Designation: F3548 – 21

Standard Specification for UAS Traffic Management (UTM) UAS Service Supplier (USS) Interoperability[1]

This standard is issued under the fixed designation F3548; the number immediately following the designation indicates the year of original adoption or, in the case of revision, the year of last revision. A number in parentheses indicates the year of last reapproval. A superscript epsilon (ε) indicates an editorial change since the last revision or reapproval.

1. Scope

1.1 This specification is intended to be a global specification providing components that may be used to satisfy requirements expected to be common to many UTM-related regulations. This specification is not intended to comprehensively address all aspects of any particular UTM-related regulation or concept of operations. Similarly, because varying terminology for the same concept is frequently used across different regulations, readers should not expect an exact terminology consistency with any particular UTM-related regulation.

1.2 This version of the specification is focused on strategic aspects of UAS operations, including strategic conflict detection, aggregate conformance of operations to their operational intents, constraint awareness, and situational awareness in the event of nonconforming or contingent operations. The intention is that this specification will evolve to address increasingly complex strategic aspects of UAS operations and potentially certain tactical aspects of UAS operations.

1.3 This specification addresses the performance and interoperability requirements, including associated application programming interfaces (APIs), for a set of UTM roles performed by UAS Service Suppliers (USSs) in support of UAS operations.[2] Roles are groupings of one or more related UTM services. A competent authority may choose to use the roles defined in this specification in establishing the granularity of authorizations granted to a USS. The roles defined in this specification are:

(1) Strategic Coordination, comprising the Strategic Conflict Detection and Aggregate Operational Intent Conformance Monitoring services;

(2) Conformance Monitoring for Situational Awareness (CMSA);

(3) Constraint Management, comprising the Constraint Management service; and

(4) Constraint Processing, comprising the Constraint Processing service.

1.4 Section 4, Conceptual Overview, provides a description of each of the services and roles and includes further discussion on their scope.

1.5 A regulator may choose to require that a USS support a minimum or prescribed set of roles and services and may adopt terminology other than USS for a software system that provides something other than that minimum or prescribed set of roles and services. However, for purposes of this specification, a USS is a system that provides one or more of the UTM services defined in this specification.

1.6 A USS is not required by this specification to perform all roles or implement all defined services, providing business case flexibility for implementers. A typical USS that supports operators in the planning and execution of UAS operations may implement the Strategic Coordination, Constraint Processing, and CMSA roles. (Note that a USS providing CMSA for a UAS operation is required to also provide Strategic Coordination for the operation.) However, other implementations more limited in scope are possible. For example, a USS may implement only the Constraint Management role and be intended for use only by authorized constraint providers; or, a USS may implement only the Constraint Processing role to provide general airspace awareness to users independent of planning UAS flights. USSs may also provide additional, value-added capabilities and still be compliant with this specification as long as the value-added capabilities do not conflict with the services defined in this specification, and the implementation of services defined in this specification conforms to the applicable requirements.

1.7 A USS may also support other UTM roles such as Remote ID and airspace access (for example, the FAA's LAANC), specified in other documents.

1.8 This specification addresses aspects common to all roles and services, such as Discovery and Synchronization Services (DSS), security, auditing, and handling of off-nominal cases (for example, USS or DSS failures).

[1] This specification is under the jurisdiction of ASTM Committee F38 on Unmanned Aircraft Systems and is the direct responsibility of Subcommittee F38.02 on Flight Operations.

Current edition approved Dec. 1, 2021. Published March 2022. DOI: 10.1520/F3548-21.

[2] Many terms describe UTM and UAS Service Suppliers. For example, UTM is referred to as U-Space, and USSs are referred to as U-Space Service Providers (USSPs) in Europe. In the United Kingdom, UTM Service Providers (UTMSP) is used. In Japan, USSs are referred to as UAS Service Providers (UASSPs). Unless otherwise stated, the terms are interchangeable in this specification.

1.9 Additional services or enhancements to the current services will be added to subsequent versions of this specification. Appendix X2, Future Work Items, identifies a set of these items.

1.10 The safety case for this version of the specification, summarized in Appendix X4, is limited to strategic deconfliction, which is accomplished using the services provided by the Strategic Coordination role. This analysis does not constitute a full safety case for any particular operator or set of operations, which will have their own unique factors and variables. It does help operators understand, however, the contribution of using strategic deconfliction to their safety case and what the key variables are in increasing or decreasing the contribution. Using assumptions similar to those documented in Appendix X4, strategic deconfliction reduces the probability of midair collisions by approximately two to three orders of magnitude, with the rate of off-nominal events and participation being the key variables.

1.11 Of particular note, this version of this specification does not establish requirements for fairness or equitable airspace access among UAS operations, but instead includes requirements for the logging of information that will inform future requirements in this area.

1.12 *Usage:*

1.12.1 In a region where participating UAS operators voluntarily agree to or are required by the competent authority to comply with this specification, it enables strategically deconflicted UAS operations as well as situational awareness for operations that may not be required to be strategically deconflicted. This specification is not dependent upon the use of segregated or nonsegregated airspace.

1.12.2 For regions where this specification is required by a competent authority, this specification assumes regulations established by the competent authority (or its delegate) identify any prioritization of operations and whether or not strategic conflicts are allowed between operations of the same priority. For example, it may be legal in some jurisdictions for recreational operations to share airspace and have overlapping operational intents, relying on UAS personnel to coordinate and maintain visual separation; whereas in other jurisdictions, this may not be allowed. The specification takes no position on allowed or disallowed strategic conflicts. Instead it addresses requirements for when conflicts are allowed by regulations (for example, notifications to involved USSs and UAS personnel) and for when conflicts are not allowed (for example, replanning, inability to activate an operation with nonallowed conflicts).

1.12.3 This specification is not intended to address the complete safety case for air collision risk. It provides a mechanism to address one portion of a safety case, specifically the strategic separation of participating UAS from other participating UAS. Other technologies or procedures, outside the scope of this specification, may be required to mitigate air risk with nonparticipating aircraft and to address other aspects of a complete safety case for air collision risk.

1.12.4 Through the use of constraints, this specification also provides awareness of geographically and time-limited airspace information to USS, UAS personnel, or the operator's automation, or combinations thereof. In circumstances where a constraint is used to represent the volume within which a manned operation is planned, it provides a mechanism to address the strategic separation of participating UAS from the manned flight. However, USS responsibility is limited to providing awareness of constraints, and it is the responsibility of the UAS personnel to comply with any regulatory aspect of constraints.

1.13 *Applicability:*

1.13.1 This specification applies to operations conducted in a connected environment, meaning the UAS personnel have access to the USS (typically by means of the internet) and connectivity to the Unmanned Aircraft (UA). This specification anticipates and accommodates limited gaps in connectivity, but does not purport to address operations in locations where persistent connectivity is unavailable.

1.13.2 This specification does not purport to address tactical conflicts between UAS. Notifications and data sharing requirements in this specification associated with Strategic Conflict Detection and Conformance Monitoring for Situational Awareness may be useful in aiding some tactical conflict detection and dynamic rerouting capabilities. However, those capabilities are beyond the scope of this specification, and an implementation cannot assert compliance for tactical conflict detection or dynamic rerouting using this specification.

1.13.3 This specification does not purport to address conflicts between UAS and manned aircraft outside of instances where a manned operation is encapsulated in a constraint.

1.13.4 This specification does not purport to address authorization for UAS to operate in controlled or uncontrolled airspace.

1.13.5 This specification does not purport to address UAS that are not participating in UTM.

1.14 *Relationship to Other International UTM Standards and Specifications:*

1.14.1 It is an objective of this specification to be compatible with certain UTM specifications that address common subject matter and are developed under other standards development organizations (SDOs).

1.14.2 The existence of multiple specifications on the same subject matter can occur when the regulatory environment in a region requires that a necessary specification be developed by a particular SDO. In these cases, ASTM International seeks to establish a cooperation arrangement with the applicable SDO to ensure consistency between the related specifications.

1.14.3 This specification also seeks to support an international audience where differing regulatory requirements can exist. Where practical, this specification accommodates the differing requirements through a superset approach using a variety of techniques such as optional features and features that are configured to support a particular regulatory ruleset.

1.14.4 A summary of related specifications and the techniques used to achieve compatibility is provided in Appendix X3.

1.15 The values stated in SI units are to be regarded as standard.

1.15.1 Units of measurement included in this specification:

cm	centimeters
km	kilometers
m	meters
deg, °	degrees of latitude and longitude, compass direction
s	seconds
Hz	Hertz (frequency)
time	unless otherwise specified, formatted in accordance with IETF RFC 3339

1.16 *Table of Contents:*

1.17 *This standard does not purport to address all of the safety concerns, if any, associated with its use. It is the responsibility of the user of this standard to establish appropriate safety, health, and environmental practices and determine the applicability of regulatory limitations prior to use.*

1.18 *This international standard was developed in accordance with internationally recognized principles on standardization established in the Decision on Principles for the Development of International Standards, Guides and Recommendations issued by the World Trade Organization Technical Barriers to Trade (TBT) Committee.*

2. Referenced Documents

2.1 *ASTM Standards:*[3]

F3060 Terminology for Aircraft

F3341 Terminology for Unmanned Aircraft Systems

F3411 Specification for Remote ID and Tracking

2.2 *EUROCAE Standard:*[4]

EUROCAE ED-269 Minimum Operational Performance Standard for UAS Geo-Fencing

2.3 *European Union (EU) Regulation:*[5]

GDPR General Data Protection Regulation

2.4 *IETC Standards:*[6]

IETF RFC 3339 Date and Time on the Internet: Timestamps[7]

IETF RFC 5905 Network Time Protocol Version 4: Protocol and Algorithms Specification[8]

IETF RFC 7519 JSON Web Token (JWT)[9]

2.5 *ISO/IEC Standards:*[10]

ISO/IEC 9001 Quality management systems — Requirements

ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements

2.6 *OAIC Document:*[11]

APPs The Australian Privacy Principles

3. Terminology

3.1 *Unique and Common Terminology:*

3.1.1 Terminology used in multiple ASTM UAS and aircraft-related standards is defined in F3341, UAS Terminology Standard, and F3060, Aircraft Terminology Standard. Terminology unique to this specification is defined in 3.2.

3.2 *Definitions of Terms Specific to This Standard:*

3.2.1 *3D volume, n*—a volume of airspace defined in terms of latitude, longitude, and altitude.

3.2.2 *4D volume, n*—a 3D volume plus a start and end time for the volume.

3.2.3 *Accepted, n*—one of the operational intent states. See 4.4 for more details.

3.2.4 *Activated, n*—one of the operational intent states. See 4.4 for more details.

3.2.5 *authorized constraint provider, n*—an organization or individual that has been granted the authority to create and manage constraints in a region by a competent authority.

3.2.6 *Aggregate Operational Intent Conformance Monitoring, n*—a USS service that monitors an operator's aggregate conformance with operational intents over time to ensure the target level of safety for strategic coordination is being met. Operators could also implement their own Aggregate Operational Intent Conformance Monitoring capability.

3.2.7 *coordinated operational intent, n*—an operational intent that has been coordinated with other relevant USSs to prevent disallowed conflicts. Operational intents are required to be coordinated prior to transitioning to the Accepted state

[3] For referenced ASTM standards, visit the ASTM website, www.astm.org, or contact ASTM Customer Service at service@astm.org. For *Annual Book of ASTM Standards* volume information, refer to the standard's Document Summary page on the ASTM website.

[4] Available from European Organisation for Civil Aviation Equipment (EUROCAE), 9-23 rue Paul Lafargue, "Le Triangle" building, 93200 Saint-Denis, France, https://www.eurocae.net/.

[5] Available from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

[6] Available from IETF Administration LLC, 1000 N West Street, Suite 1200, Wilmington, DE 19801.

[7] Visit https://datatracker.ietf.org/doc/html/rfc3339.

[8] Visit https://tools.ietf.org/html/rfc5905.

[9] Visit https://tools.ietf.org/html/rfc7519.

[10] Available from International Organization for Standardization (ISO), ISO Central Secretariat, Chemin de Blandonnet 8, CP 401, 1214 Vernier, Geneva, Switzerland, https://www.iso.org.

[11] Available from Office of the Australian Information Commissioner, 175 Pitt Street, Sydney NSW 2000, Australia, https://www.oaic.gov.au/__data/assets/pdf_file/0006/2004/the-australian-privacy-principles.pdf.

and to the Activated state (including transitioning from the Nonconforming state back to the Activated state).

3.2.8 *conflict, n*—a situation where two operational intents intersect both in space and time. For operational intents to intersect both in space and time, at least one 4D volume from each operational intent must intersect. For two 4D volumes to intersect, the spatial dimensions of the 4D volumes must share at least one point and the start/end time range for the two 4D volumes must overlap.

3.2.9 *conformance, n*—a situation where a UA is flying according to its Activated operational intent. A UA flying inside of its Activated operational intent is in conformance. A UA flying outside of its Activated operational intent is nonconforming or contingent.

3.2.10 *Conformance Monitoring for Situational Awareness, n*—a USS role and service that determines whether a UA is in conformance with its operational intent on behalf of the operator or accepts self-reported conformance data from the UAS or operator. The service also initiates the sharing of situational awareness data with relevant USSs when nonconforming or contingent situations occur.

3.2.11 *Contingent, n*—one of the operational intent states. See 4.4 for more details.

3.2.12 *constraint, n*—one or more 4D volumes that inform USSs, UAS personnel, operator's automation systems, or other stakeholders, or combinations thereof, about specific geographically and time-limited airspace information. A constraint may restrict access to airspace for some or all operations, or it may be informational.

3.2.13 *constraint intersection, n*—a situation where an operational intent and a constraint overlap in both space and time. This is similar to operational intent conflicts, but *conflicts* is deliberately not used because a constraint may not restrict access to airspace.

3.2.14 *Constraint Management, n*—a USS service and role that supports the creation, modification, and deletion of constraints, as well as the dissemination of constraint information to other USSs.

3.2.15 *Constraint Processing, n*—a USS service and role that enables the USS to ingest constraint information and relay it to the UAS personnel, operator's automation systems, or other stakeholders, or combinations thereof, for applicable operations.

3.2.16 *discovery, n*—the process of determining the set of USSs with which data exchange is required for some UTM function; discovery is accomplished by means of the discovery and synchronization service (DSS).

3.2.17 *Discovery and Synchronization Service (DSS), n*—a service defined in this specification that enables USSs to discover other USSs with which data exchange is required and to ensure that USSs use current and consistent entity data.

3.2.18 *DSS instance, n*—for availability purposes, multiple synchronized copies of the DSS supporting a DSS region. Each copy is referred to as a DSS instance. USSs can interact with any DSS instance within a pool and switch over to any other instance in the event of a failure.

3.2.19 *DSS pool, n*—a synchronized set of DSS instances where operations may be performed on any instance with the same result, and information may be queried from any instance with the same result. A DSS region will often have a production DSS pool along with one or more test or staging DSS pools.

3.2.20 *DSS region, n*—the geographic area supported by a DSS pool.

3.2.21 *Ended, n*—one of the operational intent states. See 4.4 for more details.

3.2.22 *entity, n*—a generic term referring to types of data that need to be shared between USSs. This specification defines operational intent and constraint entities.

3.2.23 *entity reference, n*—limited information about an entity (including the approximate location and contact details for the managing USS) that is stored in the DSS and supports the discovery process.

3.2.24 *fail-safe, n*—denotes a situation where the failure of a system software or hardware component or interface does not result in an unsafe condition. Note that in a fail-safe situation, a loss of service may occur. (For example, operational intents cannot be activated if the associated USS is down.)

3.2.25 *lowest bound priority status, n*—a priority status value that is lower than the lowest priority bound defined by the regulator for the strategic conflict detection prioritization schema. For example, if the regulator assigns "0" as the lowest priority value for an operation that is subjected to strategic conflict detection prioritization, then a negative integer would be an acceptable value to assign as the *lowest bound priority status*.

3.2.26 *managing USS, n*—the USS responsible for an operational intent from creation (that is, successfully transitioned to the Accepted state) or a constraint, including activities such as making it discoverable through the DSS, providing associated details when requested by other relevant USSs, and making modifications. In the context of Conformance Monitoring for Situational Awareness, the managing USS monitors position reports and operator reports of nonconformance by means of approved methods.

3.2.27 *non-coordinated operational intent, n*—an operational intent that has not been coordinated with other relevant USSs and may contain disallowed conflicts. This situation occurs for operational intents with off-nominal 4D volumes.

3.2.28 *Nonconforming, n*—one of the operational intent states. See 4.4 for more details.

3.2.29 *off-nominal, adj*—in the context of this specification, refers to situations where an operational intent is in the Noncoforming or Contingent states.

3.2.30 *off-nominal 4D volumes, n*—4D volumes that characterize where and when a UA is expected to travel while it is off-nominal. Off-nominal 4D volumes may reflect a specific route of flight when known, or a broader area when a specific route of flight is not known.

3.2.31 *opaque version number (OVN), n*—unique value associated with a version of an entity, updated when the entity

is modified. OVNs are used to ensure that USSs have the current version of entities.

3.2.32 *operational intent, n*—a volume-based representation of the intent for a UAS operation; comprises one or more overlapping or contiguous 4D volumes, where the start time for each volume is the earliest entry time, and the stop time for each volume is the latest exit time. Volumes are constructed based on the performance of the UAS and represent the airspace to which a UA must conform to a sufficient degree to achieve a target level of safety for strategic deconfliction. An operational intent's volumes normally indicate the intent for the operation in the Accepted and Activated states. However, an operational intent is supplemented with off-nominal 4D volumes when in the Nonconforming or Contingent states. Strictly speaking, off-nominal 4D volumes do not represent intent, but the underlying structure of operational intents (4D volumes) and the mechanisms for discovery and notification of relevant USSs and operations makes the operational intent a convenient vehicle for conveying the necessary information in off-nominal situations.

3.2.33 *operator, n*—the person or organization that applies for CAA approval to operate a UAS or who seeks operational approval for types of flight operations prohibited by a CAA for that UAS.

3.2.34 *operator's automation, n*—optional automation used by an operator to handle aspects of UAS operations during the preflight, in-flight, or postflight timeframe that otherwise would be performed by UAS personnel. The scope of functionality is operator-dependent. Operator's automation may interact with a USS instead of UAS personnel.

3.2.35 *position data, n*—information provided by a UAS that describes the location of an unmanned aircraft, including its latitude, longitude, altitude, and the time the unmanned aircraft was at the location.

3.2.36 *relevant operational intent, n*—an operational intent that overlaps or is in close proximity to another operational intent. Close proximity versus strict overlapping is included because the DSS defined in this specification does not determine intersection using the precise 3D extents of operational intents (or constraints), but instead using a coarser representation. The coarser representation results in actual intersections always being detected, but also in the occasional identification of operational intents that are merely close to each other. (This concept also applies to constraints.) The distance that qualifies as in close proximity is not fixed, but depends on the configuration of the DSS airspace representation. See Annex A2 for further detail.

3.2.37 *relevant USSs, n—(a)* USSs that manage operational intents or constraints, or both, that, due to their proximity, must be evaluated by the Strategic Conflict Detection or the Constraint Processing service, or both, of a USS attempting to create or modify an operational intent; *(b)* USSs that manage operational intents that, due to their proximity, are potentially affected by a Nonconforming or Contingent operational intent or a new or modified constraint; or, *(c)* a USS that has established a subscription for operational intents or constraints, or both, in an area where it may not yet manage operational intents.

3.2.38 *Strategic Conflict Detection, n*—a USS service that determines if an operational intent conflicts with other operational intents. The process of detecting conflicts by comparing operational intents. In contrast, tactical conflict detection generally relies on nonstrategic information such as current location, heading, and speed.

3.2.39 *Strategic Conflict Resolution, n*—the process of resolving conflicts through the modification of operational intents. Although there is no absolute time threshold, strategic conflict resolution requires sufficient time before the conflict to generate, coordinate, and implement the modification to the operational intent.

3.2.40 *Strategic Coordination, n*—a USS role comprising the Strategic Conflict Detection and Aggregate Operational Intent Conformance Monitoring services.

3.2.41 *Strategically Coordinated, adj*—refers to an operational intent that has been constructed with awareness of other relevant operational intents and has no disallowed conflicts.

3.2.42 *subscription, n*—a DSS mechanism that allows a USS to be notified and provided the details of any new, modified, or deleted entities in a specified area of interest defined by a 4D volume.

3.2.43 *UAS personnel, n*—refers to any personnel associated with a UAS operation, including the operator, the remote pilot in charge, and other personnel who may perform preflight, in-flight, or postflight activities. This generic reference to personnel is frequently used in order to avoid incorrect assumptions about the activities carried out by any particular role in an operator's organization.

3.2.44 *UAS Service Supplier (USS), n*—for purposes of this specification, a USS is an entity that provides one or more of the UTM services defined in this specification.

3.2.45 *UAS Traffic Management (UTM), n*—a federated set of services operated under regulatory oversight that support safe and compliant UAS operations.

3.2.46 *UAS Zone (alt. UAS Geographical Zone), n*—the terms used in EUROCAE ED-269, Minimum Operational Performance Standard for UAS Geo-Fencing, for what are defined as constraints in this specification. (From ED-269, *a UAS zone is an airspace of defined dimensions, above the land areas or territorial waters of a state, within which a particular restriction or condition for UAS flights applies.*)

3.2.47 *User notification, n*—information provided by a USS to UAS personnel or to an operator's automation system, or both. Because UAS-related concepts of operations can vary widely from operator to operator, this specification does not mandate a particular form for a user notification; possible implementations include messages or graphical indications through a user interface; text messages; email; and system to system messages.

3.2.48 *Unmanned Aircraft System (UAS), n*—composed of unmanned aircraft (UA) and all required on-board subsystems,

payload, control station, other required off-board subsystems, any required launch and recovery equipment, all required crew members, and communication links.

3.2.49 *USS network, n*—the set of USSs operating collaboratively in a region.

3.2.50 *USS role, n*—a grouping of one or more USS Services. USS roles may be used by a competent authority to establish the granularity of authorizations that can be granted to a USS. Roles are also used within this specification to indicate services that should be provided together.

3.2.51 *USS service, n*—a UTM-related function performed by a USS.

3.3 *Acronyms and Abbreviations:*

3.3.1 *3D, adj*—three dimensional

3.3.2 *4D, adj*—four dimensional

3.3.3 *AFIT, n*—Air Force Institute of Technology

3.3.4 *AIRAC, n*—aeronautical information regulation and control

3.3.5 *ANSP, n*—air navigation service provider

3.3.6 *AOI, n*—area of interest

3.3.7 *API, n*—application programming interface

3.3.8 *BVLOS, adj*—beyond visual line of sight

3.3.9 *C2, n*—command and control

3.3.10 *CAA, n*—civil aviation authority

3.3.11 *CMSA, n*—conformance monitoring for situational awareness

3.3.12 *DAA, n*—detect and avoid

3.3.13 *DAR, n*—DSS airspace representation

3.3.14 *DSS, n*—discovery and synchronization service

3.3.15 *EMI, n*—electromagnetic interference

3.3.16 *FMEA, n*—failure modes and effects analysis

3.3.17 *FTE, n*—flight technical error

3.3.18 *ISMS, n*—information security management system

3.3.19 *LAANC, n*—low altitude authorization and notification capability

3.3.20 *MAC, n*—midair collision

3.3.21 *NSE, n*—navigation system error

3.3.22 *OIV, n*—operational intent volume

3.3.23 *OVN, n*—opaque version number

3.3.24 *PBN, n*—performance-based navigation

3.3.25 *PII, n*—personally identifiable information

3.3.26 *SDO, n*—standards development organization

3.3.27 *SMS, n*—safety management system

3.3.28 *TBO, n*—trajectory-based operations

3.3.29 *TLS, n*—target level of safety

3.3.30 *TSE, n*—total system error

3.3.31 *TTL, n*—time to live

3.3.32 *UA, n*—unmanned aircraft

3.3.33 *UAS, n*—unmanned aircraft system

3.3.34 *UASSP, n*—unmanned aircraft system service provider

3.3.35 *USS, n*—UAS service supplier

3.3.36 *USSP, n*—U-Space service provider

3.3.37 *UTM, n*—UAS traffic management

3.3.38 *UTMSP, n*—UTM service provider

3.3.39 *VLOS, adj*—visual line of sight

3.3.40 *YAML, n*—YAML ain't markup language

4. Conceptual Overview

4.1 This section provides a conceptual overview for the services defined in this specification. No requirements are provided in this section.

4.2 *Scope of Standard:*

4.2.1 The scope of this specification is delineated by the dotted purple box in Fig. 1. The four USS roles defined in this specification are identified by bold text: Strategic Coordination, Conformance Monitoring for Situational Awareness, Constraint Management, and Constraint Processing. A USS may support all or a subset of the roles.

4.2.2 The USS indicated by the central, blue rectangle in Fig. 1 contains three roles: Strategic Coordination, Conformance Monitoring for Situational Awareness, and Constraint Processing.

4.2.3 Strategic Coordination is composed of two services: Strategic Conflict Detection and Aggregate Operational Intent Conformance Monitoring.

4.2.4 Strategic Conflict Detection is used to compare operational intents to detect conflicts. It is used in the context of a flight planning or authorization service in which a USS discovers or is informed of relevant operational intents and attempts to construct a conflict-free route for a new or modified operational intent. (A planning or authorization service including conflict resolution is beyond the scope of this specification. Further, it is deliberate that Strategic Conflict Detection detects conflicts rather than resolves conflicts. The manner in which a USS finds a conflict-free route during planning or resolves a conflict that arises does not need to be prescribed and should allow for innovation. There will be cases where a conflict-free route cannot be found. During the preflight period, this results in some operations not being able to be accepted. During flight, this results in situations where tactical avoidance methods or some other form of arbitration are required. These are beyond the scope of this specification.)

4.2.5 Strategic Conflict Detection assumes certain regulations are established by the competent authority (or its delegate) that guide the evaluation and processing of conflicts. These regulations include the identification of priorities of operations and whether or not conflicts are allowed to exist within a given priority level. A lower priority operation must be planned not to conflict with a higher priority operation. Where conflicts are allowed within the same priority level, notifications are provided to the USSs and UAS personnel and/or the operator's automation for both UAS. Where conflicts are not allowed within the same priority level, the first-planned operation is given priority over subsequent operations.

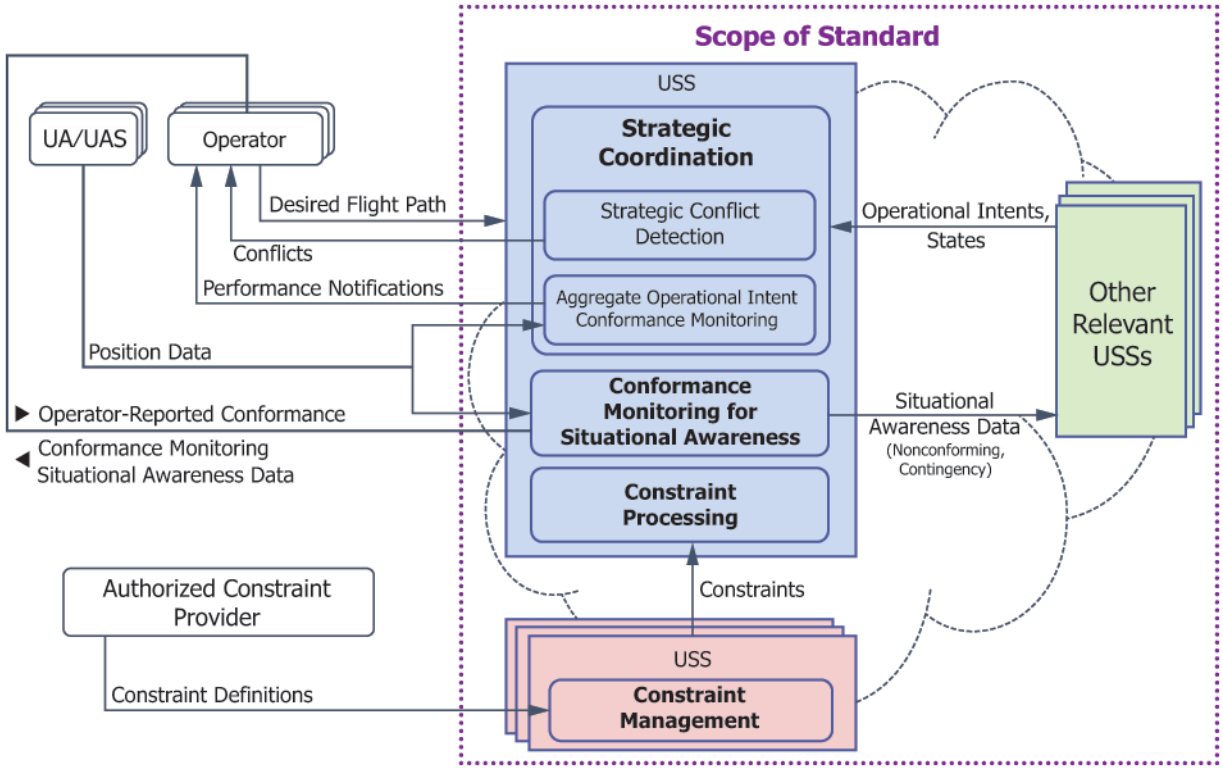

FIG. 1 Scope of Standard

4.2.6 When determining whether an operational intent is conflict free, Strategic Conflict Detection must consider other operational intents in the same vicinity. Some of the operational intents may be managed by other USSs referred to as *other relevant USSs* and denoted by the green box (upper right) in Fig. 1. The operational intents are discovered through a standardized service (the Discovery and Synchronization Service, or DSS), and relevant operational intents are shared through standardized APIs. Mechanisms are also provided in the standardized APIs and DSS to ensure that a USS has the current version of all relevant operational intents.

4.2.7 Aggregate Operational Intent Conformance Monitoring determines if operators are conforming with their operational intents over time. This verification is necessary to ensure that the target level of safety intended to be achieved through strategically deconflicting operational intents is being met. If an operator is chronically not in conformance, it could indicate a problem such as incorrect construction of the operational intents, incorrect characterization of UA performance characteristics, or an issue with some aspect of the operator's operating procedures. Performance notifications are provided to the operator when aggregate conformance is inadequate.

4.2.8 Conformance Monitoring for Situational Awareness is a role and service. Its primary function is to provide situational awareness to relevant USSs and UAS personnel or the operator's automation when a UA is not in conformance or has become contingent. This information can be used by a relevant USS for strategic planning purposes (for example, avoiding airspace where a contingent UA is located). In the future, CMSA may support ground-based tactical conflict avoidance capabilities, but in this version of this specification, any use of CMSA data for tactical purposes is beyond the scope of this specification, and the specification takes no position on the usefulness of the data for those purposes.

4.2.9 There are many possible methods to implement conformance monitoring to detect nonconformance that fall into one of two categories: USS-provided methods and operator-provided methods approved by the competent authority. This specification defines one USS-provided method based on monitoring of position reports from a UAS (position report-based detection of nonconformance). Additional USS-provided methods may be added to future versions of this specification. This specification also allows for the use of approved operator detection methods.

4.2.10 Detection of nonconformance based on position reports is accomplished by comparing ongoing position data for a UA in flight with the associated operational intent. Position data comes from the UAS. The absence of position data is also taken into consideration. If the position data indicate the UA is within the Activated operational intent, the operation is considered in conformance; if the position data indicates the UA is not within the Activated operational intent or is not received over a time threshold, the operation is considered nonconforming.

4.2.11 If an aircraft remains Nonconforming beyond a prescribed time threshold, the operational intent transitions to the Contingent state and cannot return to the Activated state. (States of operations are discussed in greater detail in 4.4.)

4.2.12 Approved methods for operator detection of nonconformance is acceptable and necessary in certain operational environments. For example, some operations may take place in

an environment where the C2 link over which position information would normally be received is unavailable due to EMI or signal blocking (for example, an operation inside an electrical transmission tower, in a tunnel or pipe, or under a bridge). In such cases, visual confirmation of conformance combined with an appropriate operator interface to the USS to communicate conformance or nonconformance could be used. Alternatively, a UA may have approved onboard conformance monitoring capabilities as well as methods to mitigate nonconformance such as autonomous course correction or geofencing, or both, in combination with DAA. In such cases, the operator may only need to communicate failures of the onboard capabilities to the USS. This specification does not specify requirements for all possible operator detection of nonconformance methods or nonconformance mitigation capabilities, but does permit their use provided the operator obtains approval for the method from the competent authority.

4.2.13 Regardless of the method used to detect nonconformance to provide situational awareness to relevant USSs and operators, for both Nonconforming and Contingent cases, the managing USS is required to add off-nominal 4D volumes to the operational intent. Relevant USSs that have operational intents that conflict with or are in close proximity to the updated Nonconforming or Contingent operational intent are notified and can use the off-nominal 4D volumes to inform actions they deem necessary.

4.2.14 In addition, if position report data are available for a nonconforming or contingent UA, relevant USSs may request the data. (This data can only be requested by a relevant USS while the UA is nonconforming or contingent. In some cases, such as a failed C2 link, the position data will not be available.)

4.2.15 The third role shown in the large blue rectangle is Constraint Processing. It is a counterpart to the Constraint Management role shown in the red box at the bottom.

4.2.16 A constraint informs UAS personnel or the operator's automation, or both, about specific geographically and time-limited airspace information. The Constraint Management service allows an authorized constraint provider to create, modify, and delete constraints. (The specification supports one or more USSs performing the Constraint Management role in a region.) Once a constraint is created or modified and made discoverable through the DSS, the associated USS performing the Constraint Management role must also support requests from other relevant USSs for information about the constraint, as well as proactively send a notification to other USSs that have operational intents or subscriptions that intersect the new or modified constraint.

4.2.17 The Constraint Processing service in the central, blue rectangle represents the consumer side of constraints. There are two use cases for Constraint Processing. First, USSs ingest the constraints from the Constraint Management service so that intersections with operational intents can be detected, and the associated 4D information can be communicated to UAS personnel or the operator's automation, or both, to inform operational intent creation, modification, or deletion. Mechanisms are also provided in the standardized APIs and DSS to ensure that a USS has the current version of all relevant constraints. Second, a USS may ingest constraints strictly for the purpose of providing geo-awareness to interested parties.

4.2.18 To achieve interoperability, all interfaces contained in the dotted purple box denoting the scope of the standard are standardized and specified in this document. See Annex A2 and Annex A3 for additional details, including an overview of the interoperability paradigm comprising the DSS and USS peer-to-peer interfaces.

4.2.19 Interfaces that traverse the dotted purple box for communication with systems or people external to the scope of the standard are predominantly left to the discretion of the implementer. For example, this specification does not mandate a particular interface for how position data is received from an aircraft. However, the specification does levy requirements on these interfaces pertaining to basic function, security, and response times.

4.3 *Operational Intents and Off-Nominal 4D Volumes:*

4.3.1 An operational intent is a volume-based representation of a UAS flight used to define the airspace and time bounds intended to contain the flight. An operational intent comprises a set of one or more contiguous or overlapping 4D volumes that define the horizontal and vertical bounds of airspace and the corresponding volume start and end times (which correspond to the earliest entry time and latest exit time, respectively) to which the flight is intended to conform. Operational intents can represent diverse operations including, but not limited to, starting/stopping on the surface and starting/stopping in the air. Operational intents are key inputs to the Strategic Conflict Detection, Aggregate Operational Intent Conformance Monitoring, and CMSA services.

4.3.2 The use of a volume-based representation of UAS flights draws on the ICAO definition of strategic deconfliction as "a service consisting of the arrangement, negotiation and prioritization of intended operational volumes, routes or trajectories of UAS operations to minimize the likelihood of airborne conflicts between operations."[12] A volume-based approach has been widely used in international UTM research, trials, and live operations for several years. Benefits of this approach are discussed further below.

4.3.3 Operational intent 4D volumes are constructed based on the performance of the UAS and represent the airspace to which a UA must conform to a sufficient degree to achieve a target level of safety for strategic deconfliction. The performance of a UA can vary throughout the flight depending on what the UA is doing, such as taking off, operating at cruise altitude, hovering, or landing. The operator may also enhance the performance of the UA in certain locations through augmentations to the operational environment, such as the use of supplemental navigational aids to improve navigation performance. Consequently, the performance-based horizontal and vertical buffering may vary across the 4D volumes comprising an operational intent.

[12] *Unmanned Aircraft Systems Traffic Management (UTM) – A Common Framework with Core Principles for Global Harmonization*, Edition 3, ICAO, September 2020, p. 11, https://www.icao.int/safety/UA/Pages/UTM-Guidance.aspx, *and* https://www.icao.int/safety/UA/Documents/UTM%20Framework%20Edition%203.pdf.

4.3.4 The intention of this specification is that the volumes are constructed (both spatially and temporally) in accordance with the minimum dimensions and time values appropriate for the target level of safety. Volumes that are larger or occupy more time than necessary could adversely impact airspace efficiency.

4.3.5 Operational intents generally fall into one of two categories: area-based or trajectory-based; however, it is possible that one operational intent has both area-based and trajectory-based 4D volumes. An area-based operational intent does not require a desired flight path for the operation, whereas a trajectory-based operational intent does require one. Typically, an area-based operational intent comprises a single volume for the flight duration; however, it is not limited to a single volume. A trajectory-based operational intent consists of a series of volumes that follow the desired flight path and overlap in space and time. An example of an operational intent with both area-based and trajectory-based 4D volumes is an operation that initially proceeds along a trajectory-based segment, enters an area-based 4D volume, and then completes with another trajectory-based segment to the destination.

4.3.6 In order to provide an upper computational bound for operational intents, this specification limits their overall size based on the total number of vertices across the constituent 4D volumes. However, the number of 4D volumes used for an operational intent is not limited or prescribed based on factors such as distance or time in the volume. Implementations must balance the potential for false conflicts that can result from insufficiently granular operational intents with unnecessary computation than can result from overly granular operational intents.

4.3.7 An underlying assumption of trajectory-based operational intents or portions of operational intents is that the desired flight path is generally along the centerline of the volumes, whereas there is no such assumption for an area-based operational intent.

4.3.8 Operational intent boundaries are constructed to buffer the intended operation, whether a path or a volume, such that the aircraft stays within the operational intent boundary for, at least, a specified percentage of the flight time and exits the volume sufficiently infrequently. An example of how to construct and size operational intent boundaries is based on the Total System Error (TSE) of the UAS. For a trajectory-based operational intent, the lateral dimensions are based on the TSE from the centerline of the intended flight trajectory. UAS TSE is a combination of the Path Definition Error (PDE), Flight Technical Error (FTE), and Navigation System Error (NSE), as is illustrated in Fig. 2. Note that this example is similar to the TSE found in Performance Based Navigation (PBN); however, a key difference is that TSE in this standard is a preflight measure, whereas TSE is an in-flight, dynamic measure in PBN.

4.3.9 For UAS operations, the operational intent creation can be composed of errors associated with the ability of the Flight Management System (FMS) to follow a lateral path, environmental factors such as wind, or the ability of a human remote pilot to fly a predefined path or stay within a predefined area. However, the specific build-up of the operational intent size could be different for each UAS or use case, and can also vary by phase of flight (for example, cruise versus vertical ascent or descent versus hover). For an area-based operational intent, the lateral dimensions can be based on the TSE from the outer boundary of the intended flight volume. See Fig. 3 for a depiction of operational intents.

4.3.10 The vertical dimensions of an operational intent can also be based on TSE; however, the vertical TSE is an abstraction of the lateral TSE construction from PBN. The vertical TSE is a function of the ability of the FMS to fly a vertical profile, the accuracy of the altitude sensing equipment, any errors associated with the definition of the vertical profile, and ground elevation uncertainty if the desired altitude references the surface.

4.3.11 The time component of an operational intent is a buffer applied to the entry and exit times of each volume to ensure that the aircraft is contained in at least one volume with the specified performance. The buffer should reflect errors that would result in timing inaccuracies, such as those caused by wind uncertainty and departure time uncertainty, among other factors.

4.3.12 The operational intent creation can include uncertainty associated with path definition, georeferencing error, FMSs, altitude and positioning systems, remote pilot proficiency, departure timing, and weather conditions, if applicable to the specific operation.

4.3.13 Buffering 4D volume-based on the performance of the UA provides significant benefits to operators and the UTM ecosystem. Operators can take advantage of investments in high performance UAs or supplementary navigation aids, or both, in the operational environment, safely allowing more closely spaced operations or varying the required spacing by

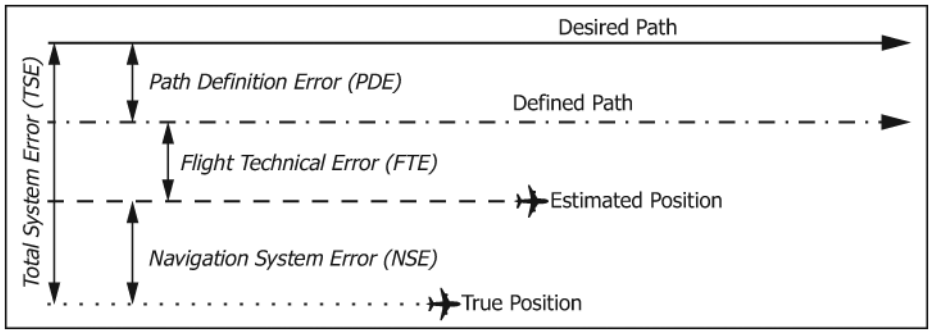

FIG. 2 Derivation of Total System Error

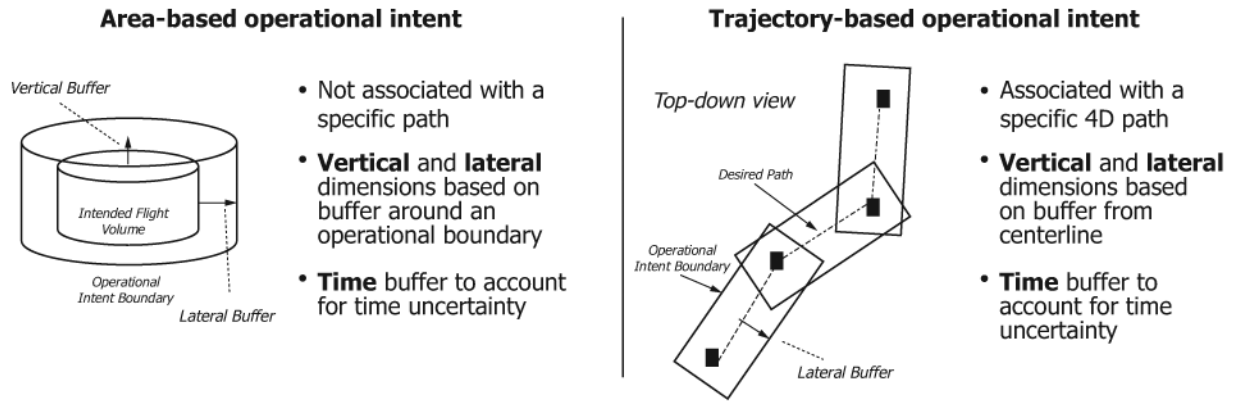

FIG. 3 Operational Intents

phase of flight. This can be critical in certain high-density areas and benefits all operators by making more efficient use of the available airspace.

4.3.14 Another benefit of sharing volume-based operational intents is that only the USS that creates the operational intent is required to have a detailed understanding of the UA performance characteristics and an operator's operational environment. That understanding is reflected in the shared operational intent, allowing every participating USS to have a consistent understanding of an operation and properly consider it in services such as Strategic Conflict Detection. Alternative approaches, such as sharing information analogous to a traditional flight plan and having each USS produce the operational intent, requires every USS to have a detailed and consistent understanding of the performance of every UAS and every operator's operational environment. If all USSs cannot keep pace with this diversity, it can result in some degree of least common denominator logic that prevents an operator from exploiting the performance of a UA or their operational environment, or both, and reduces the overall efficiency of the UTM ecosystem.

4.3.15 Sharing volume-based operational intents also means only the USS that creates it must bear the associated computational load. In addition, operational intents enable straightforward and computationally efficient conflict detection.

4.3.16 Operational intents are supplemented with one or more off-nominal 4D volumes if the operational intent enters the Nonconforming or Contingent states. The intention is that these 4D volumes confidently encompass where a UAS is expected to or may travel during off-nominal situations with minimal consumption of airspace. They can and should be updated to reflect an evolving off-nominal situation.

4.3.17 Off-nominal 4D volumes do not represent actual intent as operators, generally speaking, would never intend for their operations to be Nonconforming or Contingent. Rather, these 4D volumes are used to convey what is actually happening, to the extent possible, in off-nominal situations. They provide the basis for situational awareness for relevant USS and UAS personnel and/or the operator's automation. Associating this information with the operational intent conveniently provides the discovery, notification, and data-sharing mechanisms that are necessary when off-nominal situations arise.

4.3.18 The composition of off-nominal 4D volumes is not precisely prescribed in this specification, and the nature of an off-nominal situation affects the precision with which they can be composed. For example, in a nonconforming situation from which recovery is expected, a single, relatively small 4D volume may be sufficient to bound where the UA is expected to travel until it reestablishes conformance with the operational intent. In some contingency situations, the UA may fly a well-understood route or simply execute a quick landing as part of a contingency procedure, and that route can be characterized relatively precisely with a set of one or more 4D volumes. In other contingency situations, control of the UA may have been lost and the best that can be done is to characterize the remaining range of the UA.

4.3.19 As the density of UAS operations increase over time, it will become increasingly important that off-nominal 4D volumes accurately reflect impacted airspace as much as possible both to minimize disruptions to other operations and to contain the scope of any necessary replanning. For this version of this specification, precision is encouraged; however, the key requirement is that off-nominal 4D volumes encompass where the UAS may travel.

4.4 *Operational Intent States:*

4.4.1 To specify data exchange requirements for USSs to enable the Strategic Conflict Detection and Conformance Monitoring services, this specification uses certain operational intent states. Each operational intent managed by a USS will have a single state at any given time. Data exchange requirements differ depending on the current state of the operational intent.

4.4.2 Operational intent states correspond to nominal or off-nominal circumstances. A key principle is that operational intents in nominal states must be coordinated, meaning they are constructed with awareness of other operations and constraints in the vicinity and have no disallowed conflicts. Operational intents in off-nominal states (Nonconforming or Contingent) are not required to be coordinated and are referred to as non-coordinated operational intents. Coordination is not required in off-nominal states because the need is to communicate to other USSs what is actually happening with the UA. If a UA is able to recover from nonconformance, it must reestablish conformance to a coordinated operational intent to

reenter a nominal state. (This can be the operational intent in effect prior to nonconformance, or an updated but coordinated operational intent.)

4.4.3 Fig. 4 depicts the operational intent states and allowed transitions between states.

4.4.4 The operational intent states are described as follows:

4.4.4.1 *Accepted (nominal)*—This state is set by the USS when the operational intent is created, strategically coordinated, and made available to be shared with relevant USSs. The USS must have received and evaluated the latest airspace information prior to accepting an operational intent.

4.4.4.2 *Activated (nominal)*—To enter this state, UAS personnel or the operator's automation communicates to the managing USS their intent to commence flight operations within the coordinated operational intent. This state indicates that the UAS is within one or more of the operational intent 4D volumes, but may or may not be in flight. An action on the part of UAS personnel or the operator's automation, or UA movement, which may be detected automatically, must occur for the USS to transition the operational intent state from Accepted to Activated.

4.4.4.3 *Nonconforming (off-nominal)*—This state results from the UA being outside the coordinated operational intent while in the Activated state or upon an attempt to activate the operational intent early, late, or with the UA outside the operational intent. To provide situational awareness, off-nominal 4D volumes are added to the operational intent. Off-nominal 4D volumes are created irrespective of any resulting disallowed conflicts, and the resulting operational intent is non-coordinated. Relevant USSs that have operational intents that conflict with or are in close proximity to the non-coordinated operational intent are informed. While the UA is nonconforming, current position data can also be shared with other relevant USSs if available and requested. Other USSs are required to plan around both the nominal and off-nominal volumes of this operational intent. If the expanded operational intent overlaps an existing operation, it is the responsibility of UAS personnel or the operator's automation for the overlapped operation to take actions it deems necessary. This may include replanning to strategically deconflict or performing tactical deconfliction. The operational intent may return to the Activated state, but only after reestablishing a coordinated operational intent, meaning off-nominal 4D volumes have been removed and the UA is in conformance with the operational intent. Transitions between the Activated and Nonconforming states are automatically performed by the USS.

4.4.4.4 *Contingent (off-nominal)*—Entering the Contingent state occurs when a UA can no longer conform to an Activated operational intent. There are mutiple ways an operational intent can transition to the Contingent state, including manual initiation by UAS personnel (could occur from the Accepted, Activated, or Nonconforming states); automated initiation by the operator's automation; automated mechanisms such as the USS determining based on equipment status that control of the UA has been lost; or, as a last resort, automatically when a UA remains in the Nonconforming state beyond a defined time-out period. (A transition to the Contingent state may also be required if a tactical avoidance maneuver cannot be accommodated within the current operational intent and a conflict-free update to the operational intent cannot be devised.) To provide

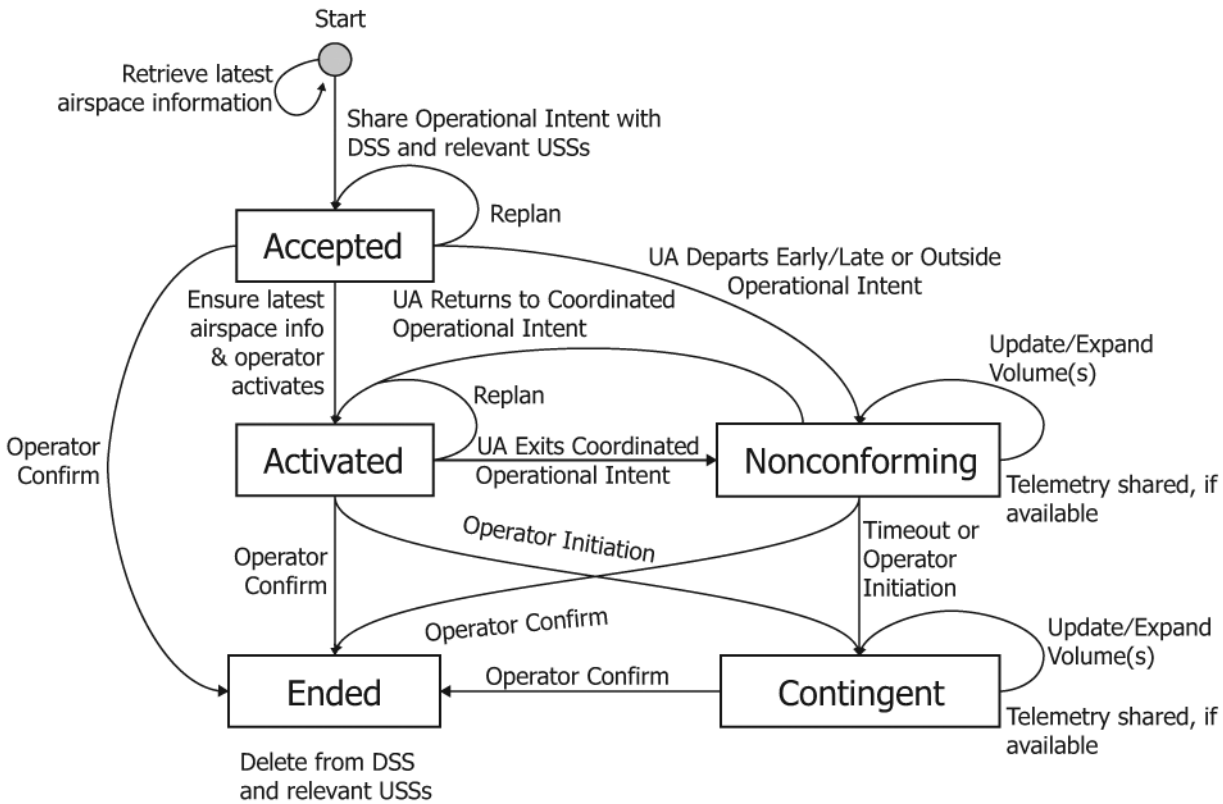

FIG. 4 Operational Intent States Transition Diagram

situational awareness, current operational intent volumes are replaced with one or more off-nominal 4D volumes. (Because an operational intent cannot return from the Contingent state to the Activated state, only off-nominal 4D volumes are appropriate in the Contingent state.). Relevant USSs are notified of the resulting non-coordinated operational intent. While the UA is in the Contingent state, current position data can also be shared with other relevant USSs if available and requested. The Contingent state is a terminal state from which the operation can only transition to the Ended state.

4.4.4.5 *Ended*—This state indicates the UAS is no longer using or will not use the operational intent. Action on the part of USS personnel or the operator's automation, or the USS, which may be automated, must occur to end the operation. When an operational intent is ended, the managing USS must delete the operational intent from the UTM system. Details about operational intents in the ended state are not communicated between USSs.

4.4.5 Figs. 5-7 illustrate representative nominal and off-nominal scenarios, including the resulting progressions through the operational intent states and the use of coordinated versus non-coordinated operational intents.

4.4.6 Fig. 5 illustrates two coordinated operational intents that do not conflict and remain nominal throughout both flights.

4.4.7 The solid line through the center of each operational intent is intended to convey that the UAs in both cases proceed along the intended route of flight, remaining in conformance throughout. Coordinated operational intents are used for the entirety of both flights. The state transition sequence for both operational intents is Accepted > Activated > Ended.

4.4.8 Fig. 6 illustrates the scenario where a UA temporarily goes out of conformance (off-nominal) but is able to correct the situation and return to a nominal state.

4.4.9 At point 1, the UA exits Operational Intent A and is transitioned to the Nonconforming state. The managing USS adds an off-nominal 4D volume to the operational intent (represented by the yellow rectangle) that encompasses the anticipated area of nonconformance. The expected route back to conformance is indicated by the dashed, yellow line. This update to Operational Intent A is non-coordinated and results in a conflict with Operational Intent B. At point 2, because Operational Intent B is in close proximity to Operational Intent A, its managing USS is notified of Operational Intent A's nonconformance. Detecting the conflict, the managing USS for Operational Intent B takes actions it deems necessary and can request position information for Operational Intent A to assist in the process. (Position data may or may not be available.) At point 3, the UA reestablishes conformance with the original operational intent. The managing USS for Operational Intent A can now remove the off-nominal 4D volume (the yellow rectangle) and reestablish a coordinated operational intent, allowing Operational Intent A to return to the nominal Activated state. The managing USS for Operational Intent B is notified of the state change for Operational Intent A and can determine through the 4D volumes that it no longer conflicts with Operational Intent B.

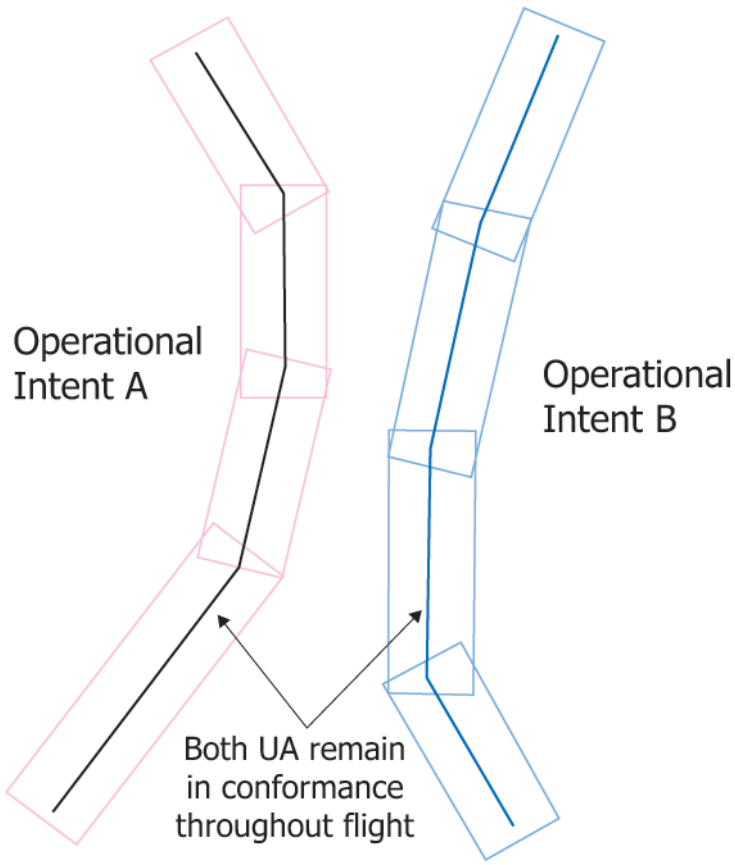

FIG. 5 Nominal, Coordinated Operational Intents

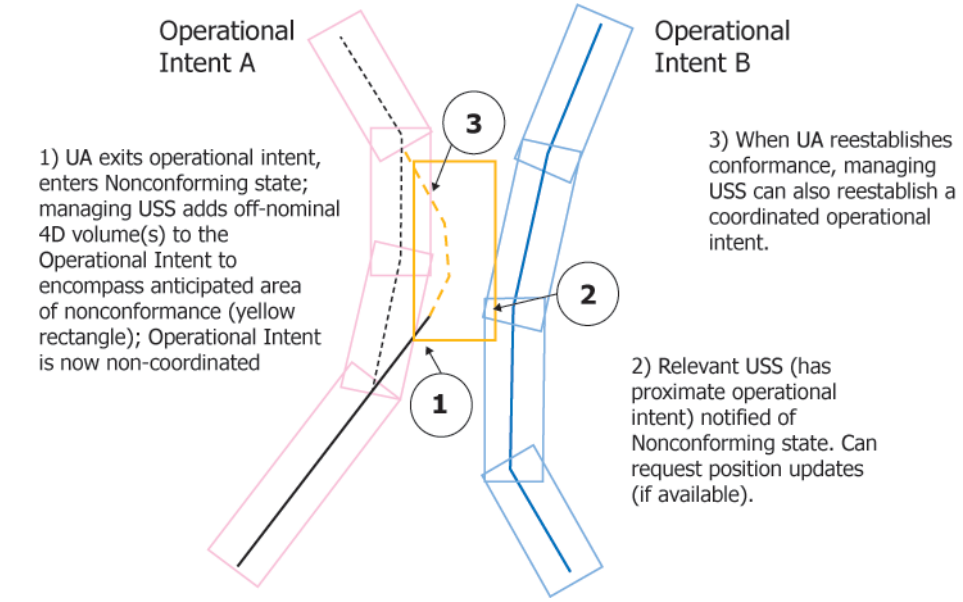

FIG. 6 Off-Nominal Operational Intent, Temporary Nonconformance

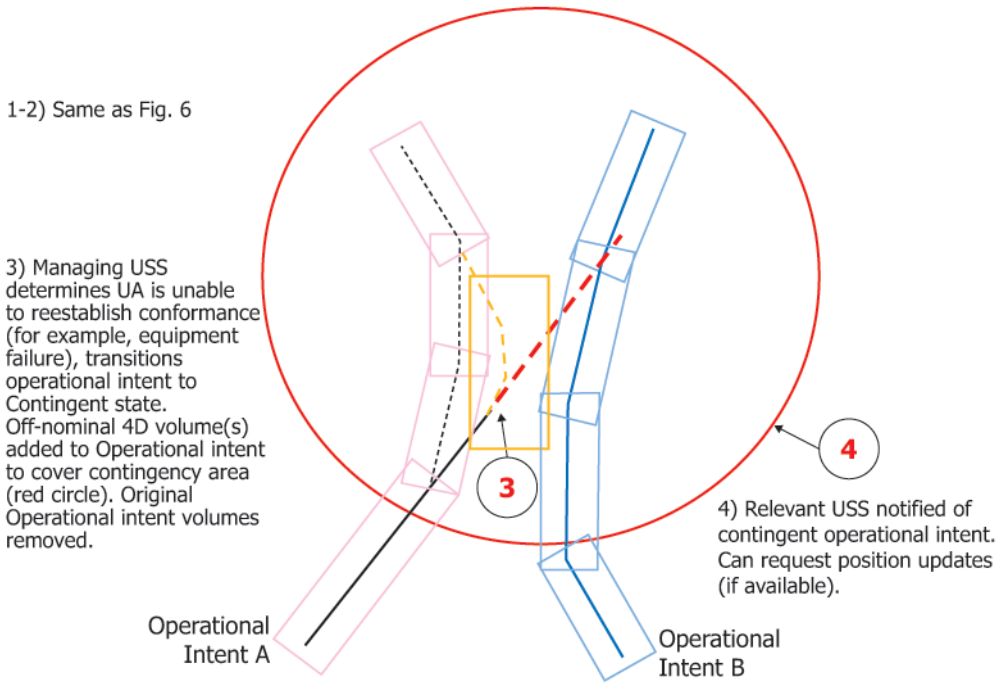

FIG. 7 Off-Nominal Operational Intent, Contingent State

4.4.10 In this scenario, the state transition sequence for Operational Intent A is Accepted > Activated > Nonconforming > Activated > Ended.

4.4.11 Fig. 7 illustrates the scenario where a UA goes out of conformance and is unable to reestablish conformance within the required period of time, resulting in a further transition to the Contingent state.

4.4.12 This scenario begins the same as in Fig. 6 with the managing USS detecting nonconformance for Operational Intent A. An off-nominal 4D volume is added to the operational intent to characterize the anticipated area of nonconformance (yellow rectangle), and the managing USS for Operational Intent B is notified. However, due to some failure, the UA is unable to fly the route that would reestablish conformance and continues along the red dashed line. This introduces an alternate point 3, where the USS recognizes the UA failure or is notified by UAS personnel or the operator's automation and transitions Operational Intent A to the Contingent state. The managing USS for operational intent A removes the original 4D volumes (since the operational intent cannot return to a nominal state) as well as the off-nominal 4D volume added for nonconformance (yellow rectangle), and replaces them with one or more off-nominal 4D volumes that cover where the UA is expected to travel (in this case, a single 4D volume, the red

circle). This resulting Operational Intent remains non-coordinated. At point 4, the Managing USS for Operational Intent B is notified again of the state transition for Operational Intent A, detects the updated conflict, and takes any actions it deems necessary. It can also request position information for Operational Intent A to assist in the process. (Position information may or may not be available.)

4.4.13 In this scenario, the state transition sequence for Operational Intent A is Accepted > Activated > Nonconforming > Contingent > Ended.

4.5 *Constraint States:*

4.5.1 A constraint is a method for informing UAS personnel or the operator's automation, or both, of specific temporal and geographic limitations of the airspace. Constraints are dynamic since they may be created and disseminated on a faster timescale than traditional aeronautical airspace information provided on the ICAO AIRAC cycle. Each constraint consists of one or more 4D volumes with relevant metadata.

4.5.2 Constraint states are simpler than operational intent states because there are no off-nominal states for constraints, and because there is no ecosystem benefit to distinguishing by means of separate states between a constraint that has been submitted but is not currently in effect versus a constraint that is currently in effect. The time information embedded in the 4D volumes is sufficient for a relevant USS to know when the constraint is in effect.

4.5.3 Fig. 8 depicts the constraint states and the valid transitions between states.

4.5.4 *Valid*—A constraint is created by a USS performing the Constraint Management Role. A constraint is made discoverable in the DSS and is available to be shared with relevant USSs when the managing USS transitions it to the Valid state. The managing USS can also update a Constraint while it is in the Valid state.

4.5.5 *Removed*—When a constraint is no longer valid or is canceled by the managing USS, it is transitioned to the Removed state. Once in the Removed state, the constraint is deleted from the UTM system and is no longer available to be shared.

5. Performance Requirements

5.1 *General Notes on Requirements:*

5.1.1 Each requirement is assigned an ID. The IDs consist of an alphabetic prefix used to group related requirements and a unique, 4-digit number. The requirement groupings are:

5.1.1.1 GENxxxx – general requirements applicable to all services

5.1.1.2 OPINxxxx – requirements specific to Operational Intents

5.1.1.3 SCDxxxx – requirements specific to Strategic Conflict Detection

5.1.1.4 ACMxxxx – requirements specific to Aggregate Operational Intent Conformance Monitoring

5.1.1.5 CMSAxxxx – requirements specific to Conformance Monitoring for Situational Awareness

5.1.1.6 CSTMxxxx – requirements specific to Constraint Management

5.1.1.7 CSTPxxxx – requirements specific to Constraint Processing

5.1.1.8 LOGxxxx – requirements specific to logging

5.1.1.9 DSSxxxx – requirements specific to the DSS

5.1.2 Constant values representing a required time, distance, precision, etc., are consolidated into Annex A1, Table of Values. The values are referenced from requirements using alphabetic identifiers created using CamelCase. Examples include:

5.1.2.1 CstrMaxDuration

5.1.2.2 OiMinConformance

5.1.3 For values that correspond to response time requirements, Annex A1 also indicates the events corresponding to the start and stop times.

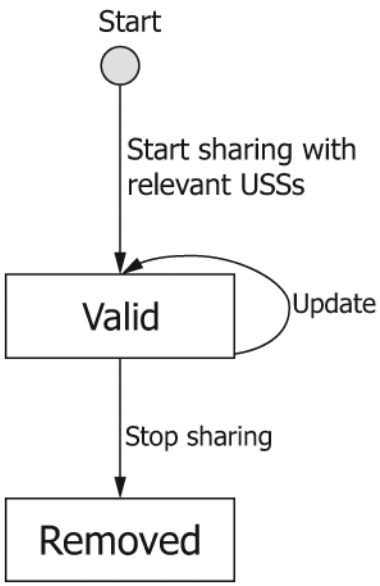

FIG. 8 Constraint States Transition Diagram

5.1.4 Several of the response time requirements refer to *sending a user notification* to UAS personnel or an operator's automation system, or both. The wording of these requirements is intended to accommodate notification by means of interactive user interface or messages sent independent of the interactive user interface (for example, a text message, email, or a system-to-system message).

5.1.5 In some cases, notes to clarify the intent of a requirement are provided. They are for clarification purposes only and do not contain requirements.

5.2 *Common Requirements:*

5.2.1 This section provides requirements common to all services defined in this specification.

5.2.2 *Security, Data Protection, Safety, and Software Assurance:*

5.2.2.1 Discussion

5.2.2.2 It is expected that competent authorities will require USSs to be developed and operated with due consideration being given to security, data protection, and safety, including software assurance.

5.2.2.3 As a foundation to address these areas, this specification requires compliance with select ISO/IEC standards. This approach was taken for two primary reasons: *1)* By referencing existing, widely accepted standards, repeating a large number of requirements in this specification was avoided; and *2)* International standards were selected to encourage global harmonization of requirements and avoid country or region-specific solutions.

5.2.2.4 In most cases, it is expected that compliance with the selected ISO/IEC standards will be sufficient to comply with country or region-specific requirements, such as the General Data Protection Regulation (GDPR) or The Australian Privacy Principles.

5.2.2.5 However, a qualifier of "or equivalent" has been included on each of the three requirements to allow for the case where an implementer chooses only to offer their services in a country or region that requires a specific standard other than the referenced ISO/IEC standards.

5.2.2.6 Note that while the general approach in this specification for the topics of security, data protection, and safety is to reference ISO/IEC standards, there may still be instances where specific requirements are included in this specification.

5.2.2.7 Requirements

5.2.2.8 USSs performing any of the roles identified in this specification shall (GEN0005) be implemented and operated under an ISO/IEC 27001-compliant Information Security Management System or equivalent.

NOTE 1—Appendix X1, Reference Architectures for Interoperability Security Controls, provides an overview of three possible architectures for security controls on the interoperability interfaces defined in this specification.

5.2.2.9 USSs performing any of the roles identified in this specification shall (GEN0010) be implemented and operated under an ISO/IEC 27701-compliant Privacy Information Management System or equivalent.

5.2.2.10 USSs performing any of the roles identified in this specification shall (GEN0015) be implemented and operated under an ISO/IEC 9001-compliant Quality Management System, or equivalent.

NOTE 2—This essentially establishes a requirement for a Safety Management System, which would encompass software assurance.

5.2.3 *Time Synchronization:*

5.2.3.1 USSs shall (GEN0100) synchronize their time to within TimeSyncMaxDifferential seconds of an industry-recognized time source TimeSyncMinPercentage, percent of the time.

NOTE 3—A Stratum-1 time server as described in IETF RFC 5905 – Network Time Protocol Version 4: Protocol and Algorithms Specification is an example of an industry-recognized time source.

5.2.3.2 USSs shall (GEN0105) use synchronized time for all timestamps.

5.2.4 *Data Retention:*

5.2.4.1 USSs shall (GEN0200) permanently delete data received from other USSs within ExternalDataMaxRetentionTime hours except when the data is required to be retained by the competent authority for a longer period of time to support incident analysis or the archival of incident analysis packages.

NOTE 4—While it is recognized that data received from other USSs is necessary to support incident analysis, the intention is to preclude long-term retention and mining of data from other USSs and their operators.

5.2.5 *Test Environment:*

5.2.5.1 Discussion

5.2.5.2 Test environment requirements are intended to support the UTM ecosystem test strategy described in Appendix X6.

5.2.5.3 Requirements

5.2.5.4 USS providers shall (GEN0300) provide an interoperability test instance of their implementation for use by other USSs when needed for interoperability testing.

5.2.5.5 An interoperability test instance shall (GEN0305) use the currently deployed version of the implementer's USS software except when testing an update to the implementer's USS software.

5.2.5.6 An interoperability test instance shall (GEN0310) provide a means for injection or generation of test data in a geographic test location.

NOTE 5—The intention is to provide the means for a USS that is testing with other USSs in the ecosystem to inject test data into each USS.

5.2.6 *User Notifications:*

5.2.6.1 Discussion

5.2.6.2 Several of the requirements in this specification refer to sending a user notification in the event of conflicts. User notifications can be provided to UAS personnel or to an operator's automation system, or both.

5.2.6.3 Requirements

5.2.6.4 If a USS is unable to perform its intended function, the USS shall (GEN0400) send a user notification within UssFunctionFailureNotificationMax seconds, 95 % of the time.

NOTE 6—This requirement is intended to cover the cases of USS system failures, a downed USS (see A2.4), a loss of communication with other USSs, a loss of communication with any DSS, etc.

5.2.6.5 A managing USS shall (GEN0405) send a user notification to UAS personnel or an operator's automation system associated with an operational intent for all state transitions of that operational intent within UserOiStateChangeNotificationMax seconds, 95 % of the time.

5.2.7 *Intersection Precision:*

5.2.7.1 For detecting conflicts between two operational intents or intersections between an operational intent and a constraint, a USS shall (GEN0500) compute intersections of the 3D, geospatial components of 4D volumes with a precision such that two 3D volumes with more than IntersectionMinimumPrecision centimeters of true overlap are indicated as intersecting, and two 3D volumes separated by more than IntersectionMinimumPrecision centimeters at their closest points are indicated as not intersecting.

NOTE 7—This requirement is to ensure USSs properly account for numerical precision in their calculations and data storage and do not incorrectly truncate values.

5.3 *Operational Intent Creation, Modification, and Deletion:*

5.3.1 Discussion

5.3.1.1 As detailed in 4.3, an operational intent represents the airspace to which a UA must conform to a sufficient degree to achieve a target level of safety for strategic deconfliction.

5.3.1.2 Operational intents are central to services defined in this specification. In addition, operational intents must be constructed to adhere to other rules where specified by the competent authority for a region, such as the avoidance of prohibited or restricted airspace, rules pertaining to flights over people, or rules pertaining to night flights -- as well as to apply potential waivers to these types of rules. This aspect of operational intent creation and modification is beyond the scope of this specification.

5.3.1.3 This specification also does not prescribe the detailed process for constructing an operational intent, focusing instead on the outcome of the operational intent — that is, a representation of the airspace to which a UA must conform to a sufficient degree to achieve a target level of safety for strategic deconfliction. A typical process for constructing an operational intent for a trajectory-based operation would include: identifying the desired flight path for the operation; generating a 4D trajectory for the desired flight path (based on the climb, cruise, and descent performance characteristics of the UA as well as environmental conditions such as winds); buffering the trajectory in the horizontal and vertical dimensions based on the expected errors that result from the performance characteristics of the UA; and buffering the entry and exit times to each volume to account for time uncertainty. Iteration on this process may be necessary in response to conflicts with other operational intents discovered by the strategic conflict detection service or intersections with constraints that restrict access to airspace discovered by the Constraint Processing service.

5.3.1.4 The operational intent conformance requirements are broken into *1)* a limit on the count of short duration excursions expected to be caused by the "tails" of statistical error distributions. and *2)* a limit on the amount of time spent outside the Activated operational intent for all excursions, which may be caused by failure modes, non-deconflicted reroutes, etc. These operational intent performance requirements are only satisfied by operational intents in nominal states. UA adhering to off-nominal 4D volumes may not consider that flight time as inside an Activated operational intent. The basis for these requirements are explained in Appendix X4.

5.3.1.5 Requirements pertaining to the construction of operational intents are deliberately written to allow for implementation alternatives. For example, an approach may be that operational intents are constructed by the USS on behalf of the operator using UAS performance characteristics provided by the operator or manufacturer. The USS might derive performance characteristics over time starting with conservative values. The USS might supplement operator or manufacturer-provided performance characteristics using a feedback loop from actual flights. Operational intents may be constructed by an operator, potentially using separate software, and provided to the USS.

5.3.1.6 As noted, operational intents that are unnecessarily conservative and large represent a potential airspace inefficiency issue, as well as a potential fairness concern. Operational data from use of this version of this specification will be used to develop appropriate requirements to address airspace efficiency and fairness issues, if necessary, in a future version of this specification.

5.3.2 Requirements

5.3.2.1 Operational intents shall (OPIN0005) be constructed such that the UA's actual position is outside an operational intent in the Activated state no more than OiMaxExcursionsPerFlightHour times per flight hour, each excursion having a duration of no more than OiMaxDurationPerExcursion seconds.

5.3.2.2 Operational intents shall (OPIN0010) be constructed such that the UA's actual position is inside an operational intent in the Activated state at least OiMinConformance percent of total flight time.

NOTE 8—The required values for OPIN0005 and OPIN0010 were selected as initial values based on a preliminary safety analysis, as summarized in Appendix X4.

These requirements can only be measured through analysis of all error contributions or a statistically significant data set. Actual position is used over reported position to ensure navigation system errors are accounted for.

To meet these requirements, operational intent times include the time between when the USS transitions the operational intent to the Activated state, and the time the UA actually commences flight on takeoff.

5.3.2.3 Operational intents in the Accepted and Activated states shall (OPIN0015) specify coordinated volumes only and must not include off-nominal 4D volumes.

5.3.2.4 The total number of vertices across all volumes comprising an operational intent shall (OPIN0020) be limited to OiMaxVertices.

NOTE 9—This requirement provides a bounding mechanism for processing time associated with operational intents.

5.3.2.5 The managing USS shall (OPIN0025) only modify an operational intent or transition an operational intent to the Accepted, Activated, Nonconforming, or Contingent states if

the managing USS can make the resulting operational intent discoverable by relevant USSs.

NOTE 10—A response time is not included for this requirement because other USSs and UAS personnel are not adversely affected by the failure of a managing USS to transition a new operational intent to the Accepted state and make it discoverable in a timely manner.

See Annex A2 for discussion and requirements pertaining to how a USS makes an entity discoverable.

5.3.2.6 An operational intent shall (OPIN0030) only transition to the Accepted state within OiMaxPlanHorizon days of the start time of the operation.

5.3.2.7 A USS shall (OPIN0035) only modify or render non-discoverable operational intents that it created.

5.3.2.8 If an operational intent is cancelled by the UAS personnel or an operator's automation system prior to activation, the managing USS shall (OPIN0040) transition an operational intent from the Accepted state to the Ended state and render the operational intent non-discoverable within OiMaxCancelTime seconds, 95 % of the time.

5.4 *Strategic Conflict Detection:*

5.4.1 Discussion

5.4.1.1 The purpose of Strategic Conflict Detection is to detect conflicts between operational intents and prevent disallowed conflicts from occurring. To be in conflict, at least one constituent 3D volume of an operational intent must share at least one point with a 3D volume of another operational intent, and there must be an intersection between the start/end time range for those two volumes.

5.4.1.2 Because priorities of UAS operations and circumstances where conflicts are or are not allowed vary between regulators, this specification cannot establish a specific priority scheme and rules regarding allowed and disallowed conflicts. Instead, this specification defines requirements that accommodate priorities and rules regarding conflicts in a generic manner. It is assumed that regulations will be established by the competent authority (or its delegate) for a given region that identify priorities of operations, and an indication of whether conflicts can exist among operations at the same priority level. (It is expected that compliance to these regulator-specific priority and conflict rules will be addressed through a Means of Compliance (MOC) document or process specific to the appropriate regulation.)

5.4.1.3 The number of priority levels and the attributes that characterize them are at the discretion of the competent authority. Attributes could include mission type, VLOS versus BVLOS, UAS capabilities, or others.

5.4.1.4 Conflict detection occurs through operational intent actions on the part of the managing USS when an operational intent is initially being planned, and when attempts are made to modify an existing operational intent. Additionally, the managing USS can conduct conflict detection functions when it is notified of another operational intent that conflicts with an existing operational intent.

5.4.1.5 In the case where operations of different priorities conflict, the USS and UAS personnel and/or the operator's automation system for the lower priority operation are notified and must resolve the conflict. When the lower priority flight has not yet been activated, the conflict must be resolved before the operational intent can be activated. When the lower priority flight has already been activated, if sufficient time exists before the conflict, UAS personnel or operator's automation associated with the lower priority operation resolve the conflict by making adjustments to the operational intent. If insufficient time exists before the conflict to resolve it through adjusting the operational intent, the UAS personnel or the operator's automation system must take other steps; however, tactical conflict resolution is beyond the scope of this specification.

5.4.1.6 For conflicts that exist between operations at the same priority level, if regulations allow these conflicts, this specification ensures that both USSs and UAS personnel and/or the operator's automation system are informed of the conflict and allows the operations to proceed unimpeded.

5.4.1.7 If regulations do not allow conflicts between operations at the same priority level, this specification ensures that the operation that was submitted first (that is, transitioned to one of the enumerated states) takes priority over later submissions. UAS personnel or the operator's automation system must deconflict subsequent operational intents at the same priority level.

5.4.1.8 The interoperability interfaces between USSs and the DSS that support several of the requirements in this section (for example, discovery and sharing of operational intents) are specified in Annex A2.

5.4.1.9 Fig. 9 provides an overview of the prioritization schema previously described. For each permutation of managing USS actions and prioritization scenarios, the associated strategic conflict detection requirement is identified. Note that this table is not a holistic capture of all strategic conflict detection requirements – rather a method to more easily orient oneself with the relationship between managing USS actions and various prioritization scenarios.

5.4.2 Requirements

5.4.2.1 A managing USS shall (SCD0005) apply the lowest bound priority status to any relevant operational intent in the Accepted state for which the relevant USS is determined to be down and does not respond to a request for the details of an operational intent.

NOTE 11—This mechanism for establishing that a USS is down is discussed further in Annex A2. In summary, authorized participants in the ecosystem can report to the DSS that a USS is down. This results in the DSS flagging the operational intents managed by the down USS, allowing other USSs to create new operational intents that overwrite the down USSs' Accepted operational intents. However, other USSs cannot plan over operational intents that may be in use.

5.4.2.2 A managing USS shall (SCD0010) apply the highest priority status defined by the regulator to any operational intent in the Activated, Nonconforming, or Contingent states for which the relevant USS is determined to be down and does not respond to a request for the details of the operational intent.

5.4.2.3 A managing USS shall (SCD0015) verify that an operational intent does not conflict with a higher priority operational intent before transitioning it to the Accepted state.

5.4.2.4 A managing USS shall (SCD0020) verify that an Accepted operational intent that is modified while remaining in the Accepted state does not conflict with higher priority operational intents before the modification is executed.

		Prioritization Scenario		
		Conflict with Higher Priority	Conflict with Equal Priority, not Permitted	Conflict with Equal Priority, Permitted
Operational Intent Action	Transition to Accepted	SCD0015	SCD0035	SCD0055
	Modified in Accepted	SCD0020	SCD0040	SCD0060
	Transition to Activated	SCD0025	SCD0045	SCD0065
	Modified in Activated	SCD0030	SCD0050	SCD0070

FIG. 9 Prioritization Schema Overview

5.4.2.5 A managing USS shall (SCD0025) verify that before transitioning an operational intent to the Activated state, it does not conflict with a higher priority operational intent.

NOTE 12—This situation arises when a higher priority operational intent is created after the lower priority operational intent is transitioned to the Accepted state. The USS and UAS personnel and/or the operator's automation system will receive notification of the new higher priority operational intent. This requirement covers the case where the activation is attempted for the lower priority operational intent before the notifications have been received.

5.4.2.6 A managing USS shall (SCD0030) verify that an Activated operational intent that is modified while remaining in the Activated state does not conflict with a higher priority operational intent before the modification is executed unless the conflict already existed at the time the modification was initiated.

5.4.2.7 A managing USS shall (SCD0035) verify that before transitioning an operational intent to the Accepted state, it does not conflict with an equal priority operational intent when regulation does not allow conflicts within the same priority level.

5.4.2.8 A managing USS shall (SCD0040) verify that an Accepted operational intent that is modified while remaining in the Accepted state does not conflict with an equal priority operational intent before the modification is executed when regulation does not allow conflicts within the same priority level.

5.4.2.9 A managing USS shall (SCD0045) verify that an operational intent does not conflict with an equal priority operational intent before transitioning it to the Activated state when regulation does not allow conflicts within the same priority level.

5.4.2.10 A managing USS shall (SCD0050) verify that an Activated operational intent that is modified while remaining in the Activated state does not conflict with an equal priority operational intent before the modification is executed when regulation does not allow conflicts within the same priority level unless the conflict already existed at the time the modification was initiated.

NOTE 13—The exception in requirements SCD0030 and SCD0050 regarding conflicts that already exist is included in recognition that not all conflicts may be resolvable through replanning due to insufficient time or other factors such as other operational intents or constraints in the area. Consequently this specification does not force replanning as the sole means to resolve the conflict. The conflict might, for example, be addressed through tactical means such as DAA onboard the UA.

5.4.2.11 When a managing USS creates a new operational intent and detects a conflict with an operational intent of the same priority, and regulation allows conflicts within that same priority level, that USS shall (SCD0055) send a notification to the USS that manages the conflicting operational intent within ConflictingOIMaxUSSNotificationTime second, 95 % of the time.

5.4.2.12 When a managing USS modifies an Accepted operational intent that remains in the Accepted state and detects a conflict with an operational intent of the same priority and regulations allow conflicts within that same priority level, that USS shall (SCD0060) send a notification to the USS that manages the conflicting operational intent within ConflictingOIMaxUSSNotificationTime second, 95 % of the time.

5.4.2.13 When a managing USS transitions an operational intent to the Activated state and detects a conflict with an operational intent of the same priority, and regulations allow conflicts within that same priority level, that USS shall (SCD0065) send a notification to the USS that manages the conflicting operational intent within ConflictingOIMaxUSSNotificationTime second, 95 % of the time.

5.4.2.14 When a managing USS modifies an Activated operational intent that remains in the Activated state and detects a conflict with an operational intent of the same priority, and regulations allow conflicts within that same priority level, that USS shall (SCD0070) send a notification to

the USS that manages the conflicting operational intent within ConflictingOIMaxUSSNotificationTime second, 95 % of the time.

5.4.2.15 Upon receipt of a properly-formed request for the details of an operational intent from another USS, the relevant managing USS shall (SCD0075) send the requested data in no more than MaxRespondToOIDetailsRequest second, 95 % of the time.

5.4.2.16 For the entire time an operational intent is in the Activated, Nonconforming, or Contingent states, the managing USS shall (SCD0080) maintain awareness of new or modified operational intents relevant to the managed operational intent.

5.4.2.17 Upon receipt of a notification that an operational intent may be relevant to a subscription, the managing USS shall (SCD0085) send the data for the operational intent to the subscribing USS in no more than MaxRespondToSubscriptionNotification second, 95 % of the time.

5.4.2.18 When a managing USS creates or modifies an operational intent that conflicts with another operational intent, that USS shall (SCD0090) send a notification reporting the conflict to UAS personnel or the operator's automation system associated with the new or modified operational intent within ConflictingOIMaxUserNotificationTime seconds, 95 % of the time.

5.4.2.19 When a managing USS becomes aware that a new or modified operational intent conflicts with an existing operational intent it manages, that USS shall (SCD0095) send a notification reporting the conflict to UAS personnel or the operator's automation system associated with the operational intent within ConflictingOIMaxUserNotificationTime seconds, 95 % of the time.

NOTE 14—The managing USS could become aware of the conflict by receipt of a notification from another USS, or it could also be the managing USS for the new or modified operational intent with which the conflict exists.

5.4.2.20 A managing USS shall (SCD0100) only transition an operational intent to the Nonconforming and Contingent states if it is also serving the role of CMSA.

NOTE 15—This requirement is intended to ensure that all CMSA performance requirements that control Nonconforming and Contingent states are adhered to regardless of which role(s) a USS serves.

5.5 *Aggregate Operational Intent Conformance Monitoring:*

5.5.1 Discussion

5.5.1.1 Aggregate Operational Intent Conformance Monitoring evaluates operational intents for an operator over time to ensure they are meeting conformance requirements and the intended target level of safety for strategic coordination.

5.5.1.2 The intention of Aggregate Operational Intent Conformance Monitoring is to detect persistent problems with an operator being in conformance with its operational intents resulting in the overall target level of safety for strategic deconfliction not being met.

5.5.1.3 Notifications are provided to the operator when aggregate operational intent nonconformance is detected. It is expected that the operator, in conjunction with its USS and other potential contributing parties, will conduct analysis to determine the root cause and take corrective action, such as increasing the size of their operational intents.

5.5.2 Requirements

5.5.2.1 For every flight conducted by an operator, within MaxAggConfMonAnalysisLatency day(s) of the end of the flight, a USS (ACM0005) shall evaluate all operational intents for flights conducted by that operator either within the last AggConfMonEvaluationPeriod days of the time of evaluation or that comprise the most recent AggConfMonEvaluationFlightHours flight hours by the operator, whichever includes a greater number of flights, to determine whether the conformance requirements (OPIN0005, OPIN0010) were met by the operator in aggregate over this period.

NOTE 16—In order to be considered "in conformance," the operational intent for a flight must be in the Activated state, which also requires a coordinated operational intent. Conformance with non-coordinated operational intents in the Nonconforming or Contingent states does not count toward aggregate conformance.

By allowing the analysis for aggregate conformance following a flight to be delayed by up to OiAggConfMonLatency, USSs have the flexibility to batch a group of flights (for example, all flights for a day) or perform the analysis for every flight.

5.5.2.2 Whenever a period of aggregate nonconformance is detected (in accordance with requirement ACM0005), the USS shall (ACM0010) send a notification to the operator (a *performance notification*) within the period of time required by regulation (if applicable) or within MaxNonPerformanceNotificationLatency hours.

5.5.2.3 A performance notification shall (ACM0015) include, at a minimum, the period of time the performance notification addresses and the aggregate performance against each applicable conformance requirement (OPIN0005, OPIN0010).

5.6 *Conformance Monitoring for Situational Awareness:*

5.6.1 Discussion

5.6.1.1 The primary purpose of CMSA is to provide situational awareness to relevant USSs and UAS personnel and/or an operator's automation system when a UA is not in conformance with its operational intent or is contingent.

5.6.1.2 Situational awareness information is provided by the managing USS to relevant USSs for operational intents in either the Nonconforming or Contingent states. This information allows the relevant USS and UAS personnel and/or the operator's automation system to understand the circumstances and possibly could assist a relevant USS in taking actions it deems necessary to avoid conflicts with the off-nominal operational intent. Conflict mitigations can be strategic or tactical in nature. A strategic conflict mitigation involves changing the operational intent for a relevant flight (that is, replanning). This generally occurs preflight but can also occur in-flight if conditions permit (for example, if sufficient time exists before the conflict to replan). Tactical conflict mitigation generally involves UA maneuvers based on immediate location, heading, and speed of involved aircraft, though the effectiveness of tactical conflict mitigations can be enhanced if there is awareness of the associated operational intent. Tactical conflict mitigation can be an onboard capability of a UA or ground-based and supported by a USS.

5.6.1.3 As noted in 1.13.2, this specification does not purport to address tactical mitigation of conflicts; instead, this version of this specification is focused on strategic capabilities. Consequently, readers should be aware that the requirements in this section do not fully address and are not intended to enable tactical conflict mitigation.

5.6.1.4 As discussed in 4.2, this specification defines a USS-provided method for detecting nonconformance based on monitoring of position reports from a UAS (position report-based detection) and also allows for approved operator detection methods.

5.6.1.5 Position information received from a UAS may be intermittent. For UAS relying on position report-based detection of nonconformance, intermittent loss of position information does not necessarily indicate loss of conformance. However, beyond a time threshold, conformance cannot be verified and the operational intent is transitioned to the Nonconforming state. Loss of position data is also communicated to UAS personnel or to the operator's automation system, or both.

5.6.1.6 Position reports are treated as accurate for the purpose of position-report-based detection of nonconformance and the triggering of notifications to UAS personnel or the operator's automation system, or both, and other relevant USS for situational awareness. Incorporation of uncertainty into the construction of operational intents is addressed in 5.2.

5.6.1.7 As discussed in 4.2, operator detection of nonconformance methods are acceptable and necessary in some operational environments, and some UAS may provide nonconformance mitigation capabilities as well. The requirements that follow are written to allow for either the use of position report-based detection of nonconformance performed by the USS or another approved detection method.

5.6.1.8 To provide situational awareness to relevant USSs, for operational intents in either the Nonconforming or Contingent states, the managing USS performing CMSA is responsible for updating the operational intent by adding (and modifying when necessary) off-nominal 4D volumes to reflect, as accurately as practicable, the anticipated area of nonconformance or contingency. (Precision can be limited in circumstances such as a UA fly-away.) This information may be provided by the UAS personnel or the operator's automation system. Relevant USSs that have operational intents in conflict with, or in close proximity to, the resulting non-coordinated operational intents are notified. Note that with approved methods for operator detection of nonconformance, the USS still updates the operational intent states and the associated 4D volumes (based on input from UAS personnel or the operator's automation system) to support situational awareness.

5.6.1.9 In addition, a relevant USS can optionally request current position information for a nonconforming or contingent UA from the managing USS. Current position information may or may not be available.

5.6.1.10 In situations where a UA is able to recover from nonconformance, situational awareness is similarly provided by the managing USS reestablishing a coordinated operational intent and transitioning the operational intent state back to Activated. This information is provided to relevant USSs, including USS that may have been temporarily relevant due only to the expanded operational intent.

5.6.2 General CMSA Requirements

5.6.2.1 A USS performing CMSA for an operational intent shall (CMSA0005) also provide Strategic Coordination for the operational intent.

5.6.2.2 When performing CMSA for an operational intent, a USS shall (CMSA0010) begin conformance monitoring upon notification from UAS personnel or the operator's automation system of commencement of flight or detection of flight in progress, whichever occurs first.

NOTE 17—For an operation that is utilizing the USS's position report-based detection of nonconformance, "begin conformance monitoring" means to begin expecting and processing position reports for the UA. For an operation that is utilizing an operator detection method, it means to begin expecting and processing detection reports from the operator.

5.6.2.3 When conformance monitoring begins, the managing USS performing CMSA shall (CMSA0015) transition an operational intent to the Activated state if the UA is in conformance.

5.6.2.4 When conformance monitoring begins, the managing USS performing CMSA shall (CMSA0020) transition an operational intent to the Nonconforming state if the UA is not in conformance.

NOTE 18—The nonconforming case addresses the activation of an operational intent early or late, or from a location outside the operational intent.

5.6.2.5 The managing USS performing CMSA shall (CMSA0025) provide a means for UAS personnel or the operator's automation system to indicate that the operational intent should be transitioned from the Accepted, Activated, or Nonconforming states to the Contingent state and, for cases where UAS personnel or the operator's automation system, or both, provides the operational intent to the USS, simultaneously supply the updated operational intent that includes appropriate off-nominal 4D volumes.

NOTE 19—This requirement is included in the general requirements section because it is applicable both to position report-based detection of nonconformance as well as operator-reported detection of nonconformance methods. It is for use in cases where UAS personnel or the operator's automation system know the UA will not be able to conform to the operational intent and enables a direct transition to the Contingent state rather than first transitioning to the Nonconforming state and/or waiting for the time-based transition from the Nonconforming state to the Contingent state. In cases where UAS personnel or the operator's automation system provides the updated operational intent with the requisite off-nominal 4D volumes, this must be done simultaneously to avoid a gap in situational awareness for relevant USSs.

5.6.2.6 Upon becoming aware that an operation corresponding to an operational intent in the Activated, Nonconforming, or Contingent state has completed, the managing USS performing CMSA shall (CMSA0030) terminate conformance monitoring, transition the operational intent to the Ended state, and render the operational intent non-discoverable within TransitionToEndedMaxTime seconds, 95 % of the time.

NOTE 20—For operational intents in the Contingent state, the USS may rely on UAS personnel or the operator's automation system to declare an operational intent ended. The manner by which a USS determines an operation is complete, or UAS personnel or the operator's automation

system notifies the USS that an operation is complete, is outside the scope of this specification.

5.6.2.7 The managing USS performing CMSA shall (CMSA0035) retain the unmodified, coordinated 4D volumes comprising an operational intent when it is transitioned to the Nonconforming state and communicate uncoordinated behavior only through off-nominal 4D volumes.

5.6.2.8 The managing USS performing CMSA shall (CMSA0040) continue to provide conformance monitoring for an operational intent until the operational intent transitions to the Ended state.

5.6.3 Requirements for Position Report-Based Nonconformance Detection

5.6.3.1 When using position report-based detection of nonconformance, a managing USS performing CMSA shall (CMSA0100) provide UAS personnel or the operator's automation system the ability to specify the intended position-reporting frequency for an operation.

NOTE 21—A minimum required reporting frequency may be required in a future version of this specification when the focus expands from strategic capabilities to include tactical services. A 1 Hz frequency has commonly been used in various research trials.

5.6.3.2 When using position report-based detection of nonconformance, a managing USS performing CMSA shall (CMSA0105) be able to ingest position data at the position reporting frequency specified by UAS personnel or the operator's automation system.

NOTE 22—It is intended that the managing USS performing CMSA bound the specification of intended position-reporting frequency by UAS personnel or the operator's automation system to values the USS accepts.

5.6.3.3 When using position report-based detection of nonconformance, a managing USS performing CMSA shall (CMSA0110) provide UAS personnel or the operator's automation system the ability to specify the maximum missing position data period for an operation after which the UA must be transitioned to the Nonconforming state.

NOTE 23—The maximum missing position data period can vary depending on the capabilities of a UAS. For example, some UAs may have onboard capabilities to maintain conformance and some may not. It is assumed this period of time will be identified in the operator's safety case.

5.6.3.4 When performing position report-based detection of nonconformance, a managing USS performing CMSA shall (CMSA0115) transition an operational intent from the Activated state to the Nonconforming state and send a notification to UAS personnel or the operator's automation system associated with the operational intent if no position data is received from the UA for a period exceeding the operator maximum missing position data period specified by UAS personnel or the operator's automation system within OiMaxUpdateTimeNonConf seconds, 95 % of the time.

5.6.4 Requirements for Operator-Detected Nonconformance

5.6.4.1 Note, the ability for a UAS personnel or the operator's automation system, or both, to report a contingency situation using an operator-reported method for detection of nonconformance is addressed by requirement CMSA0025 in 5.6.2.5.

5.6.4.2 If a managing USS performing CMSA supports an approved operator-reported method for detection of nonconformance, the USS shall (CMSA0200) provide UAS personnel or the operator's automation system a means to indicate the method is to be used for a designated operational intent.

5.6.4.3 If a managing USS performing CMSA supports an approved operator-reported method for detection of nonconformance, for an operational intent in the Accepted or Activated states, the USS shall (CMSA0205) provide UAS personnel or the operator's automation system a means to indicate that the operational intent should be transitioned to the Nonconforming state and simultaneously supply an updated operational intent that includes appropriate off-nominal 4D volumes.

NOTE 24—The updated operational intent is needed at the time nonconformance is reported in order to avoid a gap in situational awareness for relevant USSs. It could be provided by UAS personnel or the operator's automation system, or both, at the time nonconformance is reported, or it could be provided to the USS in advance based on pre-planned off-nominal procedures.

5.6.4.4 If a managing USS performing CMSA supports an approved operator-reported method for detection of nonconformance, the USS shall (CMSA0210) provide UAS personnel or the operator's automation system a means to update any off-nominal 4D volumes associated with an operational intent.

5.6.4.5 If a managing USS performing CMSA supports an approved operator-reported method for detection of nonconformance, the USS shall (CMSA0215) provide UAS personnel or the operator's automation system a means to indicate the UA has reestablished conformance with the pre-nonconforming operational intent.

5.6.5 Requirements for Situational Awareness

5.6.5.1 For an operational intent in the Activated state, when the managing USS performing CMSA becomes aware that the UA is outside its operational intent, the managing USS shall (CMSA0300) send a notification to UAS personnel or the operator's automation system, add one or more off-nominal 4D volumes to the operational intent to encompass the area and time of anticipated nonconformance, and transition the operational intent to the Nonconforming state within OiMaxUpdateTimeNonConf seconds, 95 % of the time.

NOTE 25—For an operation that is utilizing the USS's position report-based conformance monitoring service, becoming "aware that the UA is outside its operational intent" occurs when the USS receives a position report that is outside the operational intent. For an operation that is utilizing an approved operator detection of nonconformance method, it occurs when the UAS personnel or the operator's automation system reports the situation.

5.6.5.2 For an operational intent in the Nonconforming state, when the USS becomes aware that the current off-nominal 4D volumes previously added to the operational intent no longer encompass the anticipated area and time of nonconformance, the managing USS performing CMSA shall (CMSA0305) update the off-nominal 4D volumes to encompass the anticipated area and time of nonconformance within OiMaxUpdateTimeNonConf seconds, 95 % of the time.

NOTE 26—A managing USS performing CMSA can become aware that the off-nominal 4D volumes added to the operational intent no longer encompasses the anticipated area and time of nonconformance either reactively when a UA provides a position report outside the operational intent, or proactively before the UA reports outside the operational intent.

The intention is that updates to the OI encompass the entire area and time of nonconformance and not that they be updated, for example, on a per position report basis. However, the operational intent can and should be updated more than once if necessary to reflect an evolving nonconforming operation.

5.6.5.3 For an operational intent in the Nonconforming state, if the managing USS performing CMSA becomes aware that the UA has reestablished conformance with the pre-nonconforming operational intent, the managing USS performing CMSA shall (CMSA0310) remove the off-nominal 4D volumes from the operational intent and attempt to reestablish it as a coordinated operational intent and transition it to the Activated state within OiMaxUpdateRestoreConf seconds, 95 % of the time.

NOTE 27—The updated operational intent may be the original (pre-Nonconforming) operational intent or a modified operational intent as long as it is coordinated to ensure there are no disallowed conflicts.

5.6.5.4 If an operational intent remains in the Nonconforming state for more than MaxRecoverableTimeInNonConformingState consecutive seconds, the managing USS performing CMSA shall (CMSA0315) transition the operational intent to the Contingent state within OiMaxUpdateTimeContingent seconds, 95 % of the time.

NOTE 28—This timer-based transition to the Contingent state is a method of last recourse and is included strictly as a safety valve. Automated methods or a manual action on the part of UAS personnel are strongly encouraged and should result in necessary transitions to the Contingent state occurring when the need is detected.

5.6.5.5 For an operational intent in the Contingent state, when the managing USS performing CMSA becomes aware that the current off-nominal 4D volumes previously added to the operational intent no longer encompasses the anticipated area and time of contingency, the USS shall (CMSA0320) update the off-nominal 4D volumes to encompass the anticipated area of and time of contingency within OiMaxUpdateTimeContingent seconds, 95 % of the time.

NOTE 29—As noted for the Nonconforming state, the intention is that updates to the operational intent reflect the entire anticipated area and time of contingency. However, the operational intent can and should be updated more than once to reflect an evolving operation in the Contingent state.

5.6.5.6 The managing USS performing CMSA shall (CMSA0325) send a notification to relevant USSs for all operational intent state transitions and all changes to the 4D volumes associated with an operational intent within UssOiChangeNotificationMax seconds, 95 % of the time.

5.6.5.7 For an operational intent in the Nonconforming or Contingent states, if the most recent position information is available for the operational intent, the managing USS performing CMSA shall (CMSA0330) respond to a request for the position information from a requesting USS with the most recent position report and the expected time at which updated position information may be available for the operational intent within PosInfoRequestMaxResponseTime seconds, 95 % of the time.

NOTE 30—Only relevant USSs would be informed of operational intents in the Nonconforming or Contingent states. Requesting USSs is used in this requirement because the data is only provided when a relevant USS requests it. Providing an expected time at which updated position information may be available provides a mechanism to appropriately space or stop requests.

5.7 *Constraint Management:*

5.7.1 Discussion

5.7.1.1 Constraints provide a mechanism to provide information to USSs and UAS personnel and/or the operator's automation system concerning one or more 4D volumes.

5.7.1.2 Constraint information may be advisory in nature or restrict access for some or all UAS to airspace.

5.7.1.3 The Constraint Manager role applies to USSs that create and manage constraints. Because constraints can restrict access to airspace, the creation of constraints is limited to organizations or individuals authorized by a competent authority, using only USSs that have been approved for the Constraint Manager role. Authorization is specific to the geographic region over which the competent authority has jurisdiction.

5.7.2 Requirements

5.7.2.1 A USS performing the Constraint Manager role shall (CSTM0005) have authorization granted by a competent authority for the region.

NOTE 31—The manner in which a competent authority for a region grants authorization to a USS seeking to perform the Constraint Manager role is beyond the scope of this specification.

5.7.2.2 A USS performing the Constraint Manager role shall (CSTM0010) only accept constraints from authorized constraint providers.

NOTE 32—The process by which a competent authority designates authorized constraint providers is beyond the scope of this specification.

5.7.2.3 A USS performing the Constraint Manager role shall (CSTM0015) enable an authorized constraint provider to create a new constraint, including the type of constraint and 4D volume(s).

5.7.2.4 The total number of vertices across all volumes comprising a constraint shall (CSTM0020) not exceed CstrMaxVertices.

NOTE 33—This requirement provides a bounding mechanism for processing time associated with constraints.

5.7.2.5 The area across all volumes comprising a constraint shall (CSTM0025) not exceed CstrMaxArea square kilometers.

NOTE 34—This requirement provides a bounding mechanism for processing time associated with constraints. This limit will be revisited in future versions of the specification.

5.7.2.6 A USS performing the Constraint Manager role shall (CSTM0030) enable an authorized constraint provider to modify an existing constraint.

5.7.2.7 A USS performing the Constraint Manager role shall (CSTM0035) reject an attempt to create a constraint that restricts airspace access if the start time for any 4D volume comprising the constraint is not at least CstrMinEffectiveTimeBuffer minutes in the future.

NOTE 35—This limit is included to enable strategic planning to be used to avoid a constraint versus necessitating the use of tactical avoidance methods.

5.7.2.8 A USS performing the Constraint Manager role shall (CSTM0040) reject an attempt to modify a constraint that restricts airspace access if any component of the modification is within CstrMinEffectiveTimeBuffer minutes and may invalidate strategic deconfliction performed by a relevant USS.

NOTE 36—A volume can start later (until the original end time), end sooner, or be smaller but contained within the original volume without invalidating prior deconfliction. Allowing these modifications within CstrMinEffectiveTimeBuffer is desirable as it can shorten the duration or reduce the 3D volume of a constraint that restricts airspace access.

5.7.2.9 A USS performing the Constraint Manager role shall (CSTM0045) reject an attempt to create or modify a constraint if the start time for any 4D volume comprising the constraint is greater than CstrMaxPlanningHorizon days in the future.

NOTE 37—A 56-day limit was chosen to align with the standard aeronautical data update cycle.

5.7.2.10 A USS performing the Constraint Manager role shall (CSTM0050) reject an attempt to create or modify a constraint if the duration of the constraint is greater than CstrMaxDuration hours.

NOTE 38—This specification assumes most constraints will be less than 24 hours in duration. Where a constraint's duration exceeds 24 hours, the authorized constraint provider can submit a new constraint that abuts the previous constraint in time.

5.7.2.11 A USS performing the Constraint Manager role shall (CSTM0055) enable an authorized constraint provider to delete designated constraints.

5.7.2.12 A USS performing the Constraint Manager role shall (CSTM0060) only enable the authorized constraint provider that created a constraint to modify or delete the constraint.

NOTE 39—The intent is to preclude situations where an authorized constraint provider attempts to modify or delete constraints created by a different authorized constraint provider (for example, unrelated law enforcement canceling a constraint for an emergency helicopter evacuation). The authorized constraint provider can be an organization or individual. An implementation may allow a constraint created by one member of an organization to be modified or canceled by another member of the same organization.

5.7.2.13 Upon becoming aware of a relevant USS performing the Constraint Processing role, a USS performing the Constraint Management role shall (CSTM0065) send the details of a new, modified, or deleted constraint to the relevant USS within CstrMaxTimeSendDetails seconds, 95 % of the time.

NOTE 40—This requirement ensures that relevant USSs are promptly notified when new or modified constraints affect an operational intent that was previously transitioned to the Accepted state.

5.7.2.14 Upon receipt of a properly formed request for constraint details from a USS, a USS performing the Constraint Management role shall (CSTM0070) send the response in no more than CstrMaxTimeSendDetails seconds, 95 % of the time.

5.7.2.15 A USS performing the Constraint Management role for constraints shall (CSTM0075) maintain an availability of 99.9 %.

5.7.2.16 A USS performing the Constraint Management role shall (CSTM0080) render constraints non-discoverable within CstrMaxDeletion seconds following the constraint end time or an early deletion of the constraint by the authorized constraint provider.

NOTE 41—Even though constraints have an effective start and end time that will allow effective filtering, prompt deletion by the managing USS allows relevant USSs to distinguish between a positively removed constraint and a malfunctioning USS.

5.7.2.17 A USS performing the Constraint Management role shall (CSTM0085) send a notification to the authorized constraint provider of each instance where it could not successfully send the details of a constraint to a relevant USS within UnableToDeliverConstraintDetails seconds, 95 % of the time.

NOTE 42—This notification should consider instances where the relevant USS is the cause of the communication failure, and where the USS performing the Constraint Management role is the cause of the communication failure.

5.7.2.18 A USS performing the Constraint Management role shall (CSTM0090) send a notification to the authorized constraint provider following the successful creation or modification of a constraint and notification of all relevant USSs within CstrPublishedNotificationLatency seconds, 95 % of the time.

NOTE 43—The absence of this notification alerts the authorized constraint provider that a relevant USS is unaware of a constraint.

5.7.2.19 A USS performing the Constraint Management role shall (CSTM0095) only modify a constraint or transition a constraint to the Valid state if the USS makes the resulting constraint discoverable by relevant USSs.

NOTE 44—See Annex A2 for discussion and requirements pertaining to how a USS makes an entity discoverable.

5.8 *Constraint Processing:*

5.8.1 Discussion

5.8.1.1 The Constraint Processing role applies to USSs that ingest constraints.

5.8.1.2 The primary use case for ingesting constraints is to detect intersections with operational intents and relay the associated information to UAS personnel or the operator's automation system, or both. It is the responsibility of UAS personnel or the operator's automation system, or both, to adhere to regulatory requirements associated with constraints; USSs do not enforce constraints that restrict access to airspace, for example, by preventing the creation or activation of operational intents that intersect them. However, the USS must provide awareness of relevant constraints to UAS personnel or the operator's automation system, or both, before transitioning an operational intent to a coordinated state.

5.8.1.3 A USS may also ingest constraints for other purposes, such as to support an app that provides airspace information to users of the app for an area of interest not in conjunction with the creation of operational intents. (In 5.8.2, these users are referred to as *end users*.)

5.8.1.4 The requirements in 5.6.2 all pertain only to USSs performing the Constraint Processing role.

5.8.2 Requirements

5.8.2.1 Before a managing USS performing the Constraint Processing role creates or modifies an operational intent, the

USS shall (CSTP0005) notify UAS personnel or the operator's automation system, providing the details of all constraints that intersect that operational intent.

5.8.2.2 When a managing USS performing the Constraint Processing role is unable to provide UAS personnel or the operator's automation system with the details of all relevant constraints that intersect an operational intent, the USS shall (CSTP0010) send a user notification within IntersectingConstraintUserNotificationMax seconds, 95 % of the time.

5.8.2.3 For the entire time an operational intent is in the Activated, Nonconforming, or Contingent states, a managing USS performing the Constraint Processing role shall (CSTP0015) maintain awareness of new or modified constraints relevant to that operational intent.

5.8.2.4 When a managing USS performing the Constraint Processing role is notified of a constraint that intersects an operational intent it manages, the USS shall (CSTP0020) send a user notification providing the details of the intersecting constraint within IntersectingConstraintUserNotificationMax seconds, 95 % of the time.

NOTE 45—A managing USS can become aware of an intersecting constraint either because it is creating or modifying an operational intent and discovers the constraint, or because the managing USS is informed of the constraint asynchronously by the USS performing the Constraint Management role for the constraint.

5.8.2.5 Before a USS performing the Constraint Processing role creates or modifies an area of interest defined by the end user, the USS shall (CSTP0025) notify the end user providing the details of all constraints that intersect with that area of interest.

5.8.2.6 When a USS performing the Constraint Processing role is unable to provide the end user with the details of all relevant constraints that intersect an area of interest defined by the end user, the USS shall (CSTP0030) send a notification to the end user within IntersectingConstraintUserNotificationMax seconds, 95 % of the time.

5.8.2.7 When USS performing the Constraint Processing role is notified of a constraint that intersects an area of interest defined by the end user, the USS shall (CSTP0035) send a notification to the end user providing the details of the intersecting constraint within IntersectingConstraintUserNotificationMax seconds, 95 % of the time.

5.9 *Logging:*

5.9.1 Discussion

5.9.1.1 Logging (and the associated generation of metrics) is intended to:

(1) allow the performance and efficacy of individual USS implementations, as well as an ecosystem of interoperable USSs, to be analyzed;

(2) support general auditability and event reconstruction activities as required upon authorized request;

(3) inform new requirements or requirements for certain capabilities deferred to future versions of this specification for which operational data is necessary to specify an appropriate solution. Future capabilities are identified in Appendix X2, Future Work Items.

5.9.1.2 USSs can log data in the manner they prefer, including the structure of the data and storage mechanism. However, to enable event reconstruction and metric generation across the UTM ecosystem, Annex A3 specifies a *common export format* to which USSs must be able to export applicable logged data.

5.9.1.3 The common export format enables USSs to use common tools to generate metrics of interest. The intent is not that all data in the common format from all USSs be aggregated into a single dataset or provided to a single organization or system; the intent is that metrics of interest can be generated in a consistent manner for all ecosystem participants.

5.9.2 Requirements

5.9.2.1 General Logging Requirements

NOTE 46—These general logging requirements address all inputs to and outputs of USSs and are intended to enable event recreation and analysis, including response time anomalies. See 5.2.3, Time Synchronization, for timestamp-related requirements.

5.9.2.2 USSs shall (LOG0005) timestamp all logged data in UTC time without local adjustments.

NOTE 47—This data is used to generate the USSLogSet object in the common export format described in Annex A3.

5.9.2.3 Timestamps for logged data shall (LOG0010) correspond to the time at which the associated event occured.

NOTE 48—For message logging, the time of the associated event is the time the message is sent or received. For other logging, the time of the associated event corresponds to the trigger that prompted the logging activity, such as a timer expiration, a state change, an exceeded threshold, etc.

This data is used to generate the USSLogSet object in the common export format described in Annex A3.

5.9.2.4 USSs shall (LOG0015) log outgoing messages sent to other USSs and the DSS, and the responses to those messages.

NOTE 49—This data is used to generate the ExchangeRecord object in the common export format described in Annex A3.

5.9.2.5 USSs shall (LOG0020) log incoming messages received from other USSs and the responses to those messages. (See Note 49.)

5.9.2.6 USSs shall (LOG0025) log instances where an expected response to a request is not received.

NOTE 50—This data is used to generate the ExchangeRecord object to generate the common export format described in Annex A3.

5.9.2.7 USSs shall (LOG0030) log all instances of interaction required by this specification with UAS personnel, end users, or the operator's automation.

NOTE 51—This refers to USS notifications to the UAS personnel, end users, or the operator's automation as well as inputs from any of those to the USS.

This data is used to generate the UserNotificationRecord and UserInputRecord objects in the common export format described in Annex A3.

5.9.2.8 USSs shall (LOG0035) be capable of exporting logged data applicable to the USS roles they perform to the common export formats described in Annex A3.

5.9.2.9 Logging Associated with Operational Intents

5.9.2.10 USSs that manage operational intents shall (LOG0040) log data that associates an operator with operational intents that are made discoverable.

NOTE 52—Management of operational intents includes creation or ingestion from the operator or other 3rd party software, as well as modifications.

This requirement is included because the operator associated with an operational intent is not otherwise logged.

Any logging of PII (for example, name of operator) is subject to the data security and privacy requirements provided in 5.2.2, Security, Data Protection, Safety, and Software Assurance.

This data is used to generate the OperatorAssociation object in the common export format described in Annex A3.

5.9.2.11 USSs shall (LOG0045) log instances where an operational intent could not be planned or replanned due to conflicts with other operational intents or constraints.

NOTE 53—The intent of this logging is to support analysis of airspace access fairness. Fairness is primarily affected by the presence of other operational intents in the area of a desired operation. However, constraints corresponding to other aviation operations can also be a factor.

This data is used to generate the PlanningRecord object in the common export format described in Annex A3.

5.9.2.12 Logging Associated with Strategic Conflict Detection

5.9.2.13 There are no additional logging requirements for Strategic Conflict Detection beyond the general logging requirements provided in 5.9.2.1 – 5.9.2.8.

5.9.2.14 Logging Associated with Aggregate Operational Intent Conformance Monitoring

5.9.2.15 There are no additional logging requirements for Aggregate Operational Intent Conformance Monitoring beyond the general logging requirements provided in 5.9.2.1 – 5.9.2.8.

5.9.2.16 Logging Associated with Conformance Monitoring for Situational Awareness

NOTE 54—Operational intent state transitions involving nonconformance and contingency are covered by prior requirements to log all state changes and their timestamps.

5.9.2.17 USSs performing conformance monitoring shall (LOG0050) log all position data used for conformance monitoring that is ingested from the UA.

NOTE 55—This data is used to generate the OperationalIntentPositions object in the common export format described in Annex A3.

5.9.2.18 Logging Associated with Constraint Management

5.9.2.19 USSs performing Constraint Management shall (LOG0055) log data that allows the authorized constraint provider to be associated with all constraints that transition to the Valid state.

NOTE 56—This requirement is included because the authorized constraint provider associated with a constraint is not otherwise logged.

Logging of any PII (for example, name of the constraint provider) is subject to the data security and privacy requirements provided in 5.2.2, Security, Data Protection, Safety, and Software Assurance.

This data is used to generate the ConstraintProviderAssociation object in the common export format described in Annex A3.

5.9.2.20 Logging Associated with Constraint Processing

5.9.2.21 There are no additional logging requirements for Constraint Processing beyond the general logging requirements provided in 5.9.2.1 – 5.9.2.8.

TEST METHODS

6. Scope

6.1 This section outlines the test methods used to test conformance with this specification.

6.2 The test shall determine the latency, periodicity, reliability, protocol compliance, and interoperability with other USS implementations.

7. Significance and Use

7.1 This specification is intended to be used by USS developers, CAAs, and others to assess USS conformance with this UTM specification.

8. Hazards

8.1 Ensure that UAS are configured to avoid harm to individual(s) conducting the test or third parties.

8.2 UAS that are powered or operational can present hazards. Ensure that propellers are removed or caged during laboratory testing.

8.3 Field testing of UAS can present hazards. Take appropriate safety precautions when field testing UAS.

8.4 When testing UAS with power plants or lithium batteries, or both, an appropriate fire extinguisher for each application should be within reach. Participants should be made aware of the hazards of lithium batteries or flammable fuels, or both, and which fire extinguishers are appropriate for lithium or flammable fuel-based fires, or both.

9. Test Units

9.1 The UAS used in this test shall be mechanically and electrically equivalent to the actual flying configuration. The UAS must be operational and powered during testing.

10. Procedure

10.1 This section provides test procedures for common requirements and each of the UTM services defined in this specification. A self-declaration of conformity approach is presented. As part of self-declaring conformity, implementers must validate that all functional, performance, and interoperability requirements are met. Test results and a description of how requirements were validated must be documented in a product test report using the notes columns of the applicable compliance matrices and supplemental documentation as needed.

10.2 The following table shows the mapping of requirements to the three roles defined by this specification. Roles are a possible granularity of capabilities for which competent authorities may approve USSs. Column 1 identifies the possible roles, and column 2 identifies the requirements that must be satisfied for each role.

Role		Applicable Requirements
Strategic Coordination	10.4	Common Requirements
	10.5	Operational Intent Creation and Modification
	10.6	Strategic Conflict Detection
	10.7	Aggregate Operational Intent Conformance Monitoring
	10.8	Conformance Monitoring for Situational Awareness
	10.10	Constraint Processing
	10.11	Logging Requirements (Partial, see table)
Constraint Management	10.4	Common Requirements
	10.9	Constraint Management
	10.11	Logging Requirements (Partial, see table)
Constraint Processing	10.4	Common Requirements
	10.10	Constraint Processing
	10.11	Logging Requirements (Partial, see table)

10.3 Optionally, a USS may also provide a DSS to support the roles defined in this specification. Requirements for a DSS are provided in 10.11.

10.4 *Common Requirements:*

Req ID	Section Reference	Compliant (Y/N)	Notes
GEN0005	5.2.2.8		
GEN0010	5.2.2.9		
GEN0015	5.2.2.10		
GEN0100	5.2.3.1		
GEN0105	5.2.3.2		
GEN0200	5.2.4.1		
GEN0300	5.2.5.1		
GEN0305	5.2.5.2		
GEN0310	5.2.5.3		
GEN0400	5.2.6.4		
GEN0405	5.2.6.5		

10.5 *Operational Intent Creation and Modification:*

Req ID	Section Reference	Compliant (Y/N)	Notes
OPIN0005	5.3.2.1		
OPIN0010	5.3.2.2		
OPIN0015	5.3.2.3		
OPIN0020	5.3.2.4		
OPIN0025	5.3.2.5		
OPIN0030	5.3.2.6		
OPIN0035	5.3.2.7		
OPIN0040	5.3.2.8		
USS0005	A2.3.2		

10.6 *Strategic Conflict Detection Service:*

Req ID	Section Reference	Compliant (Y/N)	Notes
SCD0005	5.4.2.1		
SCD0010	5.4.2.2		
SCD0015	5.4.2.3		
SCD0020	5.4.2.4		
SCD0025	5.4.2.5		
SCD0030	5.4.2.6		
SCD0035	5.4.2.7		
SCD0040	5.4.2.8		
SCD0045	5.4.2.9		
SCD0050	5.4.2.10		
SCD0055	5.4.2.11		
SCD0060	5.4.2.12		
SCD0065	5.4.2.13		
SCD0070	5.4.2.14		
SCD0075	5.4.2.15		
SCD0080	5.4.2.16		
SCD0085	5.4.2.17		
SCD0090	5.4.2.18		
SCD0095	5.4.2.19		
SCD0100	5.4.2.20		
GEN0500	5.2.7.1		
USS0105	A2.5.2(1)		
USS0105	A2.5.2(3)		
USS0105	A2.5.2(4)		

10.7 *Aggregate Operational Intent Conformance Monitoring Service:*

Req ID	Section Reference	Compliant (Y/N)	Notes
ACM0005	5.5.2.1		
ACM0010	5.5.2.2		
ACM0015	5.5.2.3		

10.8 *Conformance Monitoring for Situational Awareness Service:*

Req ID	Section Reference	Compliant (Y/N)	Notes
CMSA0005	5.6.2.1		
CMSA0010	5.6.2.2		
CMSA0015	5.6.2.3		
CMSA0020	5.6.2.4		
CMSA0025	5.6.2.5		
CMSA0030	5.6.2.6		
CMSA0035	5.6.2.7		
CMSA0040	5.6.2.8		
CMSA0100	5.6.3.1		
CMSA0105	5.6.3.2		
CMSA0110	5.6.3.3		
CMSA0115	5.6.3.4		
CMSA0200	5.6.4.2		
CMSA0205	5.6.4.3		
CMSA0210	5.6.4.4		
CMSA0215	5.6.4.5		
CMSA0300	5.6.5.1		
CMSA0305	5.6.5.2		
CMSA0310	5.6.5.3		
CMSA0315	5.6.5.4		
CMSA0320	5.6.5.5		
CMSA0325	5.6.5.6		
CMSA0330	5.6.5.7		
USS0105	A2.5.2(2)		
USS0105	A2.5.2(4)		

10.9 *Constraint Management Service:*

Req ID	Section Reference	Compliant (Y/N)	Notes
CSTM0005	5.7.2.1		
CSTM0010	5.7.2.2		
CSTM0015	5.7.2.3		
CSTM0020	5.7.2.4		
CSTM0025	5.7.2.5		
CSTM0030	5.7.2.6		
CSTM0035	5.7.2.7		
CSTM0040	5.7.2.8		
CSTM0045	5.7.2.9		
CSTM0050	5.7.2.10		
CSTM0055	5.7.2.11		
CSTM0060	5.7.2.12		
CSTM0065	5.7.2.13		
CSTM0070	5.7.2.14		
CSTM0075	5.7.2.15		
CSTM0080	5.7.2.16		
CSTM0085	5.7.2.17		
CSTM0090	5.7.2.18		
CSTM0095	5.7.2.19		
USS0005	A2.3.2		
USS0105	A2.5.2(4)		
USS0110	A2.5.3(1)		

10.10 *Constraint Processing Service:*

Req ID	Section Reference	Compliant (Y/N)	Notes
CSTP0005	5.8.2.1		
CSTP0010	5.8.2.2		
CSTP0015	5.8.2.3		
CSTP0020	5.8.2.4		
CSTP0025	5.8.2.5		
CSTP0030	5.8.2.6		
CSTP0035	5.8.2.7		
GEN0500	5.2.7.1		
USS0110	A2.5.3(2)		
USS0110	A2.5.3(3)		

10.11 *Logging:*

Req ID	Section Reference	Compliant (Y/N)	Notes
General Logging Requirements Applicable To All Roles			
LOG0005	5.9.2.2		
LOG0010	5.9.2.3		
LOG0015	5.9.2.4		
LOG0020	5.9.2.5		
LOG0025	5.9.2.6		
LOG0030	5.9.2.7		
LOG0035	5.9.2.8		
Logging Associated with Operational Intents, Applicable to Strategic Coordination Role			
LOG0040	5.9.2.10		
LOG0045	5.9.2.11		
Logging Associated with Conformance Monitoring, Applicable to Strategic Coordination Role			
LOG0050	5.9.2.17		
Logging Associated with Constraint Management, Applicable to Constraint Management Role			
LOG0055	5.9.2.19		

10.12 *Discovery and Synchronization Service:*

Req ID	Section Reference	Compliant (Y/N)	Notes
DSS0005	A2.3.3		
DSS0010	A2.3.4		
DSS0015	A2.3.5		
DSS0020	A2.3.6		
DSS0100	A2.4.2.1		
DSS0200	A2.6.2.1		
DSS0205	A2.6.2.2		
DSS0210	A2.6.2.3		
DSS0215	A2.6.2.4		
DSS0300	A2.7.3		

11. Product Marking

11.1 USSs that are capable of meeting the threshold for compliance with this specification and have successfully completed required testing to self-declare conformity should be labeled UTM USS Interoperability capable.

11.2 USSs that are marked:

11.2.1 "ASTM xxxx-2x-Strategic Coordination Compliant" must comply with the requirements for the Strategic Coordination role.

11.2.2 "ASTM xxxx-2x-CMSA Compliant" must comply with the requirements for the Conformance Monitoring for Situational Awareness role.

11.2.3 "ASTM xxxx-2x-Constraint Management Compliant" must comply with the requirements for the Constraint Management role.

11.2.4 "ASTM xxxx-2x-Constraint Processing Compliant" must comply with the requirements for the Constraint Processing role.

11.3 USSs that are compliant to multiple roles are marked for each applicable role.

12. Packaging and Package Marking

12.1 USSs that are capable of meeting the threshold for compliance with this specification and have successfully completed required testing to self-declare conformity should be labeled UTM USS Interoperability capable.

12.2 USSs that are marked:

12.2.1 "ASTM xxxx-2x-Strategic Coordination Compliant" must comply with the requirements for the Strategic Coordination role.

12.2.2 "ASTM xxxx-2x-CMSA Compliant" must comply with the requirements for the Conformance Monitoring for Situational Awareness role.

12.2.3 "ASTM xxxx-2x-Constraint Management Compliant" must comply with the requirements for the Constraint Management role.

12.2.4 "ASTM xxxx-2x-Constraint Processing Compliant" must comply with the requirements for the Constraint Processing role.

12.3 USSs that are compliant to multiple roles are marked for each applicable role.

13. Precision and Bias

13.1 All requirements that have necessary precision attributes have the required precision stated within the requirement itself. No information can be presented on the bias of the test methods in this specification because no such requirements have an accepted reference value available.

14. Keywords

14.1 conformance monitoring; constraints; discovery and synchronization service; interoperability; operational intents; strategic conflict detection; strategic deconfliction; Unmanned Aircraft Systems (UAS); UAS Service Supplier (USS); UAS Traffic Management (UTM); U-Space Service Provider (USSP)

ANNEXES

(Mandatory Information)

A1. TABLE OF VALUES

A1.1 This annex provides the values for all named constants in this specification and provides a cross reference to requirement IDs and sections of this specification that mention the named constants.

TABLE A1.1 Table of Values

Value Name	Value	UoM	Time Start	Time End	Req Ref	Section Ref
AggConfMonEvaluationFlightHours	10	Hours	Operation is transitioned to the Active state	Operation is transitioned to the Ended state	ACM0005	5.5.2.1
AggConfMonEvaluationPeriod	7	Days	Earliest start time of the volume(s) defining the operational intent	Current time as per the managing USS	ACM0005	5.5.2.1
ConflictingOIMaxUserNotificationTime	5	Seconds	Operational intent conflicts identified by USS	Notification dispatched to UAS personnel or operator's automation system	SCD0090 SCD0095	5.4.2.18 5.4.2.19
ConflictingOIMaxUSSNotificationTime	1	Seconds	Managing USS transitions the new operational intent to the Accepted state	Notification dispatched to USS(s) that manage conflicting operational intent	SCD0055 SCD0060 SCD0065 SCD0070	5.4.2.11 5.4.2.12 5.4.2.13 5.4.2.14
CstrPublishedNotificationLatency	5	Seconds	Time after constraint has been written to DSS and any subscription notification messages have been sent	Receipt of successful return codes for DSS write and subscription notification message sends (if any)	CSTM0090	5.4.2.18
CstrMaxArea	10 000	km^2	N/A	N/A	CSTM0025	5.7.2.5
CstrMaxDeletion	5	Seconds	Constraint end time	Constraint reference Delete request dispatched to DSS	CSTM0080	5.7.2.16
CstrMaxDuration	24	Hours	Earliest start time of the volume(s) defining the constraint	Latest end time of the volume(s) defining the constraint	CSTM0050	5.7.2.10
CstrMaxPlanningHorizon	56	Days	Current Time at the time the validation is conducted	Latest end time of the volume(s) defining the constraint	CSTM0045	5.7.2.9
CstrMaxTimeSendDetails	5	Seconds	CSTM0065: Relevant USS subscription information received CSTM070: Request for constraint details received from relevant USS	Constraint details dispatched to relevant USS	CSTM0065 CSTM0070	5.7.2.13 5.7.2.14
CstrMaxVertices	1000	Vertices	N/A	N/A	CSTM0020	5.7.2.4
CstrMinEffectiveTimeBuffer	10	Minutes	Current Time at the time the validation is conducted	Earliest start time of the volume(s) defining the constraint	CSTM0035 CSTM0040	5.7.2.7 5.7.2.8
DSSMaxSubscriptionDuration	24	Hours	N/A	N/A	DSS0015	A2.3.5
ExternalDataMaxRetentionTime	24	Hours	Latest time of receipt	Time of permanent deletion	GEN0200	5.2.4.1
IntersectingConstraintUserNotificationMax	5	Seconds	For new operational intent: operational intent dispatched to DSS For existing operational intent: receipt of constraint details from managing USS	Intersecting constraint details dispatched to UAS personnel, end user, or operator's automation	CSTP0010 CSTP0020 CSTP0030 CSTP0035	5.8.2.2 5.8.2.4 5.8.2.6 5.8.2.7
IntersectionMinimumPrecision	1	Centi-meters	NA	NA	GEN0500	5.2.7.1
MaxAggConfMonAnalysisLatency	24	Hours	Operation is transitioned to the Ended state	Conformance monitoring analysis completed	ACM0005	5.5.2.1
MaxNonPerformanceNotificationLatency	6	Hours	Period of aggregate nonconformance is detected	Notification dispatched to operator	ACM0010	5.5.2.2
MaxRecoverableTimeInNonconformingState	60	Seconds	Managing USS determines UA is out of conformance	Current time as per the Managing USS	CMSA0315	5.6.5.4
MaxRespondToSubscriptionNotification	5	Seconds	Receipt of subscription notification from DSS	Entity details sent to subscribing USS	SCD0085	5.4.2.17
MaxRespondToOIDetailsRequest	1	Seconds	Receipt of OI details request from a USS	OI details sent to requesting USS	SCD0075	5.4.2.15
OiMaxCancelTime	5	Seconds	Receipt of indication operational intent to be cancelled from UAS personnel or operator's automation	Delete request sent to DSS	OPIN0040	5.3.2.8
OiMaxDurationPerExcursion	10	Seconds	Managing USS determines UA is out of conformance	Managing USS determines UA is back in conformance	OPIN0005	5.3.2.1
OiMaxExcursionsPerFlightHour	18	NA	Managing US determines UA is out of conformance	Start time + 1 hour of flight time.	OPIN0005	5.3.2.1
OiMaxPlanHorizon	30	Days	N/A	N/A	OPIN0030	5.3.2.6
OiMaxUpdateRestoreConf	5	Seconds	Managing USS determines UA reestablished conformance	Operational intent state change dispatched to DSS	CMSA0310	5.6.5.3
OiMaxUpdateTimeContingent	5	Seconds	CMSA0315: Managing USS determines operational intent must be transitioned to the Contingent state CMSA0320: Managing USS performing CMSA becomes aware that the operational intent no longer encompasses the anticipated area and time of contingency	CMSA0315: Operational intent state change dispatched to DSS CMSA0320: Operational intent update dispatched to DSS	CMSA0315 CMSA0320	5.6.5.4 5.6.5.5
OiMaxUpdateTimeNonconf	5	Seconds	Managing USS determines no position data has been received from the UA for a period exceeding the maximum missing position data period specified by UAS personnel or the operator's automation	Operational intent state change dispatched to DSS AND notification dispatched to UAS personnel or the operator's automation	CMSA0115 CMSA0300 CMSA0305	5.6.3.4 5.6.5.1 5.6.5.2
OiMaxVertices	10 000	Vertices	N/A	N/A	OPIN0020	5.3.2.4

TABLE A1.1 *Continued*

Value Name	Value	UoM	Time Start	Time End	Req Ref	Section Ref
OiMinConformance	95	Percent	N/A	N/A	OPIN0010	5.3.2.2
PosInfoRequestMaxResponseTime	5	Seconds	Position information request received from requesting USS	Position information dispatched to requesting USS	CMSA0330	5.6.5.7
TimeSyncMaxDifferential	5	Seconds	Current time in accordance with the USS	Current time in accordance with the industry-recognized time source	GEN0100	5.2.3.1
TimeSyncMinPercentage	99	Percent	N/A	N/A	GEN0100	5.2.3.1
TransitionToEndedMaxTime	5	Seconds	Managing USS becomes aware that operational intent in the Activated, Nonconforming, or Contingent state has completed	Operational intent state change dispatched to DSS	CMSA0030	5.6.2.6
UnableToDeliverConstraintDetails	5	Seconds	Failure response (after any retries) on attempt to send constraint details to relevant USS	Failure notification dispatched to authorized constraint provider	CSTM0085	5.7.2.17
UserOiStateChangeNotificationMax	5	Seconds	State transition process completed	Notification dispatched to UAS personnel or operator's automation system	GEN0405	5.2.6.5
UssFunctionFailureNotificationMax	5	Seconds	Failure identified by USS	Notification dispatched to UAS personnel or operator's automation	GEN0400	5.2.6.4
UssOiChangeNotificationMax	5	Seconds	Managing USS transitions or updates operational intent	Notification dispatched to relevant USS(s)	CMSA0325	5.6.5.6

A2. INTEROPERABILITY REQUIREMENTS AND DSS TESTING

A2.1 This annex defines interoperability requirements for the Strategic Coordination, Constraint Management, and Constraint Processing roles defined in this specification. The approach for testing the DSS in support of these roles is also provided. A YAML (OpenAPI) description of the associated APIs is provided in Annex A3.

A2.2 Interoperability Overview

A2.2.1 This specification assumes that one or more USSs provides UTM services in a given region. Participating USSs must be interoperable, sharing data as necessary to support various UTM services. For example, operational intents must be exchanged to support Strategic Conflict Detection.

A2.2.2 The interoperability paradigm described in this specification was first introduced in the ASTM Standard Specification for Remote ID and Tracking (F3411-19). This paradigm is intended to support various UTM services including those defined in this specification and possibly future UTM-related ASTM standards.

A2.2.3 The interoperability paradigm consists of two parts:

(1) A standardized discovery mechanism, referred to as the Discovery and Synchronization Service (DSS), the primary functions of which *(1)* identify USSs with which data exchange is required, and *(2)* verify that a USS considered relevant entities managed by other relevant USSs when necessary (for example, when planning a new operational intent); and

(2) Service-specific data exchange protocols (APIs) used to exchange data in a standardized way once it has been determined through the DSS with whom data exchange is required.

A2.2.4 While the interoperability paradigm is used across multiple specifications, there are service-specific aspects of the DSS API and data exchange protocols detailed in each applicable specification. Annex A2 and Annex A3 document the adaptation of the paradigm for this specification.

A2.2.5 Fig. A2.1 illustrates this paradigm's data exchanges in a service-independent manner. DSS-related interactions are shown in the top large blue-shaded rectangle; data exchange protocols between USSs are shown in the bottom center green-shaded rectangle.

A2.2.6 For safety and availability purposes, the DSS is designed to support redundancy as notionally indicated in Fig. 2. (Redundancy includes multiple DSS instances that can be hosted by one or more organizations in different physical and logical environments or cloud service providers. This specification also supports diverse implementations of the DSS.) The production instances of the DSS in a DSS region synchronize as a pool in a standardized manner, as do the instances in other deployments for that DSS region, such as those in a test pool. Unless noted otherwise, references to the DSS mean the set of DSS instances supporting the region.

A2.2.7 Only approved USSs are given access to the DSS. (Approval processes are beyond the scope of this specification; however, the requisite security tokens are included in the APIs.)

A2.2.8 Entities generically refer to types of data that must be shared between USSs. Different types of entities are used by different UTM services. Entity types for services defined in this specification include operational intents and constraints. The entity concept is extensible to future UTM services where other types of data may need to be shared. A key characteristic of entities is their associated 4D volume(s). Location and time are the factors that determine if an entity is relevant to another USS.

A2.2.9 An Entity Reference is stored in the DSS and enables discovery. Entity references comprise only limited

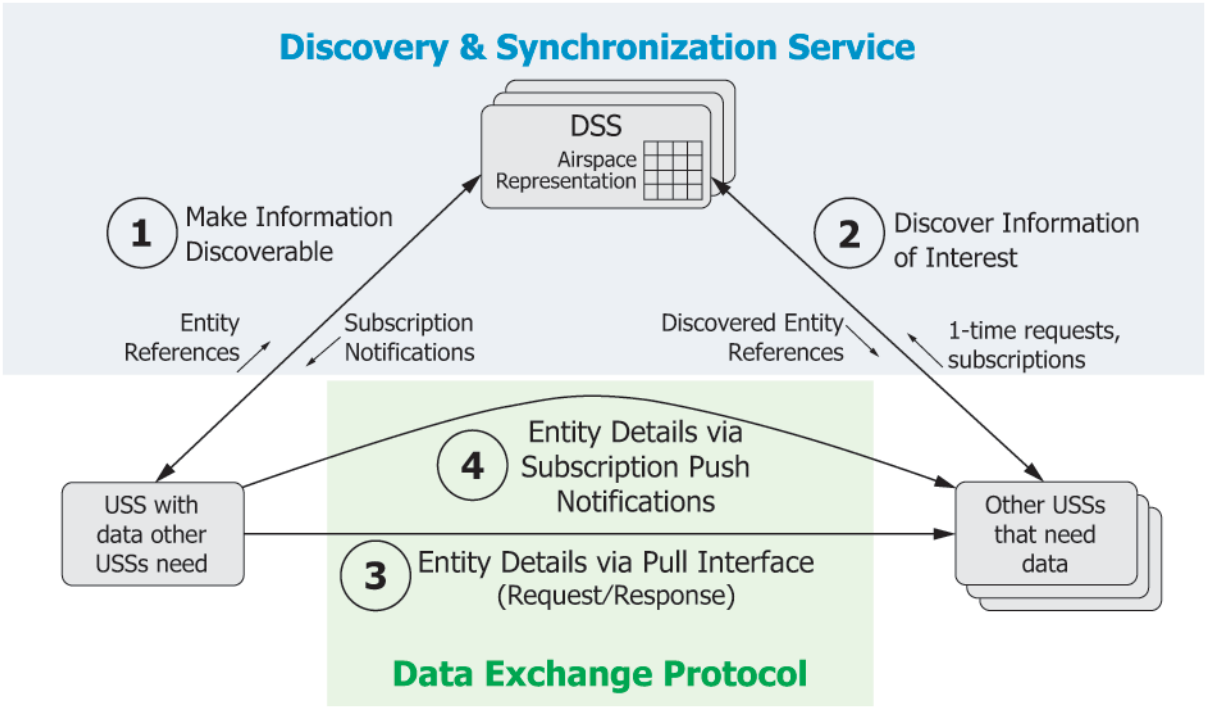

FIG. A2.1 Interoperability Paradigm

information about the corresponding entity, such as its type, unique identifier, approximate location and time range, current opaque version number (OVN) (described below), and how to contact the managing USS to request additional details. Full details of entities are not stored in the DSS but instead are held by, and must be obtained from, the managing USS.

A2.2.10 The DSS encapsulates an airspace representation into which entity references are mapped. The implementation details of this airspace representation are hidden from DSS clients, but it can be conceptualized as a grid, and mapping an entity reference into the airspace representation determines what grid cells it intersects.

A2.2.11 Given that context, the primary interactions (numbered in Fig. A2.1) are:

(1) Make Discoverable—A USS with an entity about which other USSs may need to know (for example, an operational intent, a constraint, an area where UTM services are provided) makes it discoverable by writing an entity reference to the DSS. The DSS creates the OVN for the entity and provides it to the managing USS.

(2) Discover—Other USSs interested in entities of some type query the DSS using a 4D volume to characterize the area and time of interest. USSs may also subscribe to receive future notifications of new, modified, or deleted entity references in the area of interest. The DSS maps the query onto the airspace representation and finds intersecting grid cells with entity references of the desired type (if any). Because entity references are mapped into grid cells and the DSS does not store the precise extents, the DSS will occasionally return an entity that does not intersect the precise area of interest; however, it will never omit an entity that intersects the area of interest. The DSS then returns to the requesting USS a list of the discovered entity references.

(3) Data Requests and Responses—The requesting USS uses the applicable data exchange protocol to contact the respective managing USS and obtains the details of each discovered entity reference. This request/response paradigm is often described as a pull interface.

(4) Subscription Push Notifications—If a USS established a subscription in the DSS (for a 4D area of interest), when another USS creates, modifies, or deletes an entity reference that intersects the subscription, the DSS informs the writing USS of the subscription (Subscription Notifications in Fig. 2). Upon being so informed, the writing USS must provide the subscribing USS with the details of the new, modified, or deleted entity. This paradigm is often described as a push interface.

A2.2.12 The pull and push interfaces described in A2.2.11 are not mutually exclusive and can be used in concert. That is, a USS can use the pull interface to request data from another USS while simultaneously having subscriptions in place.

A2.2.13 Providing OVNs for existing proximal entities is required when making a new entity discoverable (that is, writing a new entity reference to the DSS) if the new entity requires deconfliction with other entities. For example, an operational intent typically requires deconfliction with other operational intents, whereas a constraint does not have to be deconflicted with other constraints or operational intents in order to be created. The provision of OVNs enables the DSS to verify that the managing USS considered all relevant entities in the planning/deconfliction process. This process is summarized in Fig. A2.2.

A2.2.14 In this scenario, panel 1 shows that two operational intent entity references have previously been written to the DSS. OP1 (a linear, trajectory-based operation shown in red) is

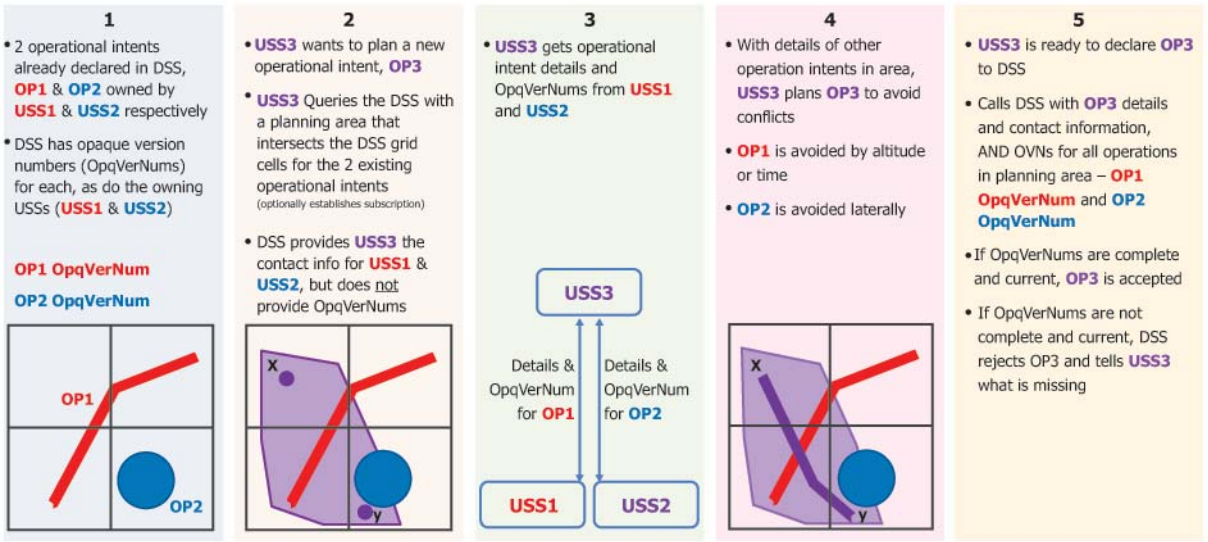

FIG. A2.2 Use of Opaque Version Numbers

managed by USS1. OP2 (a circular area-based operation shown in blue) is managed by USS2. The DSS holds a copy of the opaque version number for each. In panel 2, USS3 queries the DSS for an area (represented by the purple polygon) in which it intends to plan a new operation. The DSS maps the planning area onto the airspace representation and determines it intersects the four cells into which OP1 and OP2 are mapped. The DSS provides USS3 IDs for OP1 and OP2 and the contact details for USS1 and USS2, but does not provide the opaque version numbers for the two operations. (USS3 may also establish a subscription for the planning area so that it is automatically notified if entity references change in the planning area.) In panel 3, USS3 contacts USS1 and USS2 to obtain details of OP1 and OP2, and to obtain the opaque version numbers. Note that the opaque version numbers cannot be obtained without also receiving the operational intent details. In panel 4, USS3 uses the details of OP1 and OP2 to plan OP3 with no conflicts. In panel 5, USS3 writes the new operational intent entity reference to the DSS. It includes the opaque version numbers for all relevant operations. The DSS only allows the entity reference for the new operational intent to be added if the opaque version number set is complete and current.

A2.3 USS-DSS Interfaces

A2.3.1 Note that specific response time requirements for DSS functions are omitted because DSSs are not tested in isolation, but rather in conjunction with a USS. DSS processing time must support a USS meeting applicable response time requirement.

A2.3.2 A USS shall (USS0005) make entities discoverable using the DSS.

A2.3.3 A DSS implementation supporting the services defined in this specification shall (DSS0005), at a minimum, include the following interfaces for use by USSs, in accordance with the DSS portion of the OpenAPI specification presented in Annex A3:

(1) createOperationalIntentReference, updateOperationalIntentReference, getOperationalIntentReference, deleteOperationalIntentReference—these interfaces enable a USS to create, update, retrieve, or delete an operational intent entity reference in the DSS. (A USS can only change operational intent entity references it created.)

(2) searchOperationalIntentReferences—this interface enables a USS to query a specified geographic area and time range of interest. All relevant operational intent entity references are returned.

(3) createConstraintReference, updateConstraintReference, getConstraintReference, deleteConstraintReference—these interfaces enable a USS to create, update, retrieve, or delete a constraint entity reference in the DSS. (A USS can only change constraint entity references it created.)

(4) queryConstraintReferences—this interface enables a USS to query a specified geographic area and time range of interest. All relevant constraint entity references are returned.

(5) createSubscription, updateSubscription, getSubscription, deleteSubscription—these interfaces enable a USS to create, update, retrieve, or delete a subscription for a specified geographic area and time range of interest, and returns all operational intent references and constraint references relevant to that subscription at the time of the call. (A USS can only change or view subscriptions it created.)

NOTE A2.1—As stated, these interfaces are the minimum required. A DSS implementation may include additional interfaces for optimization or functional purposes as long as these minimum interfaces are supported.
Item 1 is the method for making an operational intent discoverable.
Item 3 is the method for making a constraint discoverable.

A2.3.4 After mapping and storing operational intent or constraint entity reference information into the DSS Airspace Representation, the DSS shall (DSS0010) not store or otherwise retain the precise geographical extents of the associated 4D volume(s).

A2.3.5 The DSS shall (DSS0015) limit the duration of subscriptions to no more than DSSMaxSubscriptionDuration hours.

NOTE A2.2—Subscriptions should only be established and persisted for areas in which a USS has or is planning operational intents, or otherwise has a user-based need for data in an area (for example, a user request to an app that provides general airspace information). Subscriptions should not be established for data mining purposes.

A2.3.6 The DSS shall (DSS0020) be implemented in a manner that allows a USS to access any instance of a DSS pool and obtain the same results.

NOTE A2.3—If there are multiple production DSS instances in a geographic region, then they nominally are all active and available for use by clients.

A2.4 Other DSS Interfaces

A2.4.1 *Discussion:*

A2.4.1.1 The requirements in this section address the situation where a USS is determined to be down.

A2.4.1.2 This specification does not mandate a particular mechanism for determining a USS is down or has been restored. For example, it could be based on a monitoring application that maintains heartbeats with all USSs; or, it could involve USS-USS collaboration where a USS that cannot contact the subject USS asks another USS if it is able to contact the subject USS. The expectation is that USS implementers and the regulator in a given region will jointly decide how to make the determination. A USS authorized by the competent authority to determine the availability status of USSs is an availability arbitrator.

A2.4.1.3 When an availability arbitrator determines that a USS is down, the availability arbitrator uses a DSS interface to inform the DSS. Use of this interface requires an *Availability Arbitrator* authorization scope granted by the competent authority.

A2.4.1.4 Once a USS is reported to the DSS as down, other USSs are allowed to plan over operational intents that are in the Accepted state and managed by the down USS, but not other states. The DSS will track the state of each operational intent and make the state information available to USSs. A USS plans over an operation by simply excluding the OVN of that operation from the key presented to the DSS when the operational intent reference is created or modified. The DSS allows the OVN to be excluded because it is aware of the managing USS being down and the current state of the operational intent.

A2.4.1.5 The availability arbitrator also uses the DSS interface to inform the DSS that the subject USS has been restored.

A2.4.1.6 When the down USS is restored and attempts to transition an operational intent to the Activated state in the DSS, the DSS will deny the request unless OVNs for all other operational intents and constraints, if applicable, are included (including the operational intent that was planned over the operational intent belonging to the down USS). This forces the managing USS to replan or cancel operations that were planned over if conflicts remain.

A2.4.2 *Requirements:*

A2.4.2.1 A DSS implementation shall (DSS0100) minimally include the following interfaces, in accordance with the DSS portion of the OpenAPI specification presented in Annex A3:

(1) setUssAvailability, getUssAvailability—these interfaces enable a USS performing availability arbitration to indicate the availability status of a USS to the DSS, or check the current DSS understanding of the availability of a USS.

(2) makeDssReport—this interface enables a USS to report a problem to the DSS that might otherwise go unnoticed.

NOTE A2.4—These interfaces are the minimum required for availability arbitration. A USS may implement additional interfaces for optimization or functional purposes as long as these minimum interfaces are supported.

A2.5 USS-USS Interfaces

A2.5.1 The requirements in this section address interfaces between USSs. Note that security requirements specified in 5.1 apply to these interfaces.

A2.5.2 A USS performing the Strategic Coordination role shall (USS0105), at a minimum, support the following interfaces for use by peer USS, in accordance with the peer-to-peer (P2P) portion of the OpenAPI specification provided in Annex A3:

(1) getOperationalIntentDetails—this interface enables a USS to request the details of operational intents from the managing USS.

(2) getOperationalIntentTelemetry—this interface enables a USS to request position data, if available, for off-nominal UAS operations (that is, operational intents in the Nonconforming or Contingent states) from the managing USS.

NOTE A2.5—The separation of position data from other data serves multiple purposes. It contributes to efficiency by reducing the volume of data transferred; it avoids sharing data that has not been requested; and it provides a mechanism for monitoring for potential abuse cases such as mining information without an associated end user request.

(3) notifyOperationalIntentDetailsChanged—this interface is called by a managing USS after the DSS informs it that a peer USS has a subscription relevant to a new, modified, or deleted operational intent.

(4) makeUssReport—this interface is called by a USS when the requesting USS encounters an issue with the hosting USS that might otherwise go unnoticed or unreported.

NOTE A2.6—These interfaces are the minimum required for strategic coordination. A USS may implement additional interfaces for optimization or functional purposes as long as these minimum interfaces are supported.

A2.5.3 A USS performing the Constraint Management role shall (USS0110), at a minimum, support the following interfaces for use by USSs performing the Constraint Processing role, in accordance with the P2P portion of the OpenAPI specification provided in Annex A3:

(1) getConstraintDetails—this interface is called by a relevant USS when it needs details of a specified constraint entity from the managing USS.

(2) notifyConstraintDetailsChanged—this interface is called by a managing USS after the DSS informs it that a peer USS has a subscription relevant to a new, modified, or deleted constraint entity.

(3) makeUssReport—this interface is called by a USS when the requesting USS encounters an issue with the hosting USS that might otherwise go unnoticed or unreported.

NOTE A2.7—These interfaces are the minimum required for constraints. A USS may implement additional interfaces for optimization or functional purposes as long as these minimum interfaces are supported.

A2.6 DSS-DSS Synchronization

A2.6.1 *Discussion:*

A2.6.1.1 This section is applicable only to implementers of the DSS.

A2.6.1.2 This section describes requirements for the data that must be synchronized between DSS instances in a pool. These requirements are necessary to support diverse implementations of DSS instances while ensuring data consistency and interoperability.

A2.6.1.3 *DSS Data Overview*—The DAR is the foundational data structure for the DSS. The DAR is a single, consistent representation of all entity references and subscriptions in the airspace of a DSS pool, and provides access to those entity references and subscriptions on the basis of an area and time of interest.

A2.6.1.4 A specific synchronization protocol is not specified in this specification. It is expected that implementers of the DSS for a region will coordinate and agree on the synchronization protocol and other implementation details specific to a DSS region. The synchronization protocol must have certain attributes to meet the safety-related needs of the architecture, and its implementation must satisfy all applicable requirements and tests in this specification.

A2.6.2 *Requirements:*

A2.6.2.1 When synchronizing data, a DSS instance shall (DSS0200) authenticate with other DSS instances in the same pool using an industry-standard authentication mechanism.

A2.6.2.2 Communication between DSSs shall (DSS0205) be encrypted using an industry-standard encryption mechanism with a minimum encryption strength of 128 bits.

NOTE A2.8—This requirement is intended to address both integrity and confidentiality of UTM data in transit. TLS is an example of an industry-standard authenticated encryption mechanism.

A2.6.2.3 DSS implementations shall (DSS0210) store and synchronize the following data:

(1) For each subscription:

(a) A unique ID for the subscription;

(b) The manager of the subscription;

(c) A means by which a USS contacts the subscriber to inform them of new information;

(d) The general area in which the subscription is relevant (perhaps by means of a set of DAR cell IDs);

(e) Start and end time of the subscription;

(f) Version of the subscription (to enable consistent read-modify-write operations);

(g) An indication of what types of entity references are relevant to the subscription;

(h) An indication for whether this subscription was created automatically to support an operational intent;

(i) The notification count for the subscription (used by a USS to detect missed notifications).

(2) For each entity reference:

(a) A unique ID for the entity,

(b) The manager of the entity,

(c) A means by which a USS contacts the managing USS to obtain the details of the entity,

(d) The operational intent state, if the entity is an operational intent,

(e) The general area in which the entity is located (perhaps by means of a set of DAR cell IDs), and

(f) The start and end time of the entity.

(3) For each USS with a known availability state as indicated by a USS performing availability arbitration:

(a) The identity of the USS,

(b) The availability state of the USS, and

(c) The version of the availability state.

A2.6.2.4 DSS implementations shall (DSS0215) only respond to the USS after the transaction has been recorded in the DAR.

NOTE A2.9—"Recorded in the DAR" means that any USS will receive the same response, reflecting the updated information, to the same query regardless of which DSS instance is queried.

A2.7 DSS Testing

A2.7.1 DSS testing requirements are intended to support the UTM ecosystem test strategy described in Appendix X6.

A2.7.2 *Approach*—When testing includes a new or modified DSS instance, the test program must demonstrate interoperability at the DSS level. This is accomplished by including verification of data synchronization between all DSS instances when testing the various DSS interfaces. The following provides specific guidance for each of the DSS interfaces (defined in A2.3 and A2.4):

(1) createOperationalIntentReference, updateOperationalIntentReference, createConstraintReference, updateConstraintReference—Tests must demonstrate that after an entity reference is created or modified on any DSS instance in the DSS pool, it can be retrieved from all DSS instances in the DSS pool with consistent results using queryOperationalIntentReferences, getOperationalIntentReference, queryConstraintReferences, and getConstraintReference.

(2) createOperationalIntentReference, updateOperationalIntentReference—Tests must demonstrate that entities may not be created or modified when necessary OVNs are not provided.

(3) deleteOperationalIntentReference, deleteConstraintReference—Tests must demonstrate that an entity reference can be deleted on any DSS instance in the DSS pool and the deletion is reflected on all DSS instances in the DSS pool using queryOperationalIntentReferences, getOperationalIntentReference, queryConstraintReferences, and getConstraintReference.

(4) createSubscription, updateSubscription—Tests must demonstrate that a subscription can be created on any DSS instance in the DSS pool, retrieved from any DSS instance in the DSS pool using getSubscription, and notifications for the subscription are triggered when intersecting entities are added or modified to any DSS instance within the DSS pool. In

addition, the end time for a subscription governs when the DSS automatically removes it from the DSS. Tests must demonstrate that automatic removal of subscriptions occurs on all DSS instances in the DSS pool.

(5) deleteSubscription—Tests must demonstrate that a subscription can be deleted on any DSS instance in the DSS pool and the deletion is reflected on all DSS instances in the DSS pool using getSubscription, and notifications for the subscription are not triggered when intersecting entities are added or modified to all DSS instances in the DSS pool.

(6) setUssAvailability—Tests must demonstrate that USS availability can be set on any DSS instance in the DSS pool, and that availability is reflected on all DSS instances in the DSS pool using getUssAvailability.

(7) All interfaces—Tests must demonstrate that access to the interfaces is denied when a properly formed authorization with an appropriate authorization scope is not provided.

A2.7.3 *Test Environment Requirements*—DSS implementers shall (DSS0300) provide a test instantiation of their DSS implementation for use by USSs when needed for interoperability testing. When not conducting a test of a new release candidate, this test instantiation must use the currently deployed version of the implementer's DSS software and be configured to perform DSS-DSS synchronization with other DSS instances in the test environment DSS pool of a DSS region.

A3. USS-DSS AND USS-USS OpenAPI YAML DESCRIPTION

A3.1 To access the YAML description, visit:
https://github.com/astm-utm/Protocol/blob/v1.0.0/utm.yaml.

APPENDIXES

(Nonmandatory Information)

X1. REFERENCE ARCHITECTURES FOR INTEROPERABILITY SECURITY CONTROLS

INTRODUCTION

This appendix describes three reference architectures for USS interoperability security controls. There are other architectures that can support this specification, but these three have either been deployed or demonstrated with regulators and multiple industry participants.

There are multiple high-level assumptions for the deployments, including:

(1) There will be an onboarding process for approving providers using the integration test environment defined in this specification.

(2) Implementers will use ISO/IEC 27001, or equivalent, as the basis for managing the information security aspects of USSs, as required by this specification, with potential additional local requirements.

(3) Message logging required by this specification as well as additional logging requirements from ISO/IEC 27001 will be implemented.

The reference architectures described in this appendix will require further security risk analysis based on the technical implementation of the reference architecture, the implementation of the assumptions above, and the minimum performance requirements for identity assurance and key management used by the implementor or mandated by the regulator. The identity assurance level will determine the viability of the use of self-signed certificates and the requirements on the self-signer for managing these certificates.

X1.1 *Base Deployment: Access Tokens with Audience Claims*:

X1.1.1 This architecture is being used in Switzerland for the deployment of Network Remote ID. It focuses on establishing the identity and authorization scope of the client USS to the server USS as outlined in Fig. X1.1.

X1.1.2 *Architecture Description:*

X1.1.2.1 In this architecture, there is a single resource provider (Auth server) that acts as the authoritative source of truth regarding the services each USS is authorized to provide (authorization scope). A client USS proves its identity and authorization scope to a server within the federated system by providing an OAuth 2.0 bearer access token containing this information along with a cryptographic signature from the Auth server proving its authenticity. The client obtains this token from the Auth server by providing the authentication secret that proves its identity to the Auth server, along with the desired authorization scope the client wishes to assert, and the audience for which this access token is intended. The server validates an incoming access token by checking the token's cryptographic signature with the Auth server's public key. The server must obtain the Auth server's public key, ideally signed by a trusted entity, by means of a trusted channel to avoid an impersonator substituting their own public key. This is accomplished by requesting the public key from a known domain name using a TLS connection, which provides a layer for authentication and encryption to mitigate the risks of a spoofing and impersonation attack between participants in the system.

X1.1.2.2 The audience claim identifies a particular organization in the federated architecture, and all other organizations within the federated architecture will reject a token for that audience in accordance with IETC RFC 7519. Due to each token specifying exactly one audience, tokens received by one organization in the federated architecture cannot be reused to impersonate that client to a different organization in the federated architecture, as is illustrated in Fig. X1.2.

X1.1.2.3 In Fig. X1.2, light-colored access tokens are used to attempt to access other servers in the federated architecture. USS A is able to correctly contact all other servers. USS B initially attempts to use the access token it received from USS A to access USS C, but the attempt is rejected because USS C does not identify itself with the 'aud' claim of "B," instead expecting "C." Similarly, USS C initially attempts to use the access token it received from USS A to access the DSS, but this attempt is rejected for a similar reason.

X1.1.2.4 Again here, the audience claim is required at a minimum because it prevents token reuse to access different USSs on all API calls, including ones where message signing (as used in the UPP2 project in the United States) does not provide any additional security when accessing different USSs. The UPP2 project used message signing with JSON Web Signatures (JWS) to sign HTTP calls with bodies. HTTP calls without bodies and replies were not signed, but still protected by means of the TLS connection.

X1.1.2.5 Short-term OAuth outages are supported by design as, in accordance with the ASTM Remote ID and Tracking Standard (Specification F3411), tokens are re-requested hourly

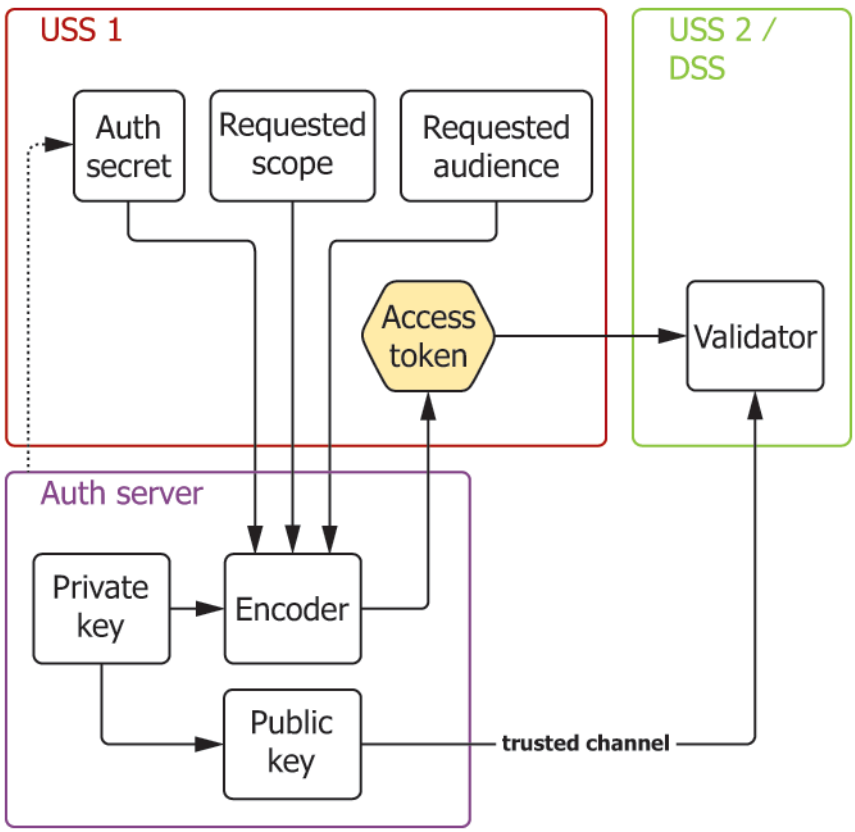

FIG. X1.1 Access Tokens With Audience Claims

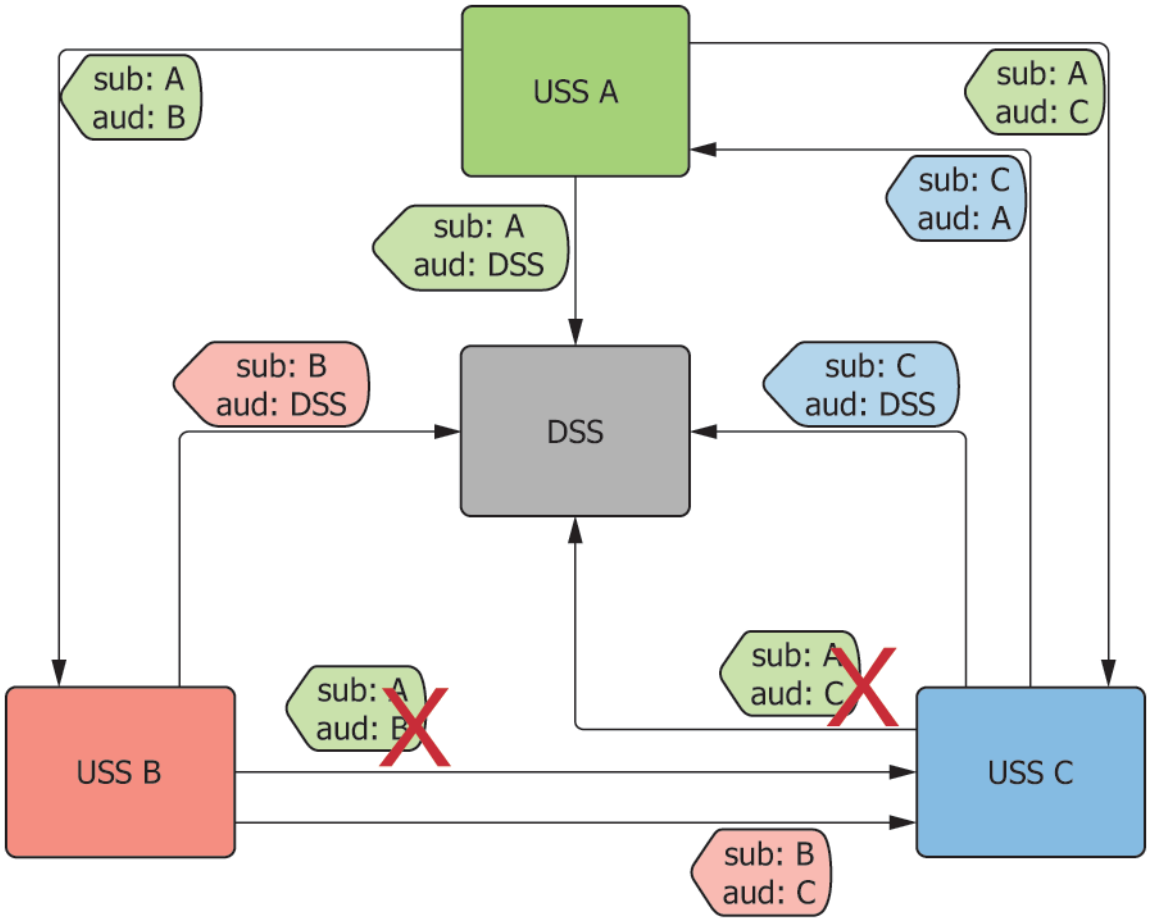

FIG. X1.2 Token Reuse Protection with Audience Claim

to enable timely revocation of the user's privileges. Token duration should be set in consideration of reliability (longer durations) versus security risk (shorter durations). Should a short-term OAuth outage occur, existing tokens can continue to be used for a short time; thereafter, a fail-safe outcome is achieved by the preclusion of creating new flights with potential conflicts.

X1.1.2.6 Both the ASTM Standard Specification for Remote ID and Tracking, F3411, and this specification require a production-like integration environment for ecosystem participants, and it would be expected to have the same deployment setup for the integration environment to provide full end-to-end testing, albeit with non-production tokens.

X1.2 *Enhanced Deployment: Access Tokens Plus Message Signing*:

X1.2.1 This architecture augments OAuth 2.0 tokens with message signing, leveraging the ICAO International Aviation Trust Framework (IATF). As with the architecture described in X1.1 (access tokens with audience claims), this architecture credibly establishes the identity and authorization scope of the client USS to the server USS. It also enables non-repudiation of some messages: the recipient of a message within the system can prove that a received message with non-empty body originated from someone with access to the private key of the USS indicated as the sender. This architecture accomplishes these goals by cryptographically signing the body content (when it exists) of every message exchanged with another server, in addition to using standard OAuth 2.0 access tokens as described in the previous architecture and transport layer encryption between clients through TLS. There are two possible ways to disseminate the information necessary to validate the message signatures: self-signing or by means of a certificate authority. To maintain non-repudiation and to mitigate impersonation attacks, self-signed certificates must be created, managed, and audited, ideally using the same processes as a certificate authority (CA) using a trusted Certificate Policy (CP). The USS using self-signed certificates acts as its own CA.

X1.2.2 Message signing can provide an additional layer of protection if the TLS layer is compromised or an insider attack is successfully carried out, resulting in internal networks being breached. TLS compromise would be considered unlikely without an attacker profile that includes access to an unusually large amount of resources.

X1.2.3 Message signing could be added to existing deployments incrementally. For example in the FAA UTM Pilot Program 2, there were a mix of providers providing different services. Providers of more safety-critical services or those USSs providing services to government agencies implemented

message signing, providing the partial non-repudiation benefits; however, the providers of basic and non-safety services like Remote ID did not implement message signing, and data exchange was still possible. Separately or in addition, message signing can be used to authenticate a client to the authorization server when requesting an access token.

X1.2.4 *Trusted Certificate Authority:*

X1.2.4.1 When a trusted certificate authority is available, that certificate authority can cross-sign CA certificates to endorse each USS's certificate. This architecture variant is illustrated in Fig. X1.3.

X1.2.4.2 Central certificate authorities can be complex and require a rigorous certificate policy framework including strict revocation. In the FAA UTM Pilot Program 2, certificates based on the ICAO Aviation Trust Framework were used. In the case of a need to revoke access, the first layer would be to revoke the OAuth token—this would still be the initial and fastest form of revocation. The certificate-based revocation process using CRLs would potentially require fast network interaction and extended time to propagate the information about revoked certs through the connected parties. By this, the certificate-based revocation process would take more time.

X1.2.4.3 Hence, the proposed approach is to base the revocation process on removing the OAuth token.

X1.3 *Alternative Deployment: Self-Signed Certificates*:

X1.3.1 A central certificate authority may not always exist or may not be immediately available or cost-effective. When a central certificate authority across all parties is not available, and given a small number of UAS Service Suppliers within a region, self-signed certificates from one party local or dedicated Certificate Authority can be utilized. Self-signed certificates would be created as part of the onboarding process of a new USS, and the Auth server can take on the additional duty of hosting and distributing each USS's self-signed certificate. This establishes the Auth server as the authority for which message-signing keys were ever used by a USS (for the purposes of non-repudiation), and the trusted source for certificates when validating signatures. This architecture variant is illustrated in Fig. X1.4.

X1.3.2 For some countries, the base deployment with access tokens with audience claims may be sufficient, and may be preferred over self-signed certificate management. To maintain non-repudiation, and to mitigate impersonation attacks, self-signed certificates must be created, managed, and audited, ideally using the same processes as a CA using a trusted CP. The USS using self-signed certificates acts as its own CA.

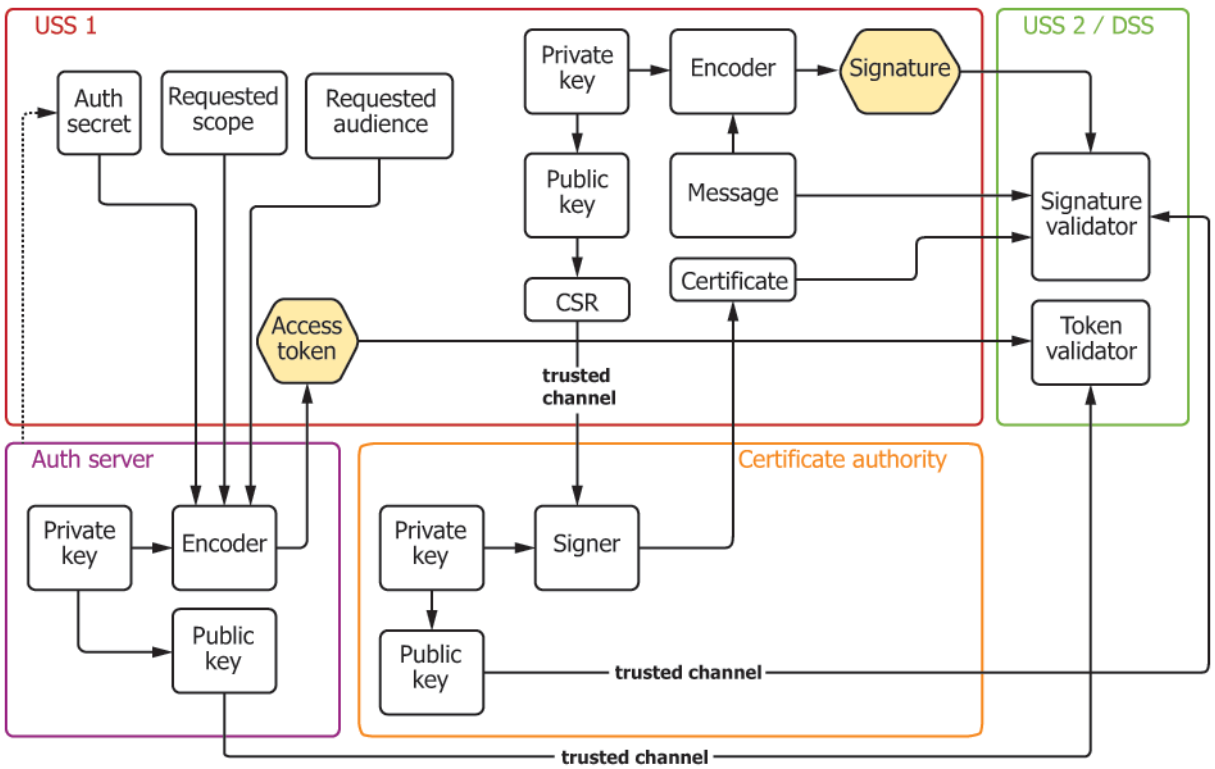

FIG. X1.3 Message Signing with Certificate Authority

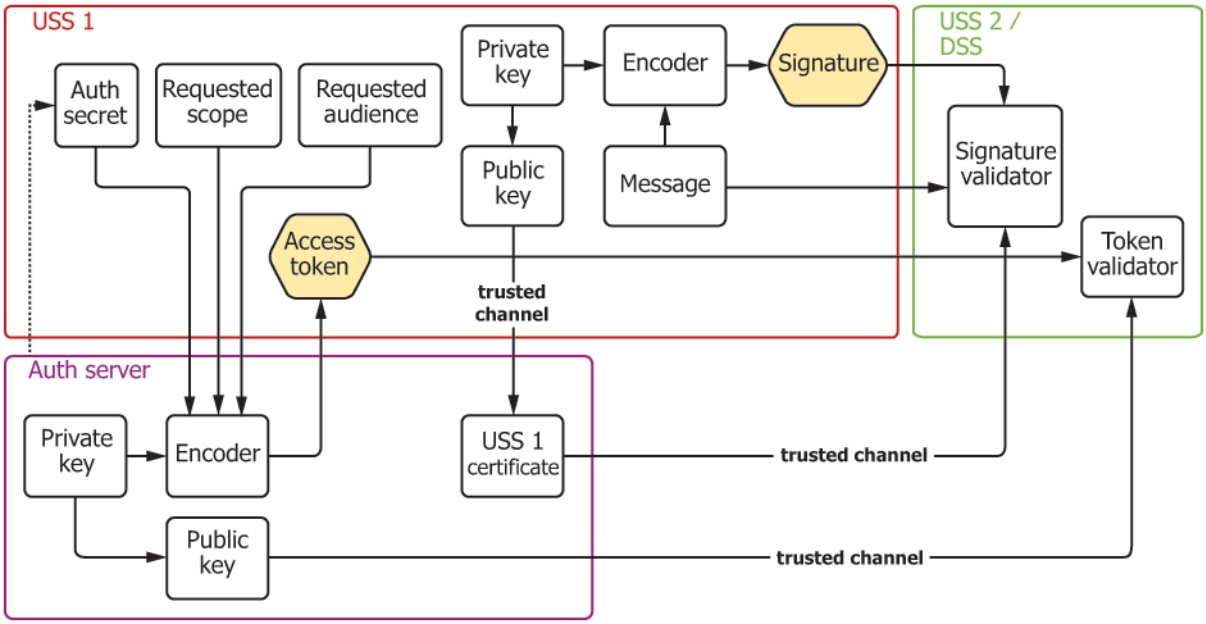

FIG. X1.4 Message Signing with Self-Signed Certificates

X2. FUTURE WORK ITEMS

INTRODUCTION

Proposed work items and key focus areas for future versions of this specification are presented below. This list is not comprehensive and will evolve.

X2.1 *Operational Intent Creation*:

X2.1.1 Re-evaluate assumptions regarding the construction of operational intent volumes as they relate to establishing a safety case.

X2.2 *Negotiations*:

X2.2.1 Basic – Phase I
X2.2.1.1 Preflight and in-flight negotiations
X2.2.1.2 Yes/no response only
X2.2.1.3 Including proposed airspace "swap"

X2.2.2 Advanced – Phase II
X2.2.2.1 Beyond yes/no
X2.2.2.2 Multiple intersections
X2.2.2.3 Shared airspace

X2.3 *Fairness*:

X2.3.1 Basic – Phase I
X2.3.1.1 Handle priority operations and preemption
(1) Example—Prioritization of flights requiring reroute around a pop-up constraint
X2.3.1.2 Limited airspace fairness rules or enforcement, or both
(1) Based on review and analysis of the data collected, leverage *v1* of the specification.

X2.3.2 Advanced – Phase II
X2.3.2.1 Advanced airspace fairness rules

X2.4 *Conformance Monitoring*:

X2.4.1 Investigate additional conformance monitoring considerations including, but not limited to, aircraft performance, position accuracy, specifically in relationship to tactical functions.

X2.5 *Constraints Management*:

X2.5.1 Extended uses for operational constraints
X2.5.1.1 Possible different types or attributes
X2.5.1.2 Specific routing based on environmental considerations

X2.6 *Auditing*:

X2.6.1 Supporting historical queries by the authorized stakeholders
X2.6.1.1 External endpoint API for auditing data collection from USSs

X2.6.2 USS/DSS Outages and Hygiene
X2.6.2.1 Operational cleanup enforcement
X2.6.2.2 Misbehaving USS
X2.6.2.3 Functional response to USS errors

X2.7 *Privileged Users*:

X2.7.1 Define a role that allows operational intents and constraints to be modified or cancelled by someone other than the originating USS/authorized constraint provider.

X2.7.1.1 This is necessary both for tactical overrides as well as cleanup should a USS fail or have access revoked.

X2.8 *Manned Aircraft Integration*:

X2.8.1 Limited manned aircraft operation integration (for example, manned aircraft providing intent and receiving UTM information for situational awareness)

X2.8.2 Advanced manned aircraft integration including two-way ATC exchanges

X2.9 *Common*:

X2.9.1 Plan for validation and refinement of numerical values

X2.9.2 Advanced security considerations

X2.9.3 Tracking Service—External surveillance sources for conformance monitoring

X2.10 *UAM Commonalities*:

X2.10.1 Augment UTM standard to include UAM integration-specific interfaces.

X2.10.2 Potential commonalities between UTM and UAM include Strategic Deconfliction, Conformance Monitoring, Prioritization.

X2.10.3 Advanced UAM integrations

X2.11 *Planning/Authorization Service*:

X2.11.1 Define a generic planning or authorization service.

X2.12 *DSS*:

X2.12.1 Provide appendix describing considerations and recommended guidance on DSS configurations.

X2.12.2 Provide broadcast notification capability for use in the event of DSS outages with flights in off-nominal scenarios.

X2.13 *Safety Case*:

X2.13.1 Bridge to Reich collision risk model

X2.13.2 Evaluate feasibility of parameterizing safety analysis to achieve a desired TLS for strategic deconfliction.

X2.14 *Others*:

X2.14.1 Swarms

X2.14.2 Upper altitude UTM

X2.14.3 ATC Notifications for Off-Nominal Operations

X3. COMPATIBILITY WITH RELATED STANDARDS

X3.1 As noted in Section 1, Scope, there are instances where this specification has been written to ensure consistency with specifications or standards developed by other SDOs.

X3.2 This appendix identifies such instances and provides a high-level summary of how compatibility was achieved.

X3.3 Even when there is agreement on the subject matter, multiple specifications can be an unavoidable situation if a regulator requires a specification be developed by a particular SDO. In these cases, ASTM seeks to establish cooperation arrangements with the applicable SDO to ensure consistency between the related specifications.

X3.3.1 *EUROCAE ED-269, Minimum Operational Performance Standard for UAS Geo-Fencing*—ED-269 identifies the structure for UAS geographical zones. UAS geographical zones are analogous to constraints in this specification.

X3.3.1.1 All attributes of all classes defined in the ED-269 UAS Geographical Zone data model are included as optional fields for constraints in the interoperability APIs described in Annex A2 and Annex A3 of this specification, with differences only in the case of 4D volume definitions. The use of optional fields enables this specification to support ED-269 as well as other standards that may arise in other countries or regions for geographical zones or constraints. Differences in the case of 4D volume definitions arose due to the prior use of this specification's volume definitions in other ASTM standards. However, ED-269 volumes can be derived from the volume definitions used in this specification and vice versa. A translation layer to convert between an ED-269 UAS geographical zone and a constraint is straightforward.

X4. SAFETY CASE FOR STRATEGIC DECONFLICTION

X4.1 Overview

X4.1.1 A key element of enabling large-scale UAS operations is understanding UA-to-UA collision risk, and the definition of the safety case for these operations. Collision risk is inversely proportional to the amount of protected airspace afforded for each vehicle's operation. This specification defines the size of airspace protections as 4D volumes that contain the aircraft for some percentage of its flight time. As a starting point, it is obvious that the collision risk can be reduced to zero by making the volumes quite large, such as being equivalent in size to the range of each UA so that the vehicle is contained 100 % of the time. While this eliminates collision risk, it would severely restrict the capacity of airspace. It is evident that there is a need to have balance between collision risk and reasonable use of the airspace. This is a preliminary safety case analysis that aims to characterize the safety benefit of deconfliction between 4D volumes that contain their respective flights 95 % of the time.

X4.1.2 In the process of selecting 95 % volumes (2 sigma), an upper bound was established from Required Navigation Performance operations in manned aviation. Specifically, these "Required Navigation Performance-Authorization Required (RNP-AR)" terminal (arrival and departure) procedures are defined with the lateral boundary of the protected volumes at 4-sigma and are fully accepted as providing safe separation from terrain and obstacles for commercial air transport operations, which is a much more rigorous requirement than UA-to-UA separation requirements. Since 4 sigma is sufficient for separation from terrain that will necessarily produce a negative outcome upon incursion, 2 sigma was selected as a starting point for separation from other aircraft volumes that only very rarely produce a negative outcome upon incursion. See X4.5 for additional discussion.

X4.1.3 It is assumed that when high-priority operations are allowed to create conflicts with other operations, other regulatory mitigations beyond this standard will be employed to achieve a similar level of safety.

X4.2 The Overarching Safety Case

X4.2.1 The overarching target level of safety (TLS) for UA operations generally corresponds to General Aviation (GA) third-party ground safety risk. GA third-party ground risk is considered as the threshold rather than GA midair collision (MAC) risk due to the critical distinction that UA operations do not have passengers onboard. In addition, we consider factors that lead to a reduced ground risk when comparing a UA-UA collision versus a GA-GA collision. As such, when assessing MAC, the rate of MAC directly impacts public perception but feeds into a larger safety question of third-party ground safety since there is no direct harm done to people at the instant of collision.

X4.2.2 Target MAC risk should be greater than target ground risk since a MAC does not always result in a fatality; it is simply a contributing factor. The probability of GA third-party fatality can be broken down as follows, where a MAC is considered as a contributing failure mode that may cause a collision with a person.

X4.2.3 P(MAC) will need to be decomposed in order for the following to be true:

X4.2.3.1 The entire philosophy is depicted in Fig. X4.1: a subset of failures result in fatal collisions. A category within failures is the risk of MAC, which proportionally contributes to lethal collisions.

X4.3 Decomposing MAC Risk with Strategic Deconfliction—The decomposition of MAC evolves with the introduction of strategic deconfliction. Without any deconfliction or mitigation strategies, the probability of collision between two UA could be modeled as completely

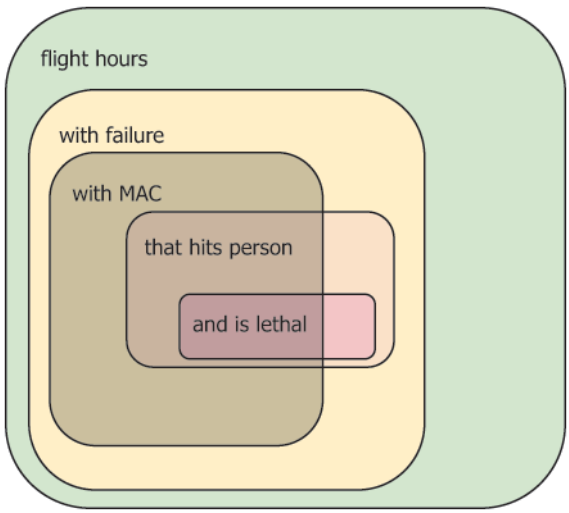

FIG. X4.1 Breakdown of Failure Conditions and Consequences

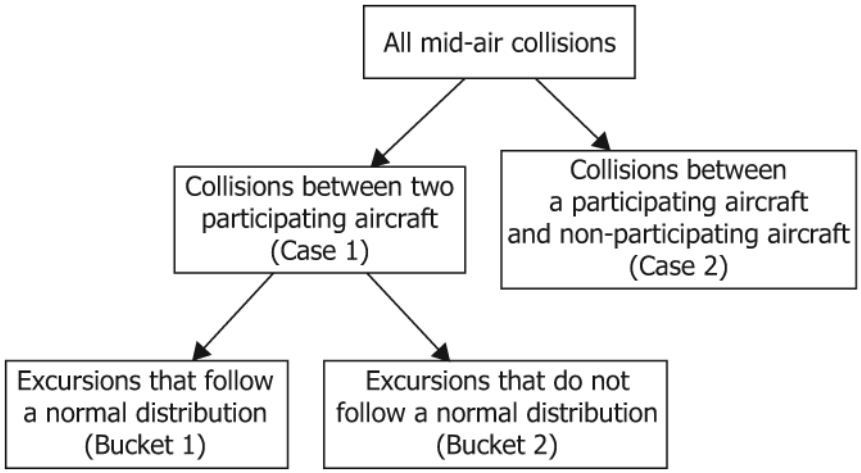

FIG. X4.2 Categorization of All Mida;ir Collisions

randomized, similar to an AFIT-developed bird-strike model.[13] The introduction of strategic deconfliction supports MAC risk reduction by communicating flight intent by means of coordinated volumes for participating aircraft. With strategic deconfliction, the overall P(MAC) is as follows:

X4.3.1 *Probability of MAC Without Mutual Strategic Deconfliction (Case 2):*

X4.3.1.1 Two fundamental cases for P(MAC) are differentiated by P(SD)—the probability that another UA is participating in strategic deconfliction. Under P(SD'), where the other aircraft in question is not participating, we assume that the relationship between the aircraft cannot be established systematically and, therefore, apply the bird strike model to estimate P(MAC|SD'). Strategic deconfliction participation levels can be mandated by regulatory bodies based on acceptable levels of overall safety risk and are represented by P(SD).

X4.3.2 *Probability of MAC With Mutual Strategic Deconfliction (Case 1):*

X4.3.2.1 The outcome achieved by successfully performing the Strategic Coordination role in this specification when planning flights is that, in general, aircraft will be contained, 95 % of flight time, in volumes that do not intersect other aircraft's volumes. The safety benefits of strategic deconfliction are obtained during these times of nominal operations.

X4.3.2.2 Fig. X4.2 depicts a categorization of all midair collisions relevant to this analysis.

X4.3.2.3 Within Case 1 (collisions between participating aircraft), there is a probability that the participating aircraft are nominally operating with excursions following a normal distribution. This can be written as P(Nominal) being the probability that the other aircraft is in a nominal state. P(Nominal') is equivalent to P(Contingency), the probability that the aircraft is in a contingency state.

X4.3.2.4 In contingency cases (off nominal), P(MAC | Nominal') reduces to the bird strike model because the relationship between the aircraft cannot be established systematically, like the case where one aircraft is not participating in strategic deconfliction. Further expansion of the nominal case is done by accounting for how often aircraft are truly adjacent to one another.

X4.3.2.5 Adjacency is defined as when two volumes overlap in time, and the minimum distance between those volumes is less than the size of the more recently announced volume in a direction perpendicular to an intended direction of flight in the more recently announced volume. When not adjacent, this results in P(MAC | Nominal | Adj') taking on an extremely small value. At a corridor half-width of 4 sigma (threshold of non-adjacency under this definition with 95 % in-volume containment), the rate of volume excursions is low enough to protect manned aircraft flying near terrain for Required Navigation Performance-Authorization Required (RNP-AR) approved operators/operations (see X4.5). The conformance assurance of manned aircraft in these operations is assessed by an Operational Safety Assessment that defines Normal, Rare-Normal, and specified Non-Normal events (aircraft-level probable (single) system failures that may not result in normal distribution of position within the defined volume, but have been demonstrated to be contained within the defined volume). So we can consider this value effectively zero when compared to risk in adjacent-volume scenarios.

X4.3.2.6 The prevalence of adjacency can be estimated in some cases using the AFIT bird-strike model by assuming that flight plans are relatively random with regard to each other, and adjacency occurs when the cross-sectional area of double-size flight volumes (rather than the cross-sectional area of the aircraft) intersect. The duration of these periods of adjacency can be estimated by assuming random near-intersection angles. Areas with more structured coordination between flights, such as dense operations within a vertiport, may require a different model to estimate prevalence of adjacency.

X4.3.2.7 Adjacency presents the dominant occurrence for interaction (collision) under strategic deconfliction between two participating, nominally behaving aircraft. When two nominally behaving aircraft are adjacent to one another, they must have instantaneous lateral, vertical, and longitudinal overlap to result in a collision.

[13] Vaira, B. J., Estimating Bird/Aircraft Collision Probabilities and Risk Utilizing Spatial Poisson Processes, Air Force Institute of Technology, 2012, https://apps.dtic.mil/dtic/tr/fulltext/u2/a563995.pdf.

X4.3.2.8 Using a normal distribution describing deviations away from the intended flight path, the probability of overlap along a particular axis can be computed for a single, specific time during the flight. To express P(MAC|Nominal|Adj) in relation to time (for example, probability per flight hour), these probabilities must be expressed in terms of time. To translate from probability at a specific time point to probability over a given duration, the fundamental sampling frequency must be determined—this is the frequency at which centerline deviations become decorrelated from each other. One way to fully constrain the problem is to choose values for the following variables:

(1) Fraction of flight time conforming to the volume (*x* percent probability of occupancy)—this defines the volume size for the aircraft when a normal distribution is assumed for deviations from intended flight path.

(2) Number of excursions per flight hour at the fundamental sampling frequency—necessary to compute the number of samples drawn from the deviation distribution defined by X4.3.2.8*(1)* to evaluate duration-based probability of collision from single-sample results.

(3) Fraction of volume dimension (perpendicular to excursion) occupied by the aircraft—probability of collision increases per excursion if more of the volume is occupied as there is less opportunity for aircraft to avoid collision by separation in the axis perpendicular to the nominal overlap.

X4.3.2.9 Once the above values are chosen, the probability of vertical overlap can be computed in a similar manner as the probability of lateral overlap, except that a different portion of the normal distribution is integrated. As a conservative assumption, the probability of longitudinal overlap can be considered equal to the probability of vertical overlap; this assumption is warranted in the case where two adjacent aircraft happen to be perfectly synchronized in time but are not intentionally maintaining that synchronization.

X4.3.2.10 Without loss of generality, "lateral" and "vertical" may be interchanged with each other to capture different flight volumes that are adjacent vertically rather than adjacent horizontally.

X4.4 *Example Applied - GA Safety Level*—For a typical consumer-level drone, an example safety analysis may look like the following:

X4.4.1 *General Assumptions:*

X4.4.1.1 Flight performance

(1) 15 minute flight duration (longer flights present more opportunity for collisions)

(2) 0.4 m^2 cross-sectional MAC area (in accordance with bird-strike model)

(3) ≥95 % of time inside volumes (fraction of flight time conforming to the volume, in accordance with this specification)

(4) ≤18 10 second excursions per flight hour (number of excursions per flight hour at the fundamental sampling frequency, in accordance with this specification)

(5) Off-nominal conditions 1 % of time (how much of the time nominal strategic deconfliction cannot be accomplished, and collisions instead follow the bird-strike model)

X4.4.2 *Ground Risk:*

X4.4.2.1 Assumptions

(1) 1 % of aircraft not participating in strategic deconfliction (how many of the other aircraft are not nominally contained within deconflicted 4D volumes)

(2) 1.0 aircraft/mi^2 (risk of collision increases as density increases)

(3) 200 ft altitude band (smaller altitude bands result in increased aircraft density)

(4) 25 mph average speed (faster aircraft sweep through more airspace and increase the opportunity for collision per flight time)

(5) 5 % of volume edge occupied by aircraft (this fraction of volume dimension, perpendicular to excursion, occupied by the aircraft affects the probability that an aircraft entering another flight's volume will actually experience a collision with that other aircraft—an aircraft that is small relative to its volumes is less likely to collide with an intruding aircraft than an aircraft that occupies a larger fraction of its volumes)

X4.4.2.2 Calculations without strategic deconfliction:

(1) P(MAC): 1.0×10^{-4}/flight hour (2.5×10^{-5}/flight)

(a) 39k flights between collisions

(b) 9.8k flight hours between collisions

X4.4.2.3 Calculations with strategic deconfliction:

(1) P(MAC) between aircraft in adjacent volumes under nominal conditions: 4.8×10^{-4}/flight hour (4.4×10^{-5}/flight)

(2) 0.03 % of flight time involves adjacent volumes

(a) 0.32 adjacencies per flight

(b) 0.7 seconds average duration of adjacency

(3) P(MAC): 2.1×10^{-6}/flight hour (5.4×10^{-7}/flight)

(a) 1861k flights between collisions

(b) 465k flight hours between collisions

X4.4.2.4 Comparison - strategic deconfliction reduces midair collisions by 97.9 %:

(1) If time inside volumes is increased from 95 % to 99.9 % and only one excursion of 3.6 seconds is allowed per flight hour, the reduction of midair collisions by strategic deconfliction increases from 97.9 % to 98.0 %. This small change in advantage at this margin indicates that the primary limiting factors are the rate of off-nominal conditions, and the nonparticipation rate rather than the performance requirements for nominal, participating aircraft.

X4.5 *RNP Separation from Terrain*:

X4.5.1 The lateral dimension of the airspace volume is defined with a "Required Navigation Performance" (RNP) level by the air navigation service provider. During airworthiness approval of the aircraft, the performance is demonstrated to a minimum RNP level by mode of flight (autopilot, flight director, etc.). In addition, an Operational Safety Assessment is conducted to understand the effects of certain system failures. The result is a 2-sigma bound of the Total System Error of the aircraft operation. Required Navigation Performance-Authorization Required (RNP-AR) terminal (arrival and departure) define the lateral boundary of the protected volumes at 4-sigma.

These procedures are deployed throughout the world and are in daily use by commercial airlines operating Boeing and Airbus aircraft and many private operators of business aircraft. It is an obvious extension, at a lower collision risk, to apply the 4-sigma airspace bound to strategic deconfliction of UA.

X5. FAILURE MODES AND EFFECTS ANALYSIS

X5.1 Overview

X5.1.1 This appendix summarizes an FMEA performed to ensure that failures of participants and infrastructural components in the UTM ecosystem described in this specification result in a fail-safe condition. There are no formal requirements provided in this appendix, but it does provide a mapping to requirements in the specification that support the approach summarized for each scenario.

X5.1.2 The emphasis on a fail-safe approach was taken because there can be many USS participants in a USS network and achieving a very high aggregate availability across those participants would be very difficult. In most cases, a fail-safe approach mitigates the need for high availability requirements. That is not to say availability requirements are inappropriate in all cases. For example, a regulator may wish to levy an availability requirement on key shared resources, such as the DSS, to ensure the ecosystem is functional a high percentage of the time. These types of requirements are beyond the scope of this specification.

X5.1.3 To achieve a fail-safe condition, requirements are included to ensure one of the following outcomes in the presence of failures:

X5.1.3.1 Unsafe situations are avoided by precluding transactions for which safety cannot be assured. For example, new operations cannot be created if the DSS fails entirely.

X5.1.3.2 Unsafe situations are avoided by providing an alternative means to achieve a safe outcome. For example, if the DSS fails entirely, and relevant USS cannot be identified for a contingent or high priority operational intent, a broadcast mechanism could be used to inform all USSs.

X5.1.3.3 Awareness when communication cannot be achieved. In some circumstances, such as an active flight whose managing USS has failed, it is not possible to alert UAS personnel or the operator's automation to certain situations, such as a new constraint or high priority flight. However, awareness can be provided to the authorized constraint provider for the constraint or UAS personnel or the operator's automation for the high priority flight alerting them to the situation and allowing an informed decision to be made. (Note also that this version of the specification does not address other potential mitigators, such as onboard DAA in the case of a high priority operation.)

X5.1.4 Although not a safety concern, another factor in devising requirements to achieve fail-safe conditions is that, as much as possible, the failed entity should bear the brunt of its failure. For example, if a USS fails entirely and cannot support Strategic Coordination, other USSs should be able to plan over Accepted flights managed by the failed USS.

X5.1.5 Scenarios for this analysis were defined based on examination of the interoperability interfaces between the various components of the UTM ecosystem described in this specification. This includes USS interactions with the DSS, USS interactions with other USSs, and USS interactions with a security authorization server. The scenario impacts are described, and mitigations to achieve one of the fail-safe outcomes enumerated in X5.1.3 are provided, along with a mapping to where the corresponding requirements are located in this specification. Because the safety case for this version of this specification is limited to strategic deconfliction, mitigations are not provided in all cases for failures affecting other services. This may change in future versions of this specification if a safety case is established for other services.

X5.1.6 Note that the FMEA considered multiple options for mitigation of some scenarios. For brevity, only the selected option is described in this summary.

X5.2 Analysis Summary

X5.2.1 *Relevant USS Fails, Planning USS Cannot Obtain Operational Intents in Accepted State:*

X5.2.1.1 *Description*—A USS fails, and other USSs attempting to plan an operation cannot obtain details of a relevant operational intent in the accepted state.

X5.2.1.2 *Mitigation*—The failed USS can be reported down to the DSS. This uses a privileged interface where the regulator or industry consortium, or both, determines what entity in the UTM ecosystem is allowed to make the determination. Once a USS is reported down, new operational intents can be added that potentially conflict with the operational intents in the accepted state that are managed by the failed USS. Because the USS is reported as down, the DSS does not require the OVNs for relevant flights managed by the failed USS when other USSs create new operational intents. When the failed USS is restored and it attempts to activate operational intents it manages, it must provide OVNs for other flights in the area and will be blocked from activation if missing a conflicting operational intent that was created while the USS was down. The operational intent it is attempting to activate must be replanned or cancelled. This approach places the penalty on the failed USS and does not block other USSs.

X5.2.1.3 *Requirements References*—Annex A2.4.2.1, requirement DSS0100; Subsection 5.4.2, requirement SCD0005.

X5.2.2 *Relevant USS Fails, Planning USS Cannot Obtain Operational Intents in Active, Nonconforming, or Contingent States:*

X5.2.2.1 *Description*—A USS fails, and other USSs attempting to plan an operation cannot obtain details of a relevant operational intent in the Active, Nonconforming, or Contingent States. The primary impact is to CMSA, which is not part of the safety case for this version of the specification.

X5.2.2.2 *Mitigation*—Mitigation may be required in the future for CMSA if it becomes part of the safety case for capabilities such as ground-based DAA.

X5.2.2.3 *Requirements References*—Subsection 5.4.2, requirement SCD0010.

X5.2.3 *Relevant USS Fails With Off-Nominal Flight:*

X5.2.3.1 *Description*—A USS fails, and a flight it manages goes Nonconforming or Contingent. Unable to provide situational awareness data to relevant USSs. (Note this scenario effectively represents a double failure.) The primary impact is to CMSA, which is not part of the safety case for this version of the specification.

X5.2.3.2 *Mitigation*—Mitigation may be required in the future for CMSA if it becomes part of the safety case for capabilities such as ground-based DAA.

X5.2.3.3 *Requirements References*—None for this version of this specification.

X5.2.4 *Single Instance of DSS Fails:*

X5.2.4.1 *Description*—In a DSS pool of *n* instances (for example, three or more), an instance that is currently being used by one or more USSs fails. (Note that a failure of a DSS instance in a pool of one would be equivalent to X5.2.6.)

X5.2.4.2 *Mitigation*—The affected USS switches to another DSS instance in the pool. DSS transactions are synchronized across DSS instances before a successful return code is provided.

X5.2.4.3 *Requirements References*—Annex A2.3.6, requirement DSS0020; X2.13 future work item.

X5.2.5 *Single Instance of DSS Fails Mid-Transaction:*

X5.2.5.1 *Description*—In a DSS pool of *n* instances (for example, three or more), the instance being used by a USS fails mid-transaction, raising the concern of inconsistent data amongst DSS instances in the pool.

X5.2.5.2 *Mitigation*—The specification requirements that transactions be synchronized before a successful return code is provided. Depending on the exact timing of the failure, the transaction will have been synchronized or not, but there is no potential for an inconsistent state across DSS instances.

X5.2.5.3 *Requirements References*—Annex A2.6.2.4, requirement DSS0215.

X5.2.6 *Complete DSS Failure:*

X5.2.6.1 *Description*—Despite redundancy and any multi-cloud hosting and/or diverse implementations of the DSS instances, failure occurs that takes down all or a majority of the DSS instances.

X5.2.6.2 *Mitigation*—In this scenario, new operational intents cannot be created, and accepted operational intents cannot be activated. The only exposure is the loss of the ability to provide situational awareness for active flights that transition to an off-nominal state. The safety case addressed in this version of this specification for strategic conflict detection does not depend on CMSA. In future versions of the specification where CMSA is potentially included in the safety case for certain tactical scenarios, a broadcast capability can be added to inform all USSs of an off-nominal situation rather than using the DSS to inform only relevant USSs.

X5.2.6.3 *Requirements References*—Subsection 5.4.2, requirements SCD0015, SCD0020, SCD0025, SCD0030, SCD0035, SCD0040, SCD0045, SCD0050, SCD0055, SCD0060, SCD0065, and SCD0070.

X5.2.7 *Managing USS Fails, New Constraint Affects Operational Intent in Accepted State:*

X5.2.7.1 *Description*—A managing USS fails with an operational intent in the Accepted state. A new constraint is issued that is relevant to the operational intent. The constraint manager USS is informed by means of a subscription notification that it needs to provide the constraint details to the managing USS, but cannot because it is down.

X5.2.7.2 *Mitigation*—The affected operational intent cannot be activated without providing the OVNs for relevant operational intents and constraints. When the managing USS is restored and attempts to activate the operational intent, the DSS will fail the request and inform the USS of the missing constraint OVN. Note, the authorized constraint provider will also be informed that not all notifications to relevant USSs could be performed.

X5.2.7.3 *Requirements References*—Annex A2.3.3, requirement DSS0005; Subsection 5.7.2.18, requirement CSTM0090.

X5.2.8 *Managing USS Fails, New Constraint Affects Operational Intent in Active or Nonconforming State:*

X5.2.8.1 *Description*—A managing USS fails with an operational intent in the active or nonconforming state. A new constraint is issued that is relevant to the operational intent. The constraint manager USS is informed by means of a subscription notification that it needs to provide the constraint details to the managing USS, but cannot because it is down. The managing USS also is unable to pass the constraint information on to the UAS personnel or to the operator's automation.

X5.2.8.2 *Mitigation*—The constraint manager USS will receive a subscription notification for the relevant operational intent and attempt to push the constraint details to the managing USS. The specification requires that if the constraint manager is unable to provide the details to a relevant USS, it must notify the authorized constraint provider. This provides awareness to the authorized constraint provider that UAS personnel or operator's automation for an active flight cannot be informed of the constraint. The authorized constraint provider can use this information to decide how to proceed.

X5.2.8.3 *Requirements References*—Subsection 5.7.2.17, requirement CSTM0085.

X5.2.9 *Constraint Manager Fails, Managing USS for Operational Intent Under Construction Cannot Obtain Constraint Details:*

X5.2.9.1 *Description*—A constraint exists in the area where a managing USS is attempting to create a new operational intent. The managing USS cannot obtain the details of the constraint to inform UAS personnel or the operator's automation system.

X5.2.9.2 *Mitigation*—The new operational intent cannot be created unless the managing USS happened to already have the constraint details from previous planning activities. While impactful to the affected operations, it precludes introduction

of a new operational intent where neither the UAS personnel nor the operator's automation system have the constraint details. Note, a regulator may choose to impose availability requirements on constraint manager USSs to limit the frequency of this scenario.

X5.2.9.3 *Requirements References*—Subsection 5.8.2.1, requirement CSTP0005.

X5.2.10 *Constraint Manager Fails before Notifications for New Constraint Provided to Relevant USSs:*

X5.2.10.1 *Description*—A constraint manager USS creates a new constraint and receives subscription notifications for relevant operational intents that are already in the Active or Nonconforming state. Before the notifications are provided to the relevant USS, the constraint manager USS fails, and the affected UAS personnel or operator's automation system(s) are not notified.

X5.2.10.2 *Mitigation*—The authorized constraint provider would be aware of the constraint manager USS failure and also would fail to receive the confirmation of successful constraint creation/modification, and dissemination of the constraint details. This provides awareness to the authorized constraint provider that neither UAS personnel nor the operator's automation system for any relevant active flights can be informed of the constraint. The authorized constraint provider can use this information to decide how to proceed.

X5.2.10.3 *Requirements References*—Subsection 5.7.2.18, requirement CSTM0090.

X5.2.11 *Failure of SCD Logic in a Planning USS:*

X5.2.11.1 *Description*—A USS is constructing a new operational intent. It has a disallowed conflict with another operational intent, but the conflict detection logic fails to detect the conflict. The new operational intent is posted to the DSS with the disallowed conflict.

X5.2.11.2 *Mitigation*—This scenario represents a logic failure as opposed to a real-time component failure. The onboarding test procedures and ongoing audit tests for USSs are the mechanisms for detecting these types of logic failures, and it is assumed regulatory operating rules would hold the responsible USS accountable. This specification does require logging of data used to support strategic conflict detection, including operational intent data produced by a USS and operational intent data sent to and received from other USSs.

X5.2.11.3 *Requirements References*—GEN0015, Subsection 5.2.5, Subsection 5.9.2.4, requirement LOG0015; Subsection 5.9.2.5, requirement LOG0020.

X5.2.12 *Operational Intent Becomes Nonconforming or Contingent, Managing USS Fails to Deliver Notifications to Relevant USSs:*

X5.2.12.1 *Description*—A USS transitions an operational intent to an off-nominal state, receives subscription notifications for relevant USSs, but fails to send the requisite notifications.

X5.2.12.2 *Mitigation*—This scenario represents a logic failure as opposed to a real-time component failure. Several mitigations for this scenario are provided by this specification including organizational requirements for a USS to be developed under an ISO/IEC 27001-compliant Information Security Management System and an ISO/IEC 9001-compliant Quality Management System; the assumed use of the mandatory ecosystem test environment to support testing for USS onboarding and ongoing audit, both of which can be prerequisites for obtaining security access tokens to support any interaction with the ecosystem; mandatory logging for all interactions with this ecosystem; and assumed regulator-approved operating rules that will hold the responsible USS accountable.

(1) In addition, the safety case for this version of this specification is not dependent upon CMSA. Mitigation may be required in the future for CMSA if it becomes part of the safety case for capabilities such as ground-based DAA.

X5.2.12.3 *Requirements References*—Subsection 5.2.2, requirements GEN0005, GEN0015; Subsection 5.2.5, requirements GEN0300, GEN0305, GEN0310; Appendix X6; Subsection 5.9.2, all logging requirements.

X5.2.13 *USS Does Not Adhere to Interoperability Requirements:*

X5.2.13.1 *Description*—A USS indicates to UAS personnel or the operator's automation system that it is operating properly, sharing intents, etc., but in fact is not. Variety of failure scenarios, such as operational intents not actually in the DSS, state changes not communicated, etc.

X5.2.13.2 *Mitigation*—This scenario represents a set of logic failures as opposed to a real-time component failure. Several mitigations for this scenario are provided by this specification, including organizational requirements for a USS to be developed under an ISO/IEO 27001-compliant Information Security Management System, and an ISO/IEC 9001-compliant Quality Management System; the assumed use of the mandatory ecosystem test environment to support testing for USS onboarding and ongoing audit, both of which can be prerequisites for obtaining security access tokens to support any interaction with the ecosystem; mandatory logging for all interactions with this ecosystem; and assumed regulator-approved operating rules that will hold the responsible USS accountable.

X5.2.13.3 *Requirements References*—Subsection 5.2.2, requirements GEN0005, GEN0015; Subsection 5.2.5, requirements GEN0300, GEN0305, GEN0310; Appendix X6; Subsection 5.9.2, all logging requirements.

X5.2.14 *USS Fails to Provide Timely Information for Off-Nominal Operational Intent:*

X5.2.14.1 *Description*—A UA becomes nonconforming or contingent, and the managing USS fails to communicate this status to relevant USSs.

X5.2.14.2 *Mitigation*—The safety case for this version of this specification is not dependent upon CMSA; it does not hinge on individual off-nominal situations, but instead on the aggregate operational intent conformance requirements. Mitigation may be required in the future for CMSA if it becomes part of the safety case for capabilities, such as ground-based DAA. The specification does require the logging of data necessary to audit and analyze these situations.

X5.2.14.3 *Requirements References*—Subsection 5.9.2, requirements LOG0010, LOG0015, LOG0020, LOG0040.

X5.2.15 *Failure of Authorization Server:*

X5.2.15.1 *Description*—Authorization server cannot issue properly formatted access tokens for one or more USS. Tokens will have a TTL so impact is generally not immediate. However, beyond the TTL, if the authorization server is not restored, all transactions requiring interoperability interfaces will cease to function. For example, new operational intents cannot be created, accepted operational intents cannot be activated, etc. The primary impact is to CMSA, which is not part of the safety case for this version of the specification.

X5.2.15.2 *Mitigation*—Mitigation may be required in the future for CMSA if it becomes part of the safety case for capabilities, such as ground-based DAA.

X5.2.15.3 *Requirements References*—No specific requirements. Tokens are required on all interoperability interfaces defined in Annex A2; architectural alternatives for security controls on interoperability interfaces are discussed in Appendix X1.

X5.2.16 *Failure of Internet Communications:*

X5.2.16.1 *Description*—A USS is unable to execute any interoperability requirements due to a failure of internet communications. (There can be multiple scenarios resulting in this outcome.) All transactions requiring interoperability interfaces will cease to function. For example, new operational intents cannot be created, accepted operational intents cannot be activated, etc. Safety concerns only exist for flights already active, and the primary impact is to CMSA which is not part of the safety case for this version of the specification.

X5.2.16.2 *Mitigation*—Mitigation may be required in the future for CMSA if it becomes part of the safety case for capabilities, such as ground-based DAA.

X5.2.16.3 *Requirements References*—Subsection 5.4.2, requirements SCD0015, SCD0020, SCD0025, SCD0030, SCD0035, SCD0040, SCD0045, SCD0050, SCD0055, SCD0060, SCD0065, and SCD0070.

X5.2.17 *Malicious or Compromised Actors/USS:*

X5.2.17.1 *Description*—Due to malicious intent or a security breach, a USS indicates to UAS personnel or the operator's automation system that it is operating properly, sharing intents, etc., but in fact is not. Variety of failure scenarios such as operational intents not actually in the DSS, state changes not communicated, etc. (The root cause differs but, thereafter, this scenario effectively is the same as X5.2.14.)

X5.2.17.2 *Mitigation*—This scenario represents a set of logic failures as opposed to a real-time component failure. Several mitigations for this scenario are provided by this specification, including organizational requirements for a USS to be developed under an ISO/IEO 27001-compliant Information Security Management System and an ISO/IEC 9001-compliant Quality Management System; the assumed use of the mandatory ecosystem test environment to support testing for USS onboarding and ongoing audit, both of which can be prerequisites for obtaining security access tokens to support any interaction with the ecosystem; mandatory logging for all interactions with this ecosystem; and assumed regulator-approved operating rules that will hold the responsible USS accountable.

X5.2.17.3 *Requirements References*—Subsection 5.2.2, requirements GEN0005, GEN0015; Subsection 5.2.5, requirements GEN0300, GEN0305, GEN0310; Appendix X6; Subsection 5.9.2, all logging requirements.

X6. UTM ECOSYSTEM TESTING STRATEGY

X6.1 This specification assumes a federated collection of USSs providing UTM services in overlapping airspace, with multiple USSs undergoing some form of regulatory oversight process to become and remain authorized service providers.

X6.2 While UTM represents a different approach from traditional ATC where typically a single system operated by an ANSP provides service for a particular volume of airspace, this specification draws on lessons learned from traditional ATC systems maintenance, as well as from a number of UTM research projects conducted over a period of several years in multiple countries, to support a testing and integration strategy for USSs. Requirements have been included for some elements of this strategy in this version of the specification, and more will be added in subsequent versions.

X6.3 Key goals of this strategy include:

X6.3.1 *Performance-Based Outcomes*—The system is tested as closely to how it will operate in production as practical, and test outcomes are based on whether key objectives of this specification are achieved. The intermediate outcomes are not tested; this is an "integration test" approach rather than a "unit test" approach.

X6.3.2 *Full Interoperability Verification*—Achieved interoperability is often not transitive in real-world deployments, so individual or pairwise testing of USSs has proven insufficient to ensure full system functionality. Because of this, tests involve as many USSs as practical in the same test.

X6.3.3 *Rapid Iteration*—It is difficult for USSs to discover many types of issues without testing with multiple other USSs. When these tests are conducted infrequently, this means that the fixes for any issues identified are hard to validate, and the deployment of fixes, updates, and improvements is tied to these infrequent tests. To support ongoing assurance of high-quality systems while enabling innovation, testing is envisioned daily or weekly not just quarterly or annually.

X6.4 Key elements of this strategy include:

X6.4.1 *Common Test Suites*—Predefined, common test suites addressing USS functionality and interoperability developed in collaboration between USS implementers and regulators reduce the overhead relative to multiple USS implementers independently developing test suites, processes, and procedures. Common test suites are also necessary to support testing of services, such as the DSS, that are specified in a

performance-based manner, but that ultimately must be tested with diverse implementations.

X6.4.2 *Automated testing*—The ability to execute tests (including USS interoperability tests) and assess the results in an automated way significantly expedites the testing process, reducing the potential for human error and shortening the time required to verify that new or updated software is functioning properly. This becomes increasingly important with multiple service providers as a fixed, infrequent update cycle hinders both corrective and innovation-driven updates to USSs.

X6.4.2.1 Automated testing also facilitates the automatic generation of test reports necessary for oversight and audit purposes.

X6.4.3 *Operational Audit*—Besides initial onboarding and testing of updates to USS implementations, common tests and automated test methods in combination with standardized interfaces and mechanisms for injecting test data and scenarios in parallel with live operations can support continuous audit of operational USSs to verify ongoing compliance to regulator-specified operating requirements. This type of mechanism is commonly used in ATC systems today, both before releasing a system by support personnel to operational personnel and to verify correct operation on an ongoing or periodic basis.

X6.4.4 *Ecosystem Test Environment*—ANSPs that support multiple, interacting ATC systems typically establish a test environment in a maintenance and support facility that includes instances of each of the systems. This enables testing not only a single system in isolation, but also the interactions between all relevant systems as it is highly undesirable to discover that a new release of one system causes problems in another system in the operational environment. Similar experience has been observed through many UTM trials. Ad hoc, pairwise integration testing as opposed to holistic, ecosystem-wide testing of interacting USSs frequently, if not inevitably, leads to problems in the operational environment. Consequently, it is desirable to mimic the traditional ANSP approach and provide the ability to test the ecosystem.

X6.4.4.1 Given the transition from singular, ANSP-provided systems to a federated collection of USSs, aggregating independent instances of every USS implementation into a common facility would be logistically challenging and would present an unnecessary cost burden to a regulator or ANSP, or both. Instead, the objective can be met by each USS implementer providing a persistently supported test instance (computing resources and software) that can be accessed by all other ecosystem participants over the internet using the same security controls as the operational UTM environment. While the ecosystem test environment is primarily provided by USS implementers, some elements may be provided by the regulator, such as a security token server.

X6.4.4.2 It is expected that governance of the test environment, including access control, will be established through collaboration between the regulator and USS implementers. There are multiple possible paradigms, including management of the test environment and associated processes by an industry consortium, an independent testing body, the regulator, or the ANSP.

X6.4.5 *Continuous Improvement Feedback Loop*—While 100 % coverage of all possible scenarios in the federated UTM environment is not possible, this strategy assumes a feedback loop to facilitate continuous improvement of the test processes. Common test suites can be expanded as necessary to address new scenarios, and can include variations unique to specific regulatory environments.

X6.5 In this version of the specification, an overview of test requirements that support the definition of a common test suite for the DSS is provided in A2.7, DSS Testing.

X6.6 Subsection 5.2.5, Test Environment, provides initial requirements for implementers to provide a test instance hosting their current operational software to support ecosystem-wide testing, and to support test data injection.

X6.7 Subsequent versions of this specification will include additional requirements, APIs, and test suites consistent with the strategy described in this appendix.

X7. LIST OF WORKING GROUP PARTICIPANTS AND CONTRIBUTORS

Name	Organization
Borda, Fred	Aerial Innovation
Campbell, Scot	Airbus
Egorov, Maxim	Airbus
Evans, Tony	Airbus
Hohtari, Henri	AirMap
Lamprecht, Andreas	AirMap
Kuhlman, Michael	Formerly AiRXOS, part of GE Aviation
Lester, Edward (Ted)	Formerly AiRXOS, part of GE Aviation
Cassidy, Sean	Amazon
Champagne, Robert	Amazon
Ganjoo, Amit, (Working Group Co-Chair)	ANRA Technologies
Murphy, David	ANRA Technologies
Klavon, Brent	ANRA Technologies
Modha, Ajay	ANRA Technologies
Cooper, Christopher	AOPA
Dicicco, J	ASTM
Kenul, Philip (Chair, ASTM F38 UAS Committee)	ASTM
Mikolajewski, Mary (ASTM F38 Staff Manager)	ASTM

Name	Organization
Daly, Brian K.	AT&T
Musgrove, Peter	AT&T
Baum, Michael S.	Aviators Code Initiative
Calhoun, Sean	CAL Analytics
Atkins, Ella	Collins Aerospace
Liberko, Nicholas	Collins Aerospace
Caina, Javier	DJI
Engelstad, Ken	EASA
Hately, Andrew	Eurocontrol
Abraham, Biruk	FAA
Albuquerque, Paul	FAA
Barefoot, Galina	FAA
Campbell, Paul	FAA
Chen, Bin “David”	FAA
Errine, Jacquelyn	FAA
Fox, Mark	FAA
Harris, Heather	FAA
Larrow, Jarrett	FAA
Magyarits, Sherri	FAA
May, Rick	FAA
Sachs, Peter T.	FAA
Segers, Rob	FAA
Fulton, Steve	Fulton Aviation
Curdy, Benoit	Swiss FOCA
Mo, Stan	Intel
Bender, Walter	JHU Applied Physics Laboratory
Belaus, Greg	Joby Aviation
Prevot, Thomas	Joby Aviation
Schwegler, Matthew	Joby Aviation
Gunnarson, Tom	Kitty Hawk
DeGarmo, Matthew T.	MITRE
Cook, Brandon	NASA
Hackenberg, Davis	NASA
Johnson, Marcus A.	NASA
Jung, Jaewoo	NASA
Levitt, Ian	NASA
Rios, Joseph	NASA
Rushton, Anthony	NATS
Nakadai, Shinji	NEC
Lacher, Andrew R.	Noblis
Thurling, Andrew	NUAIR
Davis, Mark Edward	Ollin Aviation
Driver, Ted	OneSky
Kucera, Christopher	OneSky
Daniels, Jonathan	Praxis Aerospace
Ferguson, Allison	PrecisionHawk
Martin, Terrence, Prof.	Queensland University of Technology Revolution Aerospace
Dubois, Michael	Raytheon
Naqvi, Waseem	Raytheon
Brown, Simon	RelmaTech
Hall, Philip	RelmaTech
Cruikshank, Kristian	Revolution Aerospace
Srinivasan, Gokul	Robots.Expert
Cistone, James	Sullivan Aviation Services, LLC
Deeds, Greg	Technology Exploration Group
Basti, Franco	Thales
Solomon, Adrian	Thales
Bloch-Hansen, Craig	Transport Canada
Ruff, Nathan	UASidekick
Huenaerts, Laurent	Unifly
Williame, Koen	Unifly
Nakamura, Hiroko	University of Tokyo
Bennett, Timothy	U.S. DHS
Fanelli, Matthew	Verizon/Skyward
Lincoln, David	Verizon/Skyward
Williams, Shane	Verizon/Skyward
Yanchao, Liu	Wayne State University
Blanks, Mark	Wing
Florin, Alexandra	Wing
Glasgow, Mike (Working Group Co-Chair)	Wing
Jackman, Chris	Wing
Negron, Reinaldo	Wing
Pelletier, Benjamin	Wing
Rajendran, Vishnu	Wing

RELATED MATERIAL

ASTM Standard	
ASTM F3201 Standard Practice for Ensuring Dependability of Software Used in Unmanned Aircraft Systems (UAS)	https://www.astm.org
Other Standards	
ASD-STAN Pr 4709-003 Aerospace series - Unmanned Aircraft Systems - Part 003: Geo-awareness requirements, (in draft)	https://asd-stan.org/downloads/din-en-4709-0032021-02/
IETF RFC 6749 The OAuth 2.0 Authorization Framework	https://tools.ietf.org/html/rfc6749
RTCA DO-278A Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems	https://www.rtca.org/standards/
UTM Framework Initiatives	
NASA/FAA UTM:	
FAA UTM Concept of Operations v2.0	https://www.faa.gov/uas/research_development/traffic_management/media/UTM_ConOps_v2.pdf
NASA UTM Technical Document - Home	https://www.nasa.gov/aeroresearch/utm-tech-docs-papers-presentations
Off-Nominal Reporting	https://www.nasa.gov/sites/default/files/atoms/files/2020-jung_nasa-tm-220302-508_0.pdf
Strategic Deconfliction	https://www.researchgate.net/publication/332107751_UAS_Traffic_Management_UTM_Project_Strategic_Deconfliction_System_Requirements_Final_Report
UAS Service Supplier Framework for Authentication and Authorization	https://www.nasa.gov/sites/default/files/atoms/files/2019-utm_framework-nasa-tm220364-508.pdf
European Commission / EASA:	
Commission Implementing Regulation (EU) 2019/947	https://eur-lex.europa.eu/eli/reg_impl/2019/947/oj
Commission Implementing Regulation (EU) 2021/664 of 22 April 2021 on a regulatory framework for the U-space	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0664
Opinion 01/2020: High-level regulatory framework for the U-space	https://www.easa.europa.eu/document-library/opinions/opinion-012020
SESAR:	
Concept of Operations for European UTM Systems - CORUS	https://www.sesarju.eu/projects/corus
Open Access UTM Framework UK:	
UTM System for the UK	https://s3-eu-west-1.amazonaws.com/media.cp.catapult/wp-content/uploads/2019/09/30150855/Towards-a-UTM-System-for-the-UK.pdf