain within their Operational Volume) consistent with the containment requirements of Step #09, and that their internal processes allow them to adhere to the applied strategic mitigations. |

## 2.4 Tactical Conflict Detection and Alerting Safety Service

The Tactical Conflict Detection and Alerting Safety Service (TCDASS) fulfills some elements of the Tactical Mitigation Performance Requirements (TMPR) on behalf of the Operator. The TCDASS functionality is primarily to provide real-time tracking information of manned air traffic within a predetermined area, using sensors. Depending on the service level, the TCDASS may also provide alerts about proximate traffic that poses a collision risk, so that the Operator can take action to avoid that traffic. Note that in this section, the term “potential tactical conflict” is synonymous with “intruder aircraft” terminology that is commonly used in discussions of detect and avoid (DAA) and surveillance systems.

Annex D describes how detect and avoid (DAA) can be used as a tactical mitigation for BVLOS operations. The Residual ARC, as calculated in Annex C or another methodology approved by the competent authority, determines the TMPR for a given operation. Residual ARC is a function of the strategically mitigated midair collision risk between the Operator’s UA and manned aircraft. The TMPR are intended to further reduce that collision risk. Therefore the use of the TCDASS is currently only applicable toward tactically mitigating potential encounters with manned aircraft (and not encounters between two UAS).

The five TMPR elements are:

- **Detect** aircraft in a defined volume that encloses the Operational Volume; this volume is called “Declaration Volume” in the rest of the Annex. Some of these aircraft may pose a tactical conflict, while others may not.
- **Decide** the means by which a conflict will be avoided once a potential tactical conflict is detected. *Note: This is understood to be dependent on prioritization and alerting of the potential tactical conflict, which are DAA functions defined in emerging industry standards.*
- **Command** the UA to maneuver, including accounting for C2 link latencies in sending that command.
- **Execute** the evasive maneuver, which may include doing so within a given time limit.
- **Feedback Loop** provides continued tracking of the aircraft in conflict during the conflict resolution process to ensure that the conflict is successfully resolved.

### 2.4.1 Potential elements of the TCDASS and links to the TMPR

Figure 2.6 provides a simplified view of the TCDASS elements and how they link to the different TMPR elements.

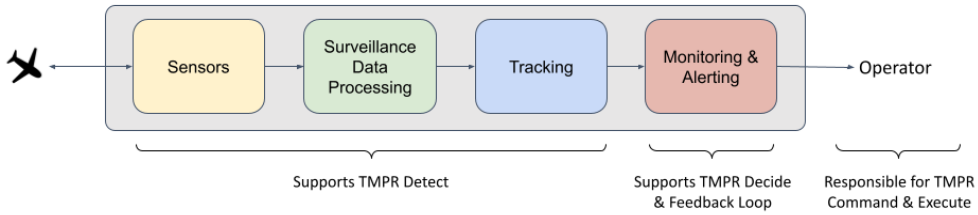


**Figure 2.6:** Simplified TCDASS componentry

There are four primary functions, although not all of them are required for all TCDASS Service Levels:

- **Sensors:** Sensors detect manned aircraft.[5] There are many possible types of sensors, but they generally fall into three types:
  - independent or primary, which detect aircraft with no assistance from the aircraft (e.g., primary radar, LIDAR, optical, acoustic);
  - cooperative or secondary, which detect aircraft with assistance from the aircraft (e.g., secondary radar);
  - and dependent, which are passive sensors that depend on the aircraft to provide location and identification information (e.g., ADS-B, ADS-A/C, FLARM).
- **Surveillance Data Processing:** Depending on the sensor type, a variety of functions may need to be performed on surveillance data to render it suitable for Tracking purposes. These may include forms of signal validation, filtering and other algorithmic processes.
- **Tracking:** The processing of surveillance data to associate plots with a particular target, establish a heading, speed, and altitude (if available) for the target, and project the next location of the target. Aircraft tracking information for the TCDASS can be provided from a single sensor, a network of sensors, or data correlated from many different sources. The resulting data, commonly referred to as tracks, is a primary input to the Monitoring & Alerting component and also enables a higher level of information on a traffic situation display.
- **Monitoring & Alerting:** Uses knowledge of the nominal or off-nominal operational intent of a UA and the track for each manned aircraft in the Declaration Volume to determine if a UA/manned aircraft pair represents a potential tactical conflict. Alerts are generated to the Operator for each potential tactical conflict. Because this component continually monitors the UA/manned aircraft pairs, it also is able to provide the feedback loop to the Operator to indicate whether Command and Execute elements of the TMPR have successfully resolved a conflict. (A lower level of feedback loop capability can also be achieved using a traffic situation display provided by TMPR Detect.)

The objective of the TCDASS is not to provide a complete, turn-key DAA solution to the Operator. However, it does provide building blocks on which DAA capabilities can be constructed. This can

[5] Future versions of this Annex may describe how to use technologies for the detection and tracking of unmanned aircraft

be a significant benefit for Operators from cost and time perspectives. For example, establishing a surveillance capability can be expensive and time consuming.

Operators can leverage the TCDASS to meet the **Detect** and **Feedback Loop** requirements of their DAA solution.

Operators may also choose to have the TCDASS provide alerts when nearby traffic poses a collision risk, partially addressing the **Decide** requirements of their DAA solution.

The responsibility to fulfill the **Command** and **Execute** TMPR will continue to lie with the Operator, since the TCDASS typically does not control vehicles.

The Operator remains responsible, in the Comprehensive Safety Portfolio, for documenting how the TCDASS connects or interfaces with the other elements of the DAA solution. This includes accounting for requirements imposed by the Competent Authority, such as to Remain Well Clear and/or to avoid Near Midair Collisions (NMAC).[6] While Annex D specifies risk ratios for the overall performance of the DAA system (including the performance of TCDASS), the Competent Authority may require adherence to other metrics.

### 2.4.2 Volumes used by the TCDASS

There are three nested volumes that are relevant to the TCDASS, as depicted in Figure 2.7. Terminology for these volumes has been adapted from RTCA DO-381, MOPS for Ground-Based Surveillance Systems. The relationship and sizing between volumes may be determined through mathematical equations as defined in industry standards. These equations take into account:

- some elements which are the Service Provider's responsibility, such as the underlying surveillance coverage and performance;
- as well as elements that are the Operator's responsibility, such as properly accounting for their system's latencies in responding to a potential tactical conflict with sufficient time to maintain the closest minimum proximity prescribed by the Competent Authority.

Note that while industry standards such as RTCA DO-381 allow for these volumes to be sized in more than one way, this Annex assumes that an "outside-in" methodology is used. This is because Operators are assumed not to have the ability to compel Service Providers to add surveillance sensors to meet individual Operator needs. Rather, Service Providers will provide coverage in a given region, and it is the Operator's responsibility, as further described below, to ensure that their Operational Volume fits within the Service Provider's described coverage area.



[6] In industry standards, Remain Well Clear may have different definitions based on the characteristics of the UA and/or the operating environment. NMAC is commonly defined as two aircraft within 500 feet laterally and ±100 feet vertically. The Competent Authority may use different definitions than these.

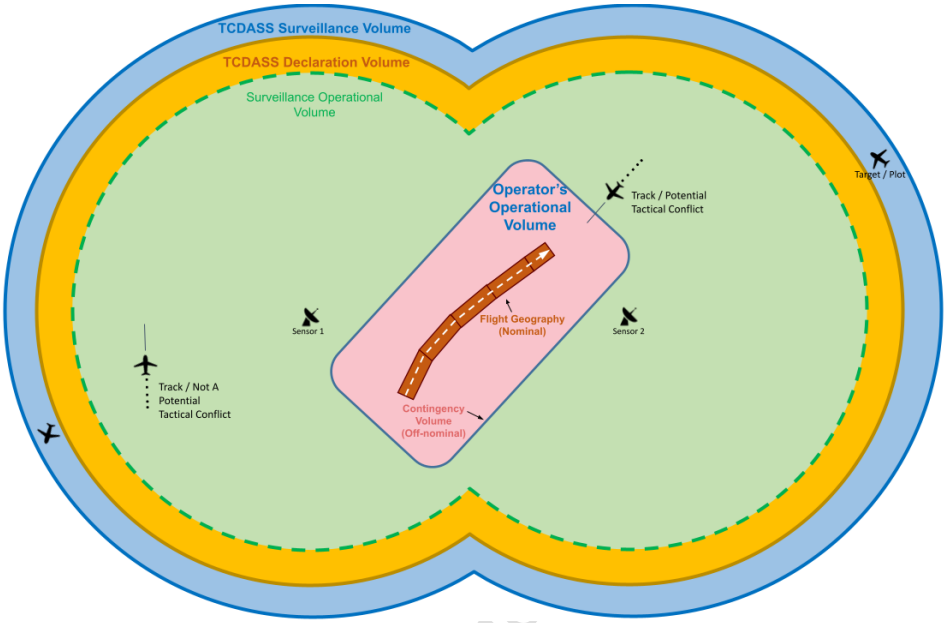


**Figure 2.7**: Notional plan view of volumes relevant to the TCDASS (not to scale)[7]

The outermost region is the TCDASS **Surveillance Volume**. This represents the area in which one or more of the sensors used by TCDASS can detect a target. The size and shape of the Surveillance Volume represents the union of all coverage provided by the underlying surveillance sensors. It is specific to the TCDASS, not to the Operator's performance characteristics. Depending on the underlying sensor technology and subsequent processing steps, it may take some amount of time for surveillance systems to determine that an observed set of targets correspond to the same object (that is, an aircraft) and that they are not a result of ground clutter, birds, or other spurious effects.

The next region, which lies within the TCDASS Surveillance Volume, is the **Declaration Volume.**[8] The TCDASS is responsible for defining the extents of the Declaration Volume, since these are determined by the performance of the TCDASS's surveillance systems, and the amount of time required to resolve targets into aircraft tracks that meet the specified performance requirements for the Declaration Volume. When the TCDASS uses more than one surveillance sensor, the Declaration Volume that is provided to the Operator is the union of the Declaration Volumes of all underlying sensors.

[7] Distances between volumes are determined by mathematical equations that consider system latencies and expected velocities of potential tactical conflicts. The Operator's Operational Volume is depicted as a rounded rectangle for illustrative purposes, and may take on other shapes based on the specifics of the Operator's Flight Geography and ground risk buffer.

[8] Annex D refers to this as the detection volume. The decision has been made in this document to use Declaration Volume, as it aligns with terminology in industry standards, such as RTCA DO-381.

DO-381 defines a 3rd volume, referred to as the Operational Volume and denoted by the green dashed line. This is labeled in Figure 2.7 as the Surveillance Operational Volume to distinguish it from the Operator's Operational Volume. To reduce confusion, the remainder of this document uses Surveillance OV to refer to the innermost dashed line, while Operational Volume maintains the conventional SORA definition. The Surveillance OV is always contained within the Declaration Volume, and represents the maximum area in which an Operator could conduct an operation and safely utilize the TCDASS, accounting for the coverage and tracking characteristics of the TCDASS, the performance of the UA, the time for the UA to perform DAA maneuvers, and velocities and other characteristics of the unmanned aircraft. The Surveillance OV is included to maintain consistency with DO-381 and shows the theoretical limits of where operations can take place and be fully supported by the TCDASS. However, it is not required to satisfy the requirements of Annex H. To satisfy the requirements of Annex H, the Operator needs only to show that their operation-specific Operational Volume (represented by the red volume in center of Figure 2.7) is supported by the TCDASS.

*Note:* The operation-specific Operational Volume also accounts for SORA air risk and ground risk considerations. In addition, in this context, it must also account for the coverage and tracking characteristics of the TCDASS, the performance of the UA, and velocities and other characteristics of the unmanned aircraft, so that there is sufficient time for the DAA solution to meet its mitigation requirements against potential conflict aircraft.

*Note:* Figure 2.7 implies homogenous coverage and tracking performance across the whole area, but in practice there may be gaps in coverage due to terrain/obstacles. Additionally, the dimensions of the Declaration Volume and the Surveillance OV will vary in practice based on characteristics of the manned aircraft, such as closure rate and detectability (e.g. radar cross-section).

The Operator is responsible for ensuring that their Operational Volume fits within the Declaration Volume with sufficient horizontal and vertical distance to account for the time to perform the DAA maneuvers.

### 2.4.3 Division of Responsibility at Each Service Level

The TCDASS consists of the following capabilities, depending on service level:

- Provide a definition of the declaration volumes, and their associated performance. This includes advising the Operator of regions where there is no surveillance coverage due to terrain or other factors.
- Provide potential tactical conflict detection capability in a given declaration volume. The TCDASS may need to adhere to one or more standards based on the underlying sensor network.
- Provide tracks of manned aircraft in a given declaration volume.
- Provide a minimum set of alerting capabilities, as determined by the service level.
- Support display interfaces for use by the human Operator, if required by the Operator's Comprehensive Safety Portfolio.

A TCDASS with Service Level 1 capabilities satisfies the Detect TMPR for operations within ARC-b airspace.

At Service Level 2, in addition to the capabilities of a Service Level 1, the TCDASS also provides a minimum set of alerting capabilities to the Operator, which can help meet the Decide requirements in the Operator's Safety Portfolio, in ARC-b airspace. This capability requires the Operator to provide additional information to the TCDASS before and/or during the mission. This can be achieved in a number of ways, such as:

- Example 1: The Operator transmits their vehicle's position and quality metrics to the TCDASS during flight. The Operator also indicates the total time required to Command and Execute in response to an alert of the potential tactical conflict. The TCDASS uses this information to continuously monitor and prioritize potential tactical conflicts in the declaration volume, sending alerts with enough advance notice that the Operator has time to respond and avoid a manned aircraft encounter.
- Example 2: The Operator notifies the TCDASS of the intended Operational Volume. The TCDASS does not know the exact position of the vehicle during flight, so alerts are based on the proximity of a potential tactical conflict to the nearest point of the Operational Volume, even if the Operator's UA is not near that point. This could result in a higher number of alerts requiring a response compared with the first example. But that may be acceptable for Operators who do not have a means to provide ownship tracking information (e.g. telemetry) to the TCDASS. Under this concept, the UA does not maneuver to avoid the potential tactical conflict, but rather flies to a predetermined safe state, such as a landing zone or low hover.

A TCDASS with Service Level 3 capabilities satisfies the Detect TMPR for operations within ARC-c airspace.

**Table 2.3**: TCDASS Integrity, Assurance, and Responsibilities

| | | Service Provider Responsibilities | | Operator Responsibilities | |
|---|---|---|---|---|---|
| | | **Integrity** | **Assurance** | **Integrity** | **Assurance** |
| **Criterion #1 (Declaration Volume)** | **Service Level 1 (Low)** | • Provide a definition of the Declaration Volume to the Operator.<br>• Document the extent of the Surveillance Volume | The Service Provider declares that the Surveillance and Declaration Volumes are defined correctly | The Operator defines the Operational Volume to fit within the Declaration Volume, and with sufficient horizontal and vertical distances to account for all latencies and maneuvering time in the DAA solution. | The Operator declares that the Operating Volume is defined correctly. |
| | **Service Level 2 (Med)** | | The Service Provider has supporting evidence that the Surveillance and Declaration Volumes are defined correctly, and that the service complies with applicable standards. This is typically done by testing, analysis, simulation, inspection, design review or through operational experience. | | The Operator has supporting evidence that the Operational Volume is defined correctly, in accordance with applicable standards. This is typically done by testing, analysis, simulation, inspection, design review or through operational experience. |
| | **Service Level 3 (High)** | | A third party validates that the Surveillance and Declaration | | A third party validates that the Operational Volume is defined correctly. |

| | | | | | |
|---|---|---|---|---|---|
| | | | Volumes are defined correctly | | |
| **Criterion #2 (Detect Function)** | **Service Level 1 (Low)** | • Provide track information about aircraft in the Declaration Volume.<br>• Coverage is provided in ARC-b airspace.<br>• The Service Provider issues alerts when normal functionality is not being provided. | The Service Provider declares that the required level of integrity has been achieved, and that the service complies with applicable standards. | • The Operator provides the Operational Volume to the Service Provider.<br>• The Operator verifies that the Operational Volume is within the surveillance & declaration volumes. | The Operator declares that the DAA system meets the required system-level risk ratio. |
| | **Service Level 2 (Med)** | | The Service Provider has supporting evidence that the required level of integrity is achieved, and that the service complies with applicable standards. This is typically done by testing, analysis, simulation, inspection, design review or through operational experience. | | System testing demonstrates that the DAA system meets the required system-level risk ratio.<br><br>The Operator takes appropriate actions if real-time performance could lead to the loss of control of the operation. |
| | **Service Level 3 (High)** | Same as for Service Levels 1 and 2, but the TCDASS is provided in ARC-b or ARC-c airspaces | The functionality of the Service Provider has been validated by a competent third party. | | Same as for Service Level 2. In addition, a third party validates that the DAA system meets the required system-level risk ratio. |
| **Criterion #3 (Decide Function)** | **Service Level 1 (Low)** | N/A | N/A | N/A | N/A |
| | **Service Level 2 (Med)** | Provide a minimum set of alerting capabilities (TMPR integrity requirements for ARC-b) | The Service Provider has supporting evidence that the required level of integrity is achieved, and that the service complies with applicable standards. This is typically done by testing, analysis, simulation, inspection, design review or through operational experience. | The Operator provides position information, including quality metrics, if applicable. The Operator also provides all system, command and maneuvering latencies to the Service Provider.<br><br>The Operator provides a documented deconfliction scheme in accordance with Annex D, Table 1, and including procedures for prioritizing and responding to multiple simultaneous threats. | The Operator has a means to monitor externally provided services which affect flight critical systems and take appropriate actions if real-time performance could lead to the loss of control of the operation. |
| | **Service Level 3 (High)** | [Reserved] | [Reserved] | [Reserved] | [Reserved] |
| **Criterion #4 (Feedback Loop Function)** | **Service Level 1 (Low)** | Tracks within the declaration volume are provided with a latency and update rate for potential tactical conflict (e.g. position, speed, altitude, track) that | The Service Provider declares that the required level of integrity has been achieved, and that the service complies with applicable standards. | Operator's own latencies, including use of other services and response times, are accounted for. | |

| | | | | | |
|---|---|---|---|---|---|
| | **Service Level 2 (Med)** | support the decision criteria. | The Service Provider has supporting evidence that the required level of integrity is achieved, and that the service complies with applicable standards. This is typically done by testing, analysis, simulation, inspection, design review or through operational experience. | | The Operator has a means to monitor externally provided services which affect flight critical systems and take appropriate actions if real-time performance could lead to the loss of control of the operation. |
| | **Service Level 3 (High)** | | The functionality of the Service Provider has been validated by a competent third party. | The Operator provides an assessment of the aggravated closure rates considering traffic that could reasonably be expected to operate in the area, traffic information update rate and latency, C2 Link latency, aircraft manoeuvrability and performance and sets the thresholds accordingly. | Same as Medium.<br><br>In addition, a competent third party validates the assessment of the closure rates, and that Service Provider-provided data supports the decision criteria |

## 2.5 Training Requirements for use of Safety Services

Training requirements for the UAS remote crew are introduced under Annex E Operational Safety Objectives to address requirements for ensuring an Operator and remote crew are competent at operating the UAS in a safe manner. With respect to an applicants use of services, OSO #VIII specifies the requirements for ensuring the level of performance is adequate for the intended operation, however the introduction of a Service Provider to support an operation allocates responsibilities to the Service Provider and the Operator. Therefore the Operator has an implied responsibility to use the service in an intended manner, as defined through the SLA, and an applicant should ensure that the intended use of the service is included in training material provided to the remote crew. The Service Provider has a responsibility to supply competency-based, theoretical, and/or practical training materials that are appropriate to support operations as defined within limits of the SLA and recommend any applicable proficiency requirements and training recurrences. These requirements have been added to Annex E OSOs related to Remote crew training (OSO#X).

# 3 Service Level Agreements

The Service Level Agreement (SLA) is an important document that provides a delineation of responsibilities between a Service Provider and Operator, and details the functionality, limitations and performance of the service. All applicable SLAs for services the Operator uses should be included as part of the Safety Portfolio. This allows the competent authority clear visibility and traceability into which services are used, the functions they perform, and how they contribute to the overall operational safety. Since an SLA describes the services used, it is important in evaluating that safety mitigations are applied appropriately when using a service. It also allows verification that responsibilities have been correctly allocated, and that there are no *unallocated* responsibilities.

It is the Service Provider's responsibility to contribute substantive details to the SLA that outlines the expected relationship between the Service Provider and the Operator, and identify any other Service Providers or vendors for which their services are dependent upon.[9] The Service Provider should have documented dependencies of any third-party vendor to ensure that any ingested and managed data has clear traceability to its source of origin.

The competent authority may consider standardization of an SLA, or common sections of all SLAs, as part of the onboarding and approval process for a Service Provider. The inclusion of the SLA in the Safety Portfolio allows the competent authority to cross reference the function, performance, and limitations specified in the SLA with the safety mitigations of the operation in which the service is being used. In seeking approval for services from a competent authority, a Service Provider should provide a description of intended use including exceptions and limitations of use, coverage area of services, role and responsibility, etc., for which bound the scope of applicability of the service, and demonstrate how the SLA reflects the use of the service. Other aspects of an SLA, such as service management and support, issue escalation, and service monitoring and arbitration, etc., may be included in the definition of the SLA but not required for assessment by the competent authority.

An SLA will contain a wide variety of information that establishes the expectations between the Operator and the Service Provider, however there is a minimum set of topics that are needed to be reviewed by the competent authority to verify usage of a service in relation to the Safety Portfolio. The subsequent sections capture the minimum required information to be established for each service described in Annex H. The SLA, through its various sections, should ensure that there is sufficient information to satisfy relevant Operational Safety Objectives (OSOs) and relevant cybersecurity obligations under Annex E. In particular, OSO #IV require the Operator to understand the limitations of "external systems," which includes Service Providers, and that the Operator addresses deterioration of external systems in the Safety Portfolio.

For safety services, detailed in Section 2, describe the intended function and associated performance of each service across different service levels. However, there are additional metrics that are necessary to document in an SLA in order to demonstrate compliance with the Operational Safety Objectives. The sections outline key performance metrics that are necessary

[9] Agreements between other Service Providers should be documented in Operational Level Agreements (OLA) and agreements between Service Providers and 3rd party vendors should be documented in Underpinning Contracts (UC).

to be established by the Service Provider in an SLA and reviewed by a competent authority. Each metric has the associated requirements across different Service Levels.

The SLA is used by the Service Provider, Operator, and competent authority at different stages of the approval processes:

- The **Service Provider** should quantify key performance indicators (e.g. performance target) associated with each metric and document that within their SLA.
- As part of the assessment of the Service Provider, the **competent authority** should verify that the SLA reflects the expected performance, function, and limitations of the service as substantiated by the Service Provider.
- When using the service to support a safety function, the **Operator** should include the SLA in their Safety Portfolio such that the competent authority can verify that the expected performance, function, and limitations are adequate for the intended operation, as is required in OSO #VIII.

## 3.1 Ground Risk OPSS SLA Requirements

**Table 3.1:** Ground Risk OPSS SLA Requirements

| Metric | Service Level 1 (SL1) | Service Level 2 (SL2) | Service Level 3 (SL3) |
|---|---|---|---|
| **Security** | ● Service Provider complies with appropriate regulations/provisions for protection of data and personal information. | ● Same as SL1.<br>● In addition, service provider and Operator must specify a security plan for all data that is exchanged. | ● Same as SL2<br>● In addition, data used in real-time calculations must be abstracted so that personal information cannot be inferred or deduced. |
| **[Functional] Performance** | Meets integrity and assurance requirements for each criterion at that service level, as defined in Section 2.2.2. | | |
| **Availability** | Not Applicable | ● Network and system performance expectations, and quality-of-service measures, are specified.<br>● Alerts for lack of availability, degradation of service, etc., are provided.<br>● Flag for availability, display indicator and follow on actions for Operator | ● Same as SL2<br>● In addition, in the event that a service is not available, the Operator has a contingency procedure.<br>Definition of an outage event and contingency procedures. |
| **Usability** | ● Agreed upon data format and geospatial reference.<br>● If a user interface or experience (UI/UX) is provided, the display provides a depiction of the functional performance requirements. | ● Same as SL1.<br>● In addition, if a user interface or experience (UI/UX) is provided, the Operator is required to take specific training -and- follow procedures for error handling. | ● Same as SL2.<br>● In addition, flag for availability, display indicator and follow on actions for Operator |
| **Data Use** | Service Provider and Operator will provide agreed upon data policies that consider:<br>● Data collection,<br>● Data classification,<br>● Intended use of the data<br>● Prohibited practices,<br>● Data sharing,<br>● Data retention and deletion,<br>● Data Accessibility | | |
| **Reliability** | Not Applicable | | The mean time between failures and/or the mean time to repair are specified |
| **Portability** | Constraints on the service are documented.<br>Operator has appropriate hardware/software to use the service. | | |
| **Scalability** | Not Applicable | | Expected/nominal system load is documented and understood by all parties. |
| **Interoperability** | Not Applicable | | |

## 3.2 Air Risk OPSS SLA Requirements

**Table 3.2:** Air Risk OPSS SLA Requirements

| Metric | Service Level 1 (SL1) | Service Level 2 (SL2) | Service Level 3 (SL3) |
|---|---|---|---|
| **Data Protection and Security** | ● Service Provider complies with appropriate regulations/provisions for protection of data and personal information. | ● Same as SL1.<br>● In addition, Service Provider and Operator must specify a security plan for all data that is exchanged. | ● Same as SL2<br>● In addition, data used in real-time calculations must be abstracted so that personal information cannot be inferred or deduced. |
| **[Functional] Performance** | Meets integrity and assurance requirements for each criterion at that service level, as defined in Section 2.4.2. | | |
| **Availability** | Not Applicable | ● Network and system performance expectations, and quality-of-service measures, are specified.<br>● Alerts for lack of availability, degradation of service, etc., are provided.<br>● Flag for availability, display indicator and follow on actions for Operator | ● Same as SL2<br>In addition, in the event that a service is not available, the Operator has a contingency procedure. Definition of an outage event and contingency procedures. |
| **Usability** | ● Agreed upon data format and geospatial reference.<br>● If a user interface or experience (UI/UX) is provided, the display provides a depiction of the functional performance requirements. | ● Same as SL1.<br>● In addition, if a user interface or experience (UI/UX) is provided, the Operator is required to take specific training -and- follow procedures for error handling. | ● Same as SL2.<br>● In addition, flag for availability, display indicator and follow on actions for Operator |
| **Data Use** | Service Provider and Operator will provide agreed upon data policies that consider:<br>● Data collection,<br>● Data classification,<br>● Intended use of the data<br>● Prohibited practices,<br>● Data sharing,<br>● Data retention and deletion,<br>● Data Accessibility | | |
| **Reliability** | Not Applicable | | |
| **Portability** | Constraints on the service are documented.<br>Operator has appropriate hardware/software to use the service. | | |
| **Scalability** | Not Applicable | | Expected/nominal system load is documented and understood by all parties. |

## 3.3 Tactical Conflict Detection and Alerting Safety Service SLA Requirements

**Table 3.3**: TCDASS SLA Requirements[10]

| Metric | Service Level 1 | Service Level 2 | Service Level 3 |
|---|---|---|---|
| **Security** | • Service Provider complies with appropriate regulations/provisions for protection of data and personal information.<br>• Service Provider and Operator must specify a security plan for all data that is exchanged. | | |
| **[Functional] Performance** | Meets integrity and assurance requirements for each criterion at that service level, as defined in Section 2.5.3. | | |
| **Availability** | • Network and system performance expectations, and quality-of-service measures, are specified.<br>• Alerts for lack of availability, degradation of service, etc., are provided.<br>• In the event that a service is not available, the Operator has a contingency procedure.<br>• Definition of an outage event, degraded quality of service and contingency procedures. | | |
| **Usability** | • Agreed upon data format and geospatial reference<br>• If a user interface or experience (UI/UX) is provided, the Operator is required to take specific training -and- follow procedures for error handling.<br>• Flag for availability, display indicator and follow on actions for Operator<br>• Documentation of system attributes and limitations of the provided surveillance feed | | |
| **Data Use** | Service Provider and Operator will provide agreed upon data policies that consider:<br>• Data collection,<br>• Data classification,<br>• Intended use of the data<br>• Prohibited practices,<br>• Data sharing,<br>• Data retention and deletion,<br>• Data Accessibility | | |
| **Reliability** | The mean time between failures and/or the mean time to repair are specified | | |
| **Portability** | • Constraints on the service are documented<br>• Operator has appropriate hardware/software to use the service. | | |
| **Scalability** | • Expected/nominal system load is documented and understood by all parties.<br>• Constraints of the service are documented. | | |
| **Interoperability** | Interface and/or established standard that describes message formats is agreed upon with the Operator | | |



[10] The service level agreement for TCDASS was determined to outline additional requirements for each of the service levels, however initial discussions resulted in the same requirements for all service levels. This mapping was due to the fact that TCDASS is satisfying TMPR functions and each service level is improving the performance and/or addressing an additional TMPR function, therefore all of the service levels maintain a common set of requirements needed for the service level agreement. Future updates to Annex H will re-assess whether additional requirements are needed for each service level.