FEBRUARY 2023

Landscape Whitepaper on UAS Cellular Ecosystem

Aerial Connectivity Joint Activity
Work Task #4

Contents

1. Introduction

1.1. Purpose

This paper is intended to describe an exhaustive set of entities involved in cellular communication of uncrewed aviation systems, their interrelationship between each other, ACJA activities, and external standardization activities. This description is intended to be used internally by all ACJA Work Tasks to help to coordinate further activities, to have a common terminology, to help to on-board new stakeholders, and to describe a scope of new ACJA tasks.

1.2. Scope

We intend to discuss all aspect of the ecosystem for UAS Voice Relay, data and information exchange, including MNOs, Service Providers for C2 services, UAV on-board components, Remote Pilot Stations or Ground Control Stations, UTM and UAM components, and any relevant ground infrastructure components used for interconnectivity for operations and planning.

This paper focus specifically on cellular MNOs and cellular connectivity. However, the technical content aims at remaining open to considering additional types of connectivity, including satellite connectivity.

In terms of applications, this White Paper intends to consider all kinds of connectivity-supported UAS and UAM capabilities including by not limited to Communication and Control (C2), UTM and AAM connectivity, Air Vehicle-to- Air Vehicle communications, and external interconnectivity between Mobile Network Operators (MNO), C2 Communication Service Providers (C2CSP), Aircraft operators and UAS Operators, Regulator, and other service providers via an Aviation Data Network(s). Distinct discussion should also consider current/envisioned standardization of the components describe, as well as information security (or cybersecurity) aspect.

In this version of this document, the term Air-Ground RF refers to cellular communications.

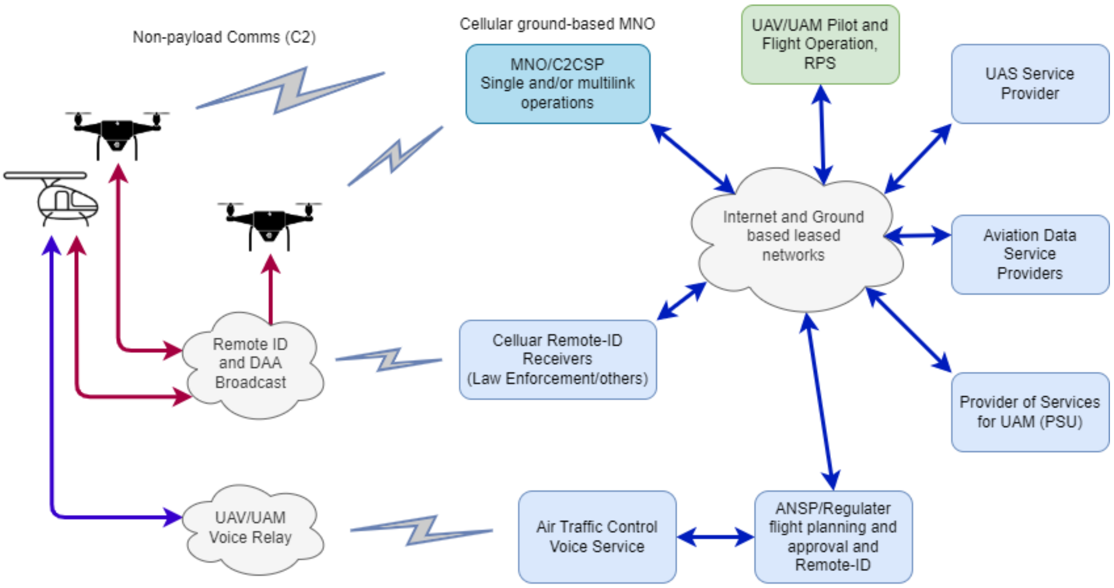

Non-payload Comms (C2)
Cellular ground-based MNO
MNO/C2CSP Single and/or multilink operations
UAV/UAM Pilot and Flight Operation, RPS
UAS Service Provider
Internet and Ground based leased networks
Aviation Data Service Providers
Remote ID and DAA Broadcast
Celluar Remote-ID Receivers (Law Enforcement/others)
Provider of Services for UAM (PSU)
UAV/UAM Voice Relay
Air Traffic Control Voice Service
ANSP/Regulater flight planning and approval and Remote-ID

Figure 1. General Scope of ACJA Landscape.

2. Terms and Abbreviations

The following sections present key abbreviations and terms of aviation and telecom domains. The terms that are valid in both domains are highlighted with *. Please note that this list follows the available guidelines for the all-inclusive terminology, but as this effort is still ongoing in global level, the latest versions are presented in this list; the newer versions will be updated in this list as they are formally available.

2.1. Aviation Abbreviations

Abbreviation	Description
ACAS	Airborne Collision Avoidance System is a stand-alone system to warn pilots about the presence of other aircraft that may present a threat of collision.
ADS-B	Automatic Dependent Surveillance – Broadcast is a surveillance technology for tracking the position of an aircraft.
ADX	The Aviation Data eXchange Network is an inter-Service Provider IP backbone dedicated to supporting aviation-specific services oriented to the UAS and AAM use cases (transport of C2, voice relay, first-person view video used to navigate, aviate, and integrate pilot's activities, payload communications and other data) and that isolation from the Internet, quality of service and experience, and assurance of security. Aviation Data eXchange Network
AGL	Above Ground Level is the actual height above the ground over which, e.g., drone is flying.

ANSP	Air Navigation Service Provider is any public or private entity providing air navigation services.
APN	Access Point Name identifies in 4G 3GPP systems the data network a mobile device gets access to.
ATC	Air Traffic Control is a service operated by appropriate authority to promote the safe, orderly and expeditious flow of air traffic.
ATM	Air Traffic Management is the dynamic and integrated management of air traffic and airspace safely, economically and efficiently.
BVLOS	Beyond Visual Line of Sight refers to environment where the pilot has the ability to operate an UAS beyond the pilot's line of sight.
C2	Command and Control data link between the remotely piloted aircraft and the remote pilot station for the purpose of managing flight.
C3	Command, Control and Communications link is similar to C2 link, with the addition of a communications link for the voice and data for the flight operation, but not the management.
CIS	Common Information Services facilitate USS-USS exchange as their primary function, serving as a single source of truth. CIS include information about manned aircraft in the U-space, using operational data held at marginal cost by air navigation service providers. *See*: U-Space. Regulation related details are at easa.europa.eu.
CNPC	Command, Control and Non-Payload Communication link connects the remote pilot located at a ground control station with the aircraft in the airspace.

CONOPS	Concept of Operations is a user-oriented document that describes systems characteristics for a proposed system from a user's perspective.
CRPS	Cloud RPS is implemented as one or more applications running in the cloud to provide the functionality of RPS.
CS	Control Station; also referred to as Flight Controller or GCS. *See:* GCS.
DAA	Detect and Avoid is the capability to see, sense or detect conflicting traffic or other hazards and take the appropriate action, and aims to ensure the safe execution of an RPA flight and to enable full integration in all airspace classes with all airspace users.
DNN	Data Network Name identifies in 5G 3GPP systems the data network a mobile device gets access to.
EVLOS	Extended Visual Line of Sight is an Unmanned Aircraft System (UAS) operation whereby the Pilot in Command (PIC) maintains situational awareness of the airspace via visual airspace surveillance, possibly aided by technology means.
eVTOL	Electric Vertical Take-off and Landing refers to aircraft that uses electric power to hover, take off, and land vertically. *See*: VTOL.
FIMS	Flight Information Management System is an aviation data exchange hub that connects air traffic management system to UAS Service Providers for safe drone operations in low-altitude airspace. Comparable to CIS. The CIS provider or FIMS manager shall enable the sharing of static and dynamic data and information that shall be commonly used by U-space service providers providing services in the U-space airspace, as stated by EASA.

FLARM	Flight Alarm provides traffic awareness and collision avoidance technology for General Aviation, light aircraft, and UAVs to avoid traffic and imminent collisions. FLASM is a proprietary technology.
FPV	First-Person View is a method to control aircraft by allowing the operator to observe the view from the vehicle's perspective.
GCS	Ground Control System is the part of a UAS that remotely controls the UA. The communication between the smaller drone and the controller is commonly via Wi-Fi or VHF. See: *RPS*.
HAE	High altitude and endurance. *See*: *HALE*.
HALE	High Altitude, Long Endurance is a UAS category that operates above the controlled manned airspace. The maximum speed of HALE UAS is 12,000 km/h requiring dedicated airspace and dynamic flow management.
HAPS	High Altitude Platform Station is easily deployable station in stratosphere to provide service to a large area or to augment the capacity of broadband service providers.
IFR	Instrument Flight Rules are established by the ICAO to govern flight under conditions in which flight by outside visual reference is not safe.
IPX	The internet Protocol (IP) Packet eXchange (IPX) Network is an inter-Service Provider IP backbone which supports multiple IPX services defined in GSMA Permanent Reference Document AA.51.
LAANC	Low Altitude Authorization and Notification Capability system is an authorisation process defined by the FAA in the US to facilitate and

	support UAS integration into national airspace, allowing drones access to controlled airspace in near real-time.
LOS*	Line of Sight refers to the unblocked "visibility" of radio signal so that the remote pilot and the UAS can be in direct radio contact (not necessarily via visual contact).
LUC	Light UAS operator Certificate. *See*: Specific Category Drone.
MASPS	Minimum Aviation System Performance Standards/Specifications are operational airspace systems characteristics for designers, installers, manufacturers, service providers and users.
MOPS	Minimum Operational Performance Standards/Specifications are characteristics and requirements of equipment for designers, manufacturers, installers, and users. Equipment refers to all components and units necessary for the system to properly perform its functions.
MSL	Mean Sea Level is the true altitude or elevation; the average height above standard sea level where the atmospheric pressure is measured in order to calibrate altitude.
NAS*	National Airspace System is a U.S. network of controlled and uncontrolled, domestic and oceanic airspace including air navigation facilities, equipment and services, airports and landing areas, aeronautical charts, information and services, rules and regulations, procedures and technical information, and manpower and material.
OSED	Operational Services and Environment Definition
PIC	Pilot In Command is the remote pilot in command directly responsible for and is the final authority as to the operation of the UAV.

PSU	Providers of Services for UAM to support the UAM community, will provide services to support operations planning, flight intent sharing, strategic and tactical deconfliction, airspace management functions, and off-nominal operations. They will exchange information with other PSUs and other entities to enable information flow across the USS/AAM network, and to promote shared situational awareness among UTM and UAM participants via a network that enables safe, efficient operation within the UAM corridors without involvement by ATC.
QoS*	Quality of Service is the collective effect of service performances which determine the degree of satisfaction of a user of a service. It considers service performance factors such as service operability, accessibility, retainability and integrity performance.
RPAS	Remotely Piloted Aircraft System is remotely piloted aircraft, its associated remote pilot stations, command and control links, and other system elements during flight.
RPS	Remote Pilot Station is the component of the remote pilot aircraft system containing the equipment used to pilot the remotely piloted aircraft.
SAA	See and Avoid is the human pilot capability of a UAS to remain clear from and avoid collisions with other airborne traffic. SAA provides self-separation and collision avoidance.
SDSP	Supplemental Data Service Provider refers to a model and/or data-based services that disseminate essential or enhanced information to ensure safe operations within an airspace, e.g., including, but not

	limited to, terrain, obstacle data, aerodrome availability, and specialized weather.
SORA	Specific Operation Risk Assessment refers to means by which an aircraft operator is granted approval by certifying authorities to operate an unmanned aircraft system.
sUAS	Small UAS is a FAA-defined category for UAS weighting less than 55 pounds (25 kg), including payload. Aircraft that are below this weight can be operated for commercial purposes under the Part 107 of the FAA regulations. This definition is for U.S. region.
UA	Unmanned Aircraft is a synonym of UAV or Drone. *See*: UAV; Drone.
UAM	Urban Air Mobility envisions a safe and efficient aviation transportation system that will use highly automated aircraft that will operate and transport passengers or cargo.
UAS	Unmanned Aircraft System refers to the combination of the vehicle or aircraft, the controller, and the links that connect them.
UAV	Unmanned Air Vehicle refers to the platform, airframe, or body of the craft. The term can be used interchangeably with Drone and UA. *See*: Drone; UA.
USS	UTM Service Supplier provides UTM services to support the UAS community, to connect UAS Operators and other entities to enable information flow across the USS network, and to promote shared situational awareness among UTM participants.
UTM	Unmanned Traffic Management safely integrates manned and unmanned aircraft into low altitude airspace helping manage traffic at low altitudes and avoid collisions of UASs being operated beyond

	visual line of sight. UTM architecture is consolidated but its deployment models may differ.
VFR	Visual Flight Rules are a set of ICAO regulations under which a pilot operates an aircraft in weather conditions clear enough to allow the pilot to see where the aircraft is going.
VLOS	An operation in which the remote pilot or remotely piloted aircraft observer maintains direct unaided visual contact with the remotely piloted aircraft. Hobbyist and consumer drones are in this category exempt from permission.
VTOL	Vertical Take-off and Landing refers to any of several unconventional aircraft with rotating wing systems, such as the helicopter and autogiro. They may also have rotatable jet systems capable of vertical lift-off and landing in areas that only slightly exceed the overall dimensions of the aircraft. *See*: eVTOL.
WRPS	Wireless RPS is a 3GPP UE with appropriate application solutions to act as an RPS.

2.2. Aviation Terms

Term	Description
Air Corridor	A route that aircraft must take through an area in which flying is restricted.
Airspace Class	Airspace Class A-E refers to Controlled Airspace that protects its users such as commercial airliners. Airspace Class F-G refers to Uncontrolled Airspace. Classes A-G are defined by ICAO, but not every region/state adopts a full set of classes.

Airworthiness	The condition of an item (aircraft, aircraft system, or part) in which that item operates in a safe manner to accomplish its intended function.
Availability	(of a data link) Availability is minimum percentage of time that the services of the system are usable with the level of guarantee on latency and throughput.
Broadcast*	Transmission of data to no specific destination or recipient. Data can be received by anyone within broadcast range.
Broadcast Remote Identification	Transmission of radio signals directly from an airborne UAS to ground receivers in the UAS's vicinity. *See*: Direct Remote Identification.
Certified Category	Category of UA operation that for risks involved requires the certification of the UAS, a licensed remote pilot and an UAS Operator approved by the competent authority.
Collision Avoidance	Collision avoidance systems of UA controlled by people or flying autonomously to prevent them from flying into fixed objects or other aircraft.
Conflict Management	Conflict management consists of three layers: strategic deconfliction, separation provision (tactical deconfliction) and collision avoidance.
Continuity	(of a data link) Continuity is an acceptable probability message is delivered successfully after its transmission was started assuming the communications system is available when the transmission is initiated.

Controlled Airspace	Airspace of defined dimensions within which air traffic control service is provided to IFR flights and to VFR flights in accordance with the airspace classification, to protect its users. *See*: Airspace Class.
Cooperative UA	Aircraft that have an electronic means of identification (i.e., a transponder) aboard and operating.
Core*	Core network a critical functional entity that allows the information to be exchanged, offering a variety of services to customers such as authentication and call control.
Criticality	The degree of impact that a malfunction has on the operation of a system.
Datalink	Provides interconnections to, from and within the remotely piloted aircraft system. It includes control, flight status, communication, and payload links.
Decentralised Strategic Deconfliction	Critical function in Unmanned Aircraft System (UAS) Traffic Management (UTM), that serves as the enabler of safe operations for cooperative traffic.
Direct Remote Identification	System that ensures the local broadcast of information about unmanned aircraft in operation without physical access to the unmanned aircraft.
Drone	Any type of unmanned vehicle, either on the ground, aerial or under water. In practice, refers often Unmanned Aerial Vehicles. *See*: UA (Unmanned Aircraft).

Drone Category	EASA has defined three drone categories that relate to the level of risk involved in carrying out the operation rather than to whether the work is being carried out commercially: Open, Specific, and Certified.
Drone Remote Pilot	*See*: UAS Remote Pilot.
Fail Safe	System that helps protect a UAS in case of a failure, e.g., if an UAS loses control signal, a Fail Safe can assist the UAS to return to the initial location or land immediately.
Fixed Wings	Drone design that provides energy-efficient aerodynamics and long flight times (45-60 minutes per flight) for high aerial coverage although with less detailed imagery.
Flight Controller	*See*: GCS (Ground Control System).
Handover*	The transfer of a user's connection from one radio channel to another in such a way that the established connection does not break down.
Hybrid Drone	Is capable of Vertical Take-off and Landing (VTOL) and flying quickly in a forward motion to cover larger areas of land, while still having the ability to hover. *See*: VTOL.
Integrity	(of a data link) Integrity is an acceptable probability of elementary message transmission was completed with an undetected error.
Interconnectivity	The communications connection methods used between two or more organizations used to securely exchange e2e information. This could be between an UAS operator and its pilot control station, or aircraft operations to a:

	• Mobile Network Operator (MNO) • USS or PSU • Aviation regulator • Other Data Service Provider
Manned Aviation	Refers to aviation technologies or activities that include or require the physical presence of one or more crew members in the aircraft, e.g., in commercial aircraft.
Mobility	The ability for the user to communicate whilst moving independently of location.
Model Aircraft	Unmanned aircraft model that is typically a scaled-down version of manned aircraft. The use of such models needs to be in accordance with the regulation.
Multi Rotor	The most popular drone types for consumer and small commercial use; easy to operate and pilot, vertical take-off and landing, ability to hover, high power consumption. Suitable, e.g., for industrial inspections, aerial mapping, site planning. *See*: Single Rotor.
Network Remote Identification	Via Network Remote Identification, UA provides a set of its identification-related information through a network. This happens in real time during the flight using an open and documented transmission protocol and based on local regulation. *See*: Remote ID.
No Fly Zone	Area, defined by the aviation authorities, where flying a drone is restricted by government regulations, such as airports, critical infrastructure and military zones.

Non-Cooperative UA	Aircraft that do not have electronic means of identification (i.e., a transponder) aboard.
Open Category Drone	Low-risk UAS operation that does not require a prior authorisation by the competent authority nor a declaration by the UAS operator prior to the operation.
Operator Location	The geographic location of the Remote Pilot of a UAS.
Part 101	FAA Part 101 consolidates the rules governing all unmanned aeronautical activities into one body of legislation, including the use of unmanned moored balloons, kites, free balloons, unmanned rockets, remotely piloted aircraft (RPA), model aircraft, and pyrotechnic displays.
Part 107	Commercial drone operator regulations of the FAA detailing restrictions and safety standards for commercial drone flights of UAS below 55 lbs (25kg).
Payload*	Physical items that are attached to or carried by the craft; examples are cameras, sensors, or other equipment like spraying tools and packages in general.
Registration	The process by which an owner or operator information and aircraft-specific information are associated with an assigned, unique identifier.
Regulated Airspace	*See*: Controlled airspace.

Reliability*	The probability that an item will perform a required function under specified conditions, without failure, for a specified period of time. In aviation, reliability in often defined in terms of integrity, continuity and availability.
Remote ID	Remote Identification is the ability of a drone in flight to provide identification and location information that can be received by other parties.
Risk	The frequency (probability) of occurrence and the associated level of hazard.
Risk Assessment	The process by which the results of risk analysis are used to make decisions.
Service	The meaning of the term depends on the context, and may refer to a telecommunications service (enabling data exchanges between different stakeholders in a opaque way), a value-added service (application-aware, such as network coverage or authentication service), or to a U-space service (cloud-based web-service providing some application-level capabilities for UAVs).
Specific Category Drone	This is a category of UAS operation that, considering the risks involved, requires an authorisation before the operation takes place except for certain standard scenarios where a declaration by the operator is sufficient or when the operator holds a Light UAS operator Certificate (LUC) with the appropriate privileges.
Tactical Deconfliction	Envisioned UTM service for provision of a safe distance or safe time between aircraft in flight. It is considered a reactive conflict management.

Type of UAS	The main types of UAS available in the commercial space are: Single or Multi Rotor, Fixed Wings, and Hybrid (VTOL, Vertical Take-Off and Landing).
UA Category	*See*: Drone Category.
UA Operator	UA Operator, or Operator, is an entity or person responsible for flight which could include a company or individual or both.
UAS Operator	UAS Operator, or Operator, is an entity or a person responsible for flight; can include a company or individual or both. *See*: UA Operator.
UAS Remote Pilot	The person who has final authority and responsibility for the operation and safety of flight. Synonymous with "remote pilot-in-command".
Uncontrolled Airspace	Refers generally to the Class G airspace where any aircraft can fly without either notifying or getting permission from the national Civil Aviation authority.
Unmanned Aviation	Refers to aviation-related technologies that do not require the physical presence of a crew member in the aircraft.
Unregulated Airspace	*See*: Uncontrolled Airspace.
U-Space	Set of new services relying on a high level of digitalisation and automation of functions and specific procedures designed to support safe, efficient and secure access to airspace for large numbers of drones. U-space is an enabling framework to facilitate routine missions in all airspace classes and environments while

	addressing an appropriate interface with manned aviation and air traffic control.
Waypoints	A set of coordinates that define a point in space. They create flight path for drones.

3. Standardization Environment

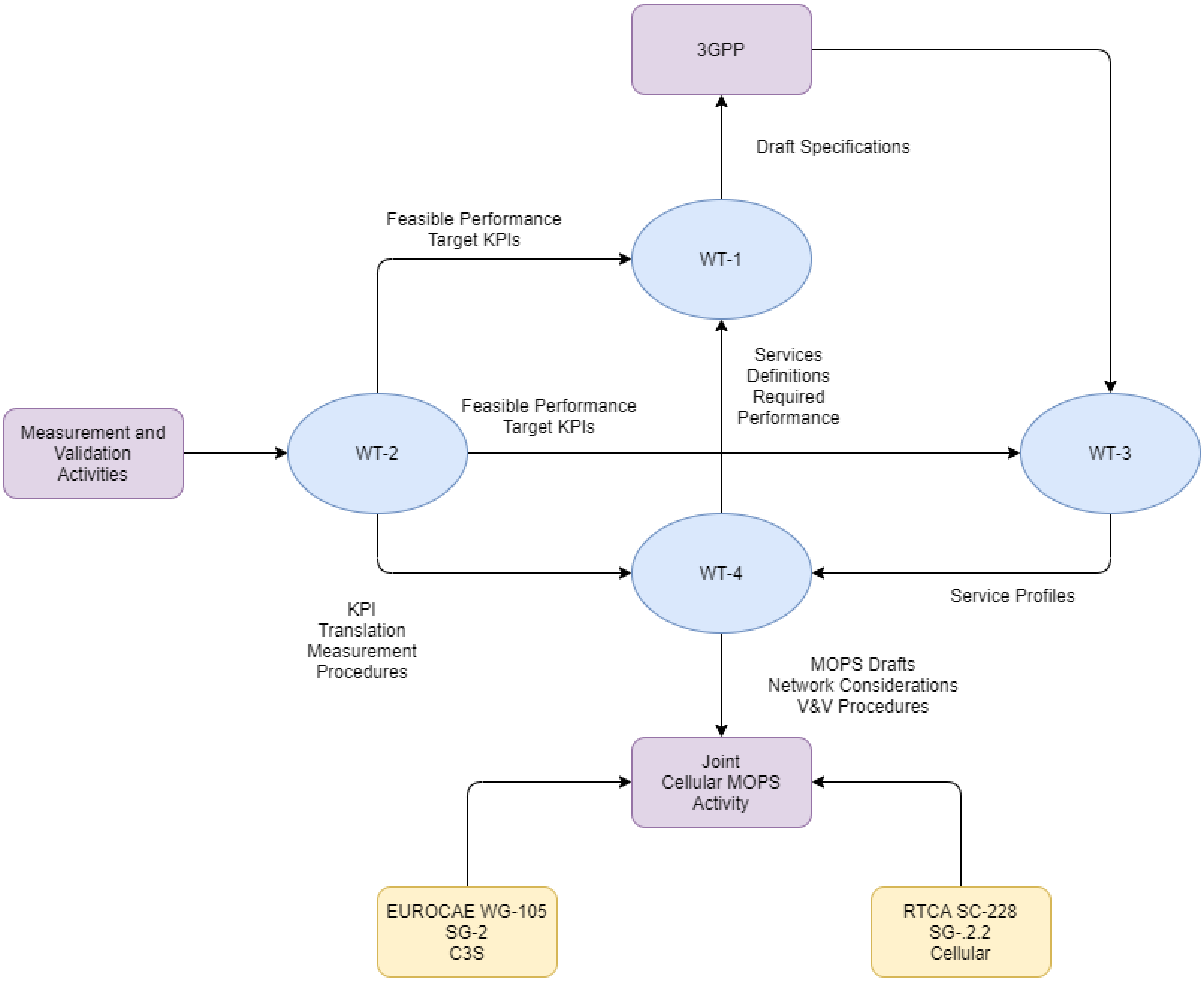

3GPP
Draft Specifications
Feasible Performance Target KPIs
WT-1
Services Definitions Required Performance
Measurement and Validation Activities
WT-2
Feasible Performance Target KPIs
WT-3
WT-4
Service Profiles
KPI Translation Measurement Procedures
MOPS Drafts Network Considerations V&V Procedures
Joint Cellular MOPS Activity
EUROCAE WG-105 SG-2 C3S
RTCA SC-228 SG-.2.2 Cellular

Figure 2. Scope of standardization discussion.

This diagram shows primary information flows between ACJA Work Tasks and external entities, for which more formal relationship has been established. These include EUROCAE (under GUTMA-EUROCAE Memorandum of Understanding) and 3GPP (via GSMA as an MRP — Market Representation Partner). However, it is important to note the much of the ACJA inputs may base on individual contribution of ACJA members, who represent and participate in a wide range of standardization and research activities.

4. Overall Ecosystem Architecture

The following figure depicts the overall UAV ecosystem architecture. Detailed components are described in section 6.

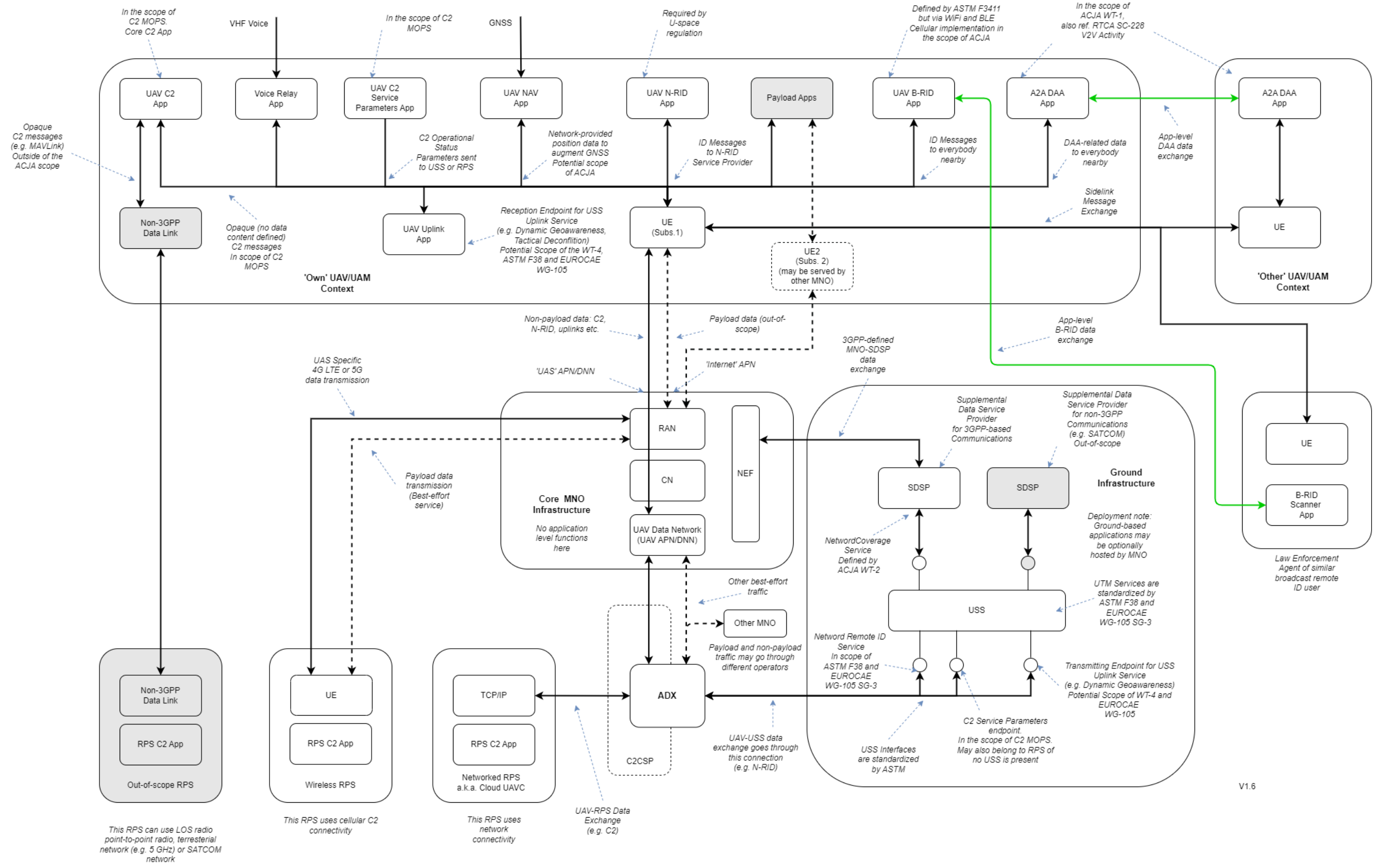

In the scope of C2 MOPS. Core C2 App
VHF Voice
In the scope of C2 MOPS
GNSS
Required by U-space regulation
Defined by ASTM F3411 but via WiFi and BLE Cellular implementation in the scope of ACJA
In the scope of ACJA WT-1, also ref. RTCA SC-228 V2V Activity
UAV C2 App
Voice Relay App
UAV C2 Service Parameters App
UAV NAV App
UAV N-RID App
Payload Apps
UAV B-RID App
A2A DAA App
A2A DAA App
Opaque C2 messages (e.g. MAVLink) Outside of the ACJA scope
C2 Operational Status Parameters sent to USS or RPS
Network-provided position data to augment GNSS Potential scope of ACJA
ID Messages to N-RID Service Provider
ID Messages to everybody nearby
DAA-related data to everybody nearby
App-level DAA data exchange
Sidelink Message Exchange
Non-3GPP Data Link
Opaque (no data content defined) C2 messages In scope of C2 MOPS
UAV Uplink App
Reception Endpoint for USS Uplink Service (e.g. Dynamic Geoawareness, Tactical Deconflition) Potential Scope of the WT-4, ASTM F38 and EUROCAE WG-105
UE (Subs.1)
UE2 (Subs. 2) (may be served by other MNO)
UE
'Own' UAV/UAM Context
'Other' UAV/UAM Context
Non-payload data: C2, N-RID, uplinks etc.
Payload data (out-of-scope)
App-level B-RID data exchange
3GPP-defined MNO-SDSP data exchange
UAS Specific 4G LTE or 5G data transmission
'UAS' APN/DNN
'Internet' APN
RAN
CN
NEF
UAV Data Network (UAV APN/DNN)
Core MNO Infrastructure
No application level functions here
Payload data transmission (Best-effort service)
Supplemental Data Service Provider for 3GPP-based Communications
Supplemental Data Service Provider for non-3GPP Communications (e.g. SATCOM) Out-of-scope
SDSP
SDSP
Ground Infrastructure
Deployment note: Ground-based applications may be optionally hosted by MNO
NetwordCoverage Service Defined by ACJA WT-2
UE
B-RID Scanner App
Law Enforcement Agent of similar broadcast remote ID user
Other best-effort traffic
Other MNO
Payload and non-payload traffic may go through different operators
USS
UTM Services are standardized by ASTM F38 and EUROCAE WG-105 SG-3
Netword Remote ID Service In scope of ASTM F38 and EUROCAE WG-105 SG-3
Transmitting Endpoint for USS Uplink Service (e.g. Dynamic Geoawareness) Potential Scope of WT-4 and EUROCAE WG-105
Non-3GPP Data Link
RPS C2 App
Out-of-scope RPS
UE
RPS C2 App
Wireless RPS
TCP/IP
RPS C2 App
Networked RPS a.k.a. Cloud UAVC
ADX
C2CSP
UAV-USS data exchange goes through this connection (e.g. N-RID)
USS Interfaces are standardized by ASTM
C2 Service Parameters endpoint. In the scope of C2 MOPS. May also belong to RPS of no USS is present
V1.6
This RPS can use LOS radio point-to-point radio, terresterial network (e.g. 5 GHz) or SATCOM network
This RPS uses cellular C2 connectivity
This RPS uses network connectivity
UAV-RPS Data Exchange (e.g. C2)

Figure 3. Birds-eye Overview of the ACJA Landscape

5. End-to-End Performance Considerations

ACJA scope is defined by the need of aviation stakeholder to have a connectivity service with known end-to-end data and information exchange, that is from UE's data interface to a remote endpoint within a remote pilot station or a service provided by the USS/PSU). Some voice scenarios (e.g., UAS voice relay) are also considered, as explained in detail in the following sections. Hence any component of the transmission chain for command and control of the aircraft or information exchange, which can influence overall connectivity performance or violate any security requirement, falls into the scope.

The security solutions deployed by MNOs to secure UAS-related data traffic shall be independent from security solutions deployed by UAS operators to protect UAS-related data traffic.

From a security point of view, based on the standards developed by RTCA and others, the following assumptions are made:

- End-to-end and secure connections for voice, C2 data and payload data between the RPS and UA that is encrypted and protected between the RPS and UA directly that is independent from the methods of protection that are implemented at a link layer for the air-ground RF link and the ground-ground interface to the service provider.
- The RF link between the UE and the ground termination point should provide a secure path further protecting the encrypted data exchange between the RPS and UA.
- The ground interface between the RPS to the MNO, C2CSP should be a secure link that provides independent and further protection for the end-to-end encrypted Voice and data information exchange of the RPS to UE communications.
- At an application level, for broadcast services like remote ID, those services must also have a level of trust as well.

As the ecosystem grows, it should be clear that not all IP protocol stacks are the same. This is important as the UA operators will be following standards for command and control that follow the international aviation standard defined in ICAO Document 9896. Each unique IP protocol stacks operate the same way at the lower level (network, Internet, IP).

For the purpose of this document to be able to use a common reference, The Open System Interconnection (OSI) model is chosen to represent the transmission chain, but the concepts can be applied to all models.

5.1. ISO OSI Model Projection

On the representation below "ACJA-Defined Connectivity Performance" layer (being virtual without direct mapping into OSI standard layers) is used to mark where the main ACJA considerations apply while standard connectivity mechanisms and protocols are generally used in the delivery of commercial telecommunications services, networks are established and have varying degrees of services associated with different types of users. The commercial telecommunications and data services associated the aviation Remotely Piloted Aircraft Systems (RPAS) ecosystem have not been fully defined or developed. As such, the ACJA will be working with many stakeholders of the ecosystem to define the performance standards that could be implemented by commercial service providers that can be considered future aviation standards and guidelines.

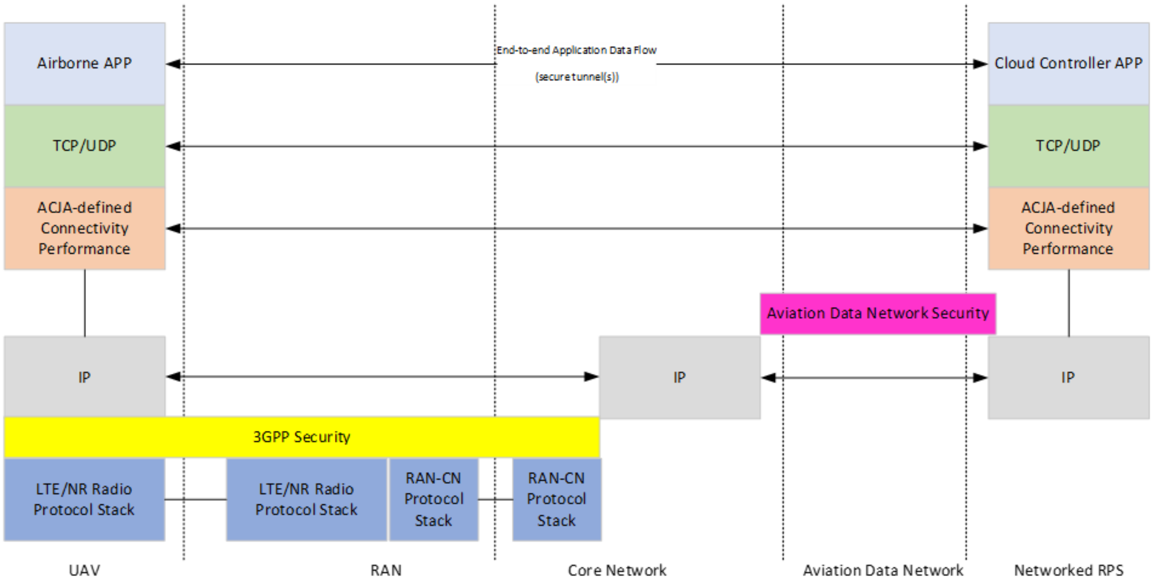

Airborne APP
End-to-end Application Data Flow
(secure tunnel(s))
Cloud Controller APP
TCP/UDP
TCP/UDP
ACJA-defined Connectivity Performance
ACJA-defined Connectivity Performance
Aviation Data Network Security
IP
IP
IP
3GPP Security
LTE/NR Radio Protocol Stack
LTE/NR Radio Protocol Stack
RAN-CN Protocol Stack
RAN-CN Protocol Stack
UAV
RAN
Core Network
Aviation Data Network
Networked RPS

Figure 4. OSI Model Representation for single Air-Ground RF link scenarios.

6. Security Considerations

6.1. End-to-End Security Considerations

This section focuses on overall security considerations for the UAS cellular ecosystem.

It is assumed that cellular security is applied as currently standardized; however, it is highly recommended that, in scenarios where radio link security is optional, it is activated for UAVs to provide confidentiality and integrity.

6.2.UAV Authentication and Authorization by MNO via USS

3GPP has defined in Release 17 (3GPP TS 23.256) a set of procedures for USS UAV authentication and authorization (UUAA) to enable an external Application Function (AF) which has an agreement with the MNO to authenticate and authorize a UAV for access to connectivity services via a 3GPP system. In particular, it is expected that the AF may be the USS serving the UAV, or the C2CSP serving the UAV. It is expected that agreements for interfacing between the MNO and the AF will be established to ensure security, and ADX may be leveraged for such communications.

Specifically, the following assumptions apply to UUAA:

- The UAV, being a 3GPP UE, is subject to traditional 3GPP authentication mechanisms to access the 3GPP system. This procedure is based on credentials related to the 3GPP subscription and independent of the fact that the 3GPP UE is a UAV and may have an Aerial UE subscription in the 3GPP system.
- Access to any features dedicated to UAVs is possible only for 3GPP UEs that have a UE Aerial subscription; this means that a UAV that is not associated to an Aerial UE subscription will not be allowed to access any 3GPP aerial features (e.g., Rel. 15 LTE RAN features) and will not be allowed to perform a UUAA procedure. Even if access to the PDU session supporting traffic to the USS is not explicitly authenticated and authorized,

the UAV without the Aerial UE subscription will never be authorized for C2 connectivity with a Wireless or Cloud RPS

- The UAV may be configured to use either a single PDU session/PDN connection for both traffic to/from USS and traffic to/from a Wireless RPS or Cloud RPS. Therefore, either a single Data Network or two Data Networks are supported, to enable flexibility in deployments (e.g., depending on regional policies or regulations)
- It is assumed that via mechanisms at application layer, the UAV is issued with a CAA-Level UAV ID by the USS or UTM, which is not a 3GPP identity and is not related to the 3GPP identifiers tied to the UE subscription. Examples of CAA-Level UAV ID are dynamic Session ID related to a specific flight, or other UAV identifiers that each CAA may decide to deploy.
- It is assumed that a CAA-Level UAV ID may be associated with security credentials, not defined in 3GPP specifications, that enable the UAV to identify and be authenticated by the AF to verify the validity of the CAA-Level UAV ID
- It is assumed that when Broadcast Remote ID or Networked Remote ID are used, the CAA-Level UAV ID may be used as the UAV identifier provided in the BRID or NRID messages by the UAV.

The mechanisms defined are as follow:

- UAV authentication and authorization
    - In the 5GS, a 3GPP UE configured to act as a UAV and provisioned with the right information (including at least the CAA-Level UAV ID), upon registering to the 3GPP system will provide the CAA-Level UAV ID to indicate its intention to operate as a UAV.
    - In a 4G system, the UAV does not present the CAA-Level UAV ID in the registration to the 4G system, since in 4G only UUAA-SM is supported (see next steps).
    - The UUAA procedure may take place upon registration to the 5G System (UUAA-MM procedure) or upon establishment of the user plane connectivity in either 5G System or 4G System (UUAA-SM).
    - For both UUAA-MM and UUAA-SM:

        - The UAV, based on configuration information provided to the UAV by the UAS operator and the AF, may either explicitly provide the address (e.g., FQDN) of the serving AF to enable the mobile network to identify the serving AF, or the serving AF may be derived by the 3GPP network based on the CAA-Level UAV ID.
        - The UAV may additionally provide an Aviation Payload that is transparent to the 3GPP system, containing information based on configuration by the UAS operator and/or the USS (e.g., authentication data or other application-level data).
    - UUAA-MM is optional and performed at 5GS registration based on operator's policy. If required by the operator, UUAA-MM is performed if the UAV has an aerial UE subscription in the Access and Mobility Subscription Data and provides the CAA-Level UAV ID in the Registration Request message.
        - In this case, it is assumed that connectivity to the Data Network for traffic to/from the USS does not require a dedicated UAV authentication and authorization procedure. The UAV can establish connectivity to the AND for traffic to/from the USS without any further UUAA procedures.
    - If UUAA-MM is not performed, the UAV shall be authenticated by UUAA-SM during the user plane connectivity establishment (PDU session or PDN connection) for UAS service.
        - This implies that connectivity to the Data Network for traffic to/from the USS does require a UUAA procedure.
        - Whether the request to establish user plane connectivity (PDN connection or PDU session) needs to trigger the UUAA-SM procedure depends on configuration in the network that identifies the requested data network and associated network slice as being subject to UUAA-SM.

    - In particular, if the data network is used only for connectivity to/from the USS, UUAA-SM is performed only when UUAA-MM was not performed.
    - If the data network is used for C2 connectivity, the establishment of the connectivity is subject to performing a UUAA-SM procedure for C2 authorization (see below).
  - Failure of UUAA-MM procedure implies that 3GPP network may, based on local network policy, either:
    - de-register the UAV from the network with an appropriate cause value that informs the UAV the reason for de-registration is failure of the UUAA procedure with the USS, thus enabling the UAV to reconnect as a regular UE to e.g., establish user plane connectivity for reconfiguration and exchange of application-level traffic to enable the UAV to obtain appropriate configuration information (e.g., update CAA-Level UAV ID or related credentials); or
    - keep the UAV registered with a failure UUAA result which does not the allow the UAV to access any UAS services. Such UE would need to use connectivity via a generic data network (e.g., Internet) establish user plane connectivity for reconfiguration and exchange of application-level traffic to enable the UAV to obtain appropriate configuration information (e.g., update CAA-Level UAV ID or related credentials).
    - once the UAV determines that the conditions for failure of the UUAA procedure have been solved (e.g., obtains new CAA-Level UAV ID or credentials), the UAV may attempt to re-register to the 3GPP system with the updated information.
  - Failure of UUAA-SM procedure implies that the corresponding user plane connectivity establishment is rejected with an indication to the UAV of the reason for rejection.

    - The USS can trigger re-authentication and/or re-authorization of the UAV at any time after initial successful UUAA procedure.
        - In case of UUAA-SM re-authentication and/or re-authorization after an initial successful UUAA-SM procedure, the USS indicates to the 3GPP system whether to release the related user plane connectivity or to maintain (e.g., to avoid interruption of C2 connectivity with the Wireless or Cloud RPS, or to maintain connectivity between the UAV and the USS).
- C2 pairing authorization/modification/re-authorization between UAV and RPS:
    - This applies mostly to Wireless RPS and Cloud RPS.
    - Authorization for C2 by the USS is required when a UAV establishes a user plane connection via the MNO for C2 operations, i.e., to transport C2 signaling with an RPS. A UAV shall be authorized by the USS to use a PDU Session/PDN connection for C2. Authorization for C2 includes authorization for pairing between the UAV and with an RPS before the UAV and the UAV-C can exchange C2 communication. In current specifications, it is assuming that one UAV can be paired with only one RPS at any given time, but an RPS may be paired with one or more UAVs at the same time.
    - In current specifications (release 17) it is assumed that the AF involved in the UUAA procedure is also involved in C2 authorization, and authorization by separate AFs (e.g., UUAA by USS and C2 authorization by a C2CSP different from the USS) is not supported.
    - The authorization enables the user plane data traffic between the UAV and the RPS for C2 and includes authorization of packet filters to enable the traffic, and the provision/selection of traffic policies (e.g., for QoS) in the 3GPP system.
    - In case of single user plane connectivity (i.e. single data network for traffic to/from USS and for C2 connectivity to Wireless or Cloud RPS) C2 authorization may be performed during the UUAA

    procedure (if UUAA is carried out at user plane establishment, i.e. PDU session/PDN connection establishment) or during user plane modification procedures when the UAV requires to use an existing connection to exchange C2 communication related messages (e.g., a user plane connection was established to communicate with the USS or C2CSP, and the UAV now needs to establish a pairing with the RPS and use the user plane connection for C2 transport). Failure of C2 authorization is indicate to the MNO and the UAV, and the existing PDU session is maintained without enabling connectivity to an RPS.

  - In case of separate user plane connectivity (i.e., two separate data networks for traffic to/from USS and for C2 connectivity to Wireless or Cloud RPS), C2 authorization is performed at the establishment of the PDU session. Failure of C2 authorization in this case implies that the user plane connection for C2 is not established and the UAV is provided an explicit indication of the failure cause.
  - RPS) When the C2 authorization is revoked by the USS,
    - In case of separate user plane connections for traffic to/from USS and for C2 with the Wireless or Cloud RPS, the network releases the user plane connectivity for C2 with an appropriate cause to inform the UAV of the event.
    - In case of common user plane connections for traffic to/from USS and for C2 with the Wireless or Cloud RPS, the network disables C2 communication with the Wireless RPS or Cloud RPS by removing the traffic filters for C2 communications and the QoS flow for C2 communication and informs the UAV of the event.
- Flight plan authorization: the UAV may include in the signaling for C2 Authorization information about a flight plan authorization request, which the mobile network transfers transparently to the AF for verification and approval. The AF would then return an authorization result transparently to the mobile network, without impacting the UE connectivity. Flight plan

authorization is an optional feature that is not required to enable the establish of user plane connectivity for C2 or UAV-RPS pairing.

At any time after an initial pairing authorization between a UAV and an RPS, the AF (e.g., USS or C2CSP) may replace the RPS by triggering a UAV re-authorization and indicating to the network that the pairing with the existing RPS needs to be removed and replaced with the pairing with a new RPS.

The UUAA procedure does not apply to a Wireless RPS that is seen by the 3GPP system as a regular 3GPP UE without any UAS-related features.

6.3.Dedicated Security Tunnels Model

Most current standards within Europe, UK, Canada, U.S., and others require the operator to encrypt its data between the Remote Pilot Control Station (RPS) and the Unmanned Aerial Vehicle (UA).

In particular, RTCA DO-377a, based upon level of risk, is currently the most reference aviation performance standard for operations and security to include where the basic security controls should be applied in the end-to-end chain.

- End-to-End encryption between the RPS and UA (responsibility of the UAS operator).
- RF Link Protection between the UA and the ground termination point of the MNO (UA manufacturer, operator, and MNO leverage 3GPP mechanisms)
- Link Protection between the Operator and the MNO external ground Interface for services (MNO and Operators must develop the best solution to meet the service delivery needs.)

An important consideration when considering securing the UAS-to-RPS traffic is how to allow both the operator and the MNO to properly manage and prioritize the data flows. RPS data to and from the UA contains several data attributes and elements that comprise the C2 link as a whole, and that require to be protected and effectively managed in transit. Data elements that fall outside the C2 command and control structure is often times important to the operator to manage flight operations and business operations, and though these data flows are not regulated, to ensure efficient management of data flows, isolation, protection and management of these data flows is still an important part of operation. Also, the nature of IP voice data flows does not handle network delays and retransmissions the same way as normal IP data. To effectively manage voice and commonly known issues like jitter and delays, it's a common practice to Prioritize voice traffic to ensure the voice relay traffic is not impacted by other network conditions. To provide the means for this capability, mechanisms that enable prioritization and/or traffic differentiation between different types of traffic (e.g., C2 with regard to voice) are required. E.g., operators consider isolating IP Voice Relay data flows within its own unique end-to-end protected data flow if it is determined that MNO networks cannot differentiate such traffic from non-voice traffic. This will allow all parties involved in the delivery of service to apply the proper controls and prioritization of the data flows based upon the traffic type.

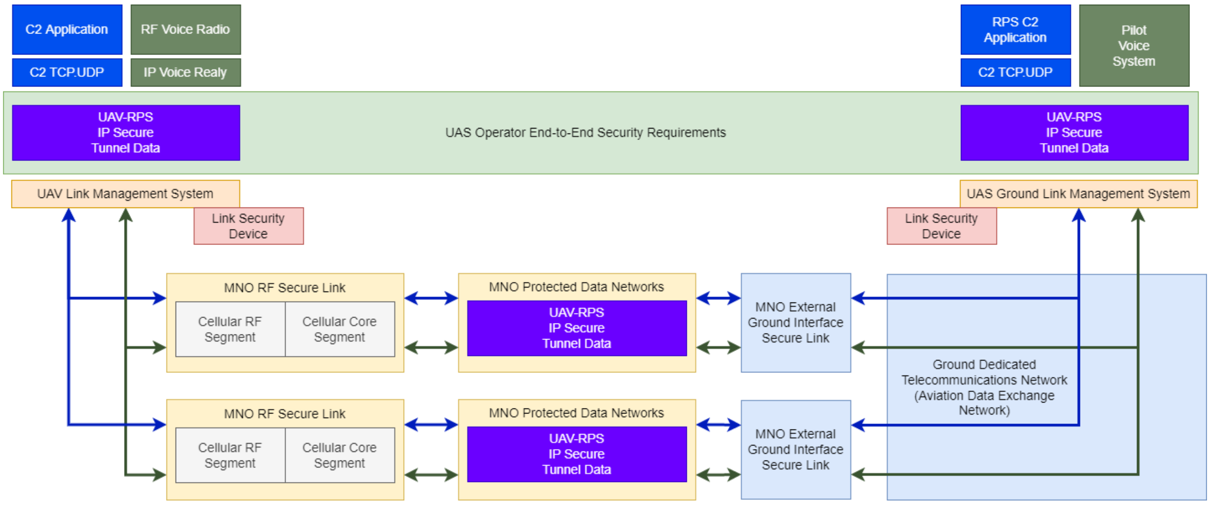

C2 Application
RF Voice Radio
C2 TCP.UDP
IP Voice Realy
RPS C2 Application
Pilot Voice System
C2 TCP.UDP
UAV-RPS IP Secure Tunnel Data
UAS Operator End-to-End Security Requirements
UAV-RPS IP Secure Tunnel Data
UAV Link Management System
Link Security Device
UAS Ground Link Management System
Link Security Device
MNO RF Secure Link
Cellular RF Segment
Cellular Core Segment
MNO Protected Data Networks
UAV-RPS IP Secure Tunnel Data
MNO External Ground Interface Secure Link
Ground Dedicated Telecommunications Network (Aviation Data Exchange Network)
MNO RF Secure Link
Cellular RF Segment
Cellular Core Segment
MNO Protected Data Networks
UAV-RPS IP Secure Tunnel Data
MNO External Ground Interface Secure Link

Figure 5. Overall representation of secure infrastructure for single tunnel scenario.

The most common approach would use a single tunnel for both data and voice communications and employs 3GPP-defined mechanisms to ensure proper performance for both streams by leveraging packet inspection and traffic filtering at the edge of the MNO network, as it is currently done for other applications.

Otherwise, if the UAS operator encrypts the data in such a way that current packet inspections solutions at the edge of an MNO network do not allow to distinguish different types of traffic, that makes it difficult for the communications services providers to perform differentiated treatment of traffic belonging to different services (e.g., data, voice, or other messaging).

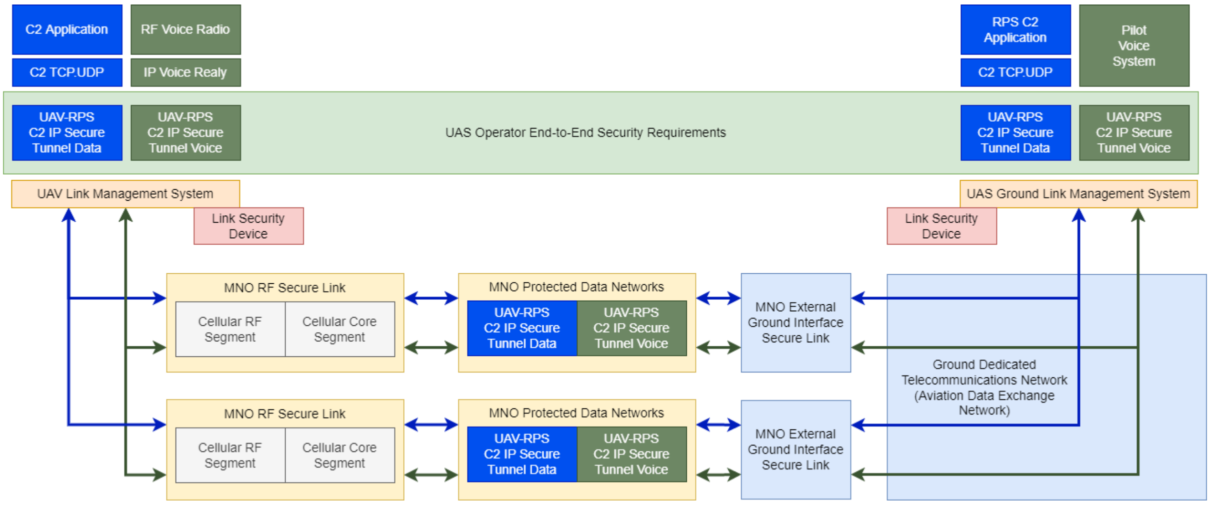

C2 Application
RF Voice Radio
C2 TCP.UDP
IP Voice Realy
RPS C2 Application
Pilot Voice System
C2 TCP.UDP
UAV-RPS C2 IP Secure Tunnel Data
UAV-RPS C2 IP Secure Tunnel Voice
UAS Operator End-to-End Security Requirements
UAV-RPS C2 IP Secure Tunnel Data
UAV-RPS C2 IP Secure Tunnel Voice
UAV Link Management System
Link Security Device
UAS Ground Link Management System
Link Security Device
MNO RF Secure Link
Cellular RF Segment
Cellular Core Segment
MNO Protected Data Networks
UAV-RPS C2 IP Secure Tunnel Data
UAV-RPS C2 IP Secure Tunnel Voice
MNO External Ground Interface Secure Link
Ground Dedicated Telecommunications Network (Aviation Data Exchange Network)
MNO RF Secure Link
Cellular RF Segment
Cellular Core Segment
MNO Protected Data Networks
UAV-RPS C2 IP Secure Tunnel Data
UAV-RPS C2 IP Secure Tunnel Voice
MNO External Ground Interface Secure Link

Figure 6. Overall representation of secure infrastructure for multiple tunnels scenario.

In this architecture, the UAS operator assumes that the MNOs enable:

(i) secure the traffic E2E to support the UAS operator security requirements, and

(ii) ensure the underlying transport network can distinguish the different types of traffic even if encrypted to perform traffic differentiation and meet the operational and performance needs of the UAS operator.

One way to achieve this, for scenarios where the E2E traffic encryption does not enable packet header inspection for traffic differentiation, is for the UAS operator to create and isolate its data flows between the RPS and UAV in a way that will allow the data to be properly managed and prioritized in transit. The following E2E secure tunnel (e.g., VPN) structure a possible solution for UAS operators to implement between the RPS and the UA:

- C2 Voice Relay IP data link (for scenarios where voice relay in the UAS is supported).
- C2 Data link.
- UA Payload Data Stream.

6.4. Lawful Intercept Considerations

Lawful Interception (LI) is currently defined for 3GPP networks as “Laws of **individual nations** and regional institutions, and sometimes licensing and operating conditions, define a need to **intercept targeted** communications traffic and related information in communication systems. Lawful Interception applies in accordance with applicable national or regional laws and technical **regulations**.” LI takes place in the MNO core network and is triggered by external authorized entities via standardized interfaces. The following figure highlights how LI would apply to UAV traffic.

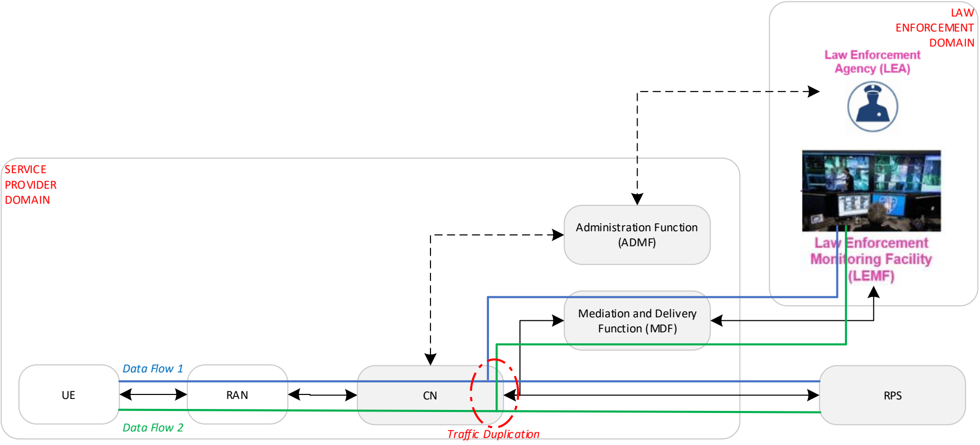

LAW ENFORCEMENT DOMAIN
Law Enforcement Agency (LEA)
Law Enforcement Monitoring Facility (LEMF)
SERVICE PROVIDER DOMAIN
Administration Function (ADMF)
Mediation and Delivery Function (MDF)
Data Flow 1
Data Flow 2
UE
RAN
CN
RPS
Traffic Duplication

Figure 7. Lawful Interception Architecture.

The parts of LI system are Administration Function (ADMF) which enables functions like provisioning and de-provisioning the Point(s) Of Interceptions (POIs) and the Mediation and Delivery Function (MDF). LI detects, captures, and delivers Interception products to Law Enforcement Monitoring Facility (LEMF) on Law Enforcement Agency (LEA). The LI system and CSP maintains user identification like UEs registered and targeted for LI. Aviation regulations may need to set requirements to LI use, functions, data retention, user identification related POIs within aviation data network controlling and control of airborne aircraft.

Requirements of LI can be found in TS 33.126 since Release 15, architecture and functions in TS 33.127 and delivery details from TS 33.128. It has to be noted that explicit LI regulations and standards have not yet been defined for UAVs.

Lawful interceptions impact the whole systems regarding both technical and legal aspects and may present significant challenges. One of the first issue identified at the time of writing was a contradiction between the end-to-end security requirement and an ability to intercept the control by an MNO. Detailed study into Lawful Interception issues was considered out of the Work Task scope.

7. C2CSP Model for UAV and RPS Connectivity and Addressing

With BVLOS scenarios in which C2 and related traffic is transported over cellular connectivity between a UAV and Wireless or Network RPS, it is expected that the pairing between a UAV and an RPS may be dynamic (i.e., at different times, an UAV may be controlled by different RPSs). More complex models are being considered where different RPSes may at different times during a flight mission have control of the UAV. It is also assumed that for some scenarios, a single RPS may control multiple UAVs.

In order to enable the dynamic pairing between a UAVs and RPSs, discovery and identification of UAVs and RPSs must be defined. It is assumed that an application-layer architectural solution (i.e., above the networking connectivity provided by MNOs and ADX Network) is present that enables:

- Assigning C2CSP Logical Name(s) to a UAV, which would be associated dynamically to the IP address assigned to the UAV for the data connection used for C2 connectivity. Note that this C2CSP Logical Name is different from the CAA-Level UAV ID defined by 3GPP networks in TS 23.256. the C2CSP Logical Name is assigned to the UAV in collaboration between the UAS Operator and the C2CSP.
- A UAV to “register” with an application server (e.g., the C2CSP) by providing the C2CSP Logical Name to the server to associate it with the UAV IP address. Also, the ability for the C2CSP or UAS Operator to update the C2CSP Logical Name.
- An RPS, also registered with the C2CSP, to address an UAV via the C2CSP using the C2CSP Logical Name.

It is foreseen that for flexibility and scalability, a C2CSP Logical Name may also be allocated to Wireless and Cloud RPSs.

It is expected that such architectural solution would also enable the C2CSP to:

- Provide QoS requirements for the establishment of QoS for C2 connectivity (and possibly other components of the traffic such as voice for voice relay, navigation-related video, and payload video).
- Monitor QoS provisioning to the UAV and Wireless RPS for the connectivity of interest to the C2CSP.
- Monitor other connectivity-related events for the UAV and Wireless RPS (e.g., loss of connectivity).

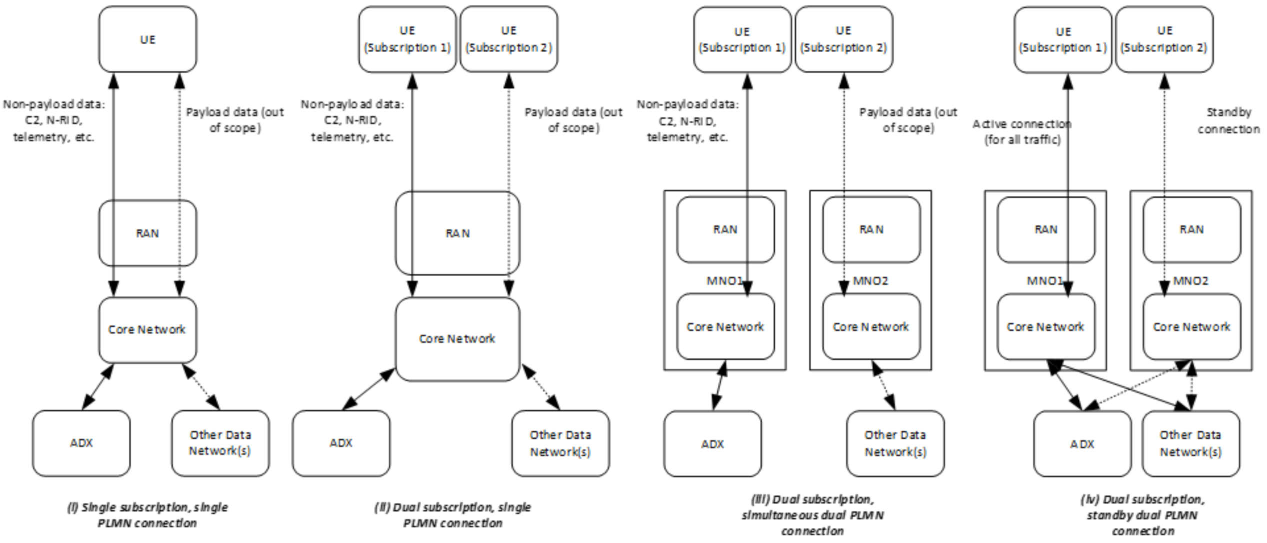
This type of C2CSP application layer infrastructure may be proprietary and specific to a UAS Operator and/or a C2CSP, however adopting a scalable and interoperable solution applicable to the industry at large would enable simplified interworking between UAVs of different vendors, different UAS operators, and different C2CSPs, and would enable various entities (e.g., C2 brokers, MNOs, etc.) to act as UAV C2CSPs. Moreover, adopting a standardized solution for C2CSP Logical Name(s) and the C2CSP application layer infrastructure would also enable global scalability and interoperability, and the ability for the C2CSP application layer infrastructure to interface with existing mechanisms provided by MNO networks to e.g., control and monitor the QoS.

8. Components

In order in address all entities represented on the full diagram (Figure 3), we divide into several subsections called domains to describe them separately:

- Ground Connectivity (Between Operator and MNO, USS/USSP, C2CSP, regulator, other service provider).
- Aircraft to MNO RF connectivity (Cellular in this version of the document).
- Unmanned Aircraft (UA) Airborne Elements.
- Remote Pilot Station (RPS).
- MNO Ground Core Network.
- MNO Ground External Interface.
- Aviation Data Segment (this may be the same as the Ground Connectivity).
- UTM Domain or USS Element.
- Broadcast Elements.
- C2CSP.

8.1. RF Radio Connectivity



(I) Single subscription, single PLMN connection

(II) Dual subscription, single PLMN connection

(III) Dual subscription, simultaneous dual PLMN connection

(Iv) Dual subscription, standby dual PLMN connection

Figure 8. RF Radio Connectivity Elements.

RF Connectivity (cellular networks in the case of this version of the document) involves two primary components, User Equipment (as an integral part of Aerial Vehicle) and Mobile Network Operator infrastructure (UE to MNO Radio Access Network, MNO internal Core Network, and external Data Network for data distribution).

While ACJA considerations and specifications may be applicable to private network, a primary ACJA assumption is that aerial connectivity may be provide to aviation users based on the standard cellular infrastructure provided by commercial telecommunications service providers. Airborne units connect to base stations of the RAN via 3GPP-defined 4G LTE or 5G NR protocol potentially simultaneously with a wide range of other customers (from general smartphones to IoT devices to ground unmanned vehicles).

However, to access aerial services with proper characteristics associated with each data flow type, airborne UE must connect to a dedicated APN/DNN (e.g., “UAS” APN) that are provided by the MNO. Additionally in order to ensure effective performance of the information exchange, how the MNO network can perform differentiated treatment of the different data flows based on traffic type (C2, voice) the UE and MNO networks should be defined. At the same time, the UE may connect to a regular (e.g., “internet.operator.tld”) APN in order to transmit non-flight-safety -critical information or “payload” information. An aerial vehicle can also incorporate several UE units (ref. Airborne Elements).

The airborne UE may actually be simultaneously connected to multiple MNO networks (i.e., different PLMNs) for reliability and redundancy of the communication link supporting C2 and other services. This can be achieved in a variety of manner which depend on deployments and regional regulations:

- different traffic types being routed over different PLMNs (scenario iii): in this case, it is expected that the UE is configured (e.g., by the UAS operator or the C2CSP) to transfer traffic related to UAV operations (e.g., C2, voice relay, navigational video, etc.) over one PLMN, and other type of traffic (e.g., payload video) over the other PLMN. This is most commonly achieved by using dual subscriptions, but scenarios are possible using a single subscription depending on the 3GPP features being utilized, and thus both scenarios must be contemplated.

- the UE being active at any single time with a single PLMN (i.e., all traffic types are transported via the active PLMN) but simultaneously registered to the other PLMN and thus capable of switching instantaneously to the other PLMN (scenario iv). In this case, it is expected that the UE is configured (e.g., by the UAS operator or the C2CSP) to transfer all types of traffic over one PLMN or switched to the other PLMN under specific conditions (connection-quality related, location related, etc.). This is most commonly achieved by using dual subscriptions, but scenarios are possible using a single subscription depending on the 3GPP features being utilized, and thus both scenarios must be contemplated.

8.1.1. Standardization

Annex II to this document provides an extensive description of current 3GPP UE standardization.

8.1.2. Security Considerations

Security must be a constant consideration in all layers of information exchange.

The UAS operator, the C2CSP, or both are responsible for the end-to-end encryption of the data exchange between the UA and RPS.

The MNO is responsible for protecting the airborne RF links.

Protection of the ground interface between the MNO and the UAS operator is achieved via security of the SLA provided by the Aviation Data Network.

8.2. Airborne Elements

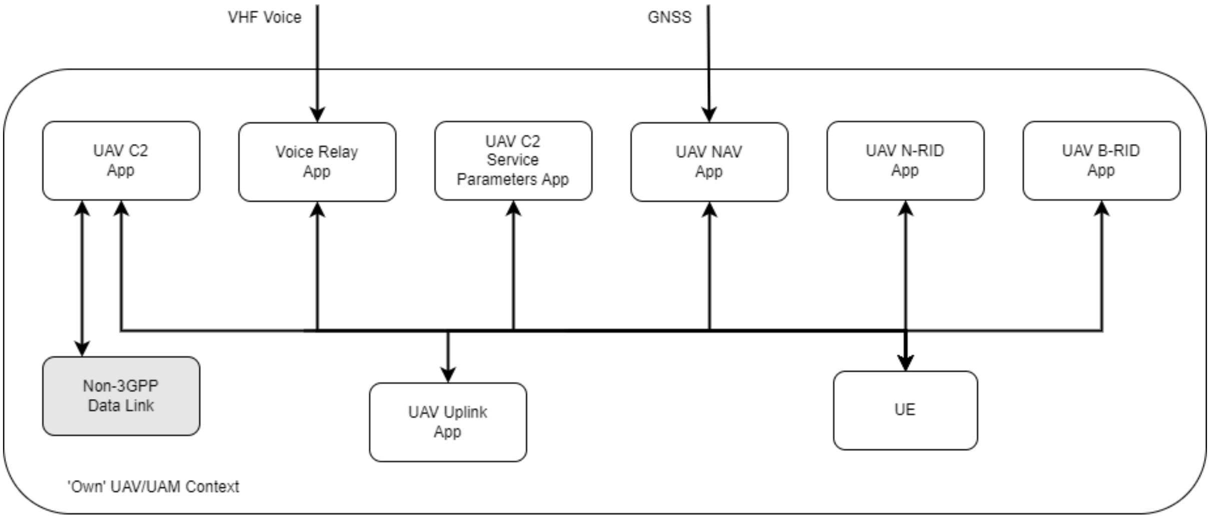


Figure 9. Airborne Elements.

Airborne component includes multiple software and hardware units and the specific functions required will depend upon the type of operating space the aircraft will be flying in. While ACJA analysis are agnostic and consider these entities on a logical level, the most straightforward aircraft architecture includes two hardware components:

- The Aircraft main computer runs a set of components we refer here to as 'applications' that will interface and manage data from the aircraft voice, command and control systems and other payload data:
    - UAV C2 Voice relay application for those aircraft that will be operating in an area whereby the aircraft will be required to communicate with the Air Traffic Control systems. The aircraft will have a compatible radio to exchange voice commands and information within the geographical airspace of the aircraft between the remote pilot and the local ATC provider.
    - UAV C2 application maintains an application-level connection with an RPS and employs connectivity for direct flight control or trajectory management.
    - UAV C2 Service Parameters application is indented to transmit auxiliary information to an RPS and Supplemental Data Service

    Provider (see. below) to support connectivity quality monitoring and performance assessment.
  - UAV Uplink application is a generic component responsible for reception of any information coming from ground component (other than RPS), for example, geofencing information coming from a corresponding UTM service.
  - UAV NAV application is a navigation (primarily, GNSS) portion of airborne software. For navigation, potential ACJA scope includes augmentation of GNSS navigation using network-provided UE location (Mobile Network Positioning).
  - UAV N-RID — network remote identification application (e.g., as per ASTM 3411 and upcoming EUROCAE standards), transmits identification and position information via packet network (basically, via TCP/IP) to a corresponding UTM service.
  - UAV B-RID — broadcast remote identification application. ACJA scope includes cellular implementation of broadcast remote ID in manner similar to currently defined capability based on Wi-Fi Aware/Bluetooth Low Energy.
- The Air-Ground RF modem (cellular in the scope of this paper) in the UE with corresponding antennas and feeders.

Both chipsets may integrate in a single or dual modem or System-on-a-Chip. Hardware components host software: we assume UE to run a standard software stack, and main vehicle's computer runs a set of components we refer here to as 'applications':

- For the sake on completeness, we also include a C2 application based on non-3GPP connectivity. Such a configuration may be employed, for example, when Remote ID is cellular based but C2 is not. Alternatively, non-3GPP (e.g., SATCOM) connectivity may serve for redundancy or support different operational conditions.

8.2.1. Standardization

Several published standards and standard development activities are relevant for the Airborne Elements.

Generic (i.e., not directly considering 3GPP-defined technologies) applicable standards and drafts include:

- For Remote Identification, both, Network RID and Broadcast (or Direct) RID, ASTM F3411-22 (developed jointly with ASD-STAN) may serve as a basis. However, B-RID portion of the standard directly uses Bluetooth/Wi-Fi technologies. ACJA envisions that the same approach may be based on 3GPP-define device-to-device communication mechanisms.
- EUROCAE have developed an unpublished ED-282 e-Identification MOPS, now put on hold. The future MOPS may potentially define some UAS-USS interoperability requirements, which are absent from ASTM F3411-22. As of the end of 2022, the proposed way forward is to develop an open-source reference implementation.
- For Command and Control, a general reference on the operational level is RTCA DO-377A MASPS (revision B is under development). This standard also applies to all other components involved in provision of C2 connectivity services.
- There are also the ICAO C2 Standards and Recommended Practices (Annex 10 Volume VI), which provide general guidance for RPAS C2 capability. Formally the SARPS are applicable to international RPAS flights.
- Terrestrial GHz C2 link airborne equipment MOPS, RTCA DO-362, while applies to another technology, can service as a reasonable template to cellular-related C2 MOPS.

Air-Ground RF-specific activities outside ACJA include a EUROCAE WG-105 SG-2 cellular activity joint with a subgroup of RTCA SC-228 (namely, SG-2.2). The joint activity is tasked to develop a MOPS for Cellular Communications for UAS. The scope includes both 4G LTE and 5G for C2 services only. The Open Consultation target is set at the end of 2022.

8.3. Remote Pilot Station

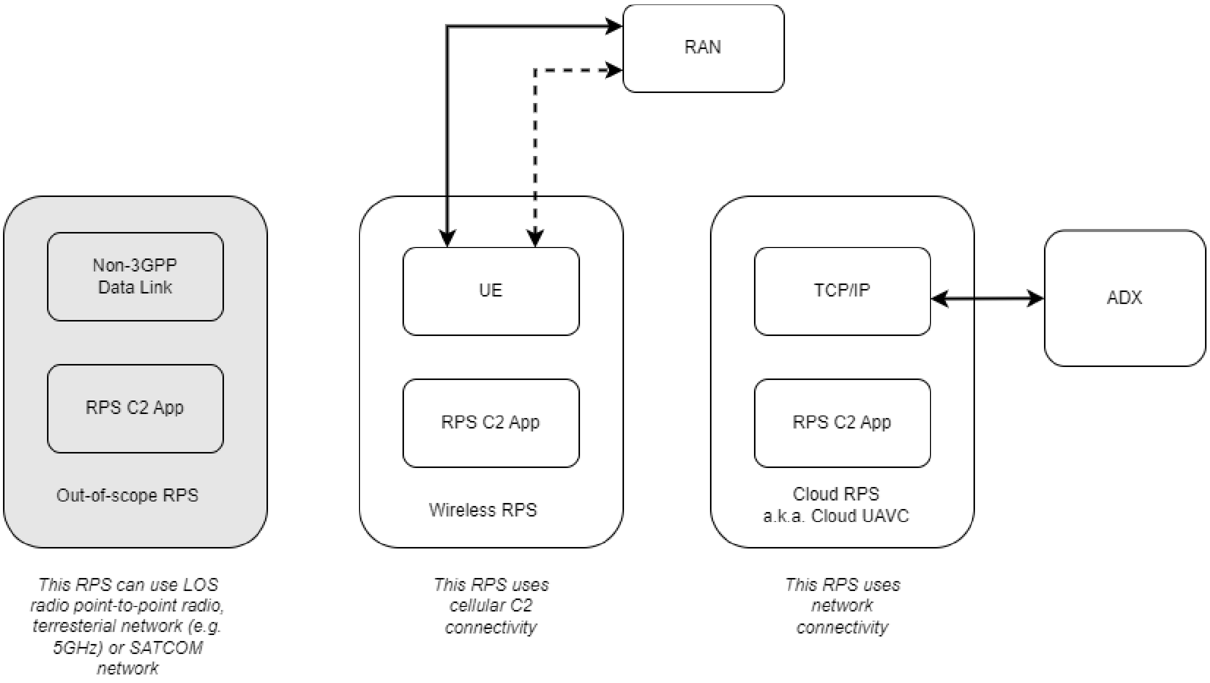

RAN
UE
RPS C2 App
Wireless RPS
Non-3GPP Data Link
RPS C2 App
Out-of-scope RPS
TCP/IP
RPS C2 App
Cloud RPS a.k.a. Cloud UAVC
ADX
This RPS can use LOS radio point-to-point radio, terresterial network (e.g. 5GHz) or SATCOM network
This RPS uses cellular C2 connectivity
This RPS uses network connectivity

Figure 10. Remote Pilot Station Options.

Remote Pilot Station may include two components of interest: hardware User Equipment unit (running standard software stack) and command and control application (a software component responsible for communication with corresponding airborne C2 application).

It is expected that various degree of automation will need to be supported for the RPS and the UAV for near- and long-term scenarios, depending on the level of necessary involvement of the pilot in command (PIC) operating the aircraft, and including at least the following scenarios:

- Human-within-the-loop (HWTL): The PIC has direct control of the aircraft automation systems. As such the PIC needs real-time visual and telemetry data and provides command and control instructions to the aircraft. There is one PIC per aircraft.
- Human-over-the-loop (HOVTL): In this case, the PIC is only passively monitoring the system and receives updates and possible alarms. Under nominal operation, this scenario requires minimal resources from the

communication network. However, even in this case, in case of an emergency command and control channels and video stream will need to be established on-demand to provide information to the remote PIC. One PIC can monitor several aircraft simultaneously.

There are two major kinds of RPS stations regarding air-ground RF connectivity:

- Networked RPS (also called cloud RPS) uses TCP/IP protocol stack to connect to airborne component. C2 data packets follow a route via:
    - Ground based network for interconnectivity with the MNO or service provider via an ADX Network,
    - MNO/service provider core network,
    - MNO/service provider ground termination point for the RF interface (RAN).
- No special hardware is required for this option.
- Wireless RPS: the MNO manages the data flows from the Wireless RPS user to ensure they can provide the performance necessary based on the criticality of the data.
    - To manage C2 data flows and C2 voice relay data flows, a dedicated APN/DNN defining an ADX Network established to support the aviation community could be established to isolate these data flows from other users of the network for the specific purpose of connecting and managing airborne C2 voice relay data flows. This will ensure the MNO can prioritize the data flows to provide the service levels and performance required. Whether a single APN/DNN is used for C2 data flows and C2 voice relay data flows, or separate APN/DNN are defined, is left to deployment decisions.
    - To manage all other data flows, the same UE may connect to a common MNO defined APN/DNN, that is categorized and prioritized as other general traffic within the MNO network to receive a payload data transmitted by a vehicle, such as video stream.

8.3.1. Wireless RPS Consideration

A Wireless RPS comprises of a regular 3GPP UE with a subscription to an MNO (may be the same one serving the UAV, or a different one). The subscription for the WRPS needs not be a 3GPP Aerial subscription. The WRPS may at any time be served by a different MNO network than the UAV (e.g., in roaming scenarios).

The Wireless RPS obtains from the MNO a subscription that allows proper Quality of Service configured to connect to the aviation APN/DNN.

The Wireless RPS may be a mobile device (e.g., handheld RPS) or a fixed device (e.g., using carrier Wi-Fi solutions or fixed connectivity provided by an MNO), in either case they use the MNO connectivity.

8.3.1.1. Wireless RPS OSI Model Representation

Wireless RPS architecture differs from generic architecture, primary because there is no need to route any traffic externally to an MNO. A picture below reflects these differences. This kind of connectivity may potentially serve as a primary means to build a C2 link, however ACJA envisions that an RPS will more often use a mobile connection as a fallback to a network connection).

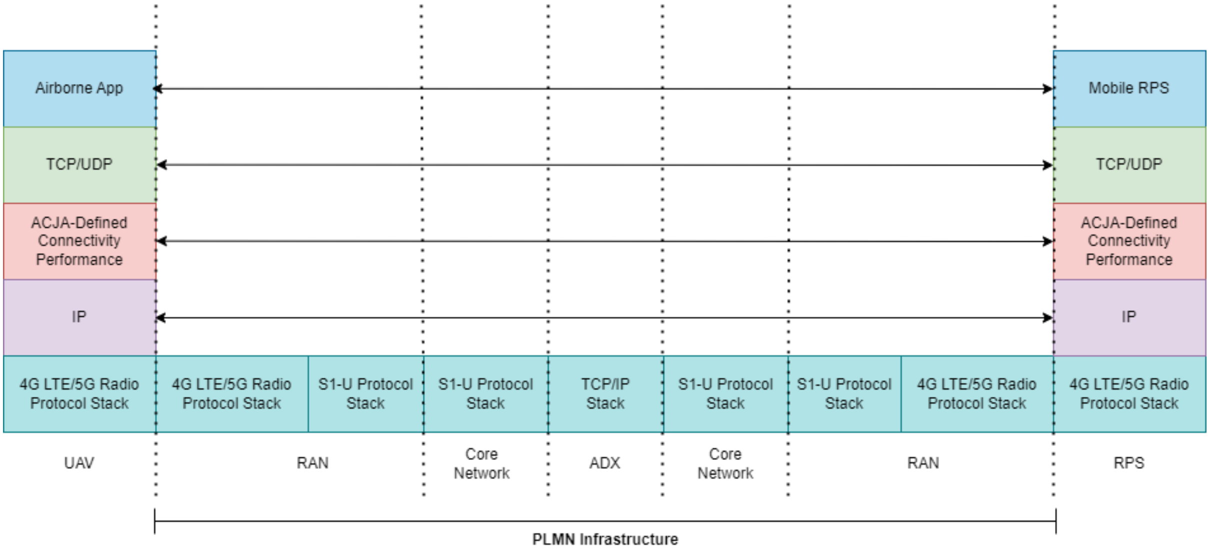

Airborne App
Mobile RPS
TCP/UDP
TCP/UDP
ACJA-Defined Connectivity Performance
ACJA-Defined Connectivity Performance
IP
IP
4G LTE/5G Radio Protocol Stack
4G LTE/5G Radio Protocol Stack
S1-U Protocol Stack
S1-U Protocol Stack
TCP/IP Stack
S1-U Protocol Stack
S1-U Protocol Stack
4G LTE/5G Radio Protocol Stack
4G LTE/5G Radio Protocol Stack
UAV
RAN
Core Network
ADX
Core Network
RAN
RPS
PLMN Infrastructure

Figure 11. Wireless RPS — Single PLMN Case

A connected UAV and a wireless RPS can also be serviced by different PLMNs as depicted on the Figure 12. An important point to note regarding this architecture is that two different networks shall be interconnected by the ADX Network.

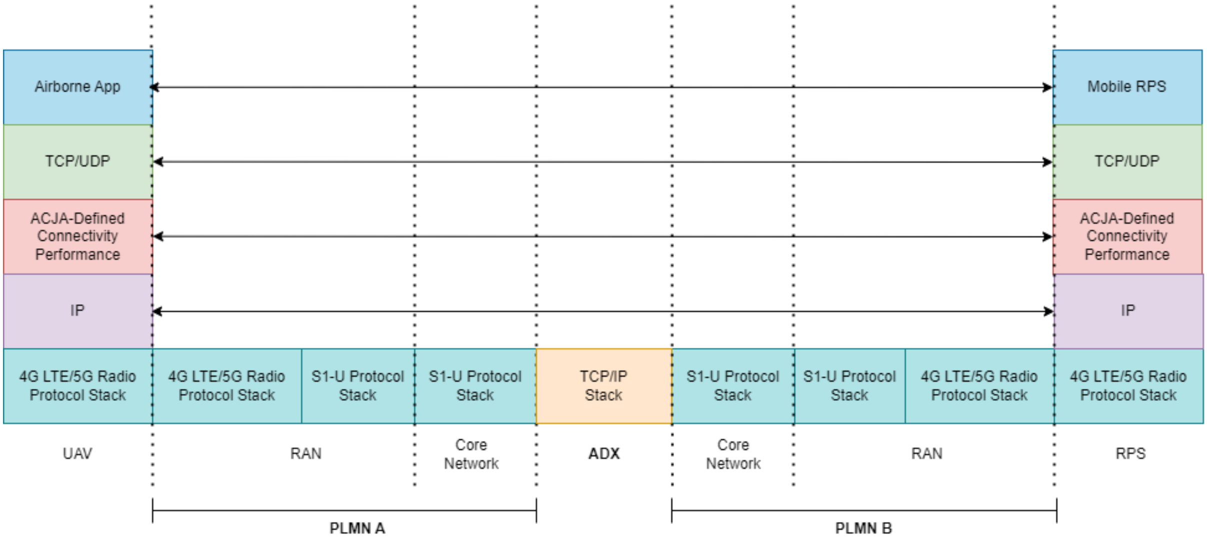

Airborne App
TCP/UDP
ACJA-Defined Connectivity Performance
IP
4G LTE/5G Radio Protocol Stack
Mobile RPS
TCP/UDP
ACJA-Defined Connectivity Performance
IP
4G LTE/5G Radio Protocol Stack
4G LTE/5G Radio Protocol Stack
S1-U Protocol Stack
S1-U Protocol Stack
TCP/IP Stack
S1-U Protocol Stack
S1-U Protocol Stack
4G LTE/5G Radio Protocol Stack
UAV
RAN
Core Network
ADX
Core Network
RAN
RPS
PLMN A
PLMN B

Figure 12. Wireless RPS — Different PLMN Case.

In this architecture, the ADX may be operated by the Interconnectivity Provider (backbone providers), which also shall be aware and comply to relevant performance requirements.

8.3.2.Cloud RPS Assumptions

The Cloud RPS is implemented as one or more applications running in the cloud to provide the functionality of RPS. The Cloud RPS is connected to the ADX network, and this can be achieved e.g., by the Cloud RPS being hosted by an MNO acting as a UAV C2CSP or being hosted by a non-MNO UAV C2CSP via interfaces subjected to the ADX SLA or being connected via an appropriate network guaranteeing the necessary ADX SLA to a UAV C2CSP.

8.4.MNO Core

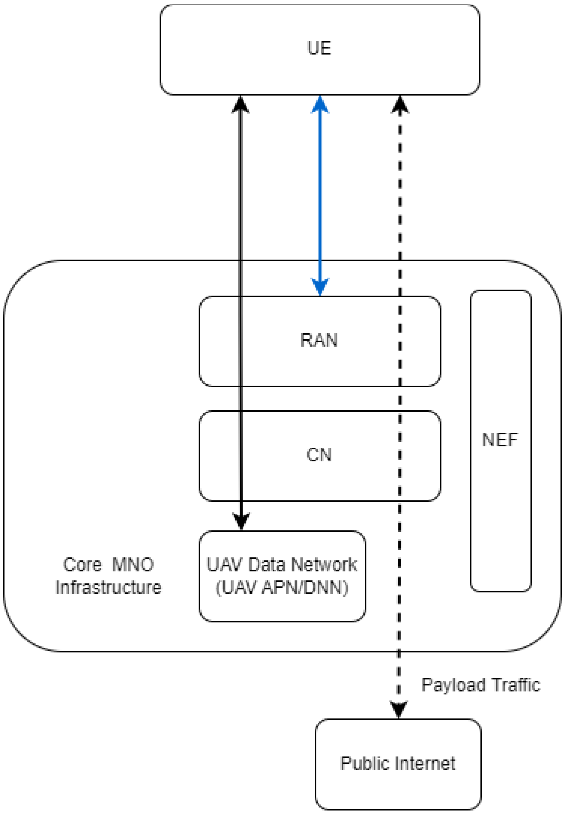


Figure 13. Mobile Network Operator Core.

The MNO network provides connectivity to the UAV. At a minimum, it provides connectivity for C2-related services, but may also provide connectivity for payload traffic. The MNO provides services to the airborne UE using a UE Aerial Subscription, which provides the UE with RAN aerial features and appropriate level of QoS associated with the UE data flows.

8.5. ADX Network Segment

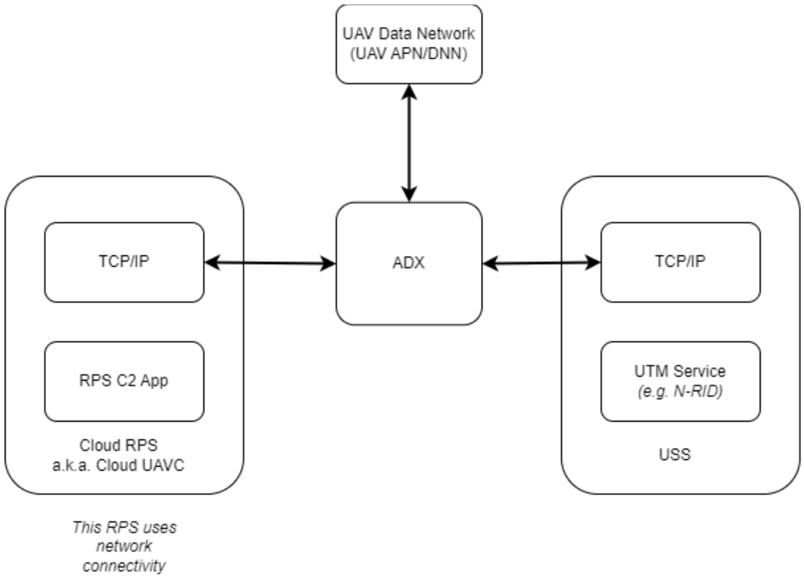


Figure 14. ADX Network Segment.

The UAS operator will have a ground interface that will provide interconnectivity to the MNO for RPS and the UE communications. It's expected that the operator will also have external connections to different services providers (USS/PSU, other) and regulator. As a special architectural case, MNO themselves may assume USS/PSU roles and host corresponding service on their infrastructure. Some UTM services that require reliable real-time communications, may also leverage operator's edge computing capabilities.

Establishing a common and standardized method for resilient and trusted ground interconnectivity between the operators and MNO's (and UAS/AAM service providers) is a considered a key consideration in the architectures developed. It's expected that organizations will implement cost effect transport solutions (dedicated circuits, Internet, other) to establish connectivity, however establishing a secure interface will be required agnostic to the types of connectivity implemented.

With a focus on just the ground-ground interfaces for information exchange (not be confused with RPS to aircraft UE end-to-end security requirement) a common method to establish secure connections between all stakeholders of the ecosystem is recommended.

The International Civil Aviation Organization (ICAO) is currently in the process of developing guidance that should be published in 2023 on common methods that can be used for establishing identity trust for the aviation community for ground-ground communications and information exchange agnostic to the types of technology used for physical connectivity (dedicated circuits, Internet).

This includes specific recommendations Data Network is assumed to be connected to the UAS Data Network (in the term of this document — ADX) with some backbone connection with proper quality-of-service, which also must be protected of an SLA.

There are two cases of a potential relationship between a unit and the Aviation Data Network:

- A unit resides on the Network Directly (e.g., N-RID hosted by a USS, with USS-internal network being the Aviation Data Network by itself).
- A unit connects to the ADX via a fixed gateways using a proper security mechanism (e.g., the mechanism used in well-established SATCOM C2 applications).

8.5.1. Command and Control Communications Service Provider

C2 Communication Service Provider, or C2CSP, is a specific entity in C2 concept.

An MNO can fulfill the function of a C2CSP, but a C2CSP may provide a level of abstraction above an MNO and may integrate service provisioning of various communication link providers. A C2CSP may combine the communication services of multiple operators.

C2CSP as a separate entity is especially useful for hybrid (e.g., cellular with SATCOM or non-cellular terrestrial with SATCOM) architecture. In this case the C2CSP provides a complex link with network switching capability under the SLA. A C2CSP may maintain subcontracts with underlying service Mobile Network Operators. The UAS operator is the agent of primary responsibility for safety of flight and operations and has ultimate responsibility to make the safety case with the regulators. C2CSP can own Aviation Data Network component and can serve as Supplemental Data Service Provider for any network availability and coverage information. Alternatively, C2CSP can leverage an ADX network operated by some external provider, likely under a subcontract.

8.5.2.Standardization

C2SCP and related networks are subject to requirements define by the ICAO C2 SARPS and the RTCA DO-377A MASPS (revision B is upcoming). EUROCAE WG-105 has launched a UAS C2 MASPS European Stakeholders Report activity.

No other on-going work is known as of the end of 2022.

8.6.USS Subsystem

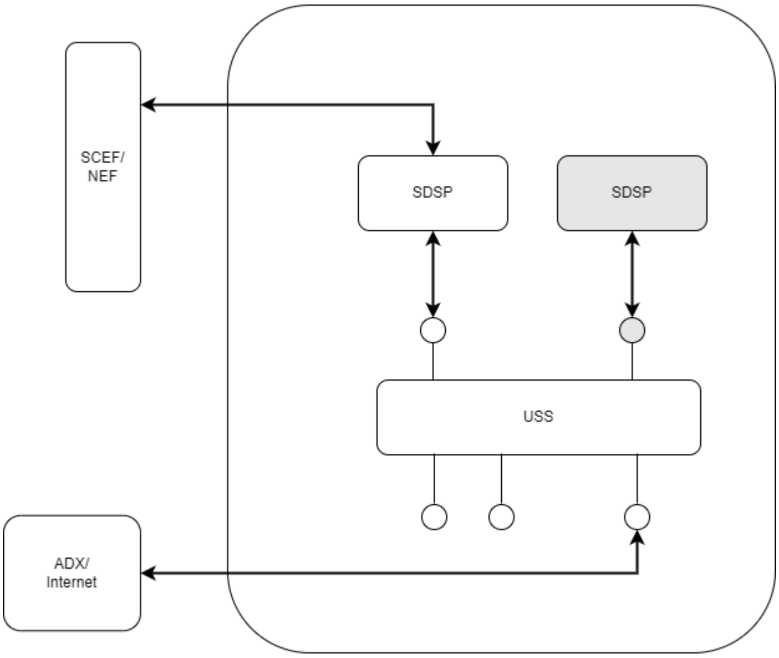


Figure 15. UTM Service Supplier Subsystem.

The UTM Services Supplier Subsystem here is viewed as a collection of ground-based services on a common information bus. UTM a broad topic mostly outside of the ACJA scope, however there is a number of actual and potential relationships between UTM service and cellular connectivity. These include:

- Downlinks: USS may use cellular connectivity to receive some information from a vehicle or from a remote pilot station (e.g., N-RID messages). C2CSP would also need to receive and monitor radio and auxiliary parameter in flight.
- Uplinks: USS may use cellular connectivity to distribute information directly to vehicles (or connected RP stations). Some more details are included in the section 9.2.
- Status and forecast: USS must a have a method acquire necessary information on actual and forecasted connectivity coverage and quality of service. Such a mechanism must be present at all times when any flight safety capability is present (such as cellular C2). Moreover, this applies to any connectivity method (e.g., SATCOM) employed by UAVs served.

A ‘status and forecast’ capability is assumed to take a form of Supplemental Data Service Provider.

8.6.1. Standardization

There are the following on-going standardization activities from this component:

- ASTM activity targets to specify multiple UTM elements, such as surveillance SDSP, weather information SDSP, USS-USS interoperability, and probably others.
- EUROCAE WG-105 SG-3 work on UTM OSED. It is expected that this activity will eventually define internal interrelationships between the services and their behavior.

At the time of writing, GUTMA Standards Harmonization Group targets to further analyze existing and required UTM standardization activities.

8.7. Broadcast Elements

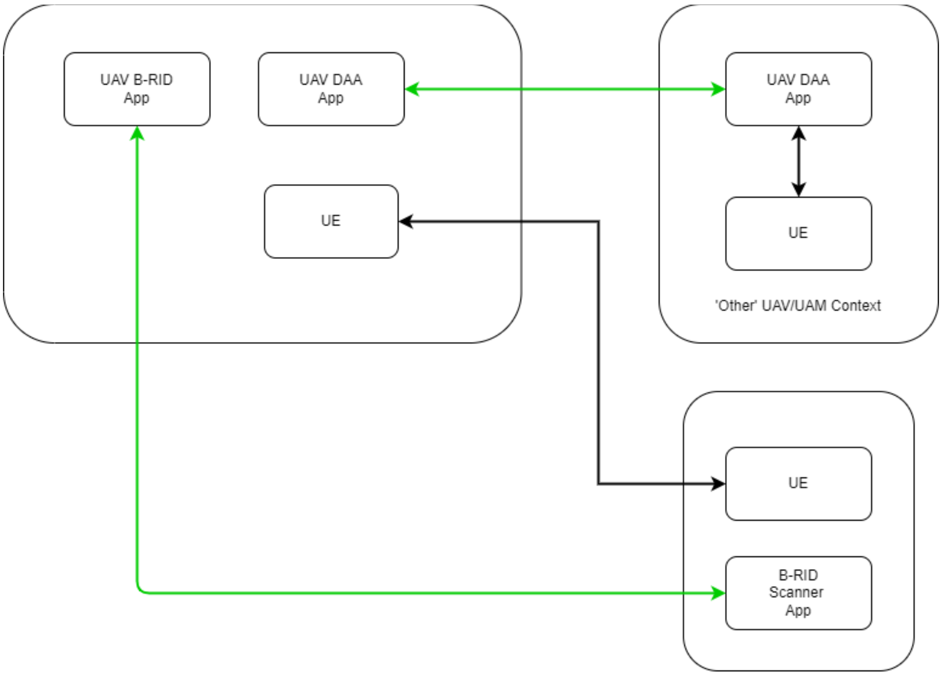


Figure 16. Broadcast Elements.

8.7.1. Standardization

ACJA WT-1 will develop a dedicated paper for non-C2 cellular communication, which will address this architecture and be based on existing and ongoing work in 3GPP.

RTCA SC-228 SG-2 have launched a dedicated Vehicle-to-Vehicle activity with V2V Whitepaper (in draft at the time of writing) focused on airborne surveillance applications. This paper may form a basis for aviation requirements for V2V cellular applications.

ASTM has started a new WG focusing on security of such broadcast solutions, focusing initially on B-RID and subsequently on DAA.

8.7.2. Security Considerations

Security considerations will be handled by a dedicated papers developed by ACJA WT-1 and ASTM F38.

9. ADX Deployment

There are several potential architectures which allow to connect the UE UAV with Wireless RPS or Cloud RPS and USS infrastructures. A fundamental assumption for ACJA is that this interconnection should have some guaranteed characteristics, and hence cannon be just using an open public Internet connection.

To emphasize this assumption, we use a term Aviation Data eXchange (ADX) Network for any network connecting an MNO network to external relevant parties including USS providers, UAS operators, CSCPs, etc. The concept of ADX is derived from GSMA IPX, which has been widely used for 3GPP services including VoIP.

The ADX network provides interconnectivity between two MNOs (e.g., between a UAV served by a first MNO and the Wireless RPS served by a second MNO) and between MNOs and external service providers (e.g., C2CSP, UAS Operators, and USS). The ADX network provides support of aviation specific services such as C2 transport, voice relay, navigational media, payload communications, and signaling for UUAA that require separation and isolation from the Internet to provide:

- Service quality management by providing guaranteed transport with SLAs assurance.
- Bandwidth-based admission and control for transport sessions.
- Guaranteed QoS compliance with priority handling of application traffic.
- Assurance of security by providing secure interconnection between ADX endpoints.

It is assumed that relevant work will take place in GSMA to define an ADX Network, similarly to the IPX network that was defined for interconnectivity for other services such as Internet access and VoIP. The use of a dedicated data network defined via GSMA enables the definition of a interconnection model which encompasses commercial, technical and operational requirements to provide interconnectivity via a global, private, multiservice, secure IP network, open to any service provider (e.g. MNO, USS provider, UAS operator, C2CSP, etc.)

under a contractual agreement which supports end-to-end security and quality of service.

9.1. Wireless RPS Deployment

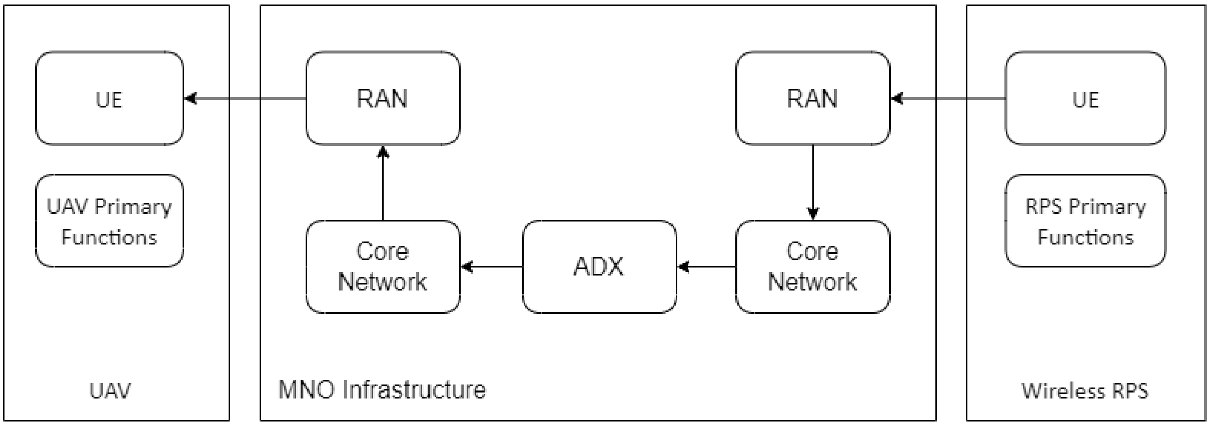


Figure 17. Wireless RPS Deployment.

9.1.1. Networking

The simplest case, represented by the Figure 17, is a total absence of interchange outside the PLMN. This case assumes a Wireless RPS with its own cellular connection, served by the same PLMN that serves a corresponding vehicle (or multiple vehicles).

While ground segment may be trivial in this architecture (e.g., may involve a sole router), is it important to emphasize that 3GPP-compiant system will always have the ADX in place.

9.1.2. Security Considerations

This deployment method benefits from sole use of internal PLMN security mechanisms, besides application level end-to-end security.

9.1.3. RPS and Human Factors

This deployment method is similar to widely used LOS setups with mobile handheld controllers, a human remote pilot operates such controllers directly.

9.2.Cloud Controller and USS Infrastructure

In this model, the Cloud RPS is implemented as an application in the cloud which implement RPS functionality. The Cloud RPS may have user interfaces towards a human who acts as remote pilot. Implementations of cloud controller may allow the cloud to be hosted in a CSCSP provider, the UAS operator infrastructure, or supported by an MNO acting as a C2CSP. Interconnection between the UAV and the Cloud RPS is via the ADX Network.

Besides C2 capability, advanced (in U-space terminology — U2 and U3 phase services) UTM services, which rely on connectivity, shall use ADX in exchange data with the UAV. Envisioned services of this kind are (uplink services):

- Collaborative interfaces with ATC.
- Tactical deconfliction / ground-based Detect-and-Avoid.
- Dynamic geofencing.
- Dynamic capacity management and airspace reconfiguration.

Also, the following data exchanges may use ADX to increase reliability:

- Data exchanges that are part of the aerial connection authentication and authorization process.
- Network remote identification services.
- USSP-USSP and USSP-CIS data exchange.

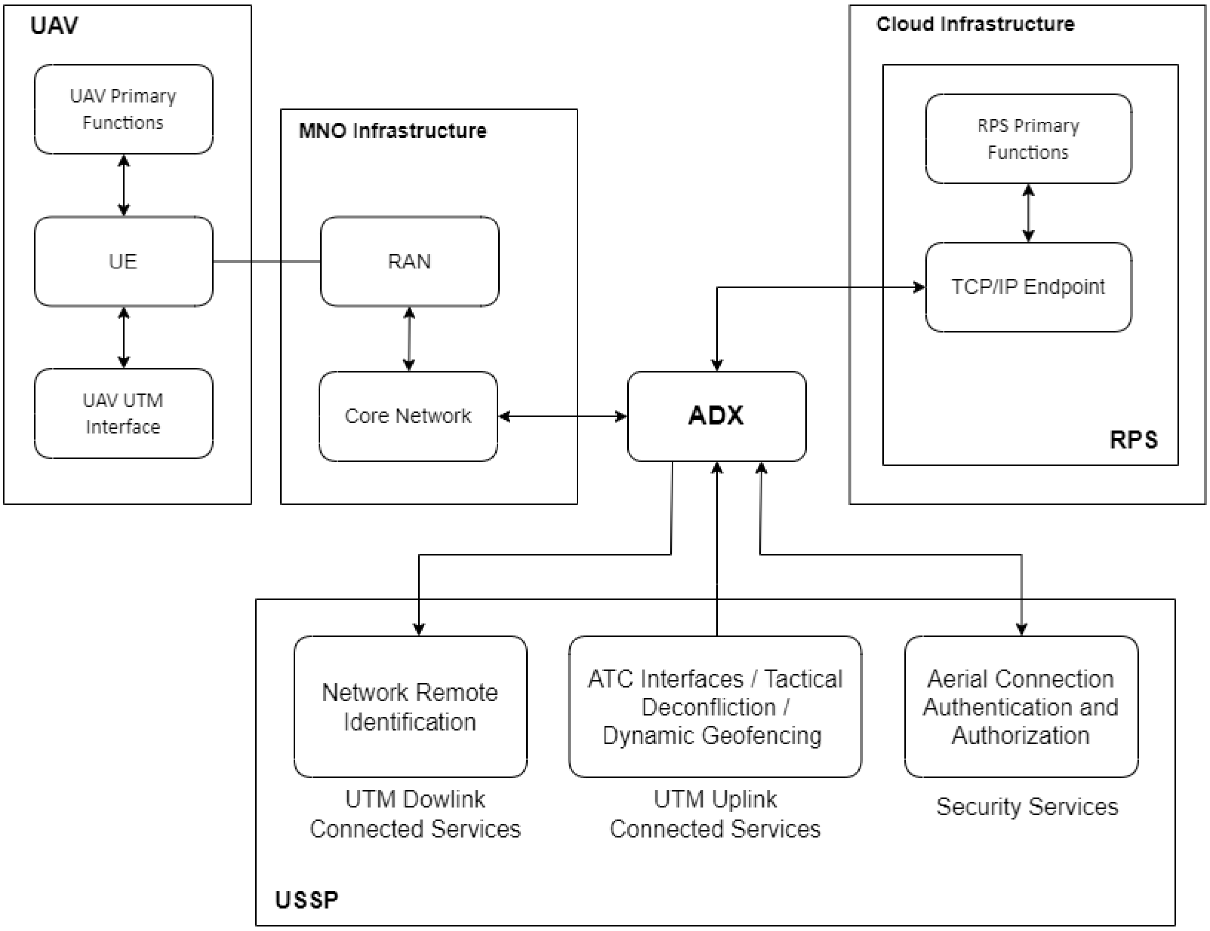

UAV
UAV Primary Functions
UE
UAV UTM Interface
MNO Infrastructure
RAN
Core Network
ADX
Cloud Infrastructure
RPS Primary Functions
TCP/IP Endpoint
RPS
Network Remote Identification
UTM Dowlink Connected Services
ATC Interfaces / Tactical Deconfliction / Dynamic Geofencing
UTM Uplink Connected Services
Aerial Connection Authentication and Authorization
Security Services
USSP

Figure 18. Cloud Controller and USS Infrastructure.

While C2CSP and USSP are separate roles in the UTM ecosystem, an MNO may assume one of these or both roles as a part of the integrated services bundle. Some regional regulatory frameworks strongly endorse this approach.

9.2.1. Networking

All the traffic exchanged between the UAV and the Cloud RPS is exchanged via the ADX Network. Mission critical data exchange between the UAV and the USSP also go through the ADX, but some exchanges without stringent requirement may use the public Internet.

9.2.2. Security Considerations

E2E security between the UAV and the Cloud RPS is supported via the security mechanisms provided by the MNO (UAV to MNO ground stations, MNO core network) and the use of the ADX Network which provides an e2e SLA for security and QoS between the edge of the MNO network and the function supporting the Cloud RPS.

9.2.3. RPS and Human Factors

As an RPS shall be operated by a human remote pilot, any interaction between a human and the RPS Primary Function shall be direct, without any additional point of failure, delay, or insecure channel. Hence, a human pilot shall have physical access to a proper terminal co-located is a cloud controller.

If any remote access technology is used to allow a pilot to access any RPS cloud functions, a link between pilot's terminal and the RPS shall be considered as a part of the Cloud Infrastructure, with all associated QoS and security requirement mechanisms.

10. Supplemental Data Service Provider

Cellular Supplemental Data Provider or SDSP provides actual and forecasted information about cellular connectivity performance to mission-critical (non-payload) applications.

WT-2 created a Network Data Service specification and at the time of writing expands this definition. Network Data Service specification defines one means to implement an SDSP based on the service-oriented architecture.

Considering deployment, SDSP implementation would require some components to be present both within the MNO infostructure and in the UTM infrastructure.

11. Annex I: Basics of 3GPP Networks

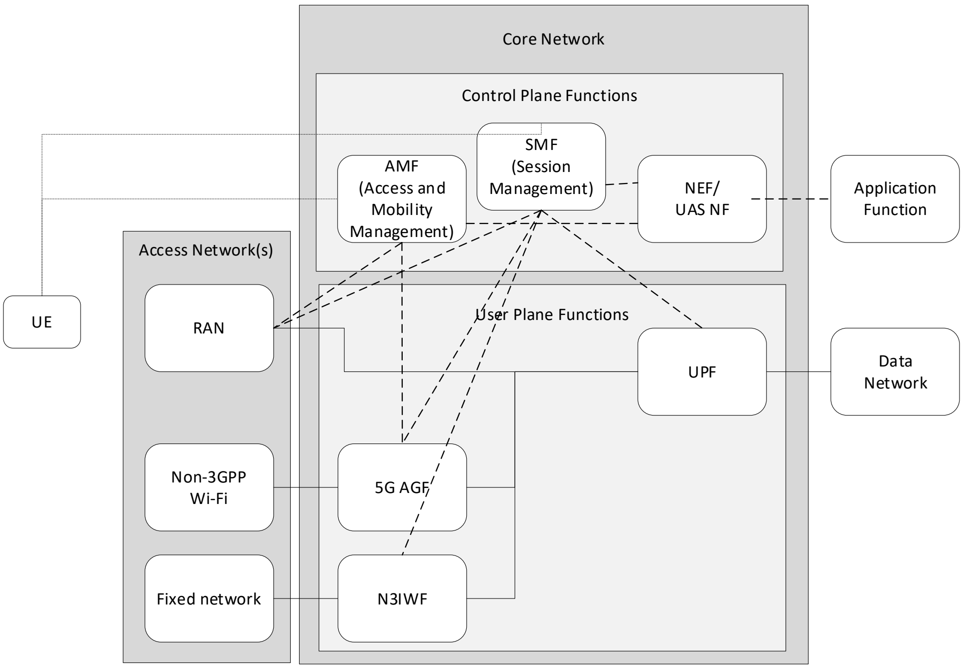


Figure 19. 5GS Architecture.

The most important network functions in the architecture are:

- AMF: Access and Mobility Management Function terminates the control plane of different access networks onto the 5G Core Network and control which UEs can access the network to exchange traffic with the DNs; it also manages the mobility of UEs when they roam from one gNB to another for session continuity.
- SMF: Session Management Function keeps trace of PDU sessions and QoS Flows in the 5GS for UEs and make sure their states and status are in sync between the Network Functions in the Control and the User Planes. It receives PCC (Policy and Charging Control) Rules from the PCF (Policy Charging Function) and convert PCC Rules into *SDF Templates*, *QoS Profiles* and *QoS Rules* for the UPF, gNB and UE respectively for QoS Flows establishment, modification and release.

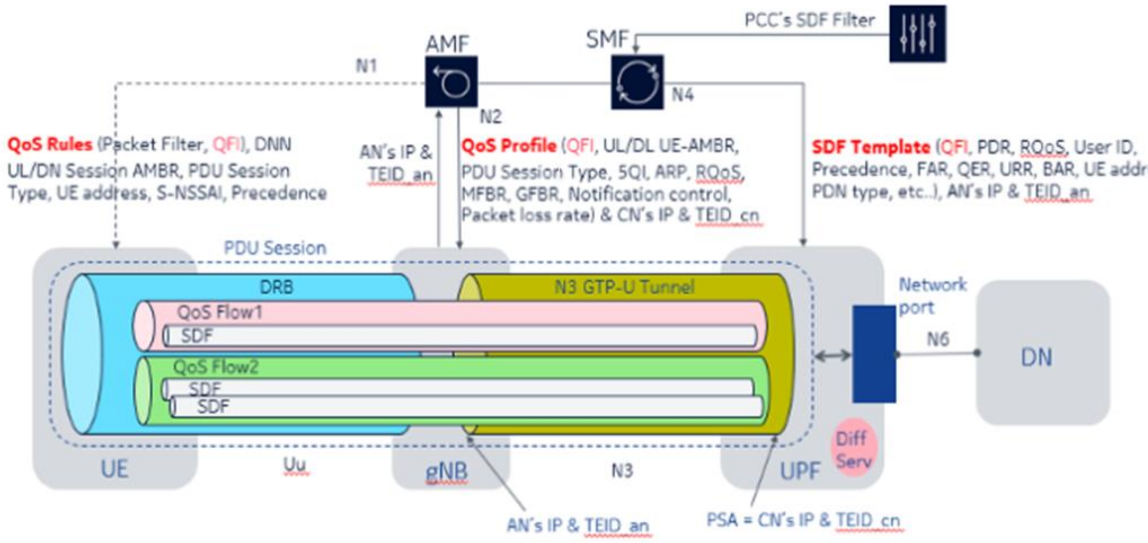
- UPF: User Plane Function forwards UE traffic between the access networks such as the gNBs in 5G-RAN and the DNs. It also enforces QoS on UE's uplink and downlink traffic in 5GC using the *SDF Templates* sent by the SMF.
- UDM: Unified Data Management stores UE encryption key to decrypt UEs' SUCI (Subscriber Concealed Identifier) to SUPI (Subscriber Permanent Identifier). It also stores UEs' subscription data.
- gNB: 5G New Radio (NR) base station.

11.1.3GPP Connectivity Model

3GPP UE(s) (User Equipment(s)) use the 3GPP system to get data connectivity between applications on the UE and Data Networks (DNs) such as the 'Internet' or networks dedicated to specific services. A PDU Session (for 5G System) or PDN Connection (for 4G System) are an abstraction of the user plane services that provides such connectivity between applications on a UE and a DN.

A UE being powered up and entering the 3GPP system performs the Registration Procedures with the 5GS for the AMF to authenticate the UE's USIM card to make sure that the UE has a valid subscription in the 5GS. When the UE's Registration Procedure is successfully completed, the UE initiates a PDU Session Establishment request to the AMF via the gNB in order to establish a default QoS Flow between the UE and the Data Network (DN) via the gNB.

For a successful PDU session established between a UE and a DN, the following wireless and wireline tunnels are setup: a bi-directional wireless Data Radio Bearer (DRB) between UE and gNB, and two unidirectional GTP-U tunnels to form a bi-directional N3 GTP-U tunnel between gNB and UPF.


PCC's SDF Filter
AMF
SMF
N1
N4
N2
QoS Rules (Packet Filter, QFI), DNN UL/DN Session AMBR, PDU Session Type, UE address, S-NSSAI, Precedence
AN's IP & TEID_an
QoS Profile (QFI, UL/DL UE-AMBR, PDU Session Type, 5QI, ARP, RQoS, MFBR, GFBR, Notification control, Packet loss rate) & CN's IP & TEID_cn
SDF Template (QFI, PDR, RQoS, User ID, Precedence, FAR, QER, URR, BAR, UE address, PDN type, etc..), AN's IP & TEID_an
PDU Session
DRB
N3 GTP-U Tunnel
QoS Flow1
SDF
QoS Flow2
SDF
SDF
Network port
N6
DN
Diff Serv
UE
Uu
gNB
N3
UPF
AN's IP & TEID_an
PSA = CN's IP & TEID_cn

QoS Flow Setup with N1, N2, and N4 messages with QoS constructs from SMF

Figure 20. PDU Sessions and QoS Flows.

In 5G, QoS Flow is the lowest granularity of a traffic flow where QoS and charging can be applied, and it is similar to a 4G's EPS Bearer. The default QoS Flow is a non-GBR (non-Guaranteed Bit Rate) QoS Flow without any Packet Filter and has the lowest *Precedence* in term of traffic mapping. If uplink (UL) or downlink (DL) traffic do not match any Packet Filters in the other QoS Flows within a UE's PDU Session, the default QoS Flow will be used to forward the UE traffic to the DN and vice versa. The default QoS Flow can also be used by a UE to signal an AF (Application Function) such as voice or video servers to establish GBR QoS Flows to support more QoS demanding network applications such as video conferencing or real-time robotic traffic.

An SDF (Service Data Flow) is a traffic stream between a UE and the DN where the SDF's QoS requirements can be satisfied by the QoS Flow carrying the SDF (e.g., various opened tabs of a web browser not requiring any specific QoS treatment can be mapped to a single SDF carried by the default QoS Flow.

If a UE requires a GBR (Guaranteed Bit Rate) QoS Flow, the UE can signal to an AF (Application Function) which will initiate a QoS Flow setup to the PCF for it to generate a *PCC Rule* to the SMF. The SMF then updates the UFP with a PDU

Session Modification Request to augment the UE’s PDU Session to either modify an existing or creating a new QoS Flow suitable for the video conference traffic or SDF. Later, the UE may need a GBR QoS Flow to support other data streams. If such data streams have the same QoS requirements (e.g., 5QI, ARP, etc.) of the existing one, the SMF can modify the existing GBR QoS Flow to support two SDFs.

When a PCF sends a PCC Rule to SMF, the SMF provides different QoS constructs and send them to each processing entities along the QoS Flow as follows: *SDF Template* to UPF over N4 PFCP (Packet Forwarding Control Protocol) interface; *QoS Profile* to gNB via AMF over the N2 interface; *QoS Rule* to UE via AMF and gNB over the N1 interface. If the UE, gNB and UPF can satisfy the QoS constructs sent from SMF, the *QFI* (QoS Flow Identifier) that is sent along with the *SDF Template*, *QoS Profile* and *QoS Rule* now represents the QoS characteristic of the QoS Flow.

5G-RAN and 5G-Core ensure quality of service (e.g., reliability and target delay) by mapping packets to appropriate QoS Flows and DRBs. Hence there is a 2-step mapping of IP-flows to QoS flows (NAS) and from QoS flows to DRBs (Access Stratum).

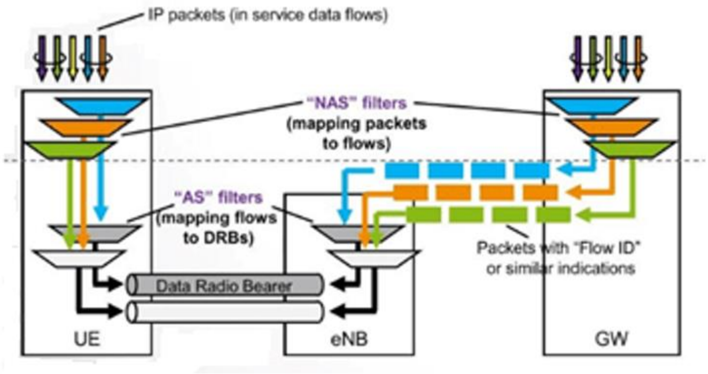

IP packets (in service data flows)
"NAS" filters (mapping packets to flows)
"AS" filters (mapping flows to DRBs)
Data Radio Bearer
Packets with "Flow ID" or similar indications
UE
eNB
GW

Figure 21. 2 Level Filtering — NAS and AS Level.

A QoS flow is identified by QFI within PDU session. For each UE, 5GC establishes one or more PDU sessions and 5G-RAN establishes at least one DRB together with PDU session. Separate DRBs may be established for QoS flows requiring different packet forwarding treatment, or several QoS Flows belonging to the same PDU session can be multiplexed in the same DRB. The QoS flow to DRB mapping by gNB is based on QFI and the associated QoS profiles (i.e., QoS parameters and QoS characteristics). At NAS level, a QoS flow is characterized by a QoS profile provided by 5GC to 5G-RAN and QoS rule(s) provided by 5GC to the UE. A QoS flow may either be GBR or Non-GBR depending on its QoS profile, which is used by gNB to determine the treatment on the radio interface.

USS and UAS Operator Influencing on UAV cellular connectivity.

UAS operator platform or USS are seen by the 3GPP system as application functions (AF) impacting connectivity. The USS and UAS Operator provide connectivity information (e.g., requested QoS, traffic filters, etc.) to the UAV Network Function (NF) in the 3GPP system to configure the connectivity of the UAV to the USS and for C2 via the PDU session/PDN connection. Such traffic influencing function is already part of the SCEF/NEF framework and APIs.

The following capabilities can be requested or influenced by USS or UAS operator:

- For monitoring capabilities:
    - Loss of Connectivity monitoring event may have more stringent latency and time-to-alert requirements, driven by data transmission performance requirement.
    - Roaming status may be enhanced to ensure that UAS connectivity is always handed over to a compliant MNO.
    - Number of UE present may raise an alert when a number of UE with “UAS” APN violates an approved threshold.
    - Downlink data delivery status
- Provisioning capability:
    - Expected UE behavioral information: it seems reasonable for this information to be synchronized with a flight plan available for the USS.
- The Policy capability may be used by USS to restrict available QoS for aerial UEs, to preclude using ‘insecure’ connectivity.

- Network’s External Identifiers may include both Remote ID-compliant UAS identifier as well as USS internal ID used to an associated UAV.

Note: section 6.5 provides a summary of the NEF services/capabilities available for UAS operators.

12. Annex II: 3GPP specifications related to UAV/UAS

12.1. General

Figure 22 summarizes the key references of the 3GPP related to the Uncrewed Aerial Vehicles and Systems (UAV/UAS) and their communications and control links between the 4G and 5G systems.

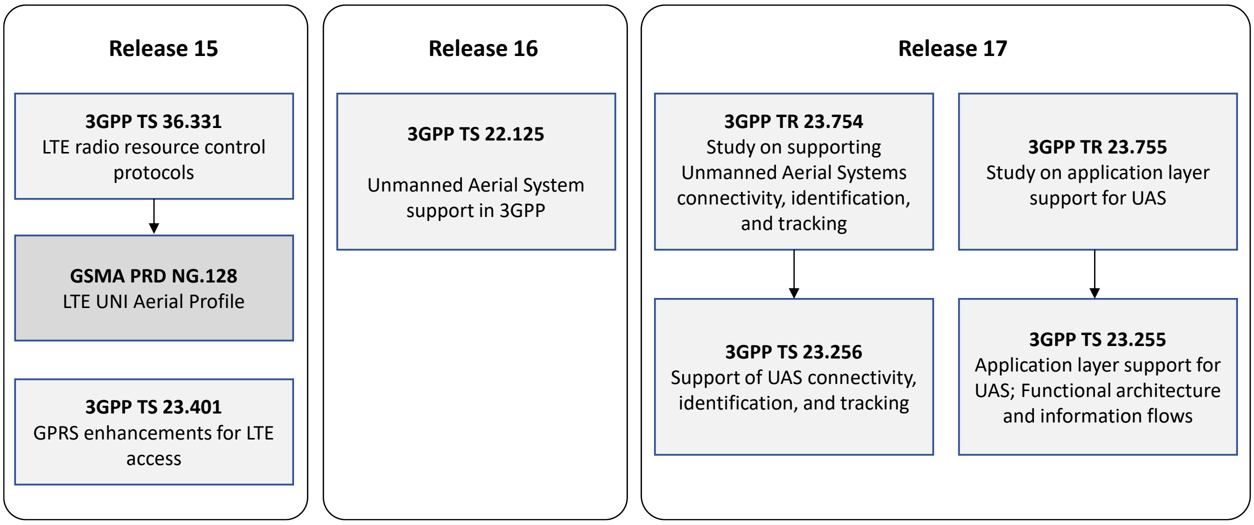

Release 15
3GPP TS 36.331
LTE radio resource control protocols
GSMA PRD NG.128
LTE UNI Aerial Profile
3GPP TS 23.401
GPRS enhancements for LTE access
Release 16
3GPP TS 22.125
Unmanned Aerial System support in 3GPP
Release 17
3GPP TR 23.754
Study on supporting Unmanned Aerial Systems connectivity, identification, and tracking
3GPP TR 23.755
Study on application layer support for UAS
3GPP TS 23.256
Support of UAS connectivity, identification, and tracking
3GPP TS 23.255
Application layer support for UAS; Functional architecture and information flows

Figure 22. The key 3GPP technical reports and specifications related to the UAV/UAS.

12.2. Release 15

The 3GPP Release 15 presents enhancements for aerial vehicles relying on 4G EPS (Evolved Packet System) architecture and LTE radio network (E-UTRAN) in the 3GPP TS 36.331 (LTE Radio Resource Control RRC; Protocol specification) Section 5.5.4 (Measurement report triggering), and in the 3GPP TS 23.401 (General Packet Radio Service enhancements for Evolved Universal Terrestrial Radio Access Network access). The key enhancements of these specifications are the following:

- The aerial UE features of the 3GPP TS 36.331 provide LTE enhancements to address the issue of aerial UE interference to the LTE eNodeB elements (base stations). The enhancements include the additional height reporting events

("H1 above" and "H2 below" UE height thresholds) to help the eNodeB see the UAV and to reduce potential interference caused by the aerial vehicles. This specification is also the key reference for the minimum set of requirements for an LTE Aerial Profile for UAV that the GSMA PRD NG.128 summarizes.

- The TS 23.401 introduces the UE aerial subscription and indication, which allows the system architecture to identify which 3GPP UE have an aerial subscription and provides the core network means to activate the UE aerial features defined for aerial UEs only for UEs that have an aerial subscription.

12.3. Release 16

Among various overall enhancements and new functions, the Release 16 focused on new requirements for aerial vehicles by defining a new set of requirements in the 3GPP TS 22.125 (Unmanned Aerial System support in 3GPP), which provides "stage one" requirements for UAV support. Please note though that such requirements did not lead to the introduction of any new standards features in Release 16.

12.4. Release 17

The 3GPP Release 17 specifications have been ready for implementation as of the second half of 2022. The work for aerial vehicles in Release 17, applicable to UAVs and Urban Air Mobility (UAM), focused on enhancements to the requirements for UAVs as presented in the Release 16 of the 3GPP TS 22.125:

- 5G System (5GS) enhancements for the support of UAVs. This item was studied in 3GPP SA2, and lead to the creation of technical report 3GPP TR 23.754 (study on supporting Unmanned Aerial Systems connectivity, identification, and tracking), which documents the results of a feasibility study on supporting UAVs in 4G and 5G.
- The conclusions of the 3GPP TR 23.754 are included in the 3GPP TS 23.256 (support of Uncrewed Aerial Systems connectivity, identification, and tracking; Stage 2). The 3GPP TS 23.256 provides support of UAV connectivity for command and control (C2), support of UAV authentication and authorization, and support for enabling Network Remote Identification and Broadcast Remote Identification. It outlines further the architecture enhancements for supporting UAS connectivity, identification, and tracking, according to the use cases and service requirements defined in 3GPP TS 22.125. Related to the architectural enhancements, it is a key reference for supporting UAS connectivity, identification, and tracking, according to the use cases and service requirements outlined in the 3GPP TS 22.125. It

specifies the following: UAV Identification, authentication, and authorization; UAV tracking in the 3GPP system, including how the 3GPP system can provide support for UAV to ground identification (e.g., to authorized third parties such as police devices); and handling of unauthorized UAVs and revocation of authorization.

- The 3GPP SA6 carried out a study and documented those in technical report **3GPP TR 23.755** (study on application layer support for UAS) on potential API support for UAS with a focus on UAV tracking and authorization.
- The **3GPP TS 23.255** (Application layer support for Uncrewed Aerial System; Functional architecture and information flows) presents the results of the TR 23.755. It also describes functional architecture model for the UAS application layer, as well as information flows including architectural requirements, identities, procedures, and APIs. The 3GPP TS 23.255 presents architectural requirements for the support for communications between UAVs, QoS provisioning for C2 communication, C2 communication mode switching, support for monitoring of UAV location deviation, and support for reporting of UAV events.

12.5. Release 18 and beyond

The 3GPP continues producing Releases that focus on 5G and previous generations. The selection of the Release 18 work items is currently under work, and the latest list and news can be found at https://www.3gpp.org/release18. Release 18 is focusing on the following aspects:

(i) Support of Broadcast remote ID using PC5 (sidelink UAV-to-UAV and UAV to ground interface without using an MNO infrastructure)

(ii) Support of DAA protocols using PC5

(iii) Support of C2 using PC5 (direct sidelink between a wireless RPS and a UAV without using MNO infrastructure)

(iv) RAN enhancements for the support of features equivalent to 4G LTE aerial features

(v) RAN enhancement for the support of PC5 based on (i) to (iii)

12.6. Future

New mobile communications generations reach the commercial markets each decade. 6G follows this trend as the ITU has already initiated considering new IMT-2030 requirements for the 6G, with the aim of paving the way for commercial phase of 6G in 2030s. The concrete requirement statements of the ITU are still under work, and the standards setting organizations are preparing to start form their specifications upon the possibilities later. Meanwhile, information about the of 6G can be found at: [https://www.itu.int/en/ITU-T/focusgroups/net2030/Pages/default.aspx].

As an example, the 6G architectural aspects are presented in Network 2030 Architecture Framework Technical Specification at: [https://www.itu.int/en/ITU-T/focusgroups/net2030/Documents/Network_2030_Architecture-framework.pdf].

About the GSMA

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators and nearly 400 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces the industry leading MWC events held annually in Barcelona, Los Angeles and Shanghai, as well as the Mobile 360 Series of regional conferences.

For more information, please visit www.gsma.com

About the GUTMA

The Global UTM Association (GUTMA) is a non-profit consortium of worldwide Unmanned Aircraft Systems Traffic Management (UTM) stakeholders. Its purpose is to foster the safe, secure and efficient integration of drones in national airspace systems. Its mission is to support and accelerate the transparent implementation of globally interoperable UTM systems. GUTMA members collaborate remotely.

For more information, please visit www.gutma.org