MOBILE-ENABLED UNMANNED AIRCRAFT

How mobile networks can support unmanned aircraft operations

FEBRUARY 2018

TABLE OF CONTENTS

Executive Summary

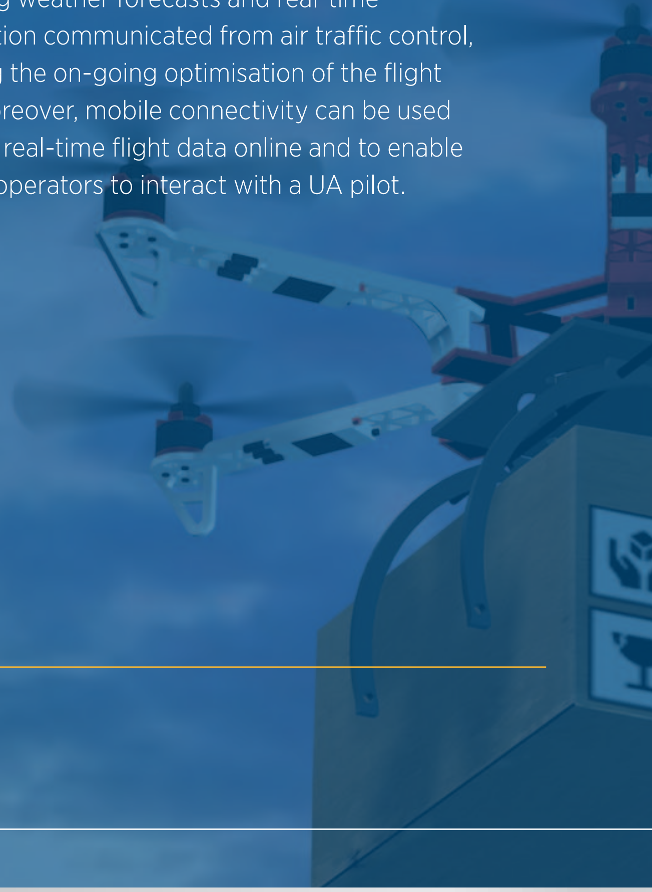
The unique capabilities of mobile networks can be used to support the safe usage of unmanned aircraft[1] (UA), which are becoming increasingly popular with consumers and business users. Today UA are generally connected to a ground control system via limited range communications over unlicensed spectrum. As a result, they tend to be restricted to visual-line-of-sight (VLOS) applications, limiting their usefulness for enterprises in particular.

Beyond-visual-line-of-sight (BVLOS) applications require much more scalable, reliable and secure connectivity, such as that provided by mobile networks. Key use cases for UA include:

- Inspection and surveys of industrial and agricultural assets and sites
- Transport and logistics – the delivery of small payloads to inaccessible places
- Surveillance and monitoring – the detection of specific events, such as a fire or a breach
- Communications and media – capturing footage of news events and filming TV and movies
- Disaster response – rapid information gathering and providing connectivity in place of damaged conventional infrastructure

In each case, the use of mobile connectivity can enhance the efficiency and effectiveness of the UA both by enabling BVLOS operation and by supporting real-time data transmissions from on-board cameras and sensors. For example, mobile networks can live stream video footage back to a central repository where it can be analysed in real-time and used to shape the rest of the UA's mission.

Mobile networks can also enable the development of new services for UA. Once the UA is cellular connected, it will be able to access changing weather forecasts and real-time information communicated from air traffic control, enabling the on-going optimisation of the flight plan. Moreover, mobile connectivity can be used to share real-time flight data online and to enable remote operators to interact with a UA pilot.



---

[1] UA are sometimes known colloquially as drones

Companies and consumers could save time and money if they can simply make a real-time request for a UA in the air to take a photograph. As with connected cars, mobile networks could enable UA manufacturers and service companies to receive real time alarms about failures or potential failures, thereby preventing accidents and reducing maintenance costs.

By harnessing existing encryption and authentication mechanisms, mobile networks can also help secure UA operations, as well as supporting the identification and location needs of law enforcement agents and air traffic control systems. The table below summarises the mobile assets and capabilities that can be used to enhance the performance of UA and improve safety:

ASSET	DESCRIPTION
standardised and scalable solution for worldwide connectivity	Globally available, mobile networks provide very cost efficient solutions: no investment is necessary to roll out a new infrastructure. In addition, mobile networks continue to evolve to match the evolving needs of UA communication platforms.
Licensed spectrum	Working with dedicated spectrum in licensed bands enables mobile networks to provide the reliable connectivity required for mission-critical applications, especially in BVLOS cases and in high-risk environments.
Secure communication channel	Mobile networks provide specific encryption mechanisms to protect communications against misuse, achieving high standards of data protection and privacy.
Lawful intercept and location verification	Mobile networks can support the lawful intercept of communications from the UA, as they do with mobile devices. Mobile operators can also provide independent verification of the location of the UA for use by the UAS (Unmanned Aircraft System) traffic management.
Trusted identification	The credentials established for mobile network authentication can meet the need for unique and trusted identification of UA.

To address the anticipated usage of cellular technologies by UA, standards body 3GPP has produced a study on enhanced LTE support for aerial vehicles ([9]). Started in 2017, the study identifies potential improvements that could be developed to more efficiently handle UA traffic and its impact on the network. 3GPP continues to explore ways in which the cellular standards could be developed to further support UA.

REFERENCES

[1] https://www.flexport.com/blog/drone-delivery-economics/
[2] https://www.faa.gov/uas/research/utm/media/FAA_NASA_UAS_Traffic_Management_Research_Plan.pdf
[3] Unmanned Aircraft System traffic management: Concept of operation and system architecture - http://ac.els-cdn.com/S2046043016300260/1-s2.0-S2046043016300260-main.pdf?_tid=9ba92242-7b60-11e7-b40c-00000aacb35f&acdnat=1502104232_ac36ebdb336588ce2f92f7ac4a7ac50d
[4] UAS Traffic Management Architecture - https://www.gutma.org/docs/Global_UTM_Architecture_V1.pdf
[5] 3GPP - http://www.3gpp.org/
[6] 3GPP TS 23.271 - Functional stage 2 description of Location Services (LCS)
[7] 3GPP TS 36.305 - Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Stage 2 functional specification of User Equipment (UE) positioning in E-UTRAN
[8] http://www.saladeprensa.vodafone.es/c/notas-prensa/np_dron_utrera_2017 [in Spanish])
[9] 3GPP TR 36.777 - Enhanced LTE support for aerial vehicles
[10] GSMA IoT Security Guidelines; https://www.gsma.com/iot/wp-content/uploads/2017/10/IoT-Security-Guidelines-Complete-Document-Set-v2.0.zip
[11] GSMA IoT Security Assessment; https://www.gsma.com/iot/wp-content/uploads/2017/11/IoT_security_checklist_web_10_17.docx
[12] UAS Identification and Tracking (UAS ID) - Aviation Rulemaking Committee (ARC); https://www.faa.gov/regulations_policies/rulemaking/committees/documents/media/UAS%20ID%20ARC%20Final%20Report%20with%20Appendices.pdf
[13] “Watch A Very Vulnerable $140 Quadcopter Drone Get Hacked Out Of The Sky”, Forbes; https://www.forbes.com/sites/thomasbrewster/2017/04/25/vulnerable-quadcopter-drone-hacked-by-ut-dallas-cyber-researchers/#31909c581037
[14] Drones wide open to hijack threats, E&T Magazine; https://eandt.theiet.org/content/articles/2017/03/drones-wide-open-to-hijack-threats/
[15] 3GPP TS 33.106, Lawful interception requirements
[16] 3GPP TS 33.107, Lawful interception architecture and functions
[17] 3GPP TS 33.108, Handover interface for Lawful Interception
[18] GSMA Intelligence; https://www.gsma.com/newsroom/press-release/number-of-global-mobile-subscribers-to-surpass-five-billion-this-year/

1. Introduction

The unique capabilities of mobile networks can enable a full continuum of use cases ranging from low cost consumer applications to high-end enterprise or government deployments. These same capabilities can also be used to support the safe usage of unmanned aircraft (UA), which are becoming increasingly popular with consumers and business users.

The ubiquitous, secure and reliable data transmission provided by mobile networks can support UA across a broad range of applications. For example, cellular networks' hand-off capabilities, which enable a phone conversation to be maintained while driving down a highway, is a key enabler for UA beyond-visual-line-of-sight (BVLOS) enterprise applications, such as linear inspection and package delivery. The regulatory safety requirements for BVLOS mean mobile network connectivity is a must-have for such applications.

Most UA are not mobile-enabled today. Instead, they are connected to a ground control system via limited range communications over unlicensed spectrum. Such connectivity can be prone to congestion, interference, and varying range and quality of service. Although these challenges are fairly limited today, the growth of UA, and other uses, in these airwaves will result in a decrease in the reliability of the communications. As well as supporting BVLOS operations, mobile networks have the scalability, reliability and security needed to support mission critical use cases with local line-of-site connectivity.

The latest mobile technologies are designed to connect a wide range of things, machines and vehicles: 4G networks can support a wide range of services, such as vehicle-to-vehicle communications, that can be used for collision detection and avoidance. The introduction of 5G will further enhance mobile networks' capabilities, which are unmatched by other technologies, while edge computing will allow for large-scale real-time data analytics with limited impact on the cost and battery life of UA.

This report outlines potential UA-related use cases for mobile networks and the benefits that mobile connectivity can bring to the UA sector. It also considers the role of mobile networks in supporting traffic management, before outlining the relevant work of cellular standards body 3GPP.

Use Cases

Although often perceived as a hobby, flying unmanned aircraft (UA) can directly or indirectly benefit society across numerous use cases, which are evolving over time. In a disaster response scenario, for example, UA can act as “flying mobile base stations” providing connectivity.

This section presents an overview of these use cases, showing how UA can be used to improve our lives and how the application of mobile technologies can increase these benefits.

This section identifies two main categories of use cases: enterprise and disaster recovery.

ENTERPRISE USE CASES

UA can improve the efficiency of business operations in many different ways. Enterprise use cases can generally be grouped into four main categories:

- **Inspection and surveys**
- **Transport and logistics**
- **Surveillance and monitoring**
- **Communications and media**

Many industries employ more than one of these uses cases, of course. In agriculture, for example, UA may be used for surveys (land mapping), monitoring (crop health and development) and logistics (crop spraying). In telecommunications or utilities, UA may be used to inspect a potential location for installing a base station or a sub station, and for monitoring the condition of the infrastructure.

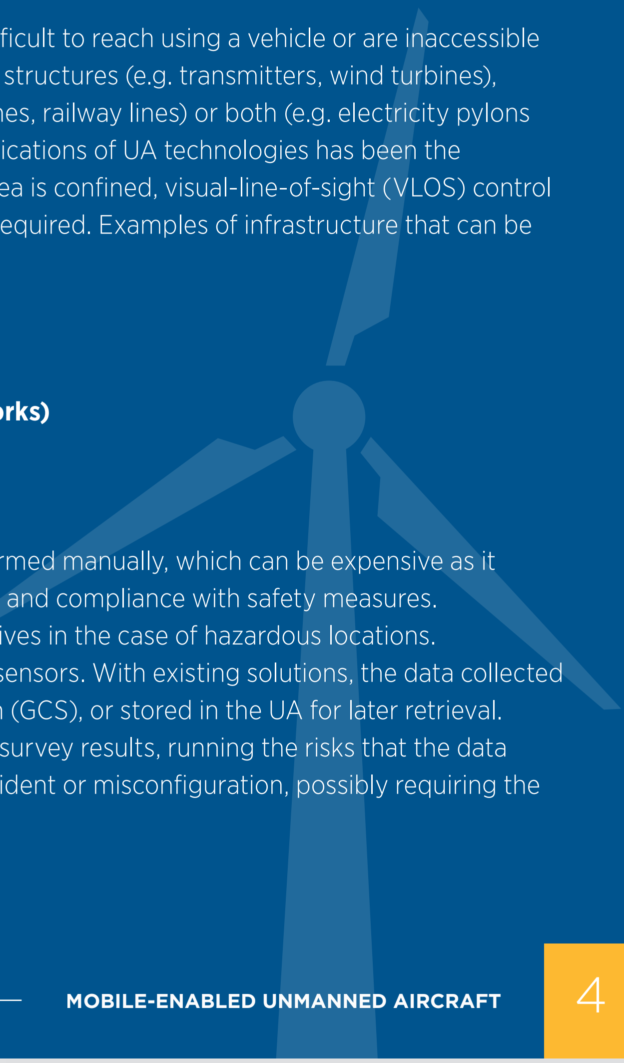
Bearing this in mind, the four use case categories are discussed below.

INSPECTION AND SURVEYS

Many industries need to inspect assets that are remote or difficult to reach using a vehicle or are inaccessible because of safety hazards. This may be because they are tall structures (e.g. transmitters, wind turbines), stretch over long distances with no parallel roads (e.g. pipelines, railway lines) or both (e.g. electricity pylons and power lines). One of the first successful commercial applications of UA technologies has been the inspections of towers, primarily because the geographical area is confined, visual-line-of-sight (VLOS) control is sufficient and the UA's batteries can easily be replaced as required. Examples of infrastructure that can be inspected using UA include:

- **Wind turbines**
- **Power station chimneys and cooling towers**
- **Transmitter sites (for TV broadcast and mobile networks)**
- **Transport infrastructure (e.g. bridges and viaducts)**
- **Land mapping (e.g. agricultural fields, quarries)**

Without a UA, inspection of these structures has to be performed manually, which can be expensive as it requires skilled personnel, specialist vehicles and equipment, and compliance with safety measures. Employing UA reduces the cost, time and the risk to human lives in the case of hazardous locations.
The UA generally carries a video camera and possibly other sensors. With existing solutions, the data collected by the UA is either streamed to a local ground control station (GCS), or stored in the UA for later retrieval. However, this approach can result in a delay in analysing the survey results, running the risks that the data was not collected properly or is lost altogether due to an accident or misconfiguration, possibly requiring the



survey to be repeated. Streaming the video and other sensor data to a remote location for instant storage, verification and analysis reduces these risks and allows the survey team to gauge whether additional data needs to be collected.

Surveys of linear assets, such as pipelines or electricity cables, or large geographical areas, such as agricultural fields, can be limited by the current requirement in most jurisdictions for the pilot to maintain VLOS. To realise the full potential of this use case, there is the need to be able to fly beyond VLOS, whilst still being able to monitor and control the UA and instantly analyse the survey data. Mobile networks can provide the geographical coverage and secure connectivity necessary for UA operators to check that the UA is flying within the boundaries agreed for the mission and is collecting suitable data.

TRANSPORT AND LOGISTICS

This use case exploits an UA's ability to travel quickly and easily between two points without being hindered, in general, by obstacles on the ground, except in no-fly zones, such as airports, prisons and military facilities, for example. The UA can carry a cargo or payload between these two points for delivery. This concept is being explored by both e-commerce and logistics companies, such as Amazon and DHL, as well as food delivery enterprises, such as Dominos, whose businesses require timely delivery of perishable or other time-sensitive products. UA can also be used in agriculture for crop planting and spraying, where the "delivery" is over a large area that is otherwise difficult to reach.

Due to current limitations in flight-time, payload weight and the regulatory requirement in some jurisdictions to maintain VLOS, commercial applications of this use case have been limited to the rapid delivery of high-value, time-sensitive cargoes over difficult terrain. This generally means medical supplies, such as vaccines or blood. Examples include the service operated by Zipline in sub-Saharan African countries, such as Rwanda and Tanzania, and the Matternet service in Lesotho. Some small UA operators have also set-up "on demand" services in developed countries to deliver small payloads, such as food, to otherwise isolated locations, such as off-shore islands. Examples include the Flytrex service in Iceland and the A-techSYN service in the west of Ireland. Moreover, Swiss Post is planning to use UA to deliver both parcels and hospital laboratory tests between hospitals.

The business case for larger scale or more general delivery services by UA remains unproven (see this report [1]) and would depend on the premium that customers would pay for such a service. Costs could be reduced by requiring pilots to remotely monitor and control the routing of several UA simultaneously, which would mostly undertake their deliveries autonomously. This approach would require secure connectivity over a large geographical area, such as that provided by mobile networks.

SURVEILLANCE AND MONITORING

Surveillance UA are used by many government organisations, such as police forces, environment agencies (for detection and management of natural events and threats) and border agencies (to detect smuggling and illegal immigrants).

UA may be used to monitor and patrol a property boundary, either looking for breaches or investigating breaches detected by other alarms. They can also detect, and give early warning of, fires, floods, traffic accidents, oil spills and other incidents. If the UA is monitoring a single location, ground-tethering systems, such as that produced by Elistair, can be used to prolong flight times, though the tether will prevent the UA from significantly changing its position.

These use cases have some similarities with the inspection and survey use cases, the main difference being that the UA here is being used to detect and react to an object or an event. The key benefits of using a UA for surveillance are the ability to rapidly deploy and provide a "bird's eye" view of an area otherwise difficult to reach, along with the UA's ability to follow a moving object on the ground.

A surveillance UA will typically be equipped with a video camera, though other sensors, such as infrared cameras, may also be used, depending on the application. The data captured by the cameras and sensors will usually be monitored locally in real-time by an observer, with the risk that events may be missed or the data not properly stored for subsequent retrieval (as evidence in court cases, for example). By contrast, streaming the data directly from the UA via a secure communications channel to a remote central location allows economies of scale in data storage and analysis, irrespective of the location of the UA. A wide-area, secure, low-latency communications channel, such as that provided by mobile networks, can also be used to remotely control the UA, its cameras and its sensors.

> "employing UA is more cost effective than employing a helicopter. Moreover, safety considerations mean a UA can generally get closer to the target than a helicopter"

COMMUNICATIONS AND MEDIA

Use cases in this category exploit a UA’s ability to oversee large areas from above and to dynamically manoeuvre in response to events. In some high-risk use cases, the expendability of a UA can also be an important factor. UA have already been successfully used by movie and documentary makers to film sequences more cost effectively, and by broadcasters to cover news events.

Specific example include:

- Flying-Cam won an Oscar for its SARAH platform, which has been used to film action sequences in movies such as SkyFall.
- Facebook, Alphabet and other internet companies have been looking to use UA to provide an internet service in remote or otherwise underserved areas
- Cellular operators, such as Sprint and Vodafone, have been experimenting with the use of UA to provide temporary coverage during special events.
- CBS News used a UA to examine the current state of the Chernobyl nuclear reactor.

Ideally, the UA will live stream the data or video it captures, particularly if the survival of the UA itself is in doubt or the rationale for the presence of the UA itself is to provide connectivity. The value of providing connectivity in response to disasters or other emergency situations is explored in the next section.

Disaster Response Use Cases

Natural disasters, such as storms, heavy snow, floods, earthquakes, tsunamis and volcanic eruptions, can make land routes and waterways temporarily inaccessible by terrestrial or marine means. Such events might also interrupt the communication infrastructure, leaving the affected area isolated.

In these circumstances, cellular-enabled UA can be deployed to collect real-time data about the scale of the damage caused by the disastrous event (see graphic). Utilising a mobile network, the UA can fly BVLOS and relay information about the disaster zone in real time to the disaster coordination base. Having prompt and correct information helps first responder agencies to distribute aid suppliers effectively and to the places most in need.

The disaster coordination base would generally prepare several mobile-enabled UA, due to their limited battery capacity. Even so employing UA is more cost effective than employing a helicopter. Moreover, safety considerations mean a UA can generally get closer to the target than a helicopter.

The UA flies from the disaster coordination base to the disaster zone, photographs the disaster zone using the installed aerial camera, collects other relevant information via various sensors and sends the data in real-time back to the base via the mobile network. If a speaker has been installed in the UA, voice messages from the disaster coordination base can be delivered to disaster victims via the cellular network, while the voice of victims can be picked up using the microphone mounted on the UA, and relayed back to the disaster coordination base.

If the communication infrastructure is damaged, impeding all mobile communications, UA can provide temporary mobile connectivity by becoming a base station. A small mobile base station installed in the UA can be used to relay the radio waves to and from the closest operational terrestrial base station.

> “employing UA is more cost effective than employing a helicopter. Moreover, safety considerations mean a UA can generally get closer to the target than a helicopter”

Benefits of Using Mobile Networks to Support Unmanned Aircraft

As mobile networks have already been deployed worldwide they are well placed to support the rapid deployment of innovative UA solutions, as well as underpinning on-going applications.

The growing usage of UA means there will be major changes to air traffic: there will be a significant increase in the volume of aircraft and a much higher level of automated operations. Ultimately, there will be an industrialisation of the (lower) airspace with flying robots performing missions with different levels of autonomy, depending on the complexity of their tasks, and the flexibility and capabilities of the UA. Systems will be needed to manage the multitude of flying objects, some acting autonomously, some periodically controlled, or at least, supervised by a remote operator, and all monitored to ensure full control and integration with the general air traffic.

At a very generic level, UA will need connectivity that meets the following requirements:

- Scalable solution, suitable for mass market: Given the high number of connected objects, any solution must be able to support the rapid growth in UA and to deliver a high capacity in the future.
- High reliability and availability: A high safety level is crucial for any implementation.
- Light and easy to integrate solution: Industrialized solutions need to be efficient and dependable: low cost solutions with a low level of complexity and proven track records will be in demand.
- Ready for immediate release: As they are already in use, UA need to be safely and fairly integrated into air traffic management as soon as possible.

Mobile operators have the assets and capabilities to fulfil these requirements:

- Standardised and scalable solution for worldwide connectivity: Mobile networks are used by billions of devices worldwide, which take advantage of the harmonized and standardized technologies defined by the 3rd Generation Partnership Project (3GPP) [5]. Globally available, mobile networks provide very cost efficient solutions: No investment is necessary to roll out a new infrastructure. In addition, mobile networks continue to evolve to match the evolving needs of UA communication platforms.

- **Licensed spectrum:** Working with dedicated spectrum in licensed bands enables mobile networks to provide the reliable connectivity required for mission-critical applications, especially in BVLOS cases and in high-risk environments.

- **Secure communication channel:** Mobile networks provide specific encryption mechanisms to protect communications against misuse, achieving high standards of data protection and privacy.

- **Law enforcement:** Mobile networks can support the lawful intercept of communications from the UA, as they do with mobile devices. Mobile operators can also provide independent verification of the location of the UA for use by the UAS (Unmanned Aircraft System) traffic management.

- **Identification through the SIM (Subscriber Identity Model) credentials and IMEI (International Mobile Equipment Identity):** The credentials established for mobile network authentication can meet the need for unique and trusted identification of UA.

Harnessing Mobile Connectivity

In general, UA are controlled using unlicensed Industrial, Scientific and Medical (ISM) spectrum bands, with the range between the UA and the pilot limited by the transmit power and frequency band used. Global, ubiquitous, scalable, secure and reliable, mobile networks can provide connectivity beyond the limited range that ISM frequencies can support: A UA controlled over the mobile network will theoretically have the same range as the mobile network coverage (assuming the network can deliver the data rates required of the UA). To ensure reliable communication, the mobile operator can control and monitor the quality parameters of the connection and provide appropriate service quality for supporting UA. The extensive coverage of mobile networks allows for long distance flights, which could not be realised by conventional UA communication.

Mobile connectivity can support the operation of a UA in a number of ways. It can support communications:

- between UA, by leveraging the work done in 3GPP on what is called sidelink communication, which can support UA identification and collision avoidance.
- between the UA and the UA operator to provide payload data, information relevant to the correct operation of the mission, for issuing command and control support.
- between the UA and traffic management for providing required information, command and control support.

In essence, mobile networks can enable monitoring of the UA's position, altitude, speed, radio condition, camera footage and any other information, controlling all operations from take off to landing.

Mobile networks are already used for UA operations in two different modes: through a ground control centre connected to a smart phone, or by having a built-in mobile connection in the UA. Both modes harness the capabilities of mobile networks, but only UA with built-in cellular connectivity can truly harness BVLOS and take advantage of all the other benefits described in this chapter. Furthermore, built-in connectivity allows for mobile network-based identification of the UA, true end-to-end security, accurate and protected location information and support for law enforcement requirements (see subsequent sections).

As mobile networks are widely deployed, they provide a ready-to-use infrastructure to support UA operations, particularly for BVLOS. A requirement to fly VLOS is one of the biggest barriers to achieving the full potential of UA applications, particularly for enterprises and disaster response as described in the Use Cases section. Utilising the existing mobile networks will eliminate the need to deploy a new infrastructure and, therefore, help to ensure connected UA are economically feasible.

Mobile networks will enable new services to proliferate for UA: mobile connectivity can supply the UA with information beyond the normal telemetry data that the UA can collect itself. Once the UA is cellular connected, it will have access to information about changing weather forecasts, ad-hoc emergency incidents and real-time information communicated from air traffic control, enabling innovation to develop and flourish.

Moreover, the manual tasks that a UA operator has to do prior to a flight could be completed remotely via cellular connectivity.

Mobile networks are constantly evolving to support the emerging services and needs of multiple industries. Many mobile operators already run 4G LTE (Long Term Evolution) networks, which can deliver high-bandwidth, low latency connectivity with an exceptional quality of service that's designed to scale. The wide range of capabilities of 4G networks can be used by the UA industry to create innovative services. The next evolution of mobile technology, 5G, is designed to connect many more devices, while delivering even faster transmission and lower latency.

> “Utilising the existing mobile networks will eliminate the need to deploy a new infrastructure and, therefore, help to ensure connected UA are economically feasible”

Transmitting Data in Real-Time

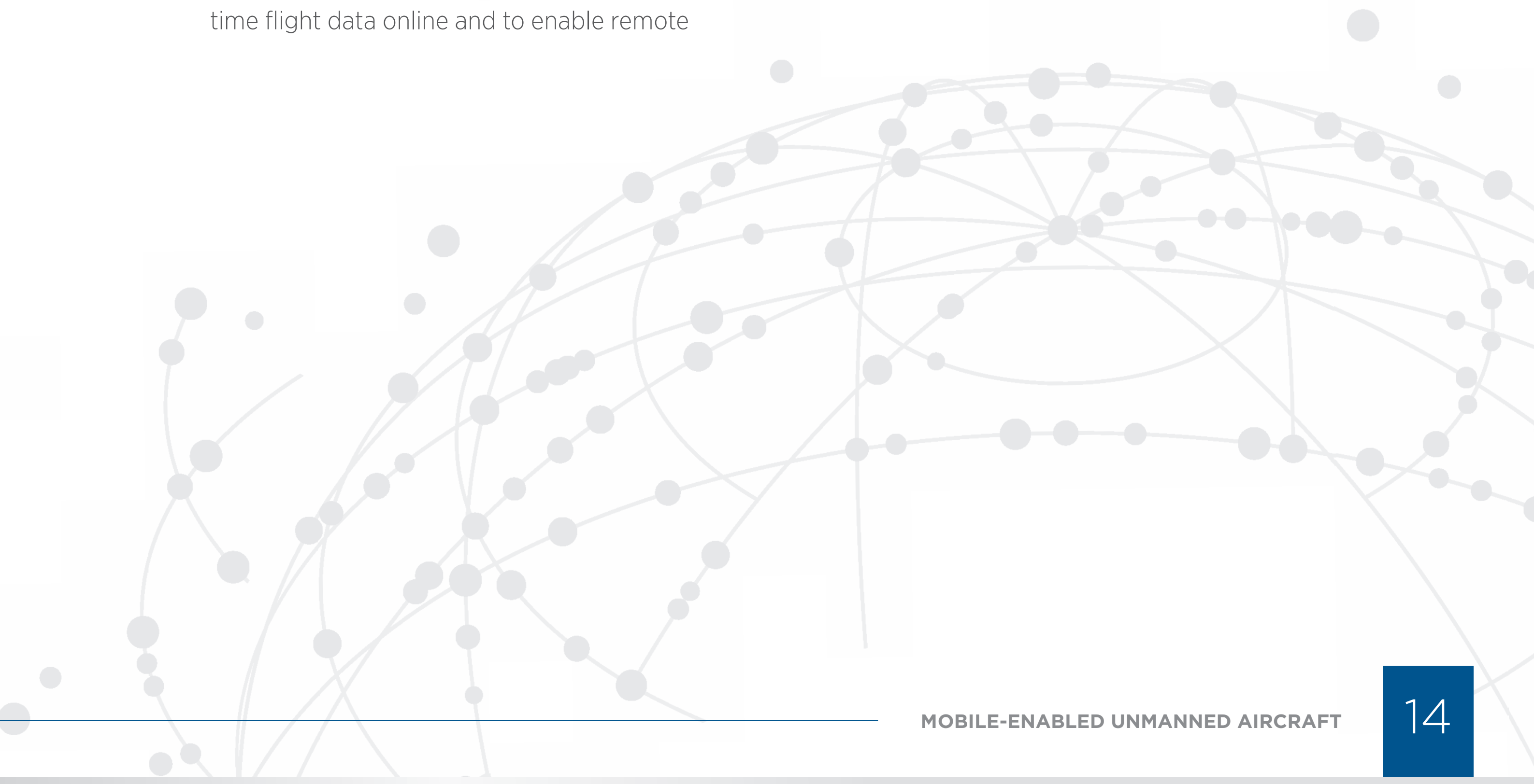
Mobile networks provide a secure mechanism to deliver data relevant to a particular use case. Traditionally, such information is called the “payload”.

Some examples of payload communications are:

- Video/images that are not used for flying, such as pictures of a construction site used for planning.
- Sensor outputs.
- Data for understanding and monitoring the status of the UA.
- Transfer to the ground of raw or processed data collected by the payload sensors.

Mobile networks provide a proven mechanism for storing the real-time data in a remote location, as required by the specific UA service.

The use of mobile connectivity to share real-time flight data online and to enable remote operators to interact with a UA pilot would lead to the emergence of many new use cases. Companies and consumers could save time and money if they could make a real-time request for a UA in-flight to take a photograph or collect some specific data. Whilst flying, the pilot can get direct instructions on how to make an optimal flight, drawing on the user or customer feedback online. Pilots will have safer flights because they will focus on flying conditions, whilst remote operators focus on images, or the other way round. As with connected cars, UA manufacturers and service companies could receive real time alarms about failures or potential failures, thereby preventing accidents and reducing maintenance costs.



Cybersecurity in the UA Ecosystem

The UA ecosystem, as with any distributed system, must pay special attention to cybersecurity risks. This section explains how cybersecurity can be addressed to engender trust in the UA ecosystem and how mobile networks can help to achieve secure solutions. The overall system needs to be secure, while remaining affordable and flexible.

To efficiently identify and locate UA, as well as enable information acquisition, the treatment of data, and the delivery of the relevant actions, each component of the ecosystem must be correctly identified and trusted. It is, therefore, vital to authenticate each component of the ecosystem, and encrypt the data exchange between them.

Two sub-systems need to be considered:

1. When used for business purposes, UA are potentially collecting and uploading sensitive data into a cloud environment. In this context, secure connectivity and information exchange is key for protecting people, companies, and strategic country assets. The IoT Institute shows how hacking is a major security issue for UA, as highlighted in this article from Forbes [13]. According to E&T Magazine, UA are wide open to hijack threats [14], UA hijacking will become a practical reality in the coming months.

2. For traffic management, the systems implemented need to enable safe, secure and efficient low-altitude operations. For full traceability, the systems have to cover the full flight lifecycle from before operations, during flight, and after completion.

UA manufacturers and UA operators need to protect their assets and services, whereas public authorities need to build systems that ensure citizen safety and law enforcement. This ecosystem needs trust at every stage, from manufacturing until deployment through to flights and post flight operations.

The telecommunications industry, which the GSMA represents, has a long history of providing secure products and services to their customers. The GSMA has published a comprehensive set of security guidelines [10] for the IoT that are also valid for UA. In particular, the overview document analyses the case of a personal drone and makes recommendations to help develop a secure system. The GSMA has also developed the GSMA IoT Security Assessment [11], which is a flexible framework that helps companies to provide secure Internet of Things solution based on the GSMA IoT Security Guidelines.

There are several aspects that need to be considered for securing UA communication and protecting data. Mobile networks can help to achieve a secure system. Some examples are listed below:

Secure registration of pilots and their UA: The registration of pilots and their UA on public authority servers needs to be secure and reliable. This is the first step for ensuring trusted flights. Public authorities need to verify the pilot's ID and check that they hold a valid license, if applicable. They also need to link each UA with a pilot, just like a vehicle's license plate links it to a driver, so if the UA goes off course, for example, the authorities can contact the pilot immediately. In some cases, mobile networks can support the pilot registration, as described on page 22 in the section 'Registration'.

Protection of sensitive data: Sensitive data could include data stored in the UA, such as firmware, software versions, allowed flight boundaries (e.g. maximum altitude limits, distance from the take-off) or data exchanged between the UA and the pilot, including commands or service related information, such as the full flight traceability. Mobile networks provide secure communication from the UA and the network, while allowing the service provider to encrypt end-to-end the data. The GSMA IoT Security Guidelines [10][9] makes several recommendations based on a risk assessment.

Seamless and secure connectivity: For easy deployment worldwide, manufacturers need to be able to connect their UA seamlessly and securely to networks in any country. Mobile networks provide secure connectivity around the world as explained in the section on Harnessing Mobile Connectivity-Connectivity.

Reliable UA location: Public authorities need to be able to identify UA and locate them, anywhere and in real-time, reliably. UA location data comprises digital IDs, such as serial numbers, and any related dynamic data (such as location, time), and this data must not be modified during the flight. Mobile networks can help to verify the information provided by the UA, as described in the section Positioning and Location Services

Enabling Accurate Identification

From their inception, mobile networks have been required to provide secure identification, in a manner that can be readily handled by IT systems and at a scale compatible with consumer and business use (billions of devices worldwide). Identification in mobile networks occurs in several layers; which have parallels in the UA world:

1. Identification of the hardware: Cellular networks employ a global hardware identifier (the IMEI). This is tied to the device, as it is stored on the electronics motherboard. For a UA, some means would need to be found to tie such an identifier for the electronics package to the visible identifier of the airframe.

2. Identification of the access service subscription: This ID identifies both the service provider and the individual wireless access subscription (not the subscriber or user). The identifiers used are allocated globally, in a hierarchical manner via national administrators (the international mobile subscriber identity or IMSI). For added privacy and security, these identifiers are replaced by random temporary IDs after initial registration on the network (temporary mobile subscriber identity, TMSI). The use of these identities is somewhat analogous to license and mission identification in UA, so something similar to the IMSI/TMSI structure should be possible. For example, the authorities could issue a permit that is semi-permanent and secured, such as an IMSI, for the licensing of a device to use the airspace, supplemented by a TMSI for identification of the use of that license for a specific mission.

3. Service-specific identification: For communications services this is a phone number, email address or equivalent. These are typically of global significance, though are commonly allocated by region and or service provider. The analogous identification in the UA world might have a specific identifier type applied to a specific type of user service, such as surveillance or package delivery, which would need to be unique in context, but not necessarily globally.

4. User identification: In telecoms, users are identified on an ad-hoc proprietary basis, and may use various identifiers from different sources, with varying levels of security and uniqueness. These include a drivers' license number, passport number, phone number, email address, etc. The GSMA is working to create a standardised identity extraction layer that can be used for user identification. It should include the ability to determine both global and contextual uniqueness for the identity, and thus could also be applicable to identification of the human or entity controlling the UA and/or its current mission.

Positioning and Location Services

With many new technologies, the initial approach to solving certain problems is not necessarily part of a final mandated solution. There are already millions of UA flying today without a proper identification system and without any traffic management (UTM) system. Many of these UA have no mechanism by which they can be located, and rely on the operator maintaining VLOS with the UA. More advanced designs have a built-in GNSS (Global Navigation Satellite System) receiver which can report the UA location, altitude and speed to a GCS.

There are many UTM projects being developed, but it will be some time before the first solutions are deployed. Clearly, all will require that the location of the UA is known to the UTM.

Whilst a separate GNSS (Global Navigation Satellite System) could continue to be built-in to the UA, these days most LTE chipsets contain an integrated GNSS receiver, which can provide this information with no additional weight penalty. The UA can then report its location to the UTM or other ground systems using the LTE network. Reporting may be periodic or queried. Similar to identification, the location information can be stored by the UTM for access by a law enforcement agency. Such data can also be used by the UTM to check the UA is complying with the approved flight plan.

Mobile networks can also offer other positioning solutions that will allow independent verification of the location reported by the UA. This is important as GNSS is vulnerable to being jammed, or spoofed into reporting a false location. LTE supports a variety of network-based location solutions such E-CID (Enhanced Cell ID), whereby the strength of the radio reception is used to estimate the location of the LTE modem. Another approach uses OTDOA (observed time difference of arrival) whereby the modem measures and reports the difference in arrival times of special signals transmitted by all cell sites (similar to the Global Positioning System, GPS, but using cell sites rather than satellites).

These capabilities have been standardised by 3GPP within a common framework known as the Location Services (LCS) architecture (Stage 2 references [6] and [7]). These specifications describe the mechanism by which measurement reports are provided to the network, but not the algorithm by which location is estimated. Hence there remains scope for innovation. For example, Vodafone recently demonstrated the ability to track a UA using its radio positioning system (RPS) technology, which is a variant of the E-CID technique and hence independent of GNSS (reference [8]). Although RPS is not widely used at the moment, given the ubiquity of GNSS receivers in LTE modems, this trial nonetheless demonstrates that such techniques can be used to complement and verify any GNSS-based location information received from a UA.

Through the GSMA, mobile operators are looking to further develop these services and work together with UA manufacturers to ensure compliance with UTM requirements.

Law Enforcement

Mobile networks can help UA comply with law enforcement (LE) requirements. While many LE requirements are country-specific, some are consistent around the world. For example, remote identification and tracking are basic LE needs that the GSMA and various cellular standardization activities are looking to support to ensure international adoption of mobile-enabled UA. LE needs this information to perform threat discrimination, determine nefarious intent associated with the use of a UA, and perform UA crash investigation. The ability to link a UA operator to a UA is also critical for LE.

Tracking and identification capabilities can help determine whether or not a UA violated restricted airspace, the likely whereabouts of the UA, whether or not the UA is still in the air, and the likely whereabouts of the operator of the UA in the event LE has the need to contact them concerning a particular UA flight. For example, if the UA has crashed, the unique identifier (i.e., similar to an auto license plate) physically associated with the UA can be used to identify the registered owner who can be contacted to assist with locating the UA pilot.

Tracking solutions from an LE perspective must take into account both real-time (i.e., where is the UA now, and where is the UA operator now) and historical information (i.e., from where did the UA take-off, where was the UA operator upon UA take-off, what was the flight path of the UA, where was the UA operator during the UA flight, where did the UA land or crash, where was the UA operator when the UA landed or crashed).

The Section Positioning and Location Services describes how mobile networks help to verify and provide the correct position of the UA to the authorized users (UA operators and UTM).

From the perspective of LE, tracking a UA includes two vital aspects:

1. tracking the geographical coordinates, altitude, and time stamp of the UA, and
2. tracking the geographical coordinates, altitude, and time stamp of the UA control station (which could default to the take-off location if real-time knowledge of the whereabouts of the UA control station (whether stationary or in motion) is not available.

From the perspective of LE, it is also desirable (although not a strict requirement) to be able to access a flight plan for a UA (if it exists).

Technical solutions for remote identification and tracking must take into account the needs of air traffic control (ATC) communities and the general public (see also [12]), as well as LE agenices. Note, mobile networks do not provide identification and location information to LE agencies directly: mobile networks provide services for identifying UA and provide location information to the authorised users, such as UA operators and UTM. It is then the responsibility of these users to provide the required information to LE.

Lawful interception of communications to/from a UA is also an important capability for LE. This can be supported by existing cellular network lawful interception procedures based on the relevant identities (e.g., IMSI, IMEI) provided by LE in a valid court order issued to a cellular operator. Lawful interception for mobile networks is defined by 3GPP in the specifications [15], [16] and [17]. From an LE point of view, the use of cellular technology that already supports lawful interception of communications is an inherent advantage of cellular technology over other UA communications mechanisms.

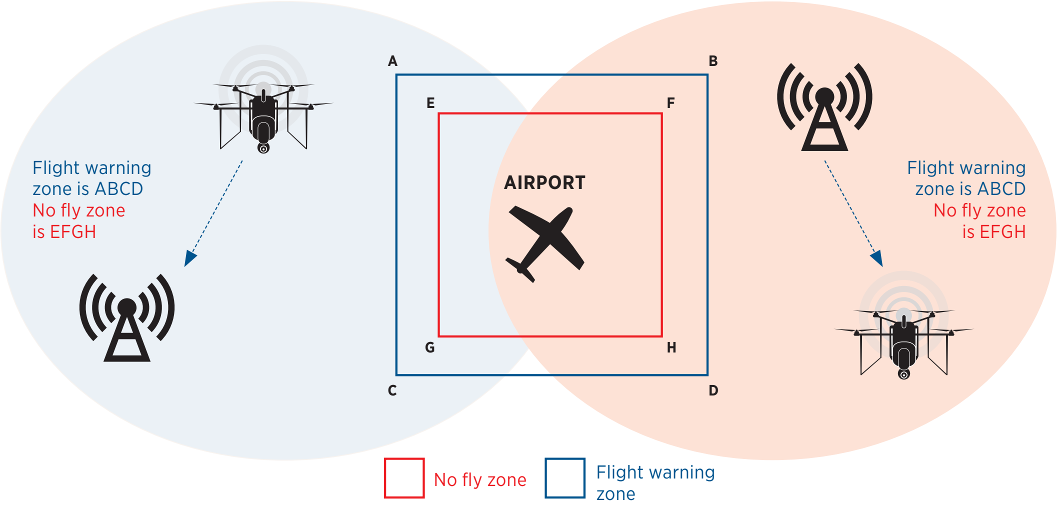
No Fly Zone Management

A mobile operator's network can be used to restrict UA flight operations from specific areas. These restrictions could be related to safety (near an airport for example), security (near sensitive government installation), or privacy (flying over private property). The cellular network can be used to transmit the coordinates of a flight advisory area.

- The flight advisory area can be in the form of a geometric shape (simple polygon shown below). The geometric shape can be in the form of a circle (single point defined with a radius) or a polygon (three to "n" coordinates defined).
- Cellular towers can periodically transmit, via the cellular signalling channel or packet data connection, the following data:
- Latitude/longitude coordinates that define the flight advisory zone
- Action to be taken by UA (examples are caution, turn around, or land immediately)
- UA will receive the flight restriction broadcast and adjust flight path.

Flight advisory zones can be static or ad hoc

- Static – typically used for a fixed facility, such as an airport. The size of the flight restriction zone can be dynamically changed through modification of the existing geometric coordinates.
- Ad hoc – typically used in live situations, such as vehicle accidents or security incidents, where the airspace needs to be clear of unauthorized UA.



An approved civil aviation authority, local government official, or NASA UTM may define the flight advisory areas. The UA can validate the legitimacy of a received message with the certificate of the sending entity.

Registration of UA

In several countries, UA regulations mandate registration of the aircraft and the pilot. For uniquely identifying a UA, LA agencies typically want to be able to associate it with the personal information of the UA owner(s) and operator(s). Names, dates of birth, home/business addresses, gender, and phone number(s) can enable LA to contact relevant individuals as necessary to assist with maximizing public safety.

Similarly, some countries require SIM card registration: consumers need to provide proof of identification in order to activate and use a mobile SIM card. Mobile operators, therefore, have experience of applying customer and device registration requirements, which could also support UA registration.

Unmanned Air Traffic Management

The vast majority of the low-altitude airspace used by UA is uncontrolled and not managed by air traffic management (ATM). Conventional ATM relies on voice communication between air traffic controllers and pilots, so cannot be used for unmanned operations. Furthermore, the existing ATM system is not designed to handle the likely high density of UA traffic, which will probably be several orders of magnitudes higher than the density of manned aircraft.

A UA traffic management (UTM) system needs to safely accommodate a large number of VLOS and BVLOS UA operations without reducing the safety of current manned operations in low-altitude airspace, which is also used by general aviation, helicopters, gliders, balloons and parachutists.

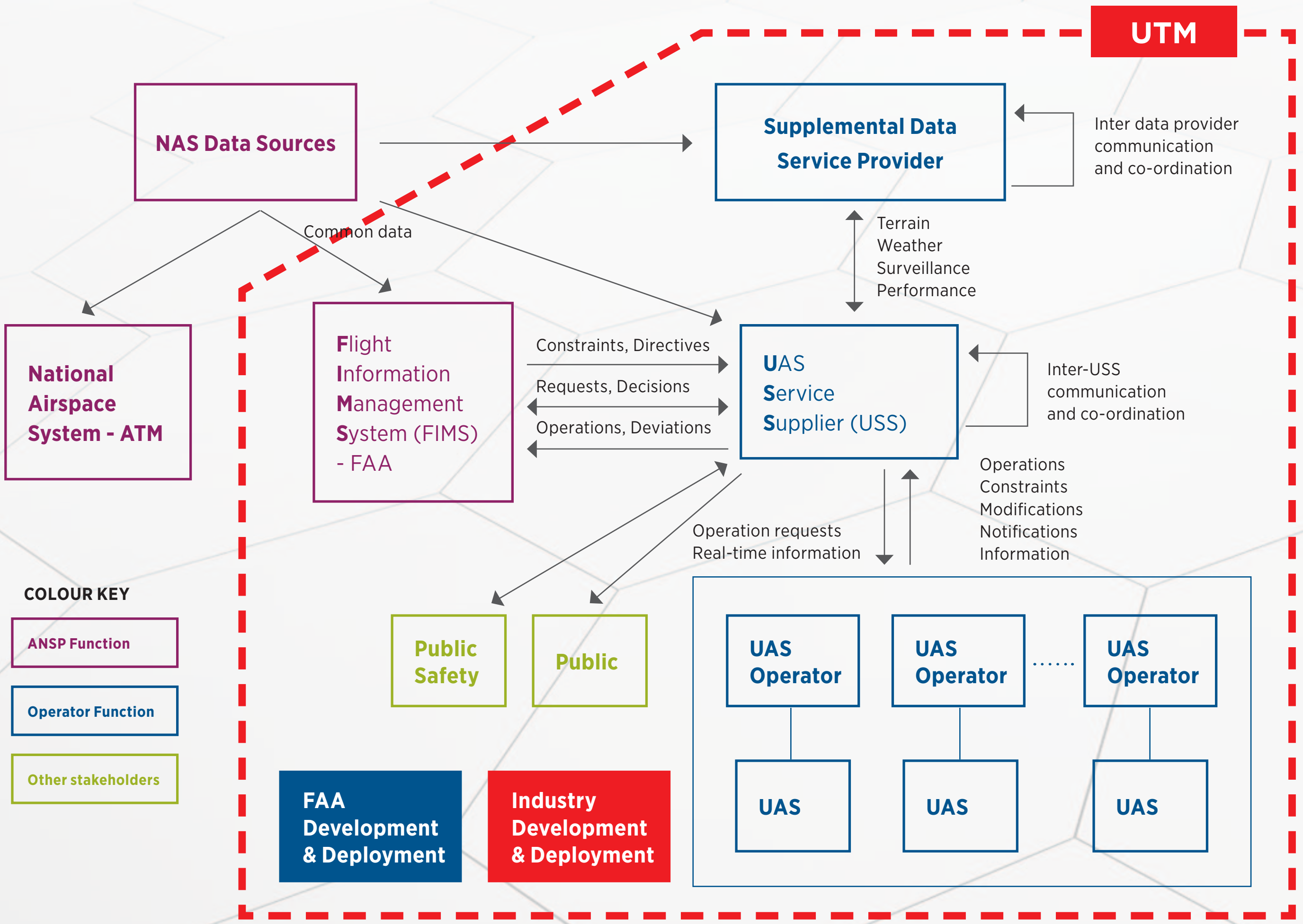


Figure 1: NASA UTM Architecture (source [2])

The UTM architecture [3] proposed by National Aeronautics and Space Administration (NASA), the US regulator, (see Figure 1) establishes the performance requirements based upon use case categories, operational environments and other factors. The regulator is responsible for defining and updating airspace constraints as necessary in real time. It may add static or dynamic geo-fences and provide notifications to the UAS service supplier (USS). The USS will play the central role in the UTM system and is responsible for airspace authorisation, UA identification, real-time UA tracking and providing updates of weather and airspace constraints to the UA operators. The USS will also provide mission-specific information and operator identity as legally required to law enforcement, regulators and other government agencies.

The ability of the mobile network to independently verify the identity of the UA and the subscriber using IMEI and IMSI is a valuable service that can be offered to the UTM.

As discussed in the previous chapter, many mobile chipsets have integrated GNSS receivers which can provide the current position and speed of the UA. The UA can report its location to UTM using the LTE network. In the future, Cellular Vehicle to Everything (C-V2X) technology, already standardized by 3GPP in Release 14, can be used to enable the UA to broadcast its identity and location directly to a C-V2X equipped device on the ground.

The UTM can also use a mobile network to provide real-time updates on airspace constraints, geo-fencing and alerts to UA operating in BVLOS. Mobile networks can also deliver weather updates that can be used in real-time by the UA's software to decide whether to adjust its mission.

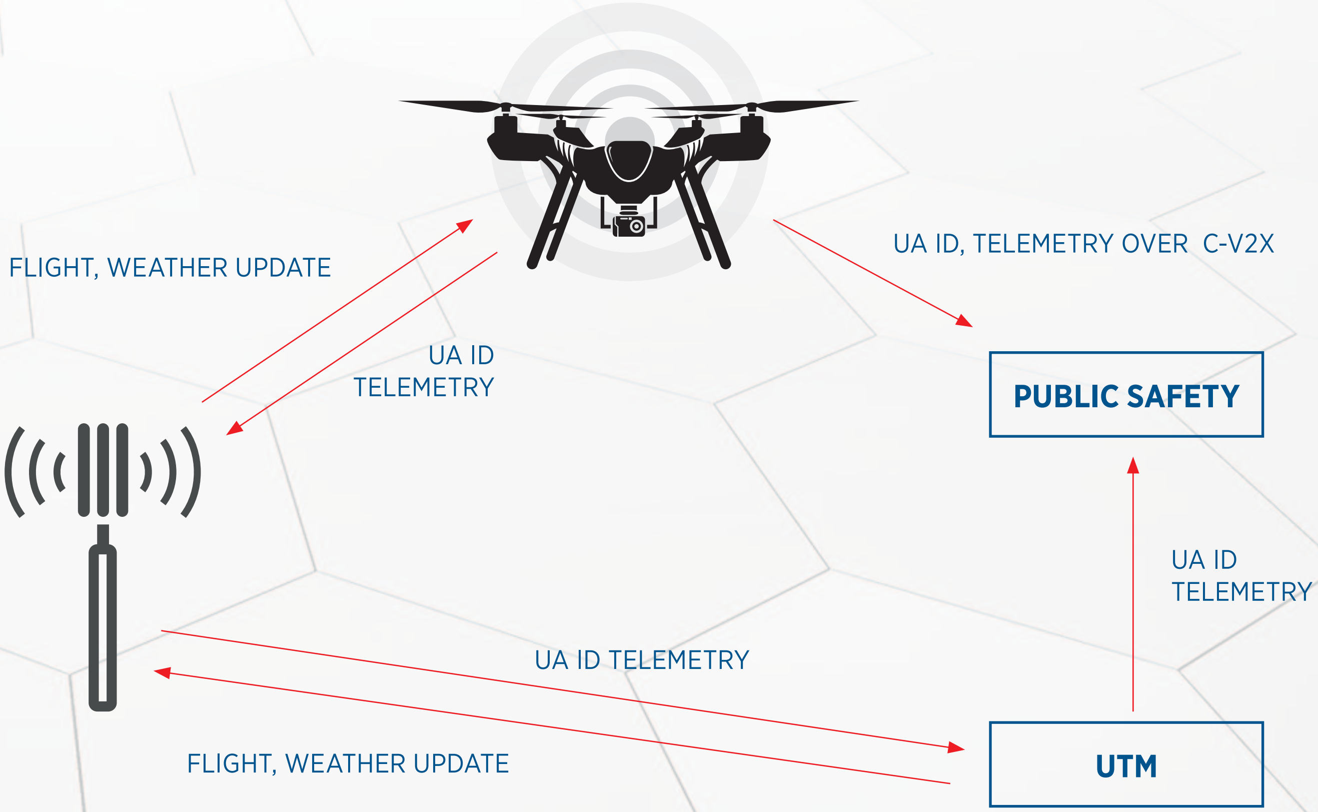


Figure 2: Use of Mobile network for UTM

3GPP’s Support for UA

The 3GPP is the global standardisation body covering the predominant cellular technologies in the world, including GSM (Global System for Mobile communication), UMTS (Universal Mobile Telecommunications Service), LTE, and now 5G. To address the anticipated usage of cellular technologies by UA, 3GPP has produced a study on enhanced LTE support for aerial vehicles ([9]). Started in 2017, the study identifies potential improvements that could be developed to more efficiently handle UA traffic and its impact on the network. The initial study focused on LTE, which is widely deployed, but the intention is that the lessons learned will be applied to 5G.

THE SCOPE OF THE STUDY

UA have several characteristics that mark them as a unique class of device. Principal among those are that UA are generally high up. This means that it terms of footprint, they can both see and be seen by large portions of the radio network. This has implications for both received signals and interference. As UA also exhibit different behaviour and can be subject to different radio conditions from other devices, the 3GPP study revisited its traffic and channel models to ensure that they were applicable to UA.

The study also considered regulatory and network management requirements

THE TRAFFIC MODEL

The 3GPP study evaluated the characteristics of UA in radio environments, corresponding to urban microcells, urban macrocells, and rural macrocells. The simulations tested scenarios with a single UA as well as those with hundreds of UA.

The study also evaluated different types and mixtures of traffic. In addition, 3GPP developed a new channel model to address UA during their complete flight profile (from take off to landing). The specific assumptions used in the evaluation as well as the test and simulation results can be found in the study itself ([9]).

3GPP STUDY RESULTS

Drawing on extensive simulations, supplemented by field trial data, the study confirmed that UA exhibit unique characteristics compared to terrestrial devices. In particular, due to their higher altitude, UA are able to see and be seen over a wider footprint. This leads to increased uplink (UL) and downlink (DL) interference.

In general, the extra interference was manageable in rural environments: the UA were able to maintain the targeted throughput and communications reliability. The simulation assumptions and target performance characteristics are given in the 3GPP technical report [9].

Urban areas were more challenging. In many cases, the UA were not able to maintain acceptable mobility functions (excessive handover failures, etc.). However, these results did not take into account various interference mitigation strategies that can be applied. Many of these are already supported and can be applied immediately. These are discussed in the next section.

MITIGATIONS

There are various techniques that can be used to improve LTE support for UA. Some of these are implementation techniques that require no specification changes. There are other improvements that have minor specification impacts and still others that require more extensive work within 3GPP. Most of these improvements need to be made in the urban macrocell environment, since that was the most problematic.

Downlink interference mitigation techniques – These focus on reducing the amount of interference that the UA itself experiences. The various available techniques include FD-MIMO (full dimensional multiple input multiple output), direction antennas on the UA, receive beamforming in the UA, intra-site JT-Comp (joint transmission), and coverage extension (techniques to enhance synchronization and initial access) that are already supported by 3GPP. No additional specification work is needed to implement these improvements. In addition, it may be possible to use coordinated data and control transmission (inter site), but more study is needed and there would likely be significant specification impacts.

> “due to their higher altitude, UA are able to see and be seen over a wider footprint. This leads to increased uplink (UL) and downlink (DL) interference.”

Uplink interference mitigation techniques – This focuses on reducing the interference that terrestrial users experience due to UA in the air. Some techniques such as FD-MIMO and directional antennas on the UA are already supported by 3GPP and can be used now. In addition, there are various power control-based mechanisms that can be used to minimize interference. Although these require specification work, some of the necessary changes are minor.

Mobility enhancements – While reducing the interference will address the root cause of the mobility issues found in high-density environments, improvements could also be made to the mobility algorithms themselves. The study identified opportunities to provide additional measurement or flight path information that could be used by the algorithms in making mobility decisions.

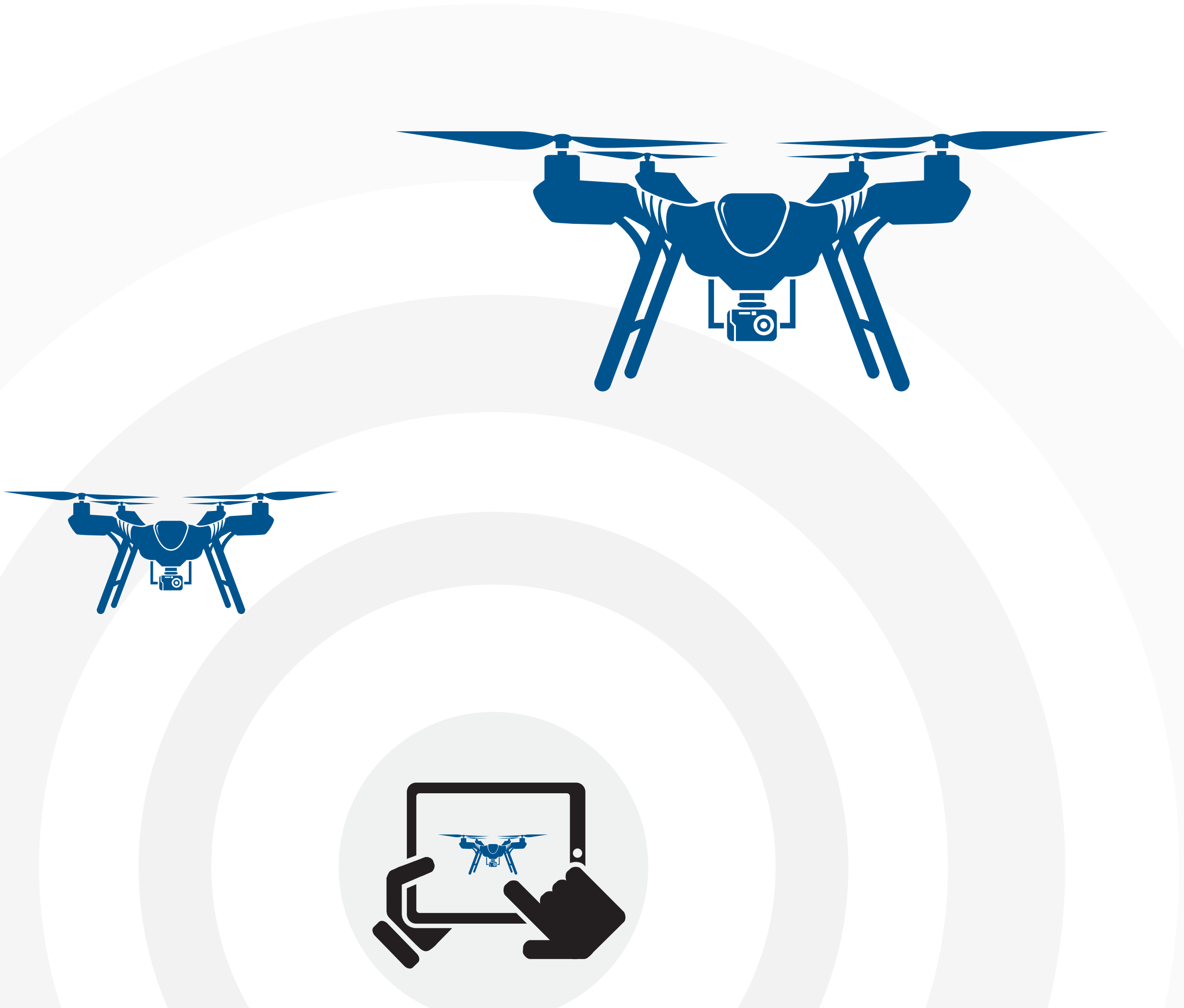
Aerial UE identification – This is an area requiring further work by 3GPP. It encompasses:

1. Identifying that the UE is in-flight (so that appropriate mitigations can be applied). This may be achieved from the UE-based reporting, e.g., in-flight mode indication, altitude or location information, or by the mobility history information available in the network.

2. Identifying whether the UE is permitted to fly (i.e., usage as a UA is permitted). This would likely be related to UE's indication of radio capability to the network in combination with the subscription information, which requires additional specification work within 3GPP. The aerial usage certification/licensing information for a UE may be provided from (non)-3GPP node(s) to a 3GPP node.

Follow Up Steps

The completed study is only the start of 3GPP's work on UA. 3GPP's next step is to work on improving mobility performance and the identification aspects of UA. Power control will also be improved. In addition, the lessons learned for LTE will be adapted for the New Radio (NR) technology, which is part of 5G.



CONCLUSIONS

The variety of capabilities and features offered by mobile networks can play a significant role in the UA ecosystem. To support BVLOS, there is a clear requirement for radio access coverage, which requires an infrastructure. Mobile networks, which currently serve more than 5 billion unique subscribers in the world, can provide this infrastructure. They support 8.4 billion connections, of which 0.5 billion are already for M2M (Machine to Machine) and IoT [18].

UA can operate securely and safely on existing 4G LTE networks and will also be supported by the cellular networks of the future, including 5G. Mobile networks deliver global interoperable and secure connectivity based on global 3GPP standards, supporting a variety of capabilities from low to high latency and throughput, and different level of quality of services. Moreover, the use of licensed spectrum provides mobile operators with the ability to better control the available resources. While LTE networks are well suited to support the initial deployment of UA, 3GPP is already working on optimising cellular networks to further improve support of UA in the future.

Glossary

Term	Description
3GPP	3rd Generation Partnership Project
ATC	Air Traffic Control
ATM	Air Traffic Management
BVLOS	Beyond Visual Line Of Sight
C-V2X	Cellular Vehicle to Everything
DL	Down Link
E-CID	Enhanced Cell ID
FD-MIMO	Full Dimensional Multiple Input Multiple Output
GCS	Ground Control Station
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GSM	Global System for Mobile communication
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
ISM	Industrial Scientific and Medical
JT-Comp	Joint Transmission
LCS	Location Services
LE	Law Enforcement
LTE	Long Term Evolution
M2M	Machine to Machine
NR	New Radio
OTDOA	Observed Time Difference of Arrival
RPS	Radio Positioning System
SIM	Subscriber Identity Model
TMSI	Temporary Mobile Subscriber Identity
UA	Unmanned Aircraft
UAS	Unmanned Aircraft System
UL	Up Link
UMTS	Universal Mobile Telecommunications Service
USS	UAS Service Supplier
UTM	UAS Traffic Management
VLOS	Visual Line Of Sight

About the GSMA

The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 300 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 industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai, Mobile World Congress Americas and the Mobile 360 Series of conferences.

Follow the GSMA on Twitter: @GSMA

GSMA™

Floor 2, The Walbrook Building
25 Walbrook, London EC4N 8AF UK
Tel: +44 (0)207 356 0600

www.gsma.com/IoT
IoT@gsma.com