Drone Remote Identification Protocol (DRIP) Requirements

Abstract

This document defines the requirements for Drone Remote
Identification Protocol (DRIP) Working Group protocols and services
to support Unmanned Aircraft System Remote Identification (UAS RID).

Objectives include: complementing external technical standards as
regulator-accepted means of compliance with UAS RID regulations;
facilitating use of existing Internet resources to support UAS RID
and to enable enhanced related services; and enabling verification
that UAS RID information is trustworthy (to some extent, even in the
absence of Internet connectivity at the receiving node).

Status of This Memo

This Internet-Draft is submitted in full conformance with the
provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering
Task Force (IETF). Note that other groups may also distribute
working documents as Internet-Drafts. The list of current Internet-
Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six
months and may be updated, replaced, or obsoleted by other documents
at any time. It is inappropriate to use Internet-Drafts as reference
material or to cite them other than as "work in progress."

This Internet-Draft will expire on 25 September 2020.

Copyright Notice

Table of Contents

1. Introduction

Many safety and other considerations dictate that UAS be remotely
identifiable. Civil Aviation Authorities (CAAs) worldwide are
mandating UAS RID. The European Union Aviation Safety Agency (EASA)
has published [Delegated] and [Implementing] Regulations. The United
States (US) Federal Aviation Administration (FAA) has published a
Notice of Proposed Rule Making ([NPRM]). CAAs currently promulgate

performance-based regulations that do not specify techniques, but rather cite industry consensus technical standards as acceptable means of compliance.

ASTM International, Technical Committee F38 (UAS), Subcommittee F38.02 (Aircraft Operations), Work Item WK65041, developed new ASTM F3411-19 [F3411-19] Standard Specification for Remote ID and Tracking. It defines 2 means of UAS RID. Network RID defines a set of information for UAS to make available globally indirectly via the Internet. Broadcast RID defines a set of messages for Unmanned Aircraft (UA) to transmit locally directly one-way over Bluetooth or Wi-Fi. Network RID depends upon Internet connectivity, in several segments, from the UAS to the observer. Broadcast RID should need Internet (or other Wide Area Network) connectivity only for UAS registry information lookup using the directly locally received UAS ID as a key.

[F3411-19] specifies 3 UAS ID types. Type 1 is a static, manufacturer assigned, hardware serial number per ANSI/CTA-2063-A "Small Unmanned Aerial System Serial Numbers" [CTA2063A]. Type 2 is a CAA assigned (presumably static) ID. Type 3 is a UAS Traffic Management (UTM) system assigned UUID [RFC4122], which can but need not be dynamic. The EU allows only Type 1; the US allows Types 1 and 3, but requires Type 3 IDs (if used) each to be used only once. [F3411-19] Broadcast RID transmits all information in the clear as plaintext, so Type 1 static IDs enable trivial correlation of patterns of use, unacceptable in many applications, e.g. package delivery routes of competitors.

An ID is not an end in itself; it exists to enable lookups and provision of services complementing mere identification.

Minimal specified information must be made available to the public; access to other data, e.g. UAS operator Personally Identifiable Information (PII), must be limited to strongly authenticated personnel, properly authorized per policy. [F3411-19] specifies only how to get the UAS ID to the observer; how the observer can perform these lookups, and how the registries first can be populated with information, is unspecified.

Although using UAS RID to facilitate related services, such as Detect And Avoid (DAA) and other applications of Vehicle to Vehicle or Vehicle to Infrastructure (V2V, V2I, collectively V2X) communications, is an obvious application (explicitly contemplated in the FAA NPRM), it has been omitted from [F3411-19] (explicitly declared out of scope in the ASTM working group discussions based on a distinction between RID as a security standard vs DAA as a safety application). Although dynamic establishment of secure communications between the observer and the UAS pilot seems to have

been contemplated by the FAA UAS ID and Tracking Aviation Rulemaking Committee (ARC) in their [Recommendations], it is not addressed in any of the subsequent proposed regulations or technical specifications.

The need for near-universal deployment of UAS RID is pressing. This implies the need to support use by observers of already ubiquitous mobile devices (smartphones and tablets). UA onboard RID devices are severely constrained in Size, Weight and Power (SWaP). Cost is a significant impediment to the necessary near-universal adoption of UAS send and observer receive RID capabilities. To accommodate the most severely constrained cases, all these conspire to motivate system design decisions, especially for the Broadcast RID data link, which complicate the protocol design problem: one-way links; extremely short packets; and Internet-disconnected operation of UA onboard devices. Internet-disconnected operation of observer devices has been deemed by ASTM F38.02 too infrequent to address, but for some users is important and presents further challenges. Heavyweight security protocols are infeasible, yet trustworthiness of UAS RID information is essential. Under [F3411-19], even the most basic datum, the UAS ID string (typically number) itself can be merely an unsubstantiated claim.

DRIP's goal is to make RID immediately actionable, in both Internet and local-only connected scenarios (especially emergencies), in severely constrained UAS environments, balancing legitimate (e.g. public safety) authorities' Need To Know trustworthy information with UAS operators' privacy. To accomplish this, DRIP WG will liaise with SDOs and complement their standards with IETF work to meet this urgent need. An Applicability Statement RFC for UAS RID, showing how to use IETF standardized technologies for this purpose, will be a central work product. Technical Specification RFCs will address any necessary enhancements of specific supporting protocols. DRIP (originally called Trustworthy Multipurpose Remote Identification, TM-RID) potentially could be applied to verifiably identify other types of registered things reported to be in specified physical locations, but the urgent motivation and clear initial focus is UAS. Existing Internet resources (business models, infrastructure and protocol standards) should be leveraged. A natural Internet architecture for UAS RID conforming to proposed regulations and external technical standards will be described in a companion DRIP Architecture document; this document describes only requirements.

2. Terms and Definitions

2.1. Requirements Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and

"OPTIONAL" in this document are to be interpreted as described in
BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all
capitals, as shown here.

2.2. Definitions

$SWaP

   Cost, Size, Weight and Power.

AAA

   Attestation, Authentication, Authorization, Access Control,
   Accounting, Attribution, Audit.

ABDAA

   AirBorne DAA. Also known as "self-separation".

AGL

   Above Ground Level. Relative altitude, above the variously
   defined local ground level, typically of an UA, typically
   measured in feet.

CAA

   Civil Aviation Authority. An example is the Federal Aviation
   Administration (FAA) in the United States of America.

C2

   Command and Control. A set of organizational and technical
   attributes and processes that employs human, physical, and
   information resources to solve problems and accomplish missions.
   Mainly used in military contexts.

DAA

   Detect And Avoid, formerly Sense And Avoid (SAA). A means of
   keeping aircraft "well clear" of each other for safety.

E2E

   End to End.

GBDAA

   Ground Based DAA.

GCS

   Ground Control Station. The part of the UAS that the remote pilot
   uses to exercise C2 over the UA, whether by remotely exercising
   UA flight controls to fly the UA, by setting GPS waypoints, or
   otherwise directing its flight.

GPS

   Global Positioning System. In this context, misused in place of
   Global Navigation Satellite System (GNSS) or more generally

SATNAV to refer generically to satellite based timing and/or
positioning.

Limited RID
Per the FAA NPRM, a mode of operation that must use Network RID,
must not use Broadcast RID, and must provide pilot/GCS location
only (not UA location). This mode is only allowed for UA that
neither require (due to e.g. size) nor are equipped for Standard
RID, operated within V-LOS and within 400 feet of the pilot,
below 400 feet AGL, etc.

LOS
Line Of Sight. An adjectival phrase describing any information
transfer that travels in a nearly straight line (e.g.
electromagnetic energy, whether in the visual light, RF or other
frequency range) and is subject to blockage. A term to be avoided
due to ambiguity, in this context, between RF-LOS and V-LOS.

MSL
Mean Sea Level. Relative altitude, above the variously defined
mean sea level, typically of an UA (but in FAA NPRM Limited RID
for a GCS), typically measured in feet.

NETDP
UAS RID Display Provider. System component that requests data
from one or more NETSP and aggregates them to display to a user
application on a device. Often an USS.

NETSP
UAS RID Service Provider. System component that compiles
information from various sources (and methods) in its given
service area. Usually an USS.

Observer
Referred to in other UAS RID documents as a "user", but there are
also other classes of UAS RID users, so we prefer "observer" to

denote an individual who has observed an UA and wishes to know something about it, starting with its ID.

PII

Personally Identifiable Information. In this context, typically of the UAS operator, Pilot In Command (PIC) or remote pilot, but possibly of an observer or other party.

RF

Radio Frequency. May be used as an adjective or as a noun; in the latter case, typically means Radio Frequency energy.

RF-LOS

RF LOS. Typically used in describing operation of a direct radio link between a GCS and the UA under its control, potentially subject to blockage by foliage, structures, terrain or other vehicles, but less so than V-LOS.

Standard RID

Per the FAA NPRM, a mode of operation that must use both Network RID (if Internet connectivity is available at the time in the operating area) and Broadcast RID (always and everywhere), and must provide both pilot/GCS location and UA location. This mode is required for UAS that exceed the allowed envelope (e.g. size, range) of Limited RID and for all UAS equipped for Standard RID (even if operated within parameters that would otherwise permit Limited RID).

UA

Unmanned Aircraft. Typically a military or commercial "drone" but can include any and all aircraft that are unmanned.

UAS

Unmanned Aircraft System. Composed of UA, all required on-board subsystems, payload, control station, other required off-board subsystems, any required launch and recovery equipment, all required crew members, and C2 links between UA and control station.

UAS ID

Unique UAS identifier. Per [F3411-19], maximum length of 20 bytes.

UAS ID Type

Identifier type index. Per [F3411-19], 4 bits, values 0-3 already specified.

UAS RID

UAS Remote Identification. System for identifying UA during flight by other parties.

UAS RID Verification Service

   System component designed to handle the authentication
   requirements of RID by offloading verification to a web hosted
   service.

USS

   UAS Service Supplier. 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. (From FAA UTM
   ConOps V1, May 2018).

UTM

   UAS Traffic Management. A "traffic management" ecosystem for
   "uncontrolled" UAS operations separate from, but complementary
   to, the FAA's Air Traffic Management (ATM) system for
   "controlled" operations of manned aircraft.

V-LOS

   Visual LOS. Typically used in describing operation of an UA by a
   "remote" pilot who can clearly directly (without video cameras or
   any other aids other than glasses or under some rules binoculars)
   see the UA and its immediate flight environment. Potentially
   subject to blockage by foliage, structures, terrain or other
   vehicles, more so than RF-LOS.

3. UAS RID Problem Space

UA may be fixed wing Short Take-Off and Landing (STOL), rotary wing
(e.g. helicopter) Vertical Take-Off and Landing (VTOL), or hybrid.
They may be single engine or multi engine. The most common today are
multicopters: rotary wing, multi engine. The explosion in UAS was
enabled by hobbyist development, for multicopters, of advanced
flight stability algorithms, enabling even inexperienced pilots to
take off, fly to a location of interest, hover, and return to the
take-off location or land at a distance. UAS can be remotely piloted
by a human (e.g. with a joystick) or programmed to proceed from
Global Positioning System (GPS) waypoint to waypoint in a weak form
of autonomy; stronger autonomy is coming. UA are "low observable":
they typically have a small radar cross section; they make noise
quite noticeable at short range but difficult to detect at distances
they can quickly close (500 meters in under 17 seconds at 60 knots);
they typically fly at low altitudes (for the small UAS to which RID
applies in the US, under 400 feet AGL); they are highly maneuverable
so can fly under trees and between buildings.

UA can carry payloads including sensors, cyber and kinetic weapons,
or can be used themselves as weapons by flying them into targets.
They can be flown by clueless, careless or criminal operators. Thus

the most basic function of UAS RID is "Identification Friend or Foe" (IFF) to mitigate the significant threat they present. Numerous other applications can be enabled or facilitated by RID: consider the importance of identifiers in many Internet protocols and services.

Network RID from the UA itself (rather than from its GCS) and Broadcast RID require one or more wireless data links from the UA, but such communications are challenging due to $SWaP constraints and low altitude flight amidst structures and foliage over terrain.

3.1. Network RID

Network RID has several variants. The UA may have persistent onboard Internet connectivity, in which case it can consistently source RID information directly over the Internet. The UA may have intermittent onboard Internet connectivity, in which case the GCS must source RID information whenever the UA itself is offline. The UA may not have Internet connectivity of its own, but have instead some other form of communications to another node that can relay RID information to the Internet; this would typically be the GCS (which to perform its function must know where the UA is). The UA may have no means of sourcing RID information, in which case the GCS must source it; this is typical in FAA NPRM Limited RID, which only needs to provide the location of the GCS (not that of the UA). In the extreme case, this could be the pilot using a web browser to designate, to an UAS Service Supplier (USS) or other UTM entity, a time-bounded airspace volume in which an operation will be conducted; this may impede disambiguation of ID if multiple UAS operate in the same or overlapping spatio-temporal volumes.

In most cases in the near term, if the RID information is fed to the Internet directly by the UA or GCS, the first hop data links will be cellular Long Term Evolution (LTE) or WiFi, but provided the data link can support at least IP and ideally TCP, its type is generally immaterial to the higher layer protocols. An UAS or other ultimate source of Network RID information feeds an USS acting as a Network RID Service Provider (NETSP), which essentially proxies for that and other sources; an observer or other ultimate consumer of Network RID information obtains it from a Network RID Display Provider (NETDP), which aggregates information from multiple NETSPs to offer coverage of an airspace volume of interest.

Network RID is the more flexible and less constrained of the defined UAS RID means, but is only partially specified in [F3411-19]. It is presumed that IETF efforts supporting Broadcast RID (see next section) can be easily generalized for Network RID.

3.2. Broadcast RID

[F3411-19] specifies 3 Broadcast RID data links: Bluetooth 4.X;
Bluetooth 5.X Long Range; and WiFi with Neighbor Awareness
Networking (NAN). For compliance with this standard, an UA must
broadcast (using advertisement mechanisms where no other option
supports broadcast) on at least one of these; if broadcasting on
Bluetooth 5.x, it is also required concurrently to do so on 4.x
(referred to in [F3411-19] as Bluetooth Legacy).

The selection of the Broadcast media was driven by research into
what is commonly available on 'ground' units (smartphones and
tablets) and what was found as prevalent or 'affordable' in UA.
Further, there must be an Application Programming Interface (API)
for the observer's receiving application to have access to these
messages. As yet only Bluetooth 4.X support is readily available,
thus the current focus is on working within the 26 byte limit of the
Bluetooth 4.X "Broadcast Frame" transmitted on beacon channels.

Finally, the 26 byte limit of the Bluetooth 4.1 "Broadcast Frame",
after nominal overheads, limits the UAS ID string to a maximum
length of 20 bytes.

3.3. DRIP Focus

DRIP WG will focus on making information obtained via UAS RID
immediately usable:

1. first by making it trustworthy (despite the severe constraints
   of Broadcast RID);

2. second by enabling verification that an UAS is registered, and
   if so, in which registry (for classification of trusted
   operators on the basis of known registry vetting, even by
   observers lacking Internet connectivity at observation time);

3. third by enabling instant establishment, by authorized parties,
   of secure communications with the remote pilot.

Any UA can assert any ID using the [F3411-19] required Basic ID
message, which lacks any provisions for verification. The Position/
Vector message likewise lacks provisions for verification, and does
not contain the ID, so must be correlated somehow with a Basic ID
message: the developers of [F3411-19] have suggested using the MAC
addresses, but these may be randomized by the operating system stack
to avoid the adversarial correlation problems of static identifiers.
The [F3411-19] optional Authentication Message specifies framing for
authentication data, but does not specify any authentication method,
and the maximum length of the specified framing is too short for
conventional digital signatures, much less certificates. The one-way

nature of Broadcast RID precludes challenge-response security protocols (e.g. observers sending nonces to UA, to be returned in signed messages). An observer would be seriously challenged to validate the asserted UAS ID or any other information about the UAS or its operator looked up therefrom.

Further, [F3411-19] provides very limited choices for an observer to communicate with the pilot, e.g. to request further information on the UAS operation or exit from an airspace volume in an emergency. An observer could physically go to the asserted GCS location to look for the remote pilot. An observer with Internet connectivity could look up operator PII in a registry, then call a phone number in hopes someone who can immediately influence the UAS operation will answer promptly during that operation.

Thus complementing [F3411-19] with protocols enabling strong authentication, preserving operator privacy while enabling immediate use of information by authorized parties, is critical to achieve widespread adoption of a RID system supporting safe and secure operation of UAS.

4. Requirements

4.1. General

The general DRIP requirements are to:

1. verify that messages originated from the claimed sender;

2. verify that the UAS ID is in a registry and identify which one;

3. lookup, from the UAS ID, public information;

4. lookup, with AAA, private information, per policy;

5. structure information for both human and machine readability;

6. provision registries with static information on the UAS and its operator, dynamic information on its current operation within the UTM, and Internet direct contact information for services related to the foregoing;

7. close the AAA-policy registry loop by governing AAA per registered policies and administering policies only via AAA;

8. dynamically establish, with AAA, per policy, E2E strongly encrypted communications with the UAS RID sender and entities looked up from the UAS ID, including the remote pilot and USS.

It is highly desirable that Broadcast RID receivers be able to stamp
messages with accurate date/time received and receiver location,
then relay them to a network service (e.g. distributed ledger),
inter alia for correlation to assess sender and receiver veracity.

4.2. UAS Identifier

A DRIP UAS ID MUST be:

1. 20 bytes or smaller;

2. sufficient to identify a registry in which the UAS is listed;

3. sufficient to enable lookup of other data in that registry;

4. unique within a to-be-defined scope;

5. non-spoofable within the context of Remote ID broadcast
   messages (some collection of messages provides proof of UA
   ownership of ID).

A DRIP UAS ID MUST NOT facilitate adversarial correlation of UAS
operational patterns; this may be accomplished e.g. by limiting each
identifier to a single use, but if so, the UAS ID MUST support
defined scalable timely registration methods.

Mechanisms standardized in DRIP WG MUST be capable of proving
ownership of a claimed UAS ID, and SHOULD be capable of doing so
immediately on an observer device lacking Internet connectivity at
the time of observation.

Mechanisms standardized in DRIP WG MUST be capable of verifying that
messages claiming to have been sent from a UAS with a given UAS ID
indeed came from the claimed sender.

5. IANA Considerations

It is likely that an IPv6 prefix or other namespace will be needed;
this will be specified in other documents.

6. Security Considerations

DRIP is all about safety and security, so content pertaining to such
is not limited to this section. DRIP information must be divided
into 2 classes: that which, to achieve the purpose, must be
published openly in clear plaintext, for the benefit of any
observer; and that which must be protected (e.g. PII of pilots) but
made available to properly authorized parties (e.g. public safety
personnel who urgently need to contact pilots in emergencies).
Details of the protection mechanisms will be provided in other

documents. Classifying the information will be addressed primarily in external standards; herein it will be regarded as a matter for CAA, registry and operator policies, for which enforcement mechanisms will be defined within the scope of DRIP WG and offered. Mitigation of adversarial correlation will also be addressed.

7. Acknowledgments

The work of the FAA's UAS Identification and Tracking (UAS ID) Aviation Rulemaking Committee (ARC) is the foundation of later ASTM [F3411-19] and IETF DRIP WG efforts. The work of ASTM F38.02 in balancing the interests of diverse stakeholders is essential to the necessary rapid and widespread deployment of UAS RID.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/ RFC2119, March 1997, <https://www.rfc-editor.org/info/ rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

8.2. Informative References

[CTA2063A] ANSI, "Small Unmanned Aerial Systems Serial Numbers", September 2019.

[Delegated] European Union Aviation Safety Agency (EASA), "Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems", March 2019.

[F3411-19] ASTM, "Standard Specification for Remote ID and Tracking", December 2019.

[Implementing] European Union Aviation Safety Agency (EASA), "Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft", May 2019.

[NPRM]   United States Federal Aviation Administration (FAA), "Notice of Proposed Rule Making on Remote Identification of Unmanned Aircraft Systems", December 2019.

[Recommendations]
               FAA UAS Identification and Tracking Aviation
               Rulemaking Committee, "UAS ID and Tracking ARC
               Recommendations Final Report", September 2017.

[RFC4122]   Leach, P., Mealling, M., and R. Salz, "A Universally
               Unique IDentifier (UUID) URN Namespace", RFC 4122, DOI
               10.17487/RFC4122, July 2005, <https://www.rfc-editor.org/
               info/rfc4122>.

Authors' Addresses

Stuart W. Card
AX Enterprize
4947 Commercial Drive
Yorkville, NY 13495
United States of America

Email: stu.card@axenterprize.com

Adam Wiethuechter
AX Enterprize
4947 Commercial Drive
Yorkville, NY 13495
United States of America

Email: adam.wiethuechter@axenterprize.com

Robert Moskowitz
HTT Consulting
Oak Park, MI 48237
United States of America

Email: rgm@labs.htt-consult.com