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.

Designation: F3411 – 22a

# Standard Specification for Remote ID and Tracking[1]

This standard is issued under the fixed designation F3411; 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.

NOTE—Subsection 5.4.3 and Table A3.3 were corrected, with other editorial changes made throughout, and the yeardate changed on June 17, 2022.

## 1. Scope

1.1 This specification covers the performance requirements for remote identification (Remote ID) of unmanned aircraft systems (UAS). Remote ID allows governmental and civil identification of UAS for safety, security, and compliance purposes. The objective is to increase UAS remote pilot accountability by removing anonymity while preserving operational privacy for remote pilots, businesses, and their customers. Remote ID is an enabler of enhanced operations such as beyond visual line of sight (BVLOS) operations as well as operations over people.

1.2 This specification defines message formats, transmission methods, and minimum performance standards for two forms of Remote ID: broadcast and network. Broadcast Remote ID is based on the transmission of radio signals directly from a UAS to receivers in the UAS's vicinity. Network Remote ID is based on communication by means of the internet from a network Remote ID service provider (Net-RID SP) that interfaces directly or indirectly with the UAS, or with other sources in the case of intent-based network participants.

1.3 This specification addresses the communications and test requirements of broadcast or network Remote ID, or both, in UAS and Net-RID SP systems.

1.4 *Applicability:*

1.4.1 This specification is applicable to UAS that operate at very low level (VLL) airspace over diverse environments including but not limited to rural, urban, networked, network degraded, and network denied environments, regardless of airspace class.

1.4.2 This specification neither purports to address UAS operating with approval to use ADS-B or secondary surveillance radar transponders, nor does it purport to solve ID needs of UAS for all operations.

1.4.3 In particular, this specification does not purport to address identification needs for UAS that are not participating in Remote ID or operators that purposefully circumvent Remote ID.

1.5 The values stated in SI units are to be regarded as standard. The values given in parentheses after SI units are provided for information only and are not considered standard.

1.5.1 Units of measurement included in this specification:

| | |
|---|---|
| m | meters |
| deg, ° | degrees of latitude and longitude, compass direction |
| s | seconds |
| Hz | Hertz (frequency) |
| dBm | decibel-milliwatts (radio frequency power) |
| ppm | parts per million (radio frequency variation) |
| µs | microseconds |
| ms | milliseconds |

1.6 *Table of Contents:*


| Title | Section |
|---|---|
| Scope | 1 |
| Referenced Documents | 2 |
| Terminology | 3 |
| Remote ID and Network Interoperability Conceptual Overview | 4 |
| Performance Requirements | 5 |
| TEST METHODS | |
| Scope | 6 |
| Significance and Use | 7 |
| Hazards | 8 |
| Test Units | 9 |
| Procedure | 10 |
| Precision and Bias | 11 |
| Product Marking | 12 |
| Packaging and Package Marking | 13 |
| Keywords | 14 |
| ANNEX A1—Broadcast Authentication Verifier Service | Annex A1 |
| ANNEX A2—Network Remote ID Interoperability Requirements, APIs, and Testing | Annex A2 |
| ANNEX A3—Tables of Values | Annex A3 |
| ANNEX A4—USS-DSS and USS-USS OpenAPI YAML Description | Annex A4 |
| ANNEX A5—Number Registrar Management Policy | Annex A5 |
| APPENDIX X1—Performance Characteristics | Appendix X1 |
| APPENDIX X2—List of Subcommittee Participants and Contributors | Appendix X2 |
| APPENDIX X3—Background Information | Appendix X3 |


[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 June 17, 2022. Published July 2022. Originally approved in 2019. Last previous edition approved in 2022 as F3411–22. DOI: 10.1520/F3411-22A.

Copyright © ASTM International, 100 Barr Harbor Drive, PO Box C700, West Conshohocken, PA 19428-2959. United States



Documents
Document Sharing Hub
Full document details: ASTM F3411-22a

1.7 *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.* Some specific hazards statements are given in Section 8 on Hazards.

1.8 *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:*[2]

F3060 Terminology for Aircraft

F3341 Terminology for Unmanned Aircraft Systems

2.2 *Other Standards:*

ANSI/CTA-2063-A Small Unmanned Aerial Systems Serial Numbers[3]

Bluetooth[4,5] Core Specification 5.0[6]

IEEE 802.11 Standard for Information technology--Telecommunications and information exchange between systems - Local and metropolitan area networks--Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications[7,5]

IEEE 1609.2 IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages[7]

IETF RFC3339 Date and Time on the Internet: Timestamps[8]

IETF RFC4122 A Universally Unique IDentifier (UUID) URN Namespace[9]

IETF RFC8126 Guidelines for Writing an IANA Considerations Section in RFCs[10]

Neighbor Awareness Networking Specification [11,5]

FAA UTM ConOps v1.0 Unmanned Aircraft System (UAS) Traffic Management (UTM) Concept of Operations[12]

WGS-84 World Geodetic System — 1984[13]

## 3. Terminology

3.1 This standard uses terminology contained within F3341, UAS Terminology Standard, and F3060, Aircraft Terminology Standard. These terms are not duplicated within this document.

3.2 *Unique and Common Terminology*—Terminology used in multiple standards is defined in F3341 and F3060. Terminology that is unique to this specification is defined in 3.3.

3.3 *Definitions of Terms Specific to This Standard:*

3.3.1 *authentication, n*—the process or action of verifying that the source of a Remote ID message is the originator of the message.

3.3.2 *broadcast, v*—to transmit data to no specific destination or recipient; data can be received by anyone within broadcast range.

3.3.3 *broadcast UAS, n*—a UAS that is equipped for and is actively broadcasting Remote ID data during an operation; being a broadcast UAS is not mutually exclusive with being a networked UAS.

3.3.4 *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).

3.3.5 *DSS entity, n*—a generic concept that refers to information that can be discovered using the discovery and synchronization service (DSS).

3.3.5.1 *Discussion*—Entities are characterized by a 4-D volume of airspace (that is, a volume defined in $x$, $y$, $z$ plus time limits). For Remote ID, the entity type is referred to as an identification service area. Operations and constraints are examples of other types of entities that are the subject of other UTM standards.

3.3.6 *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.

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

3.3.8 *dynamic data, n*—data that changes over the duration of the flight; for example, longitude and latitude.

3.3.9 *Ground Control Station (GCS), n*—the part of a UAS that remotely controls the UA. It may or may not have a remote pilot directly manipulating the controls.

3.3.10 *identify*—the result of the process to establish the identity of a specific UAS that is traceable to the owner and remote pilot.

3.3.11 *intent-based network participant, n*—a UAS for which the operator has reported an intended area (a volume of

[2] 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.

[3] Available from American National Standards Institute (ANSI), 25 W. 43rd St., 4th Floor, New York, NY 10036, http://www.ansi.org.

[4] Used throughout the specification, Bluetooth is a registered trademark of Bluetooth SIG, Inc., 5209 Lake Washington Blvd. NE, Suite 350, Kirkland, WA 98033.

[5] Other names and brands may be claimed as the property of others.

[6] Available from https://www.bluetooth.com/specifications/archived-%20specifications/.

[7] Available from Institute of Electrical and Electronics Engineers, Inc. (IEEE), 445 Hoes Ln., Piscataway, NJ 08854-4141, https://standards.ieee.org/standard/802_11-2016.html.

[8] Available from IETF Tools, https://tools.ietf.org/html/rfc3339.

[9] Available from IETF Tools, https://tools.ietf.org/html/rfc4122.

[10] Available from https://datatracker.ietf.org/doc/html/rfc8126.

[11] Available from Wi-Fi Alliance, 10900-B Stonelake Boulevard, Suite 126, Austin, TX 78759, https://www.wi-fi.org/discover-wi-fi/wi-fi-aware.

[12] Available from https://utm.arc.nasa.gov/docs/2018-UTM-ConOps-v1.0.pdf.

[13] Available from International Civil Aviation Organization (ICAO), 999 Robert-Bourassa Boulevard, Montréal, Quebec, Canada H3C 5H7, https://www.icao.int/safety/pbn/Documentation/EUROCONTROL/Eurocontrol%20WGS%2084%20Implementation%20Manual.pdf

AVA Documents
Document Sharing Hub



Full document details: ASTM F3411-22a

airspace) and time for an operation through a Net-RID service provider; such information is then reported through the network Remote ID infrastructure. Intent-based Remote ID participation is an option for non-equipped UAS or UAS operating in environments that preclude broadcast or network participation.

3.3.12 *network Remote ID (Net-RID) service provider, n*—a logical entity denoting a UTM system or comparable UAS flight management system that participates in network Remote ID and provides data for and about UAS it manages.

3.3.13 *network Remote ID (Net-RID) display provider, n*—a logical entity that aggregates network Remote ID data from potentially multiple Net-RID service providers and provides the data to a display application (that is, an app or website); in practice, it is expected that many USSs may be both Net-RID display providers and Net-RID service providers, but standalone Net-RID display providers are possible.

3.3.14 *network publishing, v*—the act of transmitting data to an internet service or federation of services; clients, whether air traffic control (ATC), public safety officials, or possibly the general public can access the data to obtain ID and tracking information for UAS for which such data has been published.

3.3.15 *networked UAS, n*—a UAS that during operations is in electronic communication with a Net-RID service provider (for example, by means of internet Wi-Fi,[14] cellular, or satellite, or other communications medium such as short burst data satellite communications).

3.3.16 *non-equipped UAS, n*—in the context of Remote ID, a UAS that is neither a networked nor broadcast UAS (for example, a radio controlled model aircraft) and cannot directly report its location or identity.

3.3.17 *operator, n*—the individual or organization who uses, causes to use, or authorizes to use an aircraft for the purpose of air navigation, including the piloting of an aircraft, with or without the right of legal control (as owner, lessee, or otherwise). **F3060**

3.3.18 *operator location, n*—the geographic location of the remote pilot in command of a UAS.

3.3.19 *position extrapolation, n*—a capability of a Net-RID service provider to predict the location of a UAS based on a modeled 4-D trajectory derived from an intended UAS operation plan.

3.3.20 *registration, n*—the process by which an owner/operator (including contact information and other PII) and aircraft (for example, make, model) are associated with an assigned, unique identifier.

3.3.21 *shall, must versus should versus may*—use of the word "shall" implies that a procedure or statement is mandatory and must be followed to comply with this practice, "should" implies recommended, and "may" implies optional at the discretion of the supplier, manufacturer, or operator.

3.3.21.1 *Discussion*—Since "shall" and "must" statements are requirements, they include sufficient detail needed to define compliance (for example, threshold values, test methods, oversight, and references to other standards). "Should" statements also represent parameters that could be used in safety evaluations, and could lead to development of future requirements. "May" statements are provided to clarify acceptability of a specific item or practice, and offer options for satisfying requirements.

3.3.22 *static data, n*—data that remains the same or does not change often over the duration of a flight (for example, Unique ID); this is in contrast to dynamic data that may change more frequently (such as longitude and latitude).

3.3.23 *UAS operation plan, n*—a UAS operation plan is developed prior to the operation and should indicate the volume of airspace within which the operation is expected to occur, the times and locations of the key events associated with the operation, including launch, recovery, and any other information deemed important (for example, segmentation of the operation trajectory by time).

**UTM ConOps v1.0**

3.3.24 *UAS registration ID, n*—an identification number or combination of letters and numbers assigned by a CAA or authorized representative to a UAS; this is sometimes referred to as a registration number (which may or may not contain letters).

3.3.25 *UAS service supplier (USS), n*—USSs provide UTM services to support the UAS community, to connect operators and other entities to enable information flow across the USS network, and to promote shared situational awareness among UTM participants. **UTM ConOps v1.0**

3.3.26 *unique ID, n*—a data element that can be traced to a unique UAS and its operator.

3.4 *Acronyms and Abbreviations:*

3.4.1 *AES, n*—advanced encryption standard

3.4.2 *AGL, adj*—above ground level

3.4.3 *API, n*—application programming interface

3.4.4 *ARC, n*—aviation rulemaking committee

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

3.4.6 *C2, n*—command and control

3.4.7 *CAA, n*—Civil Aviation Authority

3.4.8 *CONUS, n*—contiguous United States

3.4.9 *DAR, n*—DSS airspace representation

3.4.10 *DSS, n*—discovery and synchronization service

3.4.11 *EIRP, n*—effective isotropic radiated power

3.4.12 *EMI, n*—electromagnetic interference

3.4.13 *FAA, n*—Federal Aviation Administration

3.4.14 *GCS, n*—ground control station

3.4.15 *Hz*—Hertz (cycles per second)

3.4.16 *inHg*—inch of mercury

3.4.17 *km*—kilometers

3.4.18 *kts*—knots (nautical miles per hour)

3.4.19 *LAANC*—low altitude authorization and notification capability

[14] Used throughout the specification, Wi-Fi is a registered trademark of Wi-Fi Alliance, 10900-B Stonelake Boulevard, Suite 126, Austin, TX 78759.

AVA Documents
Document Sharing Hub



Full document details: ASTM F3411-22a

3.4.20 *LE*—little endian (least significant byte first)

3.4.21 *LSB*—least significant bit

3.4.22 *LTA*—lighter than air (for example, balloon or blimp)

3.4.23 *m*—meters

3.4.24 *m/s*—meters per second

3.4.25 *mb*—millibars

3.4.26 *mm*—millimeters

3.4.27 *MAC*—media access control

3.4.28 *MPH*—miles per hour

3.4.29 *MSB, n*—most significant bit

3.4.30 *Net-RID, n*—network Remote ID

3.4.31 *PHY, n*—physical layer

3.4.32 *PII, n*—personally identifiable information

3.4.33 *PPM*—parts per million

3.4.34 *Remote ID, n*—remote identification

3.4.35 *TLS, n*—transport layer security

3.4.36 *UA, n*—unmanned aircraft

3.4.37 *UAS, n*—unmanned aircraft system

3.4.38 *USS, n*—UAS service supplier

3.4.39 *UTM, n*—UAS traffic management

3.4.40 *UUID, n*—universally unique identifier based on RFC4122 (128 bit)

3.4.41 *VIP, n*—very important person

3.4.42 *VLL, adj*—very low level (airspace—generally below 150 m (500 ft))

## 4. Remote ID and Network Interoperability Conceptual Overview

4.1 This section provides a conceptual overview of Remote ID as defined in this specification, explains the scope of the specification, and clarifies the differences between broadcast and network Remote ID. This overview does not address all nuances of the specification. The intention is to provide a contextual framework to understand the requirements contained in this specification. No requirements are provided in this section.

4.2 This section also provides an overview of the general approach to interoperability between USSs for both Network Remote ID and other UTM-related services.

4.3 *Scope of Standard and Remote ID Components:*

4.3.1 Fig. 1 identifies the actors and interfaces between actors in the Remote ID environment.

4.3.2 The scope of this specification is identified by the contents of the dotted purple box in the center of the diagram.

4.4 *Broadcast Remote ID:*

4.4.1 Broadcast Remote ID is depicted in the upper, central portion of Fig. 1 in blue. Equipment on participating UAS continuously transmit Remote ID data using one of the transmit protocols in this specification (Bluetooth or Wi-Fi). It is possible that additional transmit protocols may be added in the future as warranted by available technology. The initial technologies were selected for compatibility with commonly carried hand-held devices that have their own receiver antenna. However, equipment to receive the broadcast data is not part of

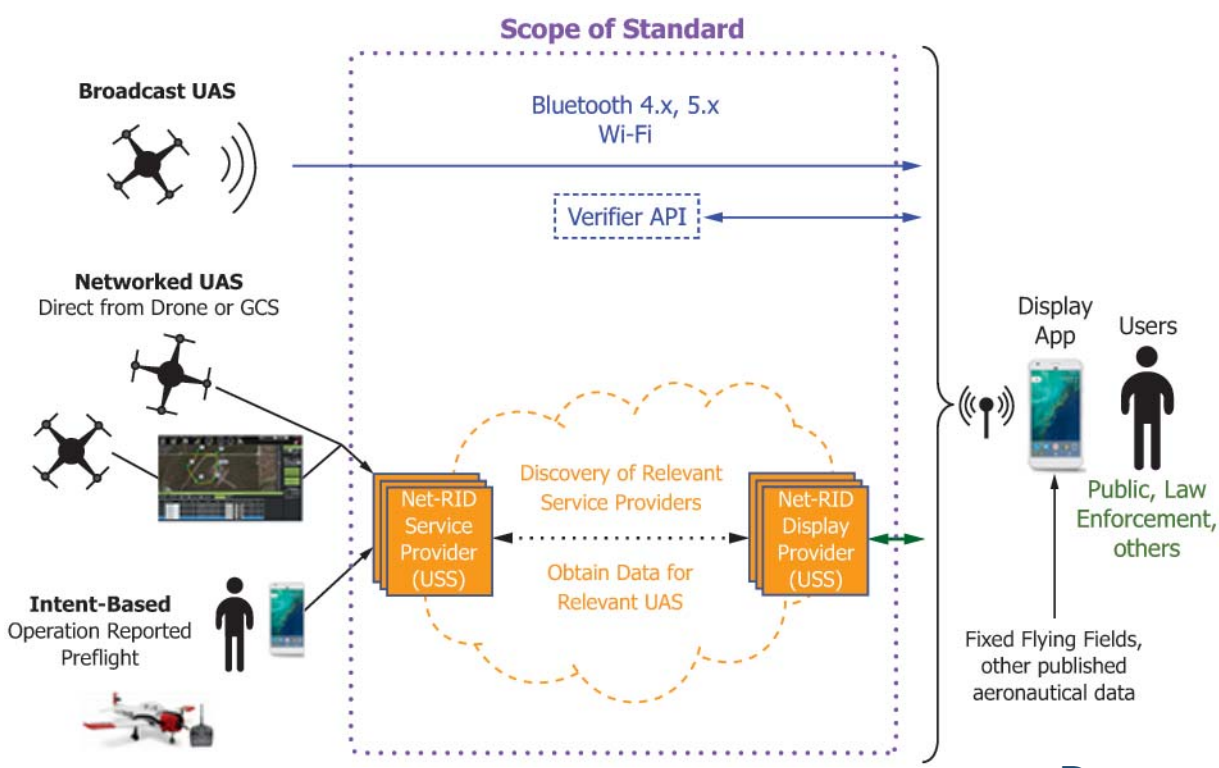


FIG. 1 Remote ID Conceptual Overview



Documents
Document Sharing Hub
Full document details: ASTM F3411-22a

the specification. Other implementations, such as receivers not integrated with hand-held devices, are possible.

4.4.2 Both Bluetooth and Wi-Fi continuously broadcast messages to advertise the presence of the associated device. These advertisements normally allow other devices to discover and establish connections with the associated device, but the advertisements themselves can carry a payload. These advertisements contain the broadcast Remote ID data. A hand-held device does not need to establish a connection to receive Remote ID data, instead it need only receive and process the advertisements.

4.4.3 Broadcast Remote ID can be used anywhere, but is necessary in areas where network coverage is unreliable, disrupted, or not available.

4.4.4 The specification also includes a range of options for authentication of broadcast data. Some of those options include digital signatures over portions or all of the Remote ID message set. While the specification does not specify the encoding format associated with signatures, it does include a standard API that would be used by a receiver of the broadcast data (for example, an app on a smartphone) to contact a verifier with the signature data for a broadcast to determine message validity. This is described in more detail in Annex A1, Broadcast Authentication Verifier Service.

4.5 *Network Remote ID:*

4.5.1 Network Remote ID can be used when both UAS operations and end users of Remote ID display applications access the internet, typically by means of cellular network. Cellular coverage tends to be higher in urban areas.

4.5.2 Network Remote ID is depicted in the lower, central portion of Fig. 1 in orange and enclosed in a dashed line cloud. The nominal case supports Networked UAS (that is, UAS that remain in contact with a Remote ID Service Provider during flight either directly or through an intermediate device such as a ground control station), although the specification accommodates intermittent loss of network connectivity. Network Remote ID also includes provisions for participation in Remote ID through intent-based preflight reporting, also referred to as Intent-Based participation. This technique provides an alternative for UAS that are non-equipped (that is, UAS that are neither broadcast capable nor equipped to communicate with a Remote ID Service Provider during flight, such as many radio-controlled model aircraft) as well as for UAS that may be equipped but are operating in an environment where participation in either broadcast or network Remote ID is infeasible due to the presence of electromagnetic interference (for example, an inspection inside an electrical tower) or radio signal blocking material (for example, areas under a bridge shielded by thick concrete or inside a tunnel). Intent-based participants report their operations (for example, aircraft ID, location in terms of a volume of airspace, operating times) in advance. The information is used to create a position report for use by Remote ID display applications where the uncertainty of the position report is defined by the airspace volume for the operation. The current telemetry of the aircraft within the volume is not known and cannot be displayed to a Remote ID end user, but the display application can display the volume and provide the identity of the UAS.

4.5.3 For Network Remote ID, two USS roles are identified: Network Remote ID (Net-RID) Service Providers and Net-RID Display Providers. In practice, these roles can be fulfilled by a single USS and potentially one that also provides flight planning and deconfliction, LAANC, or other UTM services, or combinations thereof. However, they are identified separately to provide flexibility for industry participants to pursue their preferred business objectives and implementation scope. This architecture supports one or more Net-RID Service Providers and one or more Net-RID Display Providers.

4.5.4 Net-RID Service Providers nominally remain in contact with UAS during flight and receive information (for example, position updates) used to fulfill requests from Net-RID Display Providers. For Network Remote ID, some required data (for example, the UAS ID) may be retained by the Net-RID Service provider after UAS authentication and not transmitted continuously from the UAS. As this specification does not specify the details of the UAS to Net-RID Service provider interface, implementations are generally valid as long as complete and correct Remote ID data is obtained by Net-RID Service Providers at some point and made available to Net-RID Display Providers.

4.5.5 Net-RID Service Providers may also have the ability to supply extrapolated position information for UAS that intermittently lose network connectivity.

4.5.6 Net-RID Display Providers fulfill a broker role between Remote ID Display Applications used by an end user and all Net-RID Service Providers that have flights in an area. When an end user display application requests Remote ID data for an area, the Net-RID Display Provider servicing the display application determines what Net-RID Service Providers have operations in the area and then obtains appropriate Remote ID data from each. The aggregated data is returned to the Remote ID Display Application. The aggregated data includes both current location and a window of near-real-time data for each flight.

4.5.7 Net-RID Display Providers ensure Remote ID Display Applications can only access and view data within a limited range and must dispose of aggregated data obtained from Net-RID Service Providers within a defined time period. Limiting the range helps implementations satisfy performance requirements in this specification by bounding the volume of data that must be gathered, processed, and displayed. Limiting the range (that is, only accessing required data) and disposing of such data when no longer needed helps protect privacy and sensitive data of consumers and operators.

4.5.8 For a UAS to be included in response to queries for Remote ID data, it must either be within the requested area at the time of the request or recently therein (that is, within a small window of time such as a minute). This specification does not provide remote identification data for UAS that are projected to be within an area in the future.

4.5.9 Industry-standard encryption and authentication are required from the UAS or the operator of an intent-based network participant to the Net-RID Service and from the Net-RID Service Providers to Net-RID Display providers.

4.6 *Remote ID Display Applications:*

AVA Documents
Document Sharing Hub



Full document details: ASTM F3411-22a

4.6.1 Receivers and Remote ID Display Applications are shown on the right side of Fig. 1. A typical implementation would be a smartphone or tablet with an internal receiver for Bluetooth and Wi-Fi, but other implementations are possible. The display applications ingest Broadcast Remote ID data or interact with a Net-RID Display Provider, or both, to acquire Network Remote ID data and present the information to end users.

4.6.2 A typical user interface might be map-based with symbols for UAS in the area. However, the manner in which the information is presented is beyond the scope of this specification and other implementations are possible.

4.6.3 It is anticipated that Remote ID Display Applications that integrate Broadcast and Network Remote ID data will be produced by industry; however, this also is beyond the scope of the specification.

4.6.4 From a network Remote ID perspective, this specification levies performance requirements on Net-RID Display Providers in responding to requests from Remote ID Display Applications.

4.7 *Representative Remote ID Scenario:*

4.7.1 Fig. 2 depicts a representative Remote ID scenario. The text that follows describes the flow of information amongst the Remote ID components introduced above.

4.7.2 Three UAS are simultaneously operating in close proximity (within 1 km) to each other: one is broadcasting Remote ID data, one is networked, and one is a model aircraft with no broadcast or network capability. An interested observer wants to identify the three UAS.

4.7.2.1 The broadcast UAS transmits Remote ID data using one of the methods described in 5.4. The UAS is controlled locally by the Remote Pilot and has no interface with a USS.

4.7.2.2 The networked UAS is operated under USS1. This USS acts as a Net-RID Service Provider and a Net-RID Display Provider.

4.7.2.3 The Remote Pilot of the model aircraft uses a smartphone app to report the location and time of the operation, and provides the ID for the model aircraft. The smartphone app is the user interface that connects the user to a second Net-RID Service Provider, USS2.

4.7.3 The interested observer accesses a Remote ID Display Application (RID App) that uses USS1 as its Net-RID Display Provider. This display application shows UAS locations and a near-real-time trail of position reports on a map, and associated identification information when a particular UA is selected.

4.7.4 When the interested observer opens the Remote ID app on a smartphone and centers the map on the current location, Remote ID data is acquired as follows:

4.7.4.1 The broadcast UAS is transmitting its Remote ID advertisements continuously. The smartphone uses its internal radios to listen for the advertisements from the UAS, extract the Remote ID data, and show the location of the UA on the map. As new position updates are received, the prior position reports become part of a near-real-time trail representing where the UA most recently flew.

4.7.4.2 Simultaneously, the Display App makes a request to its Net-RID Display Provider, USS1. USS1's role as a Net-RID Display Provider is to aggregate Remote ID data for all flights

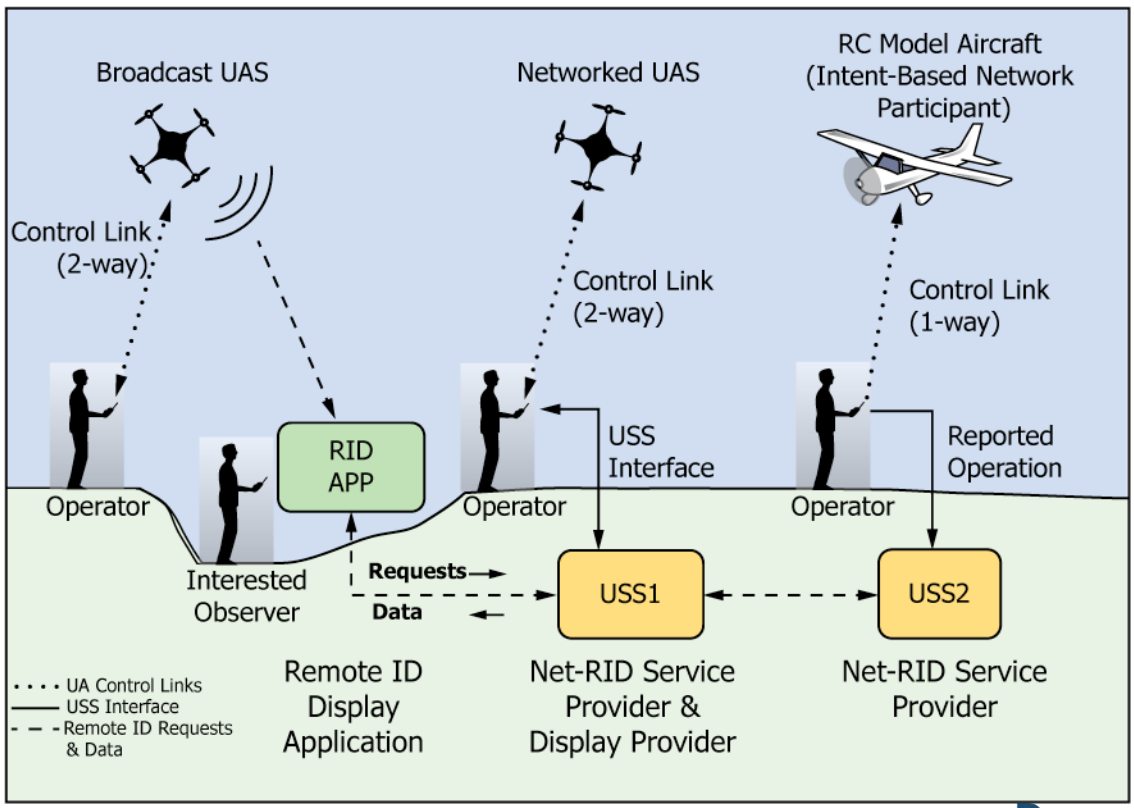


FIG. 2 Representative Remote ID Scenario

Documents
Document Sharing Hub



Full document details: ASTM F3411-22a

in the area managed by Net-RID Service Providers. USS1 knows that it is a Net-RID Service Provider and has flights in the area.

4.7.4.3 USS1 additionally discovers USS2, which has no real-time-managed flights in the area, but has an operation reported for the model aircraft (that is, the Intent-Based Network Participant). The Remote Pilot of the radio-controlled model aircraft reports the operation to USS2 prior to the flight and no dynamic position updates are provided. USS2 provides the information for this operation back to USS1.

4.7.4.4 USS1 adds the Remote ID data for the networked UAS that it is managing (fulfilling its role as a Net-RID Service Provider) and provides the aggregated data back to the Display Application (fulfilling its role as a Net-RID Display Provider).

4.7.4.5 The display app adds the network data to the map that is already showing the broadcast information. The Networked UAS is shown with up to a 60 s trail of position reports (referred to as near-real-time data). The Intent-Based Network Participant is shown as a polygon.

4.7.4.6 As long as the interested observer continues to view the Remote ID display app for the area, the app continues to communicate with USS1 as its Net-RID Display Provider to obtain position updates. Since the information for the Intent-Based network participant does not update, no additional updates are provided for it from USS2. USS1 continues to provide position updates for the Networked UAS in its role as the Net-RID Service Provider.

4.7.4.7 The interested observer selects the UA symbols for the Broadcast UAS and the Networked UAS on the map and views the corresponding ID information. The interested observer then selects the polygon for the Intent-Based Network Participant and sees the operation schedule and the ID of the aircraft.

4.7.4.8 The interested observer closes the app. After a period of time, USS1 discards the information for the Intent-Based Network Participant because it is managed by a different USS (USS2).

4.8 *USS Interoperability:*

4.8.1 This specification assumes that UTM services in a given location are provided by a set of one or more UAS Service Suppliers (USSs). USSs must be interoperable in this environment, sharing data as necessary to accomplish the objective of a particular service such as Network Remote ID or flight plan exchange for strategic deconfliction.

4.8.2 The interoperability paradigm defined in this specification is intended to support both Network Remote ID and other services that may be included in subsequent UTM-related ASTM standards. The requirements and application programming interfaces (APIs) associated with the interoperability paradigm are included in this document because it is the first UTM-related ASTM standard. Subsequent UTM-related ASTM standards may introduce additional service-specific interoperability requirements and API functions. Some of the interoperability requirements and APIs may move to a different standard in the future.

4.8.3 The interoperability paradigm consists of two parts:

4.8.3.1 A standardized discovery mechanism, referred to as the Discovery and Synchronization Service (DSS), the primary functions of which are to identify USSs with which data exchange is required, and to verify that a USS considered relevant information from other USSs when necessary (for example, when planning a new operation); and,

4.8.3.2 Service-specific data exchange protocols used to obtain the details of relevant information discovered by means of the DSS from the owning USS.

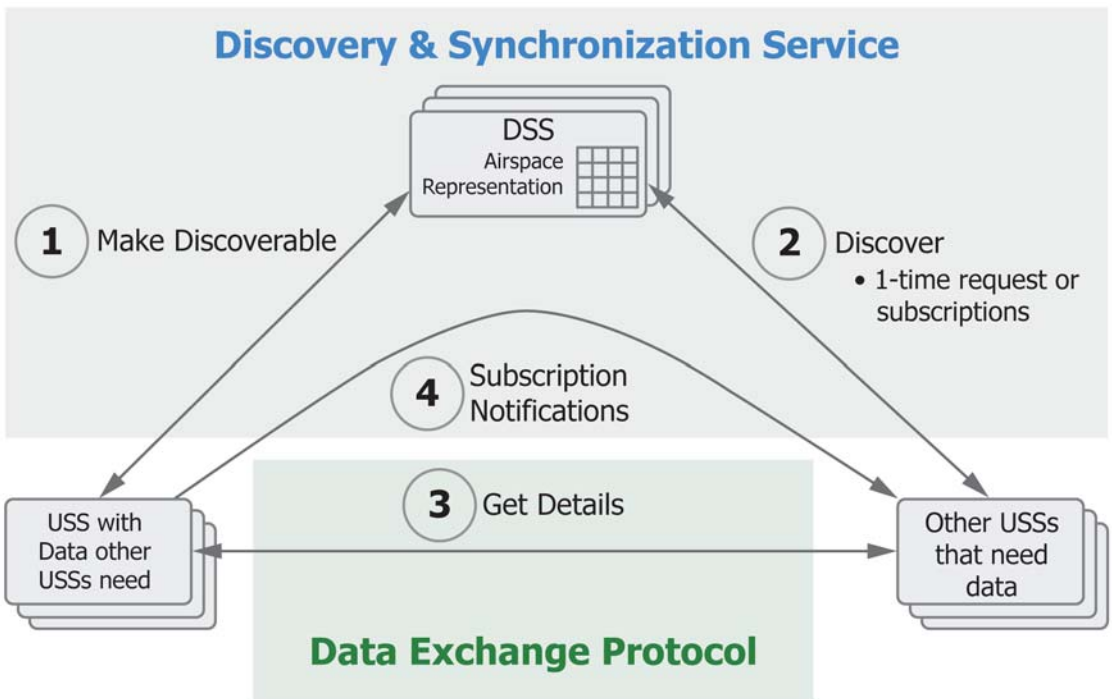


FIG. 3 USS Interoperability Overview



Documents
Document Sharing Hub
Full document details: ASTM F3411-22a

4.8.4 Fig. 3 illustrates the interactions involved in this paradigm in a service-independent manner. (The instantiation of this paradigm for Remote ID is detailed later.)

4.8.5 DSS-related interactions are shown at the top in the blue-shaded area; data exchange protocols between USSs are represented by the green-shaded area.

4.8.6 For availability purposes, the DSS is a redundant service as indicated in Fig. 3. Instances of the DSS in a region synchronize with each other in a standardized manner (described later in this specification). A region is the geographic scope supported by a set of DSS instances.

4.8.7 Only approved USSs will be given access to the DSS. (The specifics of an approval process are beyond the scope of this specification.)

4.8.8 An instance of discoverable information is referred to as an entity. There are different types of entities, such as operations, constraints, or, relevant to this specification, an area where network remote identification services are being provided. The concept is extendable to future UTM services where other types of entities may need to be discoverable. A key characteristic of entities is that they have an associated 4-D volume (that is, a volume defined in $x$, $y$, and $z$ plus time limits).

4.8.9 The DSS encapsulates an airspace model into which entities are mapped. The implementation details of this airspace representation are hidden from DSS clients; however, conceptually, the airspace model can be thought of as a grid and mapping an entity into the airspace model is determining what grid cells the entity intersects. The complete details of the entities and any associated Personally Identifiable Information (PII) are not stored in the DSS but instead are retained by the owning USS; only limited information such as the type of entity, its location (in terms of what cells of the airspace model it intersects), the current opaque version number (OVN) of the entity (OVNs are updated whenever the entity is modified), and how to contact the owner of the entity are stored in the DSS.

4.8.10 Given that context, the primary interactions (numbered in Fig. 3) are:

4.8.10.1 *Make Discoverable*—A USS with an entity about which other USSs need to know (for example, an operation, a constraint, an area where Remote ID services are provided) makes it discoverable by writing the limited entity summary information (information type, identifier, location, owner) to the DSS.

4.8.10.2 *Discover*—Other USSs that are interested in entities of some type query the DSS using a 4-D volume to characterize the area of interest. The DSS maps the query onto the airspace representation and finds intersecting grid cells with entities of the desired type (if any). (Because entities are mapped into grid cells and the DSS does not retain 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 entities and their owners. This can be a one-time query (often described as a *pull* of the information) or the requesting USS can also establish a subscription to be notified of new or modified entities in the area of interest (discussed further below).

4.8.10.3 *Get Details*—Given the list of discovered entities, the requesting USS switches to the applicable Data Exchange Protocol to contact the owning USS and obtain the complete details. Data Exchange Protocols are service-specific.

4.8.10.4 *Subscription Notifications*—If the requesting USS established a subscription in the DSS (for a 4-D area of interest), when another USS writes a new entity to the DSS that intersects the subscription, the DSS informs the writing USS of the subscription and the writing USS contacts the subscribing USS to provide the details. (This is often described as a *push* of the information.)

4.8.11 While not needed for Remote ID, OVNs come into play on interaction if the entity written to the DSS is of a type that requires deconfliction with other entities (for example, a new UAS operation requires deconfliction; a constraint does not). When writing the new operation to the DSS, the USS must provide the OVNs for all other operations and constraints in the area of the new operation. For applicable entity types, OVNs are part of the detailed information obtained from other USSs in step 3. If the DSS determines the set of OVNs is complete and current, it allows the new operation to be written; if not, the DSS informs the writing USS what OVNs are missing or obsolete.

4.8.12 Although complete details for entities are not stored in the DSS, it serves as the single source of truth for what entities exist in the airspace and provides the mechanism necessary to ensure that USSs attempting to create a new operation have considered the current version of all other relevant entities in the airspace.

4.8.13 Unless noted otherwise, references to the DSS throughout this specification refer to the set of DSS instances supporting the region in which a related activity is occurring (for example, creating entity summaries, discovering entities).

4.8.14 This overview omits many details of the DSS and data exchange protocols. The Remote ID-specific interoperability requirements, complete APIs, and additional details are provided in Annex A2.

## 5. Performance Requirements

5.1 Remote ID is comprised of a set of standardized data, messages, transport mechanisms for communicating the messages, and performance requirements governing certain attributes of an implementation such as message periodicity. For Broadcast Remote ID, the message format is the same regardless of the transport mechanism. These messages are coded as a "block message" implementation of the Data Dictionary to optimize for the transport mechanism size constraints and to minimize potential broadcast interference. For Network Remote ID, the message format is a network adaption of the Data Dictionary using common internet protocols. For broadcast messages, each message has a message type that is identified in the message header. The message type defines the message format and is classified as static or dynamic, which also sets the requirements for the minimal rate at which each message type shall be transmitted. The common name for this broadcast messaging protocol is "Open Drone ID."

5.2 Conventions used in this section

AVA Documents
Document Sharing Hub



Full document details: ASTM F3411-22a

5.2.1 Requirement IDs are shown below. The prefix to each ID identifies groupings:

5.2.1.1 BURxxxx - Broadcast Update Rate

5.2.1.2 BMGxxxx - Broadcast Messages

5.2.1.3 BB4xxxx - Broadcast Bluetooth 4

5.2.1.4 BB5xxxx - Broadcast Bluetooth 5

5.2.1.5 BWFxxxx - Broadcast Wi-Fi

5.2.1.6 NETxxxx - Network

5.2.1.7 DSSxxxx - Discovery and Synchronization Service (Annex A2)

5.2.2 Constant values representing a required time, distance, etc. are consolidated into Annex A3. These values are referenced within the requirements text in this section using square brackets around the constant name. Constants pertaining to broadcast Remote ID are prefixed with "Bc" and constants pertaining to network Remote ID are prefixed with "Net" as shown in the following examples:

5.2.2.1 [BcMinUasLocRefreshRate]

5.2.2.2 [NetMinUasLocRefreshRate]

5.2.3 In some cases, notes to clarify the intent of a requirement are provided. These notes are numbered and prefaced with "Note:." They are for clarification purposes only and do not contain requirements.

5.3 *Common Data Dictionary:*

5.3.1 Table 1 defines the required and optional data fields for Remote ID, including minimum characteristics that must be supported by both network and broadcast implementations. Since broadcast Remote ID uses size-limited messages, for some data fields it is necessary to use encoding methods that adjust the resolution or aggregate ranges of values, whereas these size-limiting techniques are not necessary for network Remote ID. The required minimum characteristics provided below ensure a prescribed degree of consistency between broadcast and network Remote ID to facilitate integration in a Remote ID display application. The specific representations for broadcast and network Remote ID are provided in their respective requirements sections.

5.3.2 An asterisk (*) adjacent to a data field name denotes an optional field. Optional fields and certain field options may be required in some jurisdictions.

5.4 *Broadcast:*

5.4.1 This section describes requirements for the RF broadcast of Remote ID messages from a participating UA. Four broadcast transport mechanisms are supported by this specification:

5.4.1.1 Bluetooth Legacy (4.x compatible)

5.4.1.2 Bluetooth 5.x Long Range (must be transmitted concurrently with Legacy mode)

5.4.1.3 Wi-Fi Neighbor Awareness Network (NAN)

5.4.1.4 Wi-Fi Beacon (vendor-specific information element in the SSID beacon frame)

5.4.2 The four transport mechanisms share common requirements for update rates and message definition.

5.4.3 *Output Power and Pattern*—For output power and pattern, the requirement (BPW0010) seeks to provide a sufficiently high power transmission that generally emits in an omni-directional pattern using commonly available components. This can be accomplished using either of the following two options:

*(a)* The average Effective Isotropic Radiated Power (EIRP) around the horizontal plane of the antenna system shall be at least [BcMinAvgEIRP] and the Peak to Average gain around the horizontal plane of the antenna system shall be no more than [BcMaxPeakToAvg]. The average EIRP is calculated by adding the conducted power into the antenna system to the average gain of the antenna system in the horizontal plane; or

*(b)* The minimum EIRP around the entire horizontal plane of the antenna system shall be at least [BcMinEIRP]. The minimum EIRP is calculated by adding the conducted power into the antenna system to the minimum gain of the antenna system in the horizontal plane.

These options are intended to allow for use of manufacturer data sheets to demonstrate compliance. The Horizontal Plane is defined as a plane of the transmission pattern that approximately corresponds to the horizontal plane during the most common average orientation of the vehicle when flying. The UAS should be mechanically designed in a way to minimize radio pattern distortion of Remote ID.

5.4.4 *Update Rates:*

5.4.4.1 For broadcast messages, dynamic messages (as indicated in the block message section) shall (BUR0010) be sent at least every [BcMinUasLocRefreshRate] second(s). Static messages (as indicated in the block message section) shall (BUR0020) be sent at least every [BcMinStatic RefreshRate] second(s) and the maximum potential time elapsed since the time of applicability of the dynamic fields in the Location/Vector Message shall (BUR0030) be no older than [BcMaxDataAge]. If a multi-sector antenna configuration is used, then these update requirements shall be applied to each sector. Should channel saturation block or interfere with transmission (as may occur due to "listen before talk" interference handling technique), the system shall (BUR0040) make a "best effort" to transmit when the saturation level allows.

5.4.4.2 *Counters*—After each frame of the same message type is updated, the Message Counter (for that message type) shall (BUR0050) be incremented and reset to 0 after 0xFF is reached. Therefore, each message type (defined in Table 3) has a separate counter. For Message Packs (message type 0xF), only 1 counter is maintained and updated each time any data within the message pack is updated. If the data being transmitted has not changed, incrementing the Message Counter is optional. If a message is multi-paged (such as a multi-page authentication message), then the Message Counter shall (BUR0060) be the same for each page in the page set.

5.4.5 *Block Messages:*

5.4.5.1 The "Block" messages are designed to be packed into lightweight direct broadcast packets within Wi-Fi or Bluetooth "Beacon Advertisements." The message types are identified in Table 3. Subsequent subsections further describe each message type.

5.4.5.2 Each message shall (BMG0010) be 25 bytes in length (padded with nulls as needed).

5.4.5.3 Each message shall (BMG0020) begin with a 1 byte header followed by 24 bytes of data, which shall be encoded as

AVA Documents Document Sharing Hub



Full document details: ASTM F3411-22a

**TABLE 1 Common Data Dictionary**

| Data Field | Description/Rationale |
|---|---|
| UAS ID | Consists of four options:<br>1. Serial Number: This is expressed in the CTA-2063-A Serial Number format.<br><br>2. Registration ID: If a CAA provides a method of registering UAS, this number is provided by the CAA or its authorized representative.<br>Format: <ICAO Nationality Mark[A] >.<CAA Assigned ID>, ASCII encoded, only uppercase letters (A-Z), dot (.), and digits (0-9) are allowed. Example (US): N.123456<br><br>3. UTM (UUID): A UTM-provided universally unique ID traceable to a non-obfuscated ID where this UTM UUID acts as a "session id" to protect exposure of operationally sensitive information.<br><br>4. Specific Session ID: A unique 20 byte ID intended to identify a specific flight (session) while providing a greater level of privacy to the operator. The first byte is the registered unique Specific Session ID Type maintained by a registrar (see Annex A5), and the remaining 19 bytes is the Session ID in accordance with the Specific Session ID Type specification.<br>Initial scheme registry entries shall include:<br>0 – reserved;<br>1 – Internet Engineering Task Force (IETF) Drone Remote Identification Protocol (DRIP) entity ID;<br>2 – IEEE 1609.2-2016 HashedID8. |
| UA Type | The UA Type can help infer performance, speed, and duration of flights, for example, a "fixed wing" can generally fly in a forward direction only (as compared to a multi-rotor). This can also help differentiate aircraft types without sharing operationally sensitive information like the make and model of a particular aircraft. Make and model are anticipated to become available during the Registration ID lookup process. UAS Type is also useful for correlating visual observation with data received. The types were formulated based on unique flight characteristics. The possible values are in Table 2. |
| UA Classification*[C] | UA Classification – Allows a region to classify UAS in a regional specific manner.<br>The format may differ from region to region. |
| UA Classification Type | Specifies the Region Number (which implies the format of UAS Classification). See Table 2. |
| Timestamp | The time of applicability of position information. This may be the time coming from the source such as a GPS, or the time when the system computes the values using an algorithm such as an Extended Kalman Filter (EKF). Timestamps must be expressed with a minimum resolution[B] of one tenth of a second and relative to UTC time.<br>Special Values: Invalid, No Value, or Unknown: 0xFFFF. |
| Timestamp Accuracy | Declaration of timestamp accuracy, which is the largest difference between Timestamp and true time of applicability for any of the following fields: Latitude, Longitude, Geodetic Altitude, Pressure Altitude, and Height to determine time of applicability of the location data provided. Expressed in 1/10ths of seconds. The accuracy reflects the 95 % uncertainty bound value for the timestamp. |
| Operational Status*[C] | Operational Status indicates whether the associated UA is on the ground, airborne, in an emergency situation, or the Remote ID system has failed. The emergency status takes precedence over the other status modes. This status can be used for filtering purposes. (See Table 2.) |
| Operation Description*[C] | This optional, free-text field enables the operator to describe the purpose of a flight, if so desired. |
| Operator ID*[C] | This optional field provides a CAA-issued registration/license ID for the remote pilot or operator.<br>Format: ASCII Text. If numeric values exist, they shall be expressed as a string of ASCII characters. |
| Latitude | Current latitude (within horizontal accuracy limits) of the UA. This is necessary to display UAS location. Minimum resolution: 7 decimal digits (~11 mm).<br>Special Values: Invalid, No Value, or Unknown: 0 deg (both Lat/Lon) |
| Longitude | Current longitude (within horizontal accuracy limits) of the UA. This is necessary to display UAS location. Minimum resolution: 7 decimal digits (~11 mm).<br>Special Values: Invalid, No Value, or Unknown: 0 deg (both Lat/Lon) |
| Geodetic Altitude | The aircraft distance above or below the ellipsoid as measured along a line that passes through the aircraft and is normal to the surface of the WGS-84 ellipsoid. This value is provided in meters and must have a minimum resolution of 1 m.<br>Special Values: Invalid, No Value, or Unknown: –1000 m |
| Pressure Altitude*[C] | The uncorrected barometric pressure altitude (based on reference standard 29.92 inHg, 1013.25 mb) provides a reference for algorithms that utilize "altitude deltas" between aircraft. This value is provided in meters and must have a minimum resolution of 1 m.<br>Special Values: Invalid, No Value, or Unknown: –1000 m |
| Height*[C] | Expressed as either height above takeoff location or height above ground level (AGL) for a UA's current location. This value is provided in meters and must have a minimum resolution of 1 m.<br>Special Values: Invalid, No Value, or Unknown: –1000 m |
| Height Type*[C] | Height above takeoff location or height above ground level. |
| Geodetic Vertical Accuracy | Provides quality/containment on geodetic altitude. This is based on ADS-B Geodetic Vertical Accuracy (GVA) (plus the three extra increments). (See Table 2.) |
| Horizontal Accuracy | Provides quality/containment on horizontal position. This is based on ADS-B NACp (plus the one extra increment). (See Table 2.) |

AVA Documents
Document Sharing Hub



Full document details: ASTM F3411-22a

**TABLE 1** *Continued*

| Data Field | Description/Rationale |
|---|---|
| Speed Accuracy | Provides quality/containment on horizontal ground speed. (See Table 2.) |
| Track Direction | Direction of flight expressed as a "True North-based" ground track angle. This value is provided in clockwise degrees with a minimum resolution of 1 degree. If aircraft is not moving horizontally, use the "Unknown" value.<br>Special Values: Invalid, No Value, or Unknown: 361 deg |
| Speed | Ground speed of flight. This value is provided in meters per second with a minimum resolution of 0.25 m/s.<br>Special Values: Invalid, No Value, or Unknown: 255 m/s, if speed is ≥254.25 m/s: 254.25 m/s |
| Vertical Speed | Vertical speed upward relative to the WGS-84 datum, meters per second.<br>Special Values: Invalid, No Value, or Unknown: 63 m/s, if speed is ≥62 m/s: 62 m/s, if speed is ≤ –62 m/s: –62 m/s |
| Auth Data*[C] | Additional Authentication Data<br>See Table 2 for specific Authentication Types |
| Operator Latitude*[C] | Provides the location associated with the Remote Pilot.<br>Special Values: Invalid, No Value, or Unknown: 0 deg (both Lat/Lon) |
| Operator Longitude*[C] | Provides the location associated with the Remote Pilot.<br>Special Values: Invalid, No Value, or Unknown: 0 deg (both Lat/Lon) |
| Operator Altitude*[C] | Provides the Operator Altitude based on WGS-84 height above ellipsoid (HAE) (See Geodetic Altitude).<br>This value is provided in meters and must have a minimum resolution of 1 m.<br>Special Values: Invalid, No Value, or Unknown: –1000 m |
| Operator Location Type*[C] | Takeoff location, fixed location, or dynamic location representing the Operator Location |
| Operating Area Radius*[C] | Farthest horizontal distance from the reported location at which any UA in a group may be located (meters). Also allows defining the area where an Intent-Based Network Participant operation is taking place. Default: 0 |
| Operating Area Polygon*[C] | A list of latitude/longitude pairs defining the area where a group or Intent-Based Network Participant operation is taking place. (This field is only applicable to Network Remote ID.) |
| Operating Area Type*[C] | Cylinder or Polygon. (This field is only applicable to Network Remote ID.) |
| Operating Area Count*[C] | Allows for operating a single UA, group, formation, or swarm: Quantity in Group. Default 1 |
| Operating Area Floor*[C] | Minimum altitude (WGS-84 HAE) for a group or an Intent-Based Network Participant.<br>Special Values: Invalid, No Value, or Unknown: –1000 m |
| Operating Area Ceiling*[C] | Maximum altitude (WGS-84 HAE) for a group or an Intent-Based Network Participant.<br>Special Values: Invalid, No Value, or Unknown: –1000 m |
| Operation Area Start*[C] | The date and time at which a group or an Intent-Based Network Participant operation starts. (This field is only applicable to Network Remote ID.) |
| Operation Area End*[C] | The date and time at which a group or an Intent-Based Network Participant operation ends. (This field is only applicable to Network Remote ID.) |

[A] ICAO Nationality Marks, https://www.icao.int/safety/airnavigation/Pages/nationality.aspx.
[B] "resolution" in this specification is used to indicate the preciseness possible of the expressed value, but not the accuracy. For example, although Lat/Lon must be expressed to 7 decimal digits of resolution, the accuracy may be far less (as indicated in the Horizontal Accuracy field).
[C] An asterisk (*) adjacent to a data field name denotes an optional field. Optional fields and certain field options may be required in some jurisdictions.

described in the "Message Details" table that corresponds with each Message Type described below. Non-magnitude values, strings, or IDs that may be or may not be numerical (such as the Unique ID) shall (BMG0030) be expressed in Network Byte Order which reads in a left to right, most significant byte (MSB) to least significant byte (LSB) order. Magnitude values expressed as 16 or 32 bit integers (such as Latitude, Longitude, Altitude, etc.) shall (BMG0040) be expressed as "little endian" (marked as "LE" in the "Message Details" tables below), where the LSB is on the left and the MSB is on the right. If not invoking an optional message, it is not necessary to send that message. Optional fields within messages being sent (see Table 1) shall (BMG0050) be filled in as stated in the corresponding block message format and if opting out, or the value is unknown, shall be filled with nulls (0s) for string values or 0 for numeric unless an alternate default/unknown value representation is stated in Table 1. This allows the block message to stay properly aligned with the field definitions. All ASCII Strings shall (BMG0060) be filled with nulls in the unused portion of the field. In the data structures below, some fields are enumerated values. Table 2 shall (BMG0065) be used to encode to those enumerations.

AVA Documents
Document Sharing Hub



Full document details: ASTM F3411-22a

**TABLE 2 Enumerated Field Definitions**

| Field Name | Details | Notes |
|---|---|---|
| UA Type | 0: None/Not Declared<br>1: Aeroplane<br>2: Helicopter (or Multirotor)<br>3: Gyroplane<br>4: Hybrid Lift (Fixed wing aircraft that can take off vertically)<br>5: Ornithopter<br>6: Glider<br>7: Kite<br>8: Free Balloon<br>9: Captive Balloon<br>10: Airship (such as a blimp)<br>11: Free Fall/Parachute (unpowered)<br>12: Rocket<br>13: Tethered Powered Aircraft<br>14: Ground Obstacle<br>15: Other | Up to 16 Types<br><br>These values were derived from the official ICAO UA Type list. Additional types were added if they had unique flight characteristics. |
| Operational Status | 0: Undeclared<br>1: Ground<br>2: Airborne<br>3: Emergency<br>4: Remote ID System Failure<br>5-15: Reserved | Up to 16 Statuses |
| Horizontal Accuracy | 0: ≥18.52 km (10 NM) or Unknown<br>1: <18.52 km (10 NM)<br>2: <7.408 km (4 NM)<br>3: <3.704 km (2 NM)<br>4: <1852 m (1 NM)<br>5: <926 m (0.5 NM)<br>6: <555.6 m (0.3 NM)<br>7: <185.2 m (0.1 NM)<br>8: <92.6 m (0.05 NM)<br>9: <30 m<br>10: <10 m<br>11: <3 m<br>12: <1 m<br>13-15: Reserved | This is the NACp enumeration from ADS-B. Value 12 was added for a more complete range for UAs. 95 % accuracy bound (estimated position uncertainty). |
| Vertical Accuracy | 0: ≥150 m or Unknown<br>1: <150 m<br>2: <45 m<br>3: <25 m<br>4: <10 m<br>5: <3 m<br>6: <1 m<br>7-15: Reserved | This is the GVA enumeration from ADS-B. Values 4–6 were added for UAs. 95 % accuracy bound. |
| Speed Accuracy | 0: ≥10 m/s or Unknown<br>1: <10 m/s<br>2: <3 m/s<br>3: <1 m/s<br>4: <0.3 m/s<br>5-15: Reserved | This is the same enumeration scale and values from ADS-B NACv. 95 % accuracy bound. |
| Operator Location Source Type | 0: Takeoff<br><br>1: Dynamic<br>2: Fixed | |



Documents
Document Sharing Hub
Full document details: ASTM F3411-22a

**TABLE 2** *Continued*

| Field Name | Details | Notes |
|---|---|---|
| UA Classifications | | |
| Classification Type | 0: Undeclared<br>1: European Union<br>2–7: Reserved | |
| For Classification Type 1 (EU) | Categories:<br>0: Undefined<br>1: Open<br>2: Specific<br>3: Certified<br>4-15: Reserved<br><br>Classes:<br>0: Undefined<br>1: Class 0<br>2: Class 1<br>3: Class 2<br>4: Class 3<br>5: Class 4<br>6: Class 5<br>7: Class 6<br>8-15: Reserved | |
| Authentication Type | 0: None<br>1: UAS ID Signature<br>2: Operator ID Signature<br>3: Message Set Signature<br>4: Authentication Provided by Network Remote ID<br>5: Specific Authentication Method<br>6-9: Reserved for Spec<br>A-F: Available for Private Use | |

**TABLE 3 Open Drone ID Block Message Summary**

| Msg Type | Message Name | Purpose |
|---|---|---|
| 0x0 | Basic ID Message | Provides ID for UA, characterizes the type of ID, and identifies the type of UA |
| 0x1 | Location/Vector Message | Provides location, altitude, direction, and speed of UA |
| 0x2 | Authentication Message[A] | Provides authentication data for the UA |
| 0x3 | Self-ID Message[A] | Message that can be used by Operators to identify themselves and the purpose of an operation |
| 0x4 | System Message[A] | Includes Remote Pilot location and multiple aircraft information (group) if applicable, and additional system information |
| 0x5 | Operator ID[A] | Provides Operator ID |
| 0xF | Message Pack[A] | A payload mechanism for combining the messages above into a single message pack. Used with Bluetooth Extended Advertising, Wi-Fi Neighbor Awareness Network, and Wi-Fi Beacon |

[A] Optional unless required by location jurisdiction.

**MESSAGE HEADER (Table 4)**

5.4.5.4 The message header includes the Message Type and Protocol Version and shall (BMG0070) be sent in each message.

**BASIC ID MESSAGE (Table 5)**

5.4.5.5 Basic ID Message Type: 0x0, Static Periodicity, Mandatory

5.4.5.6 The BasicID message includes the ID Type, UA Type, and the Unique ID. This Unique ID shall (BMG0080) default to the Manufacturer Serial number. Once the UA is provisioned, the UAS ID shall be (BMG0090) one of the following:

*(1)* Manufacturer Serial Number expressed in the ANSI/CTA-2063-A Serial Number format.

**TABLE 4 Message Header Details**

| Header (1 byte) | | Message (24 bytes) |
|---|---|---|
| Message Type<br>(4 bits)<br>Bits [7..4] | Protocol Version<br>(4 bits)<br>Bits [3..0] | Message Fields based on Message Type |
| 0x0–0xF | 0x2<br>(0xF reserved for private use) | < Message Data > |



Documents
Document Sharing Hub
Full document details: ASTM F3411-22a

**TABLE 5 Basic ID Message Details**

| Offset (Byte) | Length (Bytes) | Data Field | Details | Limitations | Example |
|---|---|---|---|---|---|
| 1 | 1 | ID Type,<br>UA Type | Bits 7..0 [0000] [0000]<br><br>ID Type: Bits [7..4]<br>0: None<br>1: Serial Number (ANSI/CTA-2063-A)<br>2: CAA Assigned Registration ID<br>3: UTM Assigned UUID<br>4: Specific Session ID<br><br>UA Type: Bits [3..0]<br>helicopter, fixed wing, hybrid lift, etc. (See Table 2 for more details.) | Up to 16 ID types<br>Up to 16 UA types | |
| 2 | 20 | UAS ID | UAS ID within the format of ID Type (padded with nulls) | Max. 20 Bytes | N.123456 |
| 22 | 3 | Reserved | | | |

*(2)* A Civil Aviation Authority (CAA) issued Registration ID for the UA formatted as described in Table 1.

*(3)* A UTM Assigned ID if operating within a UTM system (128-bit UUID) binary encoded, Network Byte Order.

*(4)* Specific Session ID according to the registered Session ID Type (see Annex A5). The first byte of the Specific Session ID must be the Specific Session ID Type (1–255) where 0 is reserved, 1–224 is the registered type, and 225–255 are available for private experimental use only. If using this method, the Specific Session ID Type must be registered through the registrar (see Annex A5). Using the experimental range is not considered "compliant" to this specification, but may be used for testing and experimentation.

NOTE 1—Multiple ID Types may be sent by sending multiple Basic ID messages.

NOTE 2—When using Specific Session ID Type, implementations may wish to use random rather than static MAC addresses (see Tables 14, 15, 17 PDU Hdr).

## LOCATION/VECTOR MESSAGE (Table 6)

5.4.5.7 Location/Vector Message Type: 0x1, Dynamic Periodicity, Mandatory

5.4.5.8 The Location/Vector message provides the location, altitude, direction, and speed of the UA. Several of the fields require special encodings to better pack the data and to allow for more precise values. If indicated, the transmitted data shall (BMG0100) be encoded according to Table 7. Additionally, any fields that require a flag bit to be set shall (BMG0110) be set according to Table 7 as well.

## AUTHENTICATION MESSAGE (Tables 8 and 9)

5.4.5.9 Authentication Message Type: 0x2, Static Periodicity, Optional* (see 5.3.2).

5.4.5.10 *Authentication Message Overview:*

5.4.5.11 The Authentication Message defines a field that provides a means for authenticating the identity of the UA sending the message (as specified in Tables 8 and 9). An implementation could send an Auth Type of 0 to deterministically communicate that no Auth Data is intended to be sent. Alternatively, an implementation could simply not send an Authentication message when there is no authentication data to send. Auth Types 1, 2, and 3 represent standard signature options. Auth Type 4 is used to communicate that authentication is provided by the Network Remote ID counterpart to the broadcast. Custom authentication implementations can be created using Auth Types A-F. The details of a custom implementation are beyond the scope of this specification.

5.4.5.12 For Auth Types 1, 2, and 3, the standard provides flexibility to allow a multitude of signature formats that are not specified in this specification. The intended implementation is that an agreed upon signature format for each Auth Type required will be shared by both the signature encoding software and the verifier software. This specification specifies an API for a receiver (for example, a Remote ID Display Application) to communicate with a verifier. (See Annex A1 for additional details.)

5.4.5.13 *Authenticate Message Requirements:*

5.4.5.14 If no authentication is used, and this message is still being sent (which is not required), the Auth Type shall be set to 0 (BMG0120) and the Signature shall be empty. When a signature is required, the signature produced by a UAS shall (BMG0130) be encoded to match the signature format expected by the verifier. When UAS ID (1) or Operator ID (2) is set as the AuthType, then the Message Signature shall (BMG0140) include the corresponding data and TimeStamp from the Authentication message in the signature. If the AuthType is set to Message Set (3), then the Signature shall (BMG0150) include the concatenation (in message type order) of all other transmitted message types (excluding this Authentication message), and TimeStamp from this Authentication message.

5.4.5.15 The Authentication Message Data Page field allows for Authentication Data sizes that may exceed the 24 bytes available per message. The Data Page shall (BMG0160) be incremented (starting from 0) for each additional message required to complete the oversized message. The Length field shall specify the exact length in bytes of the authentication payload data. Additional data may be sent (for example: additional Forward Error Correction (FEC) data) after the authentication payload data. If additional data is sent, it must begin with one (unsigned int8) byte indicating the length of the

AVA Documents
Document Sharing Hub



Full document details: ASTM F3411-22a

**TABLE 6 Location/Vector Message Details**

| Offset (Byte) | Length (Bytes) | Data Field | Details | Limitations | Example |
|---|---|---|---|---|---|
| 1 | 1 | Status, Flags | Bits [7..0] [0000] [0000]<br><br>Operational Status: Bits [7..4]<br><br><u>Flags</u><br>Reserved: Bit [3]<br>Height Type: Bit [2]<br>0: Above Takeoff, 1: AGL<br><br>E/W Direction Segment: Bit [1]<br>0: <180, 1: ≥180<br><br>Speed Multiplier: Bit [0]<br>0: x0.25, 1: x0.75 | <br><br>0..15 statuses<br>(See Table 2)<br><br><br><br><br><br><br><br>Speed Multiplier enables speeds up to 254.25 m/s. Only use 1 when speed exceeds 63.75 m/s and add 63.75. | |
| 2 | 1 | Track Direction | Direction expressed as the route course measured clockwise from true north. Encode as 0–179. If E/W Direction bit is set, then 180 should be added to the value. | 0–359 Unsigned Int (UInt) | 10 with E/W bit set = 190 deg. |
| 3 | 1 | Speed | Ground Speed in m/s encoded as specified in Table 7 | Up to 254.25 m/s UInt | 20(enc) = 5 m/s |
| 4 | 1 | Vertical Speed | Vertical Speed m/s (+ up, – down) Multiplier = 0.5 | Up to ±62 m/s (12.2k ft/min) | 15(enc) = 7.5 m/s |
| 5 | 4 | Latitude | Latitude of UA deg*10^7 | Int signed (LE) | –11989298 |
| 9 | 4 | Longitude | Longitude of UA deg*10^7 | Int signed (LE)<br>(11 mm precision) | 48123987 |
| 13 | 2 | Pressure Altitude | Pressure Altitude (Ref 29.92 inHg, 1013.24 mb)<br>(Altitude + 1000 m)/0.5 (LE) | –1000–31767 m (107503 ft)<br>16 bit UInt (LE) | 2021 (enc) = 10.5 m |
| 15 | 2 | Geodetic Altitude | WGS-84 HAE<br>(Altitude + 1000 m)/0.5 | –1000–31767 m (107503 ft)<br>16 bit UINT (LE) | 2021 (enc) = 10.5 m |
| 17 | 2 | Height | Height above takeoff location or Height above ground (indicate with Height Type Bit)<br>(Altitude + 1000 m)/0.5 | –1000–31767 m (107503 ft)<br>16 bit UInt (LE) | 2021 (enc) = 10.5 m |
| 19 | 1 | Vertical/ Horizontal Accuracy | Bits [7..0] [0000] [0000]<br><br>Vertical (Geodetic): Bits [7..4]<br>Horizontal: Bits [3..0]<br><br>Vertical: See Vertical Accuracy Enumeration<br>Horizontal: See Horizontal Accuracy Enumeration | See Table 2 | |
| 20 | 1 | Baro Altitude Accuracy/Speed Accuracy | Bits [7..0] [0000] [0000]<br><br>Baro Altitude: Bits [7..4]<br>See Vertical Accuracy Enumeration<br><br>Speed: Bits [3..0]<br>Based on Extended ADS-B NACv | Baro: see Table 2<br><br><br><br><br>Speed: see Table 2 | |
| 21 | 2 | Timestamp | Time of applicability expressed in 1/10ths of seconds since the last hour relative to UTC time | 0–36000: 16 Bit UInt (LE) | 3611 = 6 mins, 1.1 s after the hour |
| 23 | 1 | Reserved/ Timestamp Accuracy | Bits [7..0] [0000] [0000]<br>Reserved: Bits [7..4]<br>Timestamp accuracy: Bits [3..0]<br>(*0.1 s stepping resolution) | Timestamp accuracy:<br>0.1 s–1.5 s<br>0=unknown | |
| 24 | 1 | Reserved | | | |



Documents
Document Sharing Hub
Full document details: ASTM F3411-22a