Development of an Unmanned Aerospace Test Site
U-space Sandbox

Project CACTUS

U-space Sandbox Certification Considerations

September 22, 2023

Prepared by: ANRA Technologies

Table of Contents

1. Introduction

ANRA Technologies, Inc. (ANRA), in partnership with the Tartu Science Park Foundation (TSP) are pleased to submit this document in support of the Development of an Unmanned Aerospace Test Site (U-space Sandbox). The project is called CACTUS, an acronym for "Competent Authority Coordinating Testing in U-space Sandbox." This document satisfies Deliverable 5.5 (U-space Sandbox Certification Considerations).

2. Background

The principles and preliminary procedures of the certification and supervision procedures of the U-space service provider have been described. The business requirements for the USSP and technical requirements for the certification of the provision of the U-space services have also been mapped. The requirements for the competent authority have been prepared in accordance with the platform for certification and supervision in the U-space sandbox, which will allow the automation of the assessment of the U-space provider's compliance with the performance requirements.

3. Principles and Procedures for USSP Certification

Certification strategy

According to the Article 14 of the (EU) Commission Implementing regulation 2021/664, USSPs will hold a certificate issued by the competent authority of the Member State of their principal place of business. USSPs will apply for a certificate through EASA only in the cases in which their principal place of business are established, or reside in a third country or by the demonstration through the applicant business plan that the USSP is planning operations of a pan-EU nature. As part of this matter, EASA will (in any case) conclude MoC with the competent authority of the Member States where the principal place of business is and/or the applicant is planning operations in.

Once received a formal request, the competent authority will first need to send to the applicant the USSP applicant form certificate in order to retrieve the basic information in relation to applicant address and contact data, identification of activity (application for initial approval or for change), identification of service provision (mandatory, optional U-space services, conditions/ limitations), other relevant information, financial estimate request, applicant's declaration and acceptance of the General Conditions and Terms of Payment). The competent authority can refer to the template proposed in the GM1 Article 14(6).

The second step will be focused on organizing a general familiarization meeting with the applicant. The meeting agenda should focus in:

- Confirm the understanding of the applicant use-case (controlled/uncontrolled airspace, type of operations supported, services provided
- Preliminary view of the applicant strategy for the certification (activities, deliverables, set of documents ready)
- Get a preliminary insight on the organization applying for the certification, and the associated level of readiness
- Get information about the industry standards followed (U-space, software, security, etc.)

Once a general understanding of the applicant is achieved, the competent authority will issue a financial estimate, which will include the estimated working hours, and the associated total cost.
It is to be noted that the estimated working hours, and so the associated total cost, will strongly depend on the level of readiness and system maturity of the applicant and of the Competent Authority.

Project plan

The Project plan will define the execution and control stages of the project. The plan should include considerations for risk management, resource management and communications, ensuring to meet the scope, costs and schedule baselines.
The project plan should comprehend:

- GANTT Chart: in order to illustrate the expected work in relation to the time planned for the project. Being the USSP certification a novel process, the project duration at a first instance will be a tentative one.
- Project risk register: in order to identify, track and monitor any risk that might impact the project
- Work breakdown structure: in order to identify the project phases, subprojects, expected milestones and deliverables
- Statement of Work: in order to assign team members responsibilities on deliverables, milestones, and tasks

Documentation requirements

The documentation requirements for USSP certification can be immense, depending on the information already available in the organization. The minimum documentation requirements would include a project plan, the concept of operations, a compliance checklist, documentation pertaining to the management system(s), a business plan, the safety support assessment, documentation on the security management system, documentation describing software assurance practices, emergency management plan, and any documentation pertaining to provision of services compliant with the associated requirements. The documentation submitted to the competent authority is verified and based on the feedback and comments obtained, the organization may have to adjust their documentation to ensure that it is fully compliant with regulatory requirements.

Familiarization meetings

Familiarization meetings between the organization certifying as USSP and the competent authority can be held to obtain further information on the relevant processes and activities. Familiarization meetings can be organized according to the Articles in Regulation (EU) 2021/664 and the associated AMC/GM, for example Article 15(e) on the management system(s), Article 15(1) on the safety support assessment, and Article 15(1)(b) on software assurance. The agenda for the familiarization meetings can be organized according to the topics addressed in the regulatory requirements and associated guidance.

Scope and limitations of the certification

The certificate is valid indefinitely upon certification, as long as the USSP complies with the conditions and limitations stated in the certificate. It is expected that the USSP should provide the four mandatory services and any supporting U-space services, depending on the scope of the certification. The

competent authority verifies that the USSP continues to conform with the requirements, and in the event that the organization ceases to perform its activities, the competent authority must immediately be notified.

4. Business Requirements

Management system

A management system is an essential component of the certification process, and the USSP should ensure that the required technical capacity, operational capacity, and adequate resources are allocated to perform the required tasks.

Quality management system

The management system must address items related to quality management, preferably with an ISO 9001 certificate, to demonstrate that elements pertaining to quality management are integrated in the organization. A quality management system supports organizations in demonstrating their ability to provide products and services that meet statutory and regulatory requirements and ensures customer satisfaction. These include:

- Organizational context, such as determining the strategic direction and scope of the management system, identifying key processes and maintaining the required documentation.
- Leadership, namely determining a quality policy relevant to the organization, and identifying roles, responsibilities and accountabilities.
- Planning, by determining risks and opportunities, and implementing appropriate controls for key processes.
- Support with respect to provision of resources.
- Aspects related to operation, such as design and development of products and services, control of external providers, post-delivery activities, and control of nonconforming products and services.
- Performance evaluation to monitor, measure, analyze and evaluate key elements.
- Continuous improvement of the quality management system, and thereby the overall organization.

Roles, responsibilities, and accountabilities

In the roles, responsibilities, and accountabilities section, it is important to identify personnel who perform a key role in the organization and define their responsibilities. An organigram supports understanding the structure of the organization and identifying key roles. This includes the accountable manager, safety manager, compliance monitoring manager, quality manager, information security manager, and other roles the organization determines as crucial to its functioning.

(Business) Policy

The management system should contain a policy that reflects the activities performed in the organization and it should contain statements that provide proof of compliance with required regulations and standards, commit to continuous improvement of the management system, ensure the

provision of adequate resources, and ensure that the services provided meet the performance requirements, so that safety is not compromised.

Management reviews

The management system should be assessed at periodic intervals, preferably annually through management reviews, to ensure that it is suitable, adequate, and effective, need for changes to the management system, and evaluate opportunities for improvement. Records of all management reviews should be maintained and available for review if required. A management review should address the status of actions from previous management reviews, changes in external and internal issues, nonconformities and corrective actions, monitoring and measurement results, audit results, feedback from interested parties, results of risk assessment and status of risk treatment plan, and opportunities for continual improvement.

Resource management

In the section on provision of resources, an organization should ensure that the infrastructure meets the requirements for the provision of services, and a general description of this must be maintained. The organization must also ensure that personnel have the necessary competencies to execute their responsibilities. The organization should therefore determine the required competencies for the role, provide training, evaluate the results of the training, and maintain the appropriate records. Personnel should also be aware of how their role contributes to the objectives of the management system and how it could impact safety. Communication regarding the management system, its effectiveness, and measures to continuously improve it should be communicated to the personnel in the organization.

Day-to-day operations

The organization must have an operations manual that describes the information pertaining to the provision of services, such as the infrastructure and the procedures that enable the organization to provide these services in alignment with the performance requirements in a safe manner. It should describe the system, stakeholders who interact with the system, associated procedures, how operations may be supported, and the information that is provided to the users interacting with the system. The performance of the system should be measured against the safety targets and objectives set for the organization. If there are activities contracted to another organization, then the contract with these organizations must be available, and depending on whether the contracted organization is certified in accordance with the applicable regulation or not, it will be subject to different controls.

Safety, compliance monitoring, and changes to the functional system

Aspects such as safety reporting, including hazard identification, corrective and preventive actions, and reporting occurrences to the competent authority, safety reviews which would be conducted when changes are made in the provision of services, the organization structure, or when new technology is deployed, and safety surveys, which aim to identify issues in day-to-day procedures and daily operations are a mandatory requirement in the management system. In addition, a safety assessment of the functional system must be conducted, and it should include an identification of the hazards, a risk

analysis, evaluation, and mitigation, and the criteria that demonstrates that the services provided will meet the established safety requirements.

Compliance monitoring is a crucial element, as it provides evidence that the organization is compliant with statutory and regulatory requirements, as well as any applicable policies and standards. Therefore, a compliance monitoring programme should be established, which contains the scope, items to be monitored, a description of the item, relevant procedures, method and frequency of the assessment, as well as an appropriate point of contact. In order to establish the compliance monitoring programme, compliance objectives and requirements should be defined, and the methods of monitoring that would best fit the organization should be determined. Metrics or key performance indicators may be used to assess compliance, which would support in tracking progress, and they should be aligned with the compliance objectives. It is mandatory to maintain appropriate documentation of the compliance assessments, including but not limited to nonconformances, identified issues, and areas of improvement. Corrective actions must be taken to address the issues identified during the assessment and the status of the corrective action must be tracked until resolution. If any potential issues or nonconformities are noted during the assessment, it is recommended that appropriate preventive measures be taken as soon as possible.

The management system should define the scope of the functional system and define a procedure for functional change management, which includes the identification of the change, an impact analysis, planning for the change, engagement with appropriate stakeholders, implementation of the change, and monitoring the effectiveness of the change. Appropriate documentation must be maintained throughout the process, and based on the agreement with the competent authority, either an approval must be obtained or a notification should be provided prior/during the implementation of the change.

Conducting a safety assessment, ensuring appropriate compliance monitoring methods are implemented and identifying and conducting functional change management procedures is the responsibility of the applicant (USSP). However, the competent authority will need to evaluate and agree with the methods proposed and the results of these activities, identify if it satisfies the requirements, and also agree on the criteria for the change management (what can a company change without notifying the competent authority, what should they notify prior to implementation, what should they request approval for prior to implementation). An internal procedure on how these items would be evaluated, the scope, criteria and boundaries that would be required, and expected processes and outputs of these activities would have to be determined by the competent authority.

<u>Record-keeping and amendment of documentation</u>

When documentation pertaining to the management system needs to be modified, an amendment procedure should be established, which states the nature of the amendment, the amendments themselves, the reviewer, approver, and how it will be communicated to the personnel in the organization. Record-keeping is key, and all records must be traceable, accessible, and retrievable throughout the retention period. It is expected that records pertaining to the management system must

be stored for at least five years, USSP records stored for five years, operational data for at least 30 days, and any data that is subject to investigation should be stored until the conclusion of the investigation.

Business plan and financial requirements

The organization that would provide U-space services should have a business plan in place that would demonstrate evidence that the expected costs can be offset by the market prices. AMC1 Article 15(1)(h) states the requirements for the business plan document, namely a market analysis, which could be performed through a PEST, PESTLE, or the Five Forces Model, information on how the performance of the services provided will be improved, financial information and any foreseen changes, and a financial plan that defines how financial feasibility will be ensured. The business plan and financial feasibility should demonstrate that the services can consistently and continuously be provided for a period of 12 months.

5. Technical Requirements

Concept of Operations (ConOps)

The ConOps is a document submitted by the organization to explain the scope and boundaries of the certification. The objective is to define the functional system, provide in-depth information on the use cases, describe relevant processes and procedures pertaining to the organization, and ensure that the assumptions on U-space performance requirements are addressed. The business case and the context for the U-space operational environment characteristics are also described, including the functional system design and description, such as the platform architecture, the external stakeholders and interactions with their systems, and assumptions and constraints associated with the solution.
The ConOps is one of the key documents which will set up the baseline in relation to any other documents and activity produced as part of the USSP certification project.

Software assurance

Software assurance activities comprise of software planning, software development, and integration and verification process. The software planning process defines how the software produced will meet requirements and how the level of confidence can be aligned with the assurance level. The software development process defines activities to design, develop, test, deploy, and maintain software systems to ensure that requirements and quality standards are met. The integration and verification process is the verification and validation of the software to demonstrate evidence that the software quality is assured to meet established requirements.

When conducting software planning activities, the system requirements must be addressed, assurance levels must be defined, and the methods and tools for the activities of each software lifecycle process must be defined. Please, refer to the D5.3 - U-space sandbox Standards and Services in order to retrieve the requirements associated with the software development and assurance. The development activities, revision of software plans, and the software development environment should be defined by identifying the appropriate methods, tools, procedures, programming languages, and hardware to develop, test, control and produce the software product and maintain the lifecycle. Appropriate standards must be

enforced, any errors should be detected and corrective means implemented, prevention and fault tolerance methods to avoid errors should be enforced, and safety features should be included in the software.

In terms of software development, requirements should be gathered, analyzed, documented, and managed to ensure that the software meets the needs and expectations of all stakeholders. During software design, the requirements should be translated into an architectural design that is implementable in a feasible manner and meets the established requirements. The integration combines all components to form a functioning system.

The integration and verification process involves verification of the planning and development processes to ensure that it meets the requirements, adheres to standards, meets stakeholder expectations, and does not contain defects or errors. Test cases are used to analyze the software behavior. Software quality assurance, configuration management, vulnerability assessments, and penetration testing play a key role and are also an integral part of the integration and verification process.

Information security

The organization that is certifying as USSP should have requirements for establishing, implementing, maintaining, and continuously improving their information security management system. This involves identifying the relevant information, assessing risks, establishing security policies and standard operating procedures, implementing controls, monitoring and reviewing security measures, and conducting internal and external audits periodically. Sensitive information should be protected from unauthorized access, misuse, disclosure, alteration, and destruction, and an information security management system addresses security threats by complying with applicable statutory and regulatory requirements such as Regulation (EU) 2023/203 (Part-IS).

The information security management system should have policies and controls in place, including required evidence and compliance documentation. A risk register, which captures risks, their likelihood, impacts, and mitigations should be maintained. Additionally, a corrective action and improvement plan to capture deficiencies, threats, and areas of improvement, and a security incident management register, which contains security incidents that have occurred and tracks the approach to respond, mitigate, and recover from security incidents should be maintained by the organization.

Performance requirements for U-space services

There are performance requirements associated with the provision of U-space services, and this is determined in each U-space airspace based on the airspace risk assessment conducted by the Member State. The performance requirements are related to latency, proximity, deviation thresholds, frequency, and data quality requirements for the mandatory and optional services, as described in GM5 Article 3(4). When a U-space airspace is not yet established, reasonable assumptions can be made, during the collaboration process with the competent authority.

Safety support assessment

The organization should conduct a safety support assessment based on the services it will provide to ensure that it will comply with the established performance requirements, constraints, and safety requirements. The safety assessment could be based on a bowtie model, as shown in Figure 1. The assessment should take failure conditions or hazards into account, factors that contribute to the failure condition, effects of the failure occurring, means to detect the failure, and mitigations to dampen the effects of the failure such as preventive barriers and escalation controls.

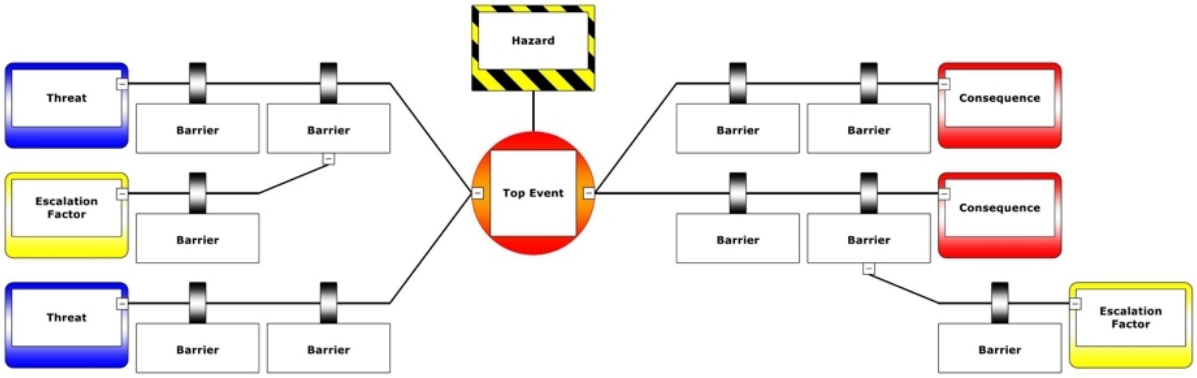

Figure 1: *Bowtie Model (Source)*

6. Automated Testing

The open source InterUSS Platform test suite enables organizations to prove compliance to common industry standards and regulation through ecosystem-wide automated testing capabilities. The automated ecosystem wide testing is used, as the manual approach to demonstrate that the USSP is compliant with the relevant standards is expensive, time consuming, and unscalable. Automated testing ensures that the ecosystem is working in a unified manner with each software release.

The open source automated test suite, developed on the InterUSS Platform, enables USSPs to continuously test their ability to meet the requirements set in the standards as means of compliance that shape the framework for the implementation of U-space services. This approach has been developed for network identification service and UAS flight authorisation service based on the relevant ASTM standards.

Using the automated testing framework, the competent authority can test whether USSPs are meeting the data exchange requirements in the U-space regulatory framework. Access to qualification environments will be granted by the authority through an authorisation service, and no human coordination will be required. The authority will receive a report, which will contain all the information required to assess the ability of the participant to join the production environment. This report will include the test configuration, test target versions, test driver version, request traces, and the list of issues the test driver encountered while submitting requests or inconsistencies in the system during the test sequence.

As major proponents of automated testing, Swiss FOCA has established automation test beds for the Network Identification, UAS Flight Authorization, and Geo-awareness services.
The FAA utilized the Flight Authorization automation test bed as a means of establishing interoperability compliance as part of the UTM Field Test (UFT) program.
In addition, the FAA is in the process of establishing a Key Site in Texas for operational U-Space tests with multiple USSPs. While this program is still being formulated it is clear that the automation test bed will have a prominent role in USSP qualification tests.

For the industry, the test framework would allow USSP applicants to prepare for a check by continuously testing their implementation of the technical standard as part of their software delivery process. Access to the shared interoperability qualification environment is generally granted upon submission of successful results of the test framework when run in the USSPs private staging environment. Once access has been granted, interoperability testing can be achieved in the shared interoperability staging environment with other participants. A successful test allows a participant to deploy its new version in the production environment. To assess the reliability of the distributed system end to end, the test should be run periodically or upon every new software release in the shared interoperability qualification environment. The objective is to highlight the issues related to connectivity, infrastructure, and in general, operations not necessarily directly linked with the software itself, which could go unnoticed on a single point in time experiment.
The consolidated automated testing approach is based on three key artifacts:

- (EU) Commission Implementing Regulation 2021/664 requirements, and associated AMC/GM
- Standards mapping and other performance requirements in relation to the requirements and associated AMC/GM
- Compliance Matrix

These artifacts will provide inputs for the InterUSS Test Suite Documentation which will determine the InterUSS Automated Test Baseline for any applicant.
The InterUSS Test Suite Documentation will provide the list of requirements which can be currently verified using automated testing, including a mapping to the test scenario which tests that requirement.
The InterUSS Automated Test Baseline will serve as an identifier of all aspects of the tests being run (codebase version, test steps, requirements tested) and the configuration used to run them.
Subsequently, the USSPs will then need to set up an Automated Test Environment which will allow for configuring the USSPs' environment specific endpoints and all the other settings required in order for the Automated Test.
At this point the InterUSS Automated Test Runner (the uss_qualifier) can be engaged in order to test the stimuli and the responses of each USSP application.
Finally, an InterUSS Automated Test Report will be created, specific to each time the automated test was run or executed. The Test Report shall include test characteristics associated with the baseline ID, USSP version, date and time.
The tested requirements will be listed as follow:

Package	Requirement	Result	Scenario	Case	Step	Check

E.g. ASTM VXXX	Req XXX	Pass/Failed/ Not tested	E.g. NETRID Interoperability	E.g. interoperability sequence	E.g. try to create subscriptions	E.g. Correctly/ Incorrectly creation

Table 1: *Requirements Test Report*

7. Compliance Matrix

A compliance matrix, similar to the one in the template below, must be developed and provided to the competent authority to ensure that the organization is compliant with the regulatory requirements in an appropriate manner. The compliance matrix must contain the requirements in Regulation (EU) 2021/664, the related AMCs and GMs, and any referenced standards, and it must indicate how these items would be satisfied. Evidence of compliance must be demonstrated through manuals, procedures, tests, or analysis, and the completeness and relevance will be verified by the competent authority.
The Compliance Matrix structure is up to the applicant. One suggested way might be the one shown in Table 2 below.

Requirements list	**Requirements text**	**Compliance statement**	**Strategy and Method for the showing of compliance**	**Evidence/Deliverable**
Complete list of applicable: -Requirements of (EU)2021/664 - AMC - GM (providing technical information, e.g. timings, standards)	Copy the text to support the requirement(s)	Substantiation / rational / limitation	Purely indicative: -[Applicant] will/has develop/ed the “manuals, procedures”, to capture…. -[Applicant] will/has establish/ed the following framework, will/has follow/ed the approach to…. -[Applicant] will/has performed the ‘activities” in order to ….	[Manual] [Procedure] [Design description] [Engineering document] [Analysis] [Inspection] [Test] [As necessary] A combination of evidence may be required.

Table 2: *Compliance Matrix structure example*