INTERNATIONAL STANDARD

ISO 23629-12

First edition
2022-07

UAS traffic management (UTM) —

Part 12: Requirements for UTM service providers

Gestion du trafic d'UAS (UTM) —

Partie 12: Exigences pour les fournisseurs de services UTM

Reference number
ISO 23629-12:2022(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 20 *Aircraft and space vehicles*, Subcommittee SC 16, *Unmanned aircraft systems (UAS)*.

A list of all published or planned parts in the ISO 23629 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

0.1 Background

The functional structure of the UAS traffic management (UTM) services, including respective role of possible services, is standardized in ISO/DIS 23629-5[1].

Conversely, this document focuses on the responsibilities of the UTM service providers (UTM SPs) for the safety, security and compliance monitoring of the provided services, as well as protection of related data and information. A UTM SP contributes to the safety, security and compliance of operations of unmanned aircraft systems (UAS), supporting the fulfilment of the responsibilities of the UAS operator. Operational procedures and requirements for the UAS operator are specified in ISO 21384-3[2].

Although UTM services are established considering the needs of UAS operators, these services also support operations of properly equipped manned air traffic in the respective designated operational coverage (DOC).

One organization may provide several UTM services; and each may have a specific DOC. The DOC may be established by the regulatory authorities, depending on applicable legislation.

0.2 Purpose of the UTM SP integrated management system

The adoption of a management system according to ISO 9001[3] by the UTM SP can enable an organization to provide high quality services. This document provides more specific guidance for safe, secure and efficient air traffic management and air navigation services within the respective DOC.

The purpose of the organisation of the UTM SP is to provide a framework for ensuring safety and security controlling related risks and opportunities. The aim and intended outcomes of the UTM services are to prevent aviation accidents and incidents through the provision of UTM digital information planned in a safe, secure and efficient way conforming to planned ISO 23629-3, while also ensuring sufficient quality and protection of data and information; consequently, it is extremely important for the organization of the UTM SP to identify hazards and minimize safety, security and privacy risks by taking effective prescriptive, reactive, proactive, predictive and inter-organizational measures.

Integration of several functions in the organisation enables reducing the required resources otherwise necessary to implement separate quality, compliance monitoring, safety, security and privacy systems.

An efficient organisation can also assist an UTM SP to fulfil applicable regulatory requirements.

Demonstration of successful implementation of this document can be used by an organization to:

- assure continuous improvement of its safety, security and privacy performance;
- give assurance to UAS operators and other affected stakeholders that an effective organisation is in place;
- give evidence to insurance companies;
- provide an acceptable means of compliance (AMC) with regulatory requirements, when accepted by the competent authority.

Adoption of this document by an UTM SP, however, will not in itself guarantee prevention of aviation-accidents and incidents, in which performance of the UTM services may be one of the causal factors.

The level of detail, the complexity, the extent of documented information and the resources needed to ensure the success of an UTM SP organisation depends on several factors, such as:

- the organization's context (e.g. number of staff, size, geographical scope, culture, legal and regulatory requirements);
- the scope of the provided UTM services;

- the nature, safety criticality and scope of the provided UTM services and the related safety, security and privacy risks.

0.3 Content of this document

This document contains requirements that can be used by an organization to provide safe, secure and efficient UTM services.

This document includes requirements on qualifications and training of personnel, UTM service provision, maintenance and competence of maintenance staff as well as occurrence reporting, safety, security and privacy.

Technical requirements for verification, and validation, of UTM constituents, systems and services (transaction time, availability, continuity, integrity, security, etc.) to comply with safety, security and quality requirements for UTM services are specified in planned ISO 23629-2 or any suitable standard published by an authoritative standard development organisation (SDO).

This document does not include requirements specific to other topics, such as those for quality, occupational health and safety (OH&S), social responsibility, environmental or financial management or use of the electro-magnetic spectrum, though its elements can be aligned or integrated in the organisation of the UTM SP.

An organization that wishes to demonstrate conformity to this document can do so by:

- making a self-determination and self-declaration;
- seeking confirmation of its conformity by parties having an interest in the organization, such as UAS operators using the services provided by the UTM SP;
- seeking confirmation of its self-declaration by an independent, accredited and competent third-party external to the organization; or
- seeking certification of its organisation by an aviation authority, when required by applicable regulations.

NOTE The International Accreditation Forum (IAF) is the world association of conformity assessment accreditation bodies and other bodies interested in conformity assessment in the fields of management systems, products, services, personnel and other similar programmes of conformity assessment. Its primary function is to develop a single worldwide program of conformity assessment which reduces risk for business and its customers by assuring them that accredited certificates can be relied upon. Accreditation assures users of the competence and impartiality of the body accredited. These bodies are referred under different terms in different states, like, e.g. “designees”, “notified bodies”, “qualified entities” or else.

UAS traffic management (UTM) —

Part 12: Requirements for UTM service providers

1 Scope

This document includes compliance monitoring, safety, security, privacy and other organisational requirements for providers in the context of UAS traffic management services.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 21384-4, *Unmanned aircraft systems — Part 4: Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 21384-4 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
constituent
tangible objects such as hardware and intangible objects such as software upon which the provision of *UTM services* (3.9) depends

Note 1 to entry: The definition is adapted from Reference [4].

3.2
designated operational coverage
DOC
geographic volume of airspace within which an *UTM service* (3.9) is available in compliance with designation by competent authorities if applicable, with sufficient performance including availability, continuity, integrity and timeliness and, if applicable, with sufficient radio signal quality and protection from other users of the electromagnetic spectrum

Note 1 to entry: The definition is adapted from Reference [5].

3.3
in-time system-wide safety assurance
ISSA
safety net utilising system-wide information to provide alerting and to trigger mitigation strategies in time to address emerging risks

Note 1 to entry: It is part of proactive safety management.

Note 2 to entry: The definition is adapted from Reference [6].

3.4
operation support service
web-based tools and information provided by a service provider (SP) to an UAS operator or its staff, to support safe and efficient planning and execution of a flight mission, as well as post-flight activities

Note 1 to entry: Operation support services cover a time span much wider than *UTM services* (3.9). Although they support UAS operations, they are neither traffic management nor air navigation services.

3.5
safety-critical UTM service
UTM service (3.9) providing functions that, if lost or degraded, or as a result of incorrect or inadvertent operation, could result in catastrophic consequences

[SOURCE: ISO 14620-1:2018, 3.1.17, modified — The term has been changed from "safety critical function"; "function" has been changed to "UTM service providing functions"; "or critical" has been removed before "consequences". See Reference [7].]

3.6
safety-related UTM service
UTM service (3.9) providing functions that have the potential to contribute to the violation of or achievement of a safety goal, but whose loss of degradation would not in itself produce catastrophic consequences

[SOURCE: ISO 26262-1:2018, 3.1.17, modified — The term has been changed from "safety-related function"; "function" has been changed to "UTM service providing functions"; "but whose loss of degradation would not in itself produce catastrophic consequences" has been added at the end. See Reference [8].]

3.7
UAS traffic management
UTM
set of traffic management and air navigation services (ANS) aiming at safe, secure and efficient integration of multiple manned and unmanned aircraft flying inside the respective *DOC* (3.2) of each service

Note 1 to entry: The definition is adapted from Reference [9] and harmonised with the one in Reference [10].

Note 2 to entry: In accordance with Reference [10], *UTM services* (3.9) initiate when the UAS operator files a request for clearance to enter airspace and terminates when the UA reaches the parking position, the primary propulsion systems are switched off and the operational plan is closed.

[SOURCE: ISO 23629-7:2021, 3.11, modified — Notes 1 and 2 to entry have been added.]

3.8
UTM actor
role played by an *UTM user* (3.12) or *UTM SP* (3.10) or provider of *operation support* (3.4) that interacts with the *UTM subject* (3.11)

Note 1 to entry: An actor models a type of role played by an entity that interacts with the subject (e.g., by exchanging signals and data), but which is external to the subject.

Note 2 to entry: The definition is adapted from ISO/IEC 19501[11].

3.9
UTM service
result of at least one activity necessarily performed at the interface between the *UTM SP)* (3.10) or *operation support* (3.4) provider and the *UTM user* (3.12), which consist in the provisions of digital data and information

Note 1 to entry: The definition is adapted from ISO/IEC 19501[11].

Note 2 to entry: To provide the service, the SP uses facilities, trained and qualified staff, organizational procedures as well as systems and devices executing one or more functions.

3.10
UTM service provider
UTM SP
organization playing the role of an *UTM actor* (3.8) which provides, normally in exchange of a fee, digital data and information to *UTM users* (3.12), which may choose to take advantage from the offered service

Note 1 to entry: The definition is adapted from ISO/IEC 19501[11].

3.11
UTM subject
information technology (IT) entity (including subsystem, component, or even class) representing a software system residing on a physical system or platform, supporting the exchange of digital data and information among several *UTM users* (3.12) and several *UTM SPs* (3.10) or *operation support SPs* (3.4), and to which a set of use cases applies in the *UTM* (3.7) context

Note 1 to entry: The definition is adapted from ISO/IEC 19501[11].

Note 2 to entry: Utilisation of at least one UTM subject is a necessary technical enabler for any *UTM service* (3.9), but it is not a service in itself.

3.12
UTM user
organization or system, which uses digital data and information offered by an *UTM SP* (3.10) to fulfil their mission that is neither an UTM SP nor an *operations support SPs* (3.4)

Note 1 to entry: The definition is adapted from ISO/IEC 19501[11].

Note 2 to entry: The UTM user is an *UTM actor* (3.8).

Note 3 to entry: In addition to UAS operators, a non-exhaustive list of UTM users includes public authorities and civil aviation authorities, law enforcement agencies (for safety, security and privacy), search and rescue, fire brigades and other emergency services, providers of ATM/ANS to manned aviation, operators of aerodromes, vertiports or other facilities supporting take-off/launch or landing/recovery of UAS, UAS manufacturers and owners, insurance companies, ISO certifying bodies and qualified entities, training organizations, general public.

Note 4 to entry: In the digital ecosystem, at least three IT entities are typically under the responsibility of the UAS operator:

a) the unmanned aircraft which during the flight exchanges digital information;

b) the station of the remote pilot, also exchanging digital data with other IT entities, but only when activated; and

c) the workstation of the fleet manager (FM) potentially active full time and used in particular for planning the flight exploiting some of the UTM or operation support services.

4 Abbreviated terms

AIMU	aeronautical information management for UAS
AMC	acceptable means of compliance
ANS	air navigation service(s)
ATM	air traffic management
COMO	compliance monitoring officer
DAL	design assurance level
DPO	data protection officer
DSM	digital surface model

DTM	digital terrain model
FM	fleet manager
HT	head of training
IAF	International Accreditation Forum
IT	information technology
IUEI	intentional unauthorised electronic interaction
OH&S	occupational health and safety
OJT	on-the-job training
SAFO	safety officer
SDO	standard development organisation
SECO	security officer
SLA	service level agreement
SP	service provider
TBO	trajectory-based operations
UAS	unmanned aircraft system
V&V	verification and validation

5 Service provision

5.1 SP key tasks

All providers of the UTM services listed in Annexes A and B and all providers of operation support services listed in Annex C SPs shall establish and apply policies and procedures to ensure that:

a) a risk assessment is conducted for every type of service;

b) all personnel executing safety-related tasks are professionally competent and qualified in compliance with Clause 12;

c) all systems necessary to provide UTM are maintained in accordance with the maintenance programme consistent with the manufacturer's instructions;

d) all activities are conducted according to appropriate checklists;

e) terms of service provision are clearly communicated to users, through conditions to be accepted by the UAS operator or other service user, before registering to benefit from a given service; and

f) service level agreements (SLA) with other SPs or relevant organisations are in place when cooperation has been established.

5.2 Geographical scope

The UTM SP shall define and communicate to potential users the designated operational coverage within which services are available.

5.3 Technical requirements

The UTM SP shall control the accuracy and currency of information originated by the SPs or obtained from external providers, in accordance with:

a) applicable industry standards, including in the series ISO 23629 and those developed by ISO/IEC joint technical committee JTC 1 or those listed in the bibliography to this document;

b) procedures developed by the SP to complement a).

5.4 Interoperability and electromagnetic compatibility

The UTM SP shall implement technical means and procedures with regards to:

a) protocols to exchange information with UTM users and other SPs;

b) control of the interfaces with other UTM SPs, other service providers and UTM users;

c) ensuring that radio transmitting equipment generating minimum harmful interferences to other users of the electromagnetic spectrum.

5.5 Subcontracts

Where contracts exist with third party organization(s), the UTM SP shall be responsible for the conformance of the outsourced services with this document.

6 Safety

6.1 Requirements for all SPs

All UTM and operation support SPs listed in Annexes A, B and C shall:

a) address the structure, responsibilities, processes and procedures that promote and establish an environment and culture of continuing improvement and enhancement of service provision safety;

b) appoint a person as compliance monitoring officer (COMO);

c) appoint a person as safety officer (SAFO);

d) designate the COMO and the SAFO based on professional qualities and, in particular, expert knowledge of laws, regulations and practices on safety of unmanned aviation and the ability to fulfil the tasks, respectively referred to in 6.4 and 6.5;

e) train and qualify personnel on safety management of provided services;

f) establish procedures for prescriptive safety including as a minimum:

   1) monitoring and assessing changes to regulations which can affect service provision;

   2) establish evidence that all applicable regulations are complied with;

g) establish procedures to support reactive safety through:

   1) maintaining records of any service activity for at least three months, or longer taking into account relevant regulations or because the state or other authority competent for the matter has opened an accident or incident investigation;

   2) timely provision of any information required by such an authority;

h) establish procedures for proactive safety including as a minimum:

   1) possibility for staff, users, subcontractors or other partner SPs to report any relevant and perceived safety occurrence;

   2) mandatory reporting of safety occurrences to the competent authority, based on applicable regulations;

   3) voluntary reporting to the competent authority of any additional and relevant observed safety occurrence, in a manner that would allow a further safety analysis by the authority, if deemed appropriate by the latter;

   4) collection of received or originated safety occurrence reports;

5) timely feedback to originators of the report;

6) storage of received or originated safety occurrence reports;

7) protection of related information, in particular identity of the author of the report, according to Clause 11;

8) dissemination of safety information to involved personnel and affected stakeholders;

9) taking decisions, implementing and monitoring effect of corrective actions originated by received reports;

i) establish procedures for interorganizational safety, allowing exchange of safety information with affected stakeholders.

NOTE 1 The COMO or SAFO can be employees of the SP or not.

NOTE 2 A single COMO or single SAFO can perform such a function on behalf of several organisations, providing that no conflict of interest will arise.

NOTE 3 A single physical person can perform both the function of COMO and of SAFO.

6.2 Additional requirements for safety-related UTM SPs

In addition to 6.1, all SP of UTM safety-related services listed in Annex B shall:

a) not change configuration of the systems used for UTM service provision or the procedures thereof, without prior evaluation of the related hazards, considering safety, security and privacy, and emerging risks, complemented by verified implementation of the mitigations stemming from the evaluation;

b) control system configuration, operational procedures and management changes, verifying their compliance with applicable regulations, monitoring actual application of such procedures and maintaining related records for at least two years;

c) establish procedures for predictive safety including as a minimum, safety assessment of any change affecting service provision, which should include;

1) identification of the scope of the change;

2) verification that the foreseen change is compliant with applicable regulations;

3) identification of related hazards;

4) determination of the safety criteria applicable to the change;

5) risk analysis in relation to the harmful effects or improvements in safety related to the change;

6) risk evaluation and, if required, risk mitigation for the change to meet the applicable safety criteria;

7) verification that the change conforms to the scope that was subject to safety assessment, and meets the safety criteria, before the change is put into operation;

8) acquisition of prior approval to implement the change, from the competent authority, taking into account relevant regulations;

9) specification of the monitoring requirements necessary to ensure that the UTM service provision operation continues to meet the safety criteria after the change has been implemented.

NOTE Procedures for managing changes can include analysis, calculations, simulation, laboratory testing, regression testing for software or testing in real environment, as well as distribution of necessary information to service users and additional training for staff.

6.3 Additional requirements for safety-critical UTM SPs

In addition to 6.1 and 6.2, all SP of UTM safety-critical services listed in Annex A shall:

a) establish a manual containing all safety procedures and reporting lines;

b) in the context of prescriptive safety, establish a system of periodical internal audits to ensure continuing compliance with applicable regulations and organization procedures and maintain related internal audit records;

c) in the context of reactive safety, establish procedures for internal safety investigations on significant safety occurrences;

d) as part of the proactive processes for safety, establish ISSA real time monitoring of possible failure conditions, through one or more of the following measures, as appropriate for the provided safety-critical service(s):

   1) architecture for real time data collection and data exchange model with UAS operators and operators of aerodromes, vertiports or other facilities supporting take-off/launch or landing/recovery;

   2) data mining tools and techniques to detect and identify anomalies and precursors to safety threats system-wide, including statistical analysis of collected occurrence reports;

   3) tools and techniques to assess and predict safety margins system-wide to assure air traffic safety;

   4) prognostic decision support tools and techniques capable of supporting real-time safety assurance;

   5) verification and validation (V&V) tools and techniques for assuring the safety of provided UTM services throughout the lifecycle of operational UTM systems, and techniques for supporting the in-time monitoring of safety requirements during operation;

   6) decision support tools and automation for reducing safety risks for normal and abnormal operations;

   7) alerting strategies, protocols or techniques which consider the operational context, as well as the UAS state and intent;

   8) methodologies and tools for integrated prevention, mitigation and recovery plans with information uncertainty and system dynamics in a UAS and in related trajectory-based operations (TBO) environment;

   9) measurement methods and metrics for human-machine team performance and mitigation resolution;

   10) system-level performance models and metrics that include interdependencies and relationships among human and machine system elements.

e) As part of the inter-organizational processes for safety, establish arrangements with other relevant organizations (e.g. UAS operators, aerodrome or vertiport operators) to ensure continuous improvement of the safety of provided services.

The arrangements with other organizations may include inter-organizational teams for joint safety investigation, safety analysis and development of joint corrective action plans.

NOTE The safety manual can be combined with other manuals of the organisation.

6.4 Tasks of the COMO

The SP shall ensure that the COMO receives any instructions regarding the exercise of the tasks in this subclause only from the SP top management or from the competent state authorities or other competent authorities.

The COMO shall not be dismissed or penalized by the SP for performing her or his tasks.

The COMO shall directly report to the highest management level of the SP organization.

The COMO shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, taking into account applicable legislation.

The COMO may fulfil other tasks and duties in the organisation, providing that any such tasks and duties do not result in a conflict of interests. Therefore, the COMO may be responsible, for example, for data protection, safety or security, but not for service provision, maintenance or other activities related to production.

The COMO shall have at least the following tasks:

a) inform and advise the SP top management and the employees who carry out tasks having regulatory compliance implications of their obligations pursuant to applicable regulatory provisions;

b) monitor compliance with applicable legislation, with this document and with the policies of the SP in relation to regulatory provisions, in particular in the context of prescriptive safety management and including the assignment of responsibilities, awareness-raising and training of staff involved in relevant services;

c) manage the related internal audits, if applicable, report the findings to the highest management level in the organization, advice on corrective action plans and monitor implementation of corrective actions;

d) support possible audits or inspections by competent authorities and prepare responses to respective protocol questions;

e) provide advice to the SP top management where requested as regards regulatory compliance;

f) act as the contact point for the authorities on issues relating to regulatory compliance;

g) analyse any information relevant for its task, draw up reports and verify maintenance of documentation listed in Clause 13.

6.5 Tasks of the SAFO

The SP shall ensure that the SAFO receives any instructions regarding the exercise of the tasks in this subclause only from the SP top management or from the competent State authorities or other competent authorities.

The SAFO shall not be dismissed or penalized by the SP for performing her or his tasks.

The SAFO shall directly report to the highest management level of the SP organization.

The SAFO shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, taking into account applicable legislation.

The SAFO may fulfil other tasks and duties in the organisation, providing that any such tasks and duties do not result in a conflict of interests. Therefore, the SAFO may be responsible, for example, for data protection, compliance monitoring or security, but not for service provision, maintenance or other activities related to production.

The SAFO shall have at least the following tasks:

a) compile, update and control the configuration of the safety manual, if applicable;

b) inform and advise the SP top management and the employees who carry out tasks having safety implications of their obligations pursuant to applicable safety provisions;

c) monitor all SP activities for reactive, proactive, predictive and inter-organizational safety in compliance with applicable legislation, with this document and with the policies of the SP in relation to safety, including the assignment of responsibilities, awareness-raising and training of staff involved in safety relevant services;

d) participate to joint safety teams, where established;

e) provide advice to the SP top management where requested as regards any safety matters;

f) cooperate with the national authorities on safety matters, where applicable;

g) act as the contact point for the authorities on issues relating to safety.

7 Security

7.1 Requirements for all SPs

Taking relevant security regulation into consideration, all providers of UTM and of operation support services listed in Annexes A, B and C shall:

a) ensure that their facilities, systems and procedures comply with applicable security legislation, including that covering good repute of personnel;

b) ensure security of their facilities and systems used for provisions of respective services as far as reasonably practicable;

c) ensure that suitable procedures are in place to securely store, exchange and dispose of all data gathered during service provision;

d) ensure that data are not distributed to non-eligible entities;

e) equip the premises, compartment or room where the systems for service provision are operated with a door capable of being locked or with other means to prevent access of unauthorised persons;

f) ensure that this door be closed and locked during operation, except when necessary to permit access and egress by authorised persons;

g) establish means to reasonably prevent unauthorised access, comprising as a minimum means for monitoring the area outside the door to identify persons requesting entry and to detect suspicious behaviour or potential threat;

h) ensure the physical protection of the systems used for provisions of respective services when no personnel are inside the premises, room or compartment;

i) release portable equipment for service provision, only for use to authorised personnel and only for the time necessary;

j) ensure that portable equipment for service provision, when not in use, is stored in a secure place.

NOTE Security of systems includes cyber-security.

While UTM services can be cloud-based, nevertheless the servers have to be somewhere and under responsibility of either the UTM SP maintaining them or through an SLA of the cloud service provider. The latter is not in itself an UTM service provider, but the cloud service provider would be a sub-contractor of the UTM SP, in which case 5.5 applies.

7.2 Additional requirements for safety-related UTM SPs

In addition to 7.1, all SP of safety-related UTM services listed in Annex B shall:

a) address the structure, responsibilities, processes and procedures that promote and establish an environment and culture of continuing improvement and enhancement of service provision security;

b) appoint a person as security officer (SECO);

c) designate the SECO based on professional qualities and, in particular, expert knowledge of laws, regulations and practices on national security, aviation security and cyber-security and the ability to fulfil the tasks referred to in 6.4;

d) train and qualify personnel to effectively recognize and respond to possible acts of unlawful interference against provided services;

e) ensure, directly or through service level agreements (SLA) with UTM communication SPs, that any communication link supporting UTM is secured and assured, in a way proportionate to the related safety, security and privacy risks;

f) establish procedures for checking identity of users before allowing them to access services;

g) deny to unauthorised users the ability to access provided services;

h) establish procedures to report to the competent authority any information on observed security occurrences, in a manner that would allow a further impact analysis by the authority, if appropriate;

i) take into account, if established by the state or other competent authority, geographical zones within which operations of civil UAS are restricted or excluded to address risks pertaining to security.

NOTE 1 Registration is an essential enabler for security and enforcement, but it also contributes to safety, since providing data is essential for other traffic management services, such as tracking.

NOTE 2 The registration process, does not issue any authorisation.

NOTE 3 The SECO can be an employee of the UTM SP or not.

NOTE 4 A single SECO can perform such a function on behalf of several organizations, providing that no conflict of interest will arise.

7.3 Additional requirements for safety-critical UTM SPs

In addition to 7.1 and 7.2, all SP of safety-critical UTM services listed in Annex A shall:

a) establish a security system comprising a threat-based, risk approach under which to assess and control their own security risks, threats and impacts;

b) ensure that the security system includes a comprehensive, transparent and reliable risk policy, focusing at least on the most severe risks to safety-critical UTM services;

c) assess the information systems essential for provision of safety-critical UTM services, against any potential inadvertent or intentional unauthorised electronic interaction (IUEI) security threat and vulnerability that could result in an unsafe condition;

d) ensure that the assessment includes as a minimum:

   1) determination of the security environment for the information security of the UTM service;

   2) identification of the relevant assets or systems;

   3) identification of the attack paths;

    4) assessment of the safety consequences of the security threat to the affected assets;

    5) evaluation, by considering the existing security protection means, of the level of threat that would have an impact on safety;

    6) determination of whether the risks, which are the result of the combination of the severities and the potentiality to attack (or, inversely, the difficulty of attacking), are acceptable:

        i) if they are acceptable, preparation of a justification statement, including the means to maintain the risk at an acceptable level;

        ii) if they are not acceptable:

            a) analysis of the proposed means of mitigation to ensure an acceptable level of safety;

            b) implementation of means of mitigation;

            c) evaluation of the effectiveness of the means of mitigation with respect to the level of risk (combination of the level of threat and severity of the threat condition);

    7) iteration from 6) until all the residual risks are acceptable;

e) establish procedures ensuring that the result of this assessment, after any necessary means of mitigation have been identified, lead to either to a statement that the systems have no identifiable vulnerabilities, or to documented implementation of sufficient mitigation measures;

f) provide, when mitigation measures are necessary, sufficient grounds for evaluating that the residual risk is acceptable;

g) establish procedure to make the documentation on the means of mitigation available in a timely manner to the competent authority when requested by the latter;

h) once the overall security risk has been deemed acceptable, if necessary, develop instructions for personnel and users to maintain the information security risk of the systems or services at an acceptable level, after the entry into service of the system or service or modification thereof.

7.4 Tasks of the SECO

The UTM SP shall ensure that the SECO receives any instructions regarding the exercise of the tasks in this subclause only from the SP top management or from the competent state authorities or other competent authorities.

The SECO shall not be dismissed or penalized by the UTM SP for performing her or his tasks.

The SECO shall directly report to the highest management level of the UTM SP organization.

The SECO shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, taking into account applicable legislation or confidentiality clause in the employment contract.

The SECO may fulfil other tasks and duties in the organisation, providing that any such tasks and duties do not result in a conflict of interests. Therefore, the SECO may be responsible, for example, for compliance monitoring, data protection or safety, but not for service provision, maintenance or other activities related to production.

The SECO shall have at least the following tasks:

a) inform and advise the UTM SP top management and the employees who carry out tasks having security implications of their obligations pursuant to applicable security provisions;

b) monitor compliance with applicable legislation, with this document and with the policies of the UTM SP in relation to security, including the assignment of responsibilities, awareness-raising and training of staff involved in security relevant services, and the related audits;

c) provide advice to the UTM SP top management where requested as regards the security assessment and monitor its performance;

d) cooperate with the national authorities on security matters, where applicable;

e) act as the contact point for the authorities on issues relating to security.

8 Software safety assurance

8.1 Requirements for all SPs

All providers of UTM and operation support services listed in Annexes A, B and C shall ensure that all computer software used in the operation of respective systems is:

a) regularly updated with security patches, with critical level patches released as soon as possible according to the contingency plans;

b) modified by applying security patches only if coming from a verified source or patch source code is reviewed and accepted by SP;

c) accompanied by records of any upgrade or modification.

8.2 Additional requirements for safety-related UTM SPs

In addition to 8.1, all SP of safety-related UTM services listed in Annex B shall:

a) where software modifications are developed without design assurance level (DAL), conduct and obtain results of regression tests, at a minimum, to ensure that the software is effective and safe for operational use;

b) provide users forms and procedures to report any perceived software anomalies;

c) investigate and possibly solve any reported issue;

d) give a written feedback to the author of the report;

e) record all received defect reports and respective closure.

8.3 Additional requirements for safety-critical UTM SPs

In addition to 8.1 and 8.2, all SP of safety-critical UTM services listed in Annex A shall:

a) determine the necessary level of software design assurance (DAL), considering the safety implications of the involved function and, in case the EUROCAE document ED-12C[12] or RTCA DO-278[13] are selected to verify and validate the computer software, choosing among Level A, Level B, Level C, Level D, or Level E for each software module;

b) alternative to a), demonstrate that high level objectives established by competent authorities are answered through documented company processes or through alternative standards for DAL, depending on the criticality of the service and providing the same level of safety;

c) establish records to document that the level (or levels) to which the computer software has been verified and validated have been achieved;

d) if the equipment incorporates more than one software level, incorporate appropriate partitioning of different software levels.

NOTE EUROCAE WG 117 and RTCA SC 240 are jointly working on simpler software requirements for low/medium risk applications.

9 Contingencies

9.1 Requirements for all SPs

All providers of UTM and operation support services listed in Annexes A, B and C shall establish a contingency plan including, as a minimum:

a) define and implement contingency plans in the event of disruption, or potential disruption, of the provided services;

b) the contingency plan shall include handling of:

   1) security incidents including reporting and isolating compromised data or components;

   2) privacy breaches including reporting and isolating compromised data or components;

   3) total system failure or some functionality failures regardless of whether they are technical or operational failures or caused by unexpected situations.

NOTE Each contingency plan is unique and tailored to address the anticipated failures of the specific services provided by the SP.

9.2 Additional requirements for safety-related UTM SPs

In addition to 9.1, all SP of safety-related UTM services listed in Annex B shall:

a) establish a plan for monitoring and detection of service failure, malfunctions or anomalous behaviour which includes a reporting mechanism to other SPs.

b) establish a plan for handling external service malfunctions;

c) manage lost or degraded communications with connected SPs and users.

NOTE 1 Contingencies can be related to failure conditions originated inside the UTM service provision or related to failure conditions related to UAS operations. Only the formers are covered in this document.

NOTE 2 Plans can include methods of bandwidth reduction, buffering, or secondary communication paths.

9.3 Additional requirements for safety-critical UTM SPs

In addition to 9.1 and 9.2, all SP of safety-critical UTM services listed in Annex A shall:

a) include, in respective contingency plans, all applicable items from the following list:

   1) purpose and applicability;

   2) policy inputs;

   3) legal requirements;

   4) roles and responsibilities;

   5) contingency principles (e.g. safety, continuity);

   6) contingency key events (i.e. foreseen contingency situations) and related risks;

   7) relationship with other contingency plans (e.g. ATM);

   8) contingency procedures;

   9) description of the contingency environment; and

10) summary of the operational impacts and analysis of changes.

b) Establish an emergency response plan defining a process, ideally automated, to restore normal operating conditions in the event of a system failure or malfunction; estimated restoration times should be communicated to connected SPs;

c) establish an emergency management plan defining a process, ideally automated, to restore normal operating conditions in the event of a system failure or malfunction; estimated restoration times should be communicated to connected SPs;

a) establish an emergency management plan defining a process, ideally automated, to handle external service malfunctions of services which provide data to the safety-critical service; if the external service malfunction affects the quality or performance of the safety-critical function, the current quality or performance level should be communicated to connected SPs.

NOTE 1 The objective of contingency planning for providers of safety-critical UTM services is to assist in providing safe and orderly flow of UA traffic in the event of disruptions of the UTM system or related supporting services.

NOTE 2 Contingency plans can involve procedural as well as automated steps.

NOTE 3 UTM SPs can use the following process for managing contingencies:

a) recognise the failure;

b) identify the appropriate procedure within the overall contingency plan;

c) initiate measures as per the contingency plan procedure;

d) resume normal operations;

e) assess the effectiveness of the contingency procedure; and

f) update the contingency plan as necessary.

NOTE 4 Contingency plans can involve third party organizations, systems or services.

10 Maintenance

10.1 Requirements for all SPs

All providers of UTM and operation support services listed in Annexes A, B and C shall:

a) ensure that maintenance instructions are available or developed for all the systems essential to provide respective services;

b) such instructions are not contrasting the designer instructions and requirements, where available;

c) the maintenance staff is competent in accordance with Clause 12

d) the maintenance staff use the maintenance instructions while performing maintenance.

10.2 Additional requirements for safety-related UTM SPs

In addition to 10.1, all SP of safety-related UTM services listed in Annex B shall:

a) ensure that all maintenance or change procedures are executed only by personnel having received an authorisation by the UTM SP to carry out the specific types of maintenance or change operations;

b) establish procedures to implement all instructions issued by the manufacturers, designers or developers, to ensure that all systems being operated are kept updated and, where necessary, returned where a recall order is active;

c) implement all applicable safety or telecommunication directives issued by the competent authorities of the state covered by the DOC of a service;

d) organize scheduled maintenance of each system used to provide safety-related UTM services, in accordance with a maintenance programme;

e) use a maintenance log system to record all maintenance conducted and completed on the systems used to provide safety-related UTM services.

10.3 Additional requirements for safety-critical UTM SPs

In addition to 10.1 and 10.2, all SP of safety-critical UTM services listed in Annex A shall:

a) establish a maintenance procedure manual that provides information and procedures relevant to the maintenance facilities, records, instructions, release, tools, material, components, defect deferral, etc.;

b) ensure that after maintenance, modification or update, the affected system is released to service by a competent and responsible person;

c) ensure that a maintenance release is signed only by a staff member who has received a maintenance release authorisation by the UTM SP, for that particular task.

11 Privacy and data protection

11.1 Requirements for all SPs

Taking relevant data protection regulation into consideration, all providers of UTM and operation support services listed in Annexes A, B and C shall ensure that:

a) operations comply with the data privacy regulations/laws;

a) systems are in place to protect data gathered during provisions of respective services as far as reasonably practicable;

b) suitable procedures are in place to securely store or dispose of all data gathered during service provision and to avoid that data are distributed to non-eligible entities.

11.2 Additional requirements for UTM SPs

In addition to 11.1, all SP of safety-critical UTM services and safety-related UTM services listed in Annexes A and B shall:

a) establish policies and procedures for data protection;

b) since the core activities of the UTM SP consist of systematically processing data related to UAS operations on a large scale, appoint a person as data protection officer (DPO) unless a data protection impact assessment demonstrates that a DPO is not necessary;

c) designate the DPO based on professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in 11.3;

d) ensure that the contact details of the DPO are provided to all users and other relevant SPs, when establishing service provision arrangements;

e) ensure that personnel involved in the handling of sensitive data are suitably trained and qualified;

f) where a type of data processing, taking into account the nature, scope, context and purposes of such processing, is likely to result in a high risk to the rights and freedoms of natural persons, prior to the processing, carry out an assessment of the impact of the envisaged data processing operations on the protection of personal data.

NOTE 1 The DPO can be an employee of the UTM SP or not.

NOTE 2 A single DPO can perform such a function on behalf of several organisations, providing that no conflict of interest would arise.

NOTE 3 A single data protection assessment can address a set of similar processing operations that present similar high risks in relation to privacy and data protection.

11.3 Tasks of the DPO

The UTM SP shall ensure that the DPO receives any instructions regarding the exercise of the tasks in this subclause only from the SP top management or from the competent state authorities or other competent authorities.

The DPO shall not be dismissed or penalized by the UTM SP for performing her or his tasks.

The DPO shall directly report to the highest management level of the UTM SP organization.

UAS operators, UTM users or other UTM SPs may contact the DPO with regard to all issues related to processing of their operational, commercial or personal data and to the exercise of their rights under applicable legislation.

The DPO shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, taking into account applicable legislation.

The DPO may fulfil other tasks and duties in the organisation, provided that any such tasks and duties do not result in a conflict of interests. Therefore, the DPO may be responsible, for example, for compliance monitoring, security or safety, but not for service provision, maintenance or other activities related to production.

The DPO shall have at least the following tasks:

a) inform and advise the UTM SP top management and the employees who carry out data processing of their obligations pursuant to applicable data protection provisions;

b) monitor compliance with applicable legislation, with this document and with the policies of the UTM SP in relation to the protection of operational, commercial or personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in data processing operations, and the related audits;

c) provide advice to the UTM SP top management where requested as regards the data protection assessment and monitor its performance;

d) cooperate with the national supervisory authority on data protection, where applicable;

e) act as the contact point for the authorities on issues relating to data processing.

12 Personnel competency

12.1 Requirements for all SPs

All providers of UTM and operation support services listed in Annexes A, B and C shall:

a) use, for the operational and technical tasks related to the services they provide, only suitably trained and qualified personnel.

b) ensure that quantity of personnel is commensurate with the provided services and respective DOC, considering duty time of people and level of automation;

c) establish a policy and procedures to ensure that all personnel executing tasks related to safety, security or privacy within their organisation are competent to discharge respective duties within the limits of their remit;

d) establish and keep up to date records of all relevant qualifications, experience and/or trainings completed by the staff involved in operation of provided services.

12.2 Additional requirements for safety-related UTM SPs

In addition to 12.1, all SP of safety-related UTM services listed in Annex B shall:

a) appoint a person as head of training (HT);

b) ensure independency from the HT position and tasks and duties in the organisation, to avoid conflict of interests;

c) establish an initial training syllabus and competency standard, including theoretical knowledge, practical skill and attitude;

d) include in such a syllabus, for personnel involved in service provision, as a minimum:

   1) legislation and authority requirements on UTM service provision;

   2) requirements and procedures on security and data protection;

   3) systems being operated, respective DOC, functions and users;

   4) data sources and data quality;

   5) contingency and emergency procedures;

e) include in such a syllabus, for personnel involved in system maintenance, as a minimum:

   1) legislation and authority requirements on UTM service provision;

   2) requirements and procedures on security and data protection;

   3) systems being operated, respective DOC, functions and users;

   4) procedures to inspect, check, test or replace components in accordance with the manufacturer's instructions and as appropriate to the service being provided;

   5) tool control procedures;

   6) maintenance reporting procedures;

   7) deferred defect procedures;

   8) power supply and cooling;

   9) software safety assurance.

f) Define duration of initial training and possible on-the-job training (OJT), commensurate with the operational tasks related to the provided services;

g) provide training directly, having established competency requirements for the instructors, or through a suitable external organization;

h) assess the competency of personnel through competent and qualified examiners or assessors, while ensuring that the assessors or examiners have provided no more than 25 % of training to a person, to avoid conflict of interest.

NOTE 1 The HT, instructors, assessors or examiners can be employees of the UTM SP or not.

NOTE 2 A single HT, instructor, assessor or examiner can perform such a function on behalf of several organizations, providing that no conflict of interest will arise.

NOTE 3 The HT can have other functions connected to service provision (e.g. operations or maintenance).

12.3 Additional requirements for safety-critical UTM SPs

In addition to 12.1 and 12.2, all SP of safety-critical UTM services listed in Annex A shall:

a) establish additional training for staff enjoying the privilege of signing release of systems to service after maintenance;

b) establish a programme for recurrent training, appropriate to the complexity of each job position, to ensure that all personnel executing tasks related to safety, security or data protection within their organization remain competent;

c) ensure that such programme includes procedures to evaluate the proficiency of all personnel executing tasks related to safety, security or data protection within their organization, to ensure that they would continue to meet respective competency standards.

13 Manuals, procedures and records

13.1 Requirements for all SPs

The following documents, manuals and information specific to the organization shall be available, in the authentic form, at the location of the provider of the UTM or operation support services listed in Annexes A, B and C:

a) certificate of registration of the legal entity;

b) third party liability insurance certificate(s), if applicable;

c) any certificate for privacy, cyber-security, quality, social responsibility, environment, if available;

d) declarations of conformity, verification or validation of systems and equipment, if applicable;

e) operating manual(s) of such systems and equipment;

f) notices to airmen (NOTAM) and aeronautical information circulars and publications or electronic access to it, where relevant for the provided services;

g) additional geographical information for UAS operations, issued by State having jurisdiction on the DOC, or on behalf of that State, or electronic access to it, where relevant for the provided services;

h) operational procedures and related checklists;

i) contracts and SLAs between the SP and other organizations contributing to service provision or maintenance of the systems, as applicable;

j) training records and qualification of all personnel involved in service provision;

k) records of regulatory compliance activities;

l) occurrence or defect reports and related documents in the context of data protection, security and safety;

m) any other document required by applicable regulations.

As a minimum, operating and maintenance manuals for UTM systems shall be those issued by the original equipment manufacturer.

The documents or parts of manuals or procedures shall be made available to all relevant staff or contractors, as a function of respective duties.

The SP shall establish a system of record-keeping that allows adequate storage and reliable traceability of all activities developed, covering all the elements related to provided services.

The format of the documents or records (i.e. paper or electronic) shall be specified in the SP’s procedures.

Records shall be stored in a manner that ensures protection from damage, alteration and theft, for a period of three months, unless differently determined by the competent authority.

The SP shall ensure, to the extent possible, in the event an aircraft using the provided services became involved in an accident or incident, the preservation of all related records and, if necessary, their retention in safe custody pending their disposition as determined by the competent authority.

13.2 Additional requirements for safety-related UTM SPs

In addition to the documents listed in 13.1, the following documents, manuals and information specific to the organisation, shall be available, in the authentic form, at the location of the provider of safety-related UTM services’ listed in Annex B:

a) radio station licence(s), if applicable;

b) maintenance instructions and procedures;

c) system(s) maintenance logs, including configuration and software;

d) names, qualifications and duties of the person or persons required for service provision;

e) information concerning search and rescue services in the DOC of the provided services;

f) emergency response plan.

13.3 Additional requirements for safety-critical UTM SPs

In addition to the documents listed in 13.1 and 13.2, the following documents, manuals and information specific to the organisation shall be available, in the authentic form, at the location of the provider of safety-critical UTM services’ listed in Annex A:

a) any approval or certification by the competent authority, if applicable, and related terms of approval, specific authorisations and privileges;

b) operations manual amended or revised as necessary to ensure that the information contained therein is kept up to date;

c) maintenance manual containing a description of the maintenance procedures and the procedures for completing and signing a maintenance release;

d) maintenance programme covering the maintenance tasks and the intervals at which these are to be performed, as well as software safety assurance;

e) safety manual and related records.

14 Insurance

All providers of UTM and operation support services listed in Annexes A, B and C, unless they can demonstrate that third party liability is borne by public authorities, shall hold valid insurance coverage, commensurate to their services as well as to number of users and types of supported UAS operations and covering, as a minimum, risks for third parties in the air and on the ground.