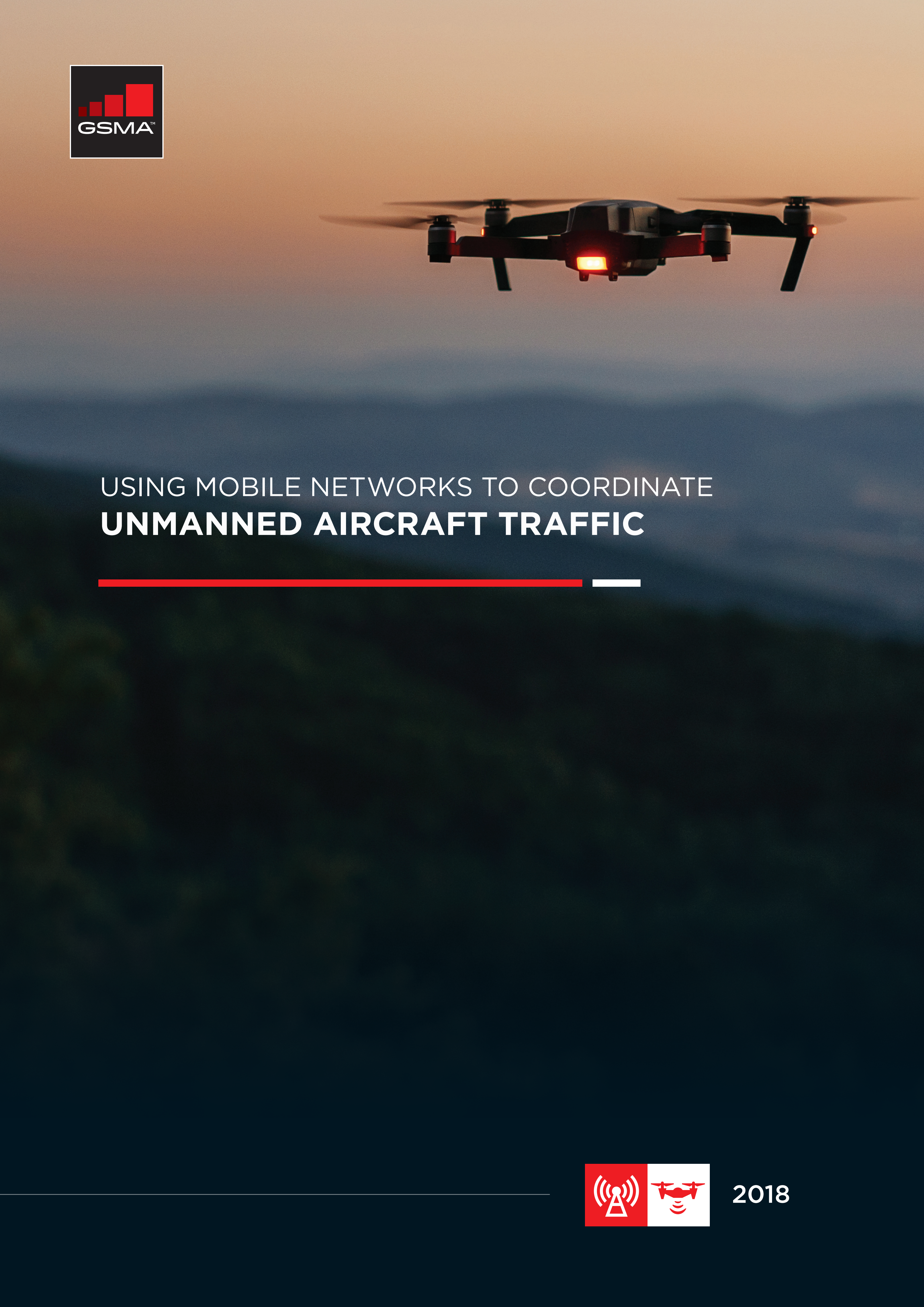


USING MOBILE NETWORKS TO COORDINATE UNMANNED AIRCRAFT TRAFFIC

2018

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with over 350 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 the GSMA corporate website at www.gsma.com.

Follow the GSMA on Twitter: @GSMA.

About the GSMA IoT Programme

The GSMA Internet of Things programme is an initiative to help operators add value and accelerate the delivery of new connected devices and services in the IoT. This is to be achieved by industry collaboration, appropriate regulation, optimising networks as well as developing key enablers to support the growth of the IoT in the longer term. Our vision is to enable the IoT, a world in which consumers and businesses enjoy rich new services, connected by an intelligent and secure mobile network.

Visit gsma.com/iot to find out more.

TABLE OF CONTENTS

1. Executive Summary

In developed markets, such as the United States, the number of unmanned aircraft (UA) has quickly surpassed the number of regular aircraft and continues to grow rapidly. Growing at more than 50 per cent per annum.

This growth is taking place despite severe limitations on commercial UA flights, notably the need for pilots to keep the aircraft in sight. At the same time, the wireless technologies used to control UA have a very limited range, restricting the usefulness of these aircraft. If pilots were able to operate unmanned aircraft beyond-visual-line-of-sight (BVLOS), UAS could be used for many new applications, such as inspection and surveys, transport and logistics, surveillance and monitoring, and communications and media. Safe BVLOS operations would also enable UAS to play a much greater role in disaster response and law enforcement.

The next step would be to move to full automation, which could reduce the operating cost per mission more than 100 fold, as the cost of each flight falls towards the cost of electricity (as little as one cent) and the depreciation of the equipment involved. Reliable, secure and cost-effective cellular technologies, such as LTE and 5G, could help enable BVLOS operation of UAS and ultimately full automation. These technologies are capable of system performance levels that would satisfy aviation regulators' concerns about automated flight, while also being cost-effective enough for widespread adoption.

Enabling the industrialisation of the lower airspace

With a significant increase in the volume of aircraft and a much higher level of automated operations there will ultimately be an industrialisation of the (lower) airspace: flying robots will perform 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

Both national and international authorities are investigating the development of a new traffic management ecosystem for unmanned operations that is separate, but complementary, to the existing air traffic management (ATM) systems used for commercial aircraft. Normally referred to as unmanned traffic management (UTM), the proposed systems would manage both visual and BVLOS UA activities at low altitudes, generally below 400 feet.

Wireless connectivity will be required to deliver many facets of UTM, such as registration and identification, flight planning and approval, the transmission of meteorological information, geo-fencing, geo-caging and tracking. Mobile operators have the assets and capabilities to fulfil the UTM requirements:

- **Existing infrastructure:** The existing mobile networks can be reused without the need to deploy dedicated infrastructure for coverage in the air. Mobile networks support a standards-based approach and, therefore, offer a scalable connectivity solution: Mobile networks take advantage of the harmonisation

[3] 3GPP http://www.3gpp.org/

and standardisation of cellular technologies defined by the 3rd Generation Partnership Project (3GPP). With a global mandate, 3GPP continues to develop the capabilities of mobile networks.

- **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 could help national security and law enforcement agencies to identify and monitor UAS that may be of interest, by enabling the near real-time recording of UAS flight information in a UTM, as well as remote identification and tracking. This information could be used to perform threat discrimination, to determine nefarious intent associated with the use of a UAS, and to perform UAS crash investigations. Mobile operators can also provide independent verification of the location of the UAS for use by the UTM, while supporting lawful intercept of communications from the UAS.
- **Identification capabilities** through the SIM (Subscriber Identity Module) credentials and IMEI (International Mobile Equipment Identity): The credentials established for mobile network authentication can meet the need for unique and trusted identification of UAS: Identity regulation is likely to be mandated ahead of the availability of UTM in most countries. The ability to link a UAS operator to a UAS is also critical for law enforcement

The evolving capabilities of mobile networks

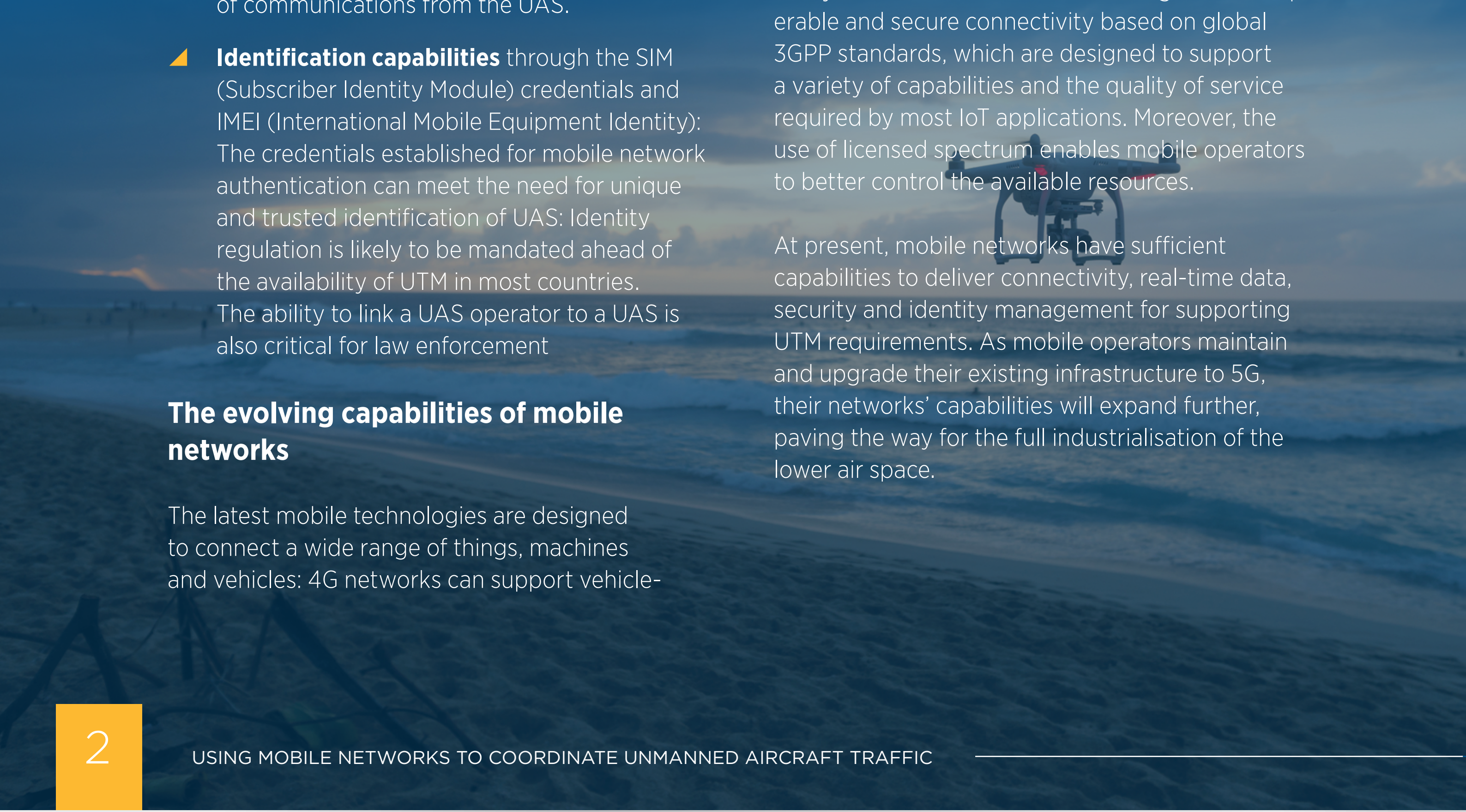
The latest mobile technologies are designed to connect a wide range of things, machines and vehicles: 4G networks can support vehicle-to-vehicle communications, which can be used for collision detection and avoidance. Low power wide area technologies operating in licensed spectrum (LTE-M and NB-IoT) are well suited to providing position and identification information.

Moreover, the evolution of cellular networks towards 5G will bring a whole new set of capabilities that can be utilised for UAS operation and UTM operations, such as:

- Higher bandwidth, allowing enhanced payload data transmission capabilities, such as high resolution video.
- Lower latency, enabling faster command and control (C2) link and detect and avoid triggered by off-board data sources.
- Multi access edge computing, offloading detect and avoid compute from vehicles to lower the overall vehicle cost.
- Network slicing, allowing the creation of a dedicated virtual slice with optimised configuration for UAS and UTM operation support.
- Higher reliability.

In conclusion, mobile network operators can and will play a key role in the emerging UAS and UTM ecosystem. Mobile networks deliver global interoperable and secure connectivity based on global 3GPP standards, which are designed to support a variety of capabilities and the quality of service required by most IoT applications. Moreover, the use of licensed spectrum enables mobile operators to better control the available resources.

At present, mobile networks have sufficient capabilities to deliver connectivity, real-time data, security and identity management for supporting UTM requirements. As mobile operators maintain and upgrade their existing infrastructure to 5G, their networks' capabilities will expand further, paving the way for the full industrialisation of the lower air space.



2. Introduction

Intrinsic in cellular networks, mobile connectivity is the key enabler for beyond-visual-line-of-sight (BVLOS) use of unmanned aircraft (UA). A wide variety of applications will benefit from being able to operate UA BVLOS, once a system for managing unmanned air traffic allows for the safe operation of all flights.

Both national and international authorities are investigating the development of a new traffic management ecosystem for unmanned operations that is separate, but complementary to the existing air traffic management (ATM) systems used for commercial aircraft. Normally referred to as unmanned traffic management (UTM), the proposed system will manage both visual and BVLOS UA activities at low altitudes, generally below 400 feet above ground level. Scalable, reliable and secure, mobile network connectivity will help to fulfil the regulatory safety requirements for BVLOS operations.

The latest mobile technologies are designed to connect a wide range of things, machines and vehicles: 4G networks can support vehicle-to-vehicle communications, which can be used for collision detection and avoidance. Low power wide area technologies operating in licensed spectrum (LTE-M and NB-IoT) are well suited to providing position and identification information. 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 UTM architecture and requirements, highlighting the UTM-related use cases for mobile networks and the benefits that mobile connectivity can bring to UTM. It considers the role of mobile networks in supporting air traffic management.

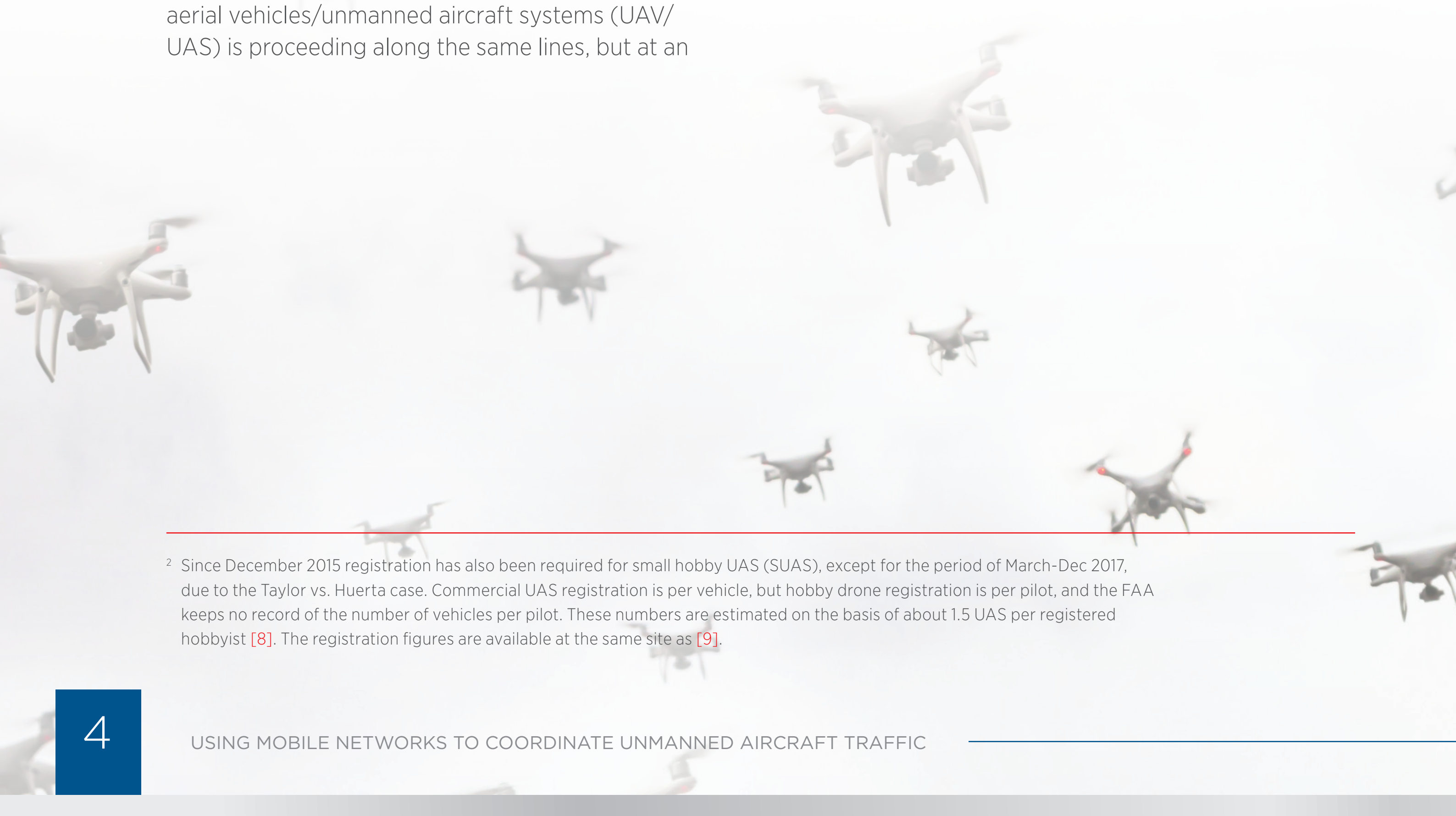
3. About Unmanned Traffic Management

THE GROWTH OF UNMANNED AIRCRAFT SYSTEMS

When manned aircraft were first invented, a traffic control system was not needed, due to the extremely low density of aircraft. In the rare cases where another aircraft was sighted, pilots proceeded on an ad-hoc "see-and-avoid" basis. Eventually, encounters were common enough to justify creation of standard rules and procedures for "see-and-avoid".

Still later, a formal traffic control infrastructure was introduced. This system is under revision, introducing more automation and data capability to assist pilots and air traffic controllers. As with road management systems, the development of air traffic control has evolved step by step, over the course of about a century.

The development and management of unmanned aerial vehicles/unmanned aircraft systems (UAV/UAS) is proceeding along the same lines, but at an unprecedented pace. Figure 1 shows the number of registered aircraft in the US since 1990, for both traditional aircraft and unmanned aircraft.[2] Since the start of registration at the end of 2015, the number of UA quickly surpassed the number of regular aircraft and continues growing rapidly even today. Figures for other countries are qualitatively similar.



[2] Since December 2015 registration has also been required for small hobby UAS (SUAS), except for the period of March-Dec 2017, due to the Taylor vs. Huerta case. Commercial UAS registration is per vehicle, but hobby drone registration is per pilot, and the FAA keeps no record of the number of vehicles per pilot. These numbers are estimated on the basis of about 1.5 UAS per registered hobbyist [8]. The registration figures are available at the same site as [9].

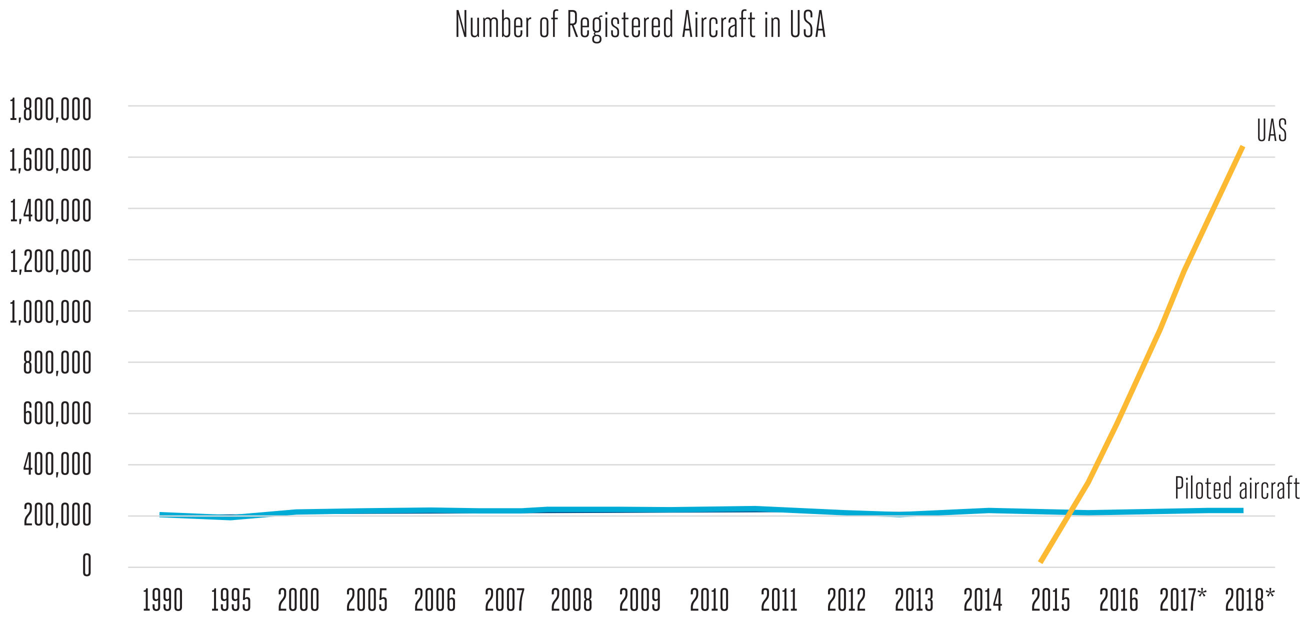


Figure 1 Number of Registered Aircraft in USA – Source: FAA

Not surprisingly, the number of "UAS sighting" incidents reported to the US Federal Aviation Authority (the FAA) has also skyrocketed over the past three years [9], as indicated in Figure 2. These are incidents in which the pilot of a manned aircraft, citizens and law enforcement sight an UAS.

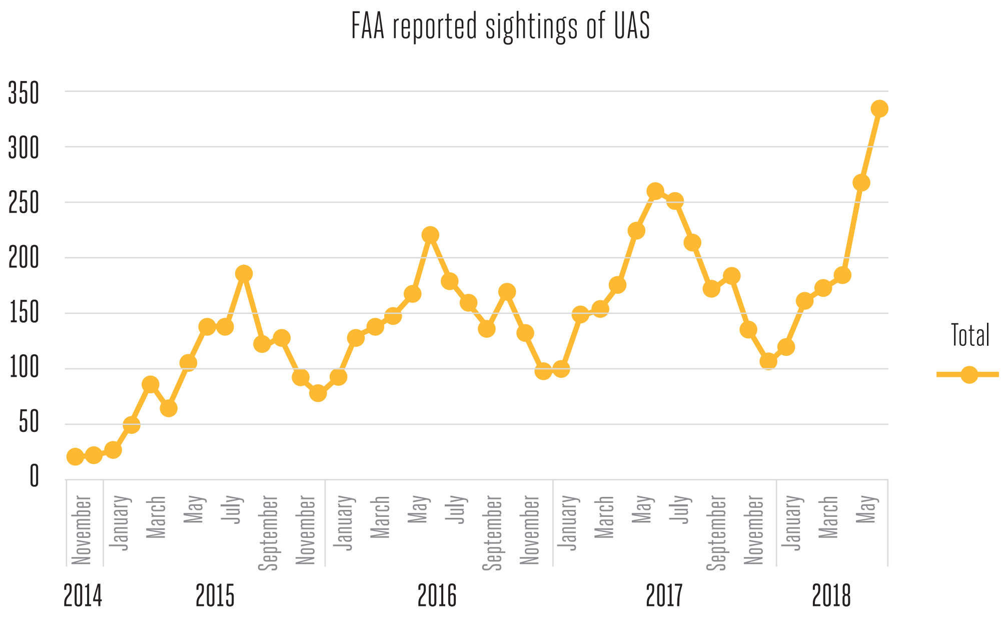


Figure 2 Number of “drone sighting” incidents from pilots, citizens and law enforcement in USA – Source: FAA

Civil aviation authorities (CAAs) around the globe are observing a similar pattern. Clearly, UAS will continue to have a growing impact on airspace worldwide, and additional traffic controls are desperately needed.

Meanwhile, the value of data and services based on UAS is also growing exponentially. Figure 3 shows the total revenues for commercial UA (including hardware and services) from 2016 to 2025.

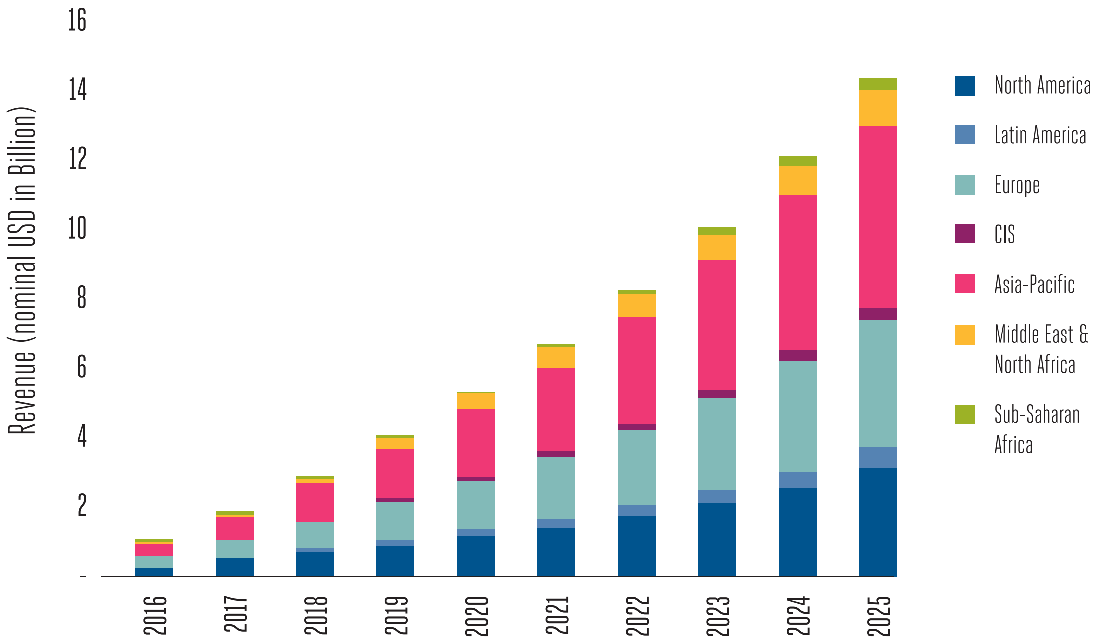


Figure 3 Commercial UAV revenues – Source: Analysys Mason

The forecasts shown in Figure 3 represents growth to 21% share in 2025, reaching over $14 billion in 2025. Exponential growth is likely to continue after this timeframe.

UAS UTILITY AND REQUIREMENTS

The market is growing despite severe limitations on commercial UAS flights. Today in most countries, commercial UAS flight is subject to four main restrictions, unless waived by special arrangement:

- A 1:1 correspondence between licensed commercial pilot and a vehicle.
- Vehicles flown within visual line-of-sight (VLOS) of the licensed pilot.
- Flight restricted to low-altitude uncontrolled air spaces (e.g. less populated areas).
- Strict control in urban areas.

While many missions are able to meet these requirements, they do impose a minimum cost per flight. The operating cost (opex) of a single mission can be estimated by looking at the several open-market freelancing websites for drone pilots, such as [10]. The simplest mission will usually cost about US$150, and the majority of that cost relates to paying the licensed pilot for their time. With full automation, however, the opex per mission could be reduced to the cost of electricity (as little as 1 cent) and depreciation. Depending on battery wear and vehicle cost, this could represent about a 100X to 1,000X reduction in opex per mission.

Reliable, secure, and economic communications technologies, such as LTE and 5G, could help enable full automation. These technologies must be able to demonstrate system performance levels that satisfy aviation regulators' concerns about automated flight, while also being cost-effective enough to be attractive for adoption. As the industry reaches this low opex threshold, wide-scale adoption of UAS will grow rapidly.

In summary, the UAS market is substantial and exponentially growing - clearly there are practical use cases and applications. The introduction of full automation could radically reduce mission costs, opening up many new use cases and compounding the already exponential growth in value. However, that will depend on the implementation of automated controlled airspace that cannot be achieved with the existing air traffic management systems (ATM).

Note also that UAS encompass a wide variety of physical forms, posing an additional challenge for regulators. Examples of UAS include:

- Hobby drones ranging in size from a few grams to tens of kilograms.
- Commercial inspection craft.
- Fixed wing aircraft.
- Hybrid Vertical Take-Off and Landing (VTOL)/ fixed wing craft.
- Larger/heavier drones for delivering packages, pesticides, etc.
- Optionally Piloted Aircraft (OPA) used as air taxis or other passenger services.
- High Altitude Long Endurance (HALE) vehicles that may stay aloft for months at a time.
- Long endurance balloons, such as those proposed by the Loon project.

Clearly not all of these need or deserve the same traffic control. The risks associated with an unmanned craft with small kinetic energy, or over unpopulated terrain, are completely different in type and severity from those posed by a large air taxi with human passengers flying in a dense urban area.

Still, law enforcement agencies, defence departments, and even the general public have expressed a strong concern about the security risks posed by larger numbers of UAS. Security concerns have elevated the need to identify UAS, referred to as eID (electronic ID) in Europe, and Remote ID in the US. While details vary, identity regulation is likely to be mandated ahead of the availability of UTM in most countries. Note that registration and electronic ID can be considered a foundational service that UTM can later leverage. For example, if every UAS is emitting an ID of some kind, detection of this ID can also be leveraged for detect-and-avoid processes.

Further information about UTM architecture and command & control requirements can be found in Appendix A.

4. Use Cases

The GSMA paper *Mobile-enabled Unmanned Aircraft* [1] describes the benefits of using mobile networks to support a variety of UAS use cases, such as:

- Enterprise use cases:
  - Inspection and surveys
  - Transport and logistics
  - Surveillance and monitoring
  - Communications and media
- Disaster and response
- Law enforcement
- Multi UTM landscape

This paper will explore the same use cases from the UTM perspective and how mobile networks cansupport the operations required by UTM.
In addition to the above use cases, this paper also considers the needs of a multi UTM landscape.

For each use case, there are four phases for the traffic management related to a flight (as shown in the following chart).

1	**INITIAL PREPARATION**	Electronic registration Electronic Identification	
2	**FLIGHT PREPARATION**	Flight planning Flight approval Capacity management	Geofencing Meteorological information
3	**FLIGHT EXECUTION**	Tracking Airspace dynamic information	Conflict detection Interface with other Traffic Control (ATC/ATM)
4	**POST FLIGHT**	Recording Playback/Logs	

Most of the services that are required in the four phases indicated above can be supported by mobile networks' capabilities, as described in the section on *Benefits of Mobile Networks*. For the initial preparation, the mobile network provides specific capabilities for the registration and identification. Flight planning, approval and meteorological information require a connectivity channel that can be used to transmit the information. Geo-fencing, geo-caging and tracking are features that mobile operators can offer and support by mean of providing and verifying the location of the UAS. However, some of the services listed above are purely in the domain of the traffic management provider, such as capacity management, conflict detection, interfacing to other traffic management, recording and playback.

Another approach is to classify the type of information and communications services that are required from a UTM point of view. The table below provides an overview, showing the applications related to verification and authorisation, applications related to the current flight and potential changes, and, finally, applications purely related to the provision of additional data to support the flight, such as weather information.

AUTHORISATION APPLICATIONS	FLIGHT SUPPORT APPLICATIONS	DATA APPLICATIONS
↘ Registration ↘ Identification (also done during the flight) ↘ Flight planning ↘ Flight configuration ↘ Flight authorisation ↘ Flight log, playback	↘ Flight control ↘ Geo-locating/tracking ↘ Geo-fencing ↘ Flight path deviation ↘ Remote intervention ↘ Airtime monitoring ↘ Collision avoidance	↘ Weather data ↘ Airspace info

> “For the initial preparation, the mobile network provides specific capabilities for registration and identification. Flight planning, approval and meteorological information require a connectivity channel that can be used to transmit the information.”

ENTERPRISE USE CASES

Most of the enterprise use cases described in detail in the *GSMA Mobile-enabled Unmanned Aircraft report* [1] involve similar interactions with traffic management. In each case, the UTM is required to authorise a flight, based on a set of information such as the time of the flight, the type of UAS, the nature of the flight and the priorities. For example, inspections of infrastructure or a media-related application can be scheduled in advance, but deliveries or services related to emergencies, such as the transport of samples or organs between hospitals requires a quick decision and different priority. As the UTM will need to manage the amount of traffic in a dedicated area, the decision and resolution could be easier for agricultural use cases, for example, compared to airborne deliveries in densely populated area where the UAS traffic could be higher. Note, the UTM will only require a limited set of information to monitor the flight, while the service provider will maintain all the relevant information that is needed for the service.

For some enterprise use cases, long-range flights may be needed. The UTM can provide much needed co-ordination between UAS. For example, there is the potential to use air corridors in pre-defined airspace, whereby UAS can operate at a specific altitude or using defined routes between points. These air corridors can be efficiently managed by the UTM system to enable a variety of use cases, such as powerline inspections from point A to B with the assistance of real-time data provided via a mobile network. The UTM can input information on other UAS flights nearby and manned aviation in the vicinity.

Although all enterprise use cases require similar functionality from the UTM, the condition of operation, the time required for a flight approval and the speed required to manage the flight requests and decongestion are very different.

DISASTER AND RESPONSE

The UTM can co-ordinate search and rescue efforts when there are multiple manned and unmanned aircraft running missions in an area of interest. A connection to a mobile network makes it possible to implement changes in real-time to the mission plan of a aircraft in a developing situation.

For example, in the case of a search and rescue mission to find an injured hiker in the bush that urgently requires assistance, first responders may plan to use a combination of ground search teams and a fleet of UAS until a manned helicopter can arrive. The team would use the UTM system to coordinate the search by UAS. Once the injured hiker is found, a UAS could deliver the first aid kit. When the manned helicopter approaches the search area, the UTM would broadcast an alert to all UAS operators, both flying and with scheduled flights, to create a dynamic no fly zone around the helicopter. Using a mobile network, the UTM would update the UAS with this information in real time.

LAW ENFORCEMENT

Law enforcement agencies need to respond to a variety of complaints about UAS. One common request is to identify or react to a report of an UAS flying in a specific area. Police could request the UTM identify any vehicle in a designated zone.

The UTM could then provide the identification information, including the pilot registration and any further relevant information. Police could also request the UTM establish ad hoc dedicated no-fly zones in areas where accidents happen or in the case of an improvised demonstration, for example.

Note, the UTM would need to authenticate the identity and authority of the official making a request for UAS identity and information.

MULTI UTM LANDSCAPE

Most likely, there will be several service providers (mobile operators or/and service suppliers) acting as UTM providers in a country. In such a multi UTM landscape, each service provider will host their individual UTM solutions and each mobile operator will use its network to provide services to their customers (UAS operators). This scenario would involve a complex architecture with multiple interfaces with the national aviation authority and other stakeholders. A multi UTM landscape would need to consider:

- Which stakeholder will ensure data (e.g. keeping track of all UAS that are operating in a low shared airspace) is consistent between the UTMs and how this will be done?
- Should all the UTMs be aware of each operators' UAS or would this be a legal obligation for the national aviation authority, perhaps through an aggregator layer to harmonise the multiple interfaces from UTMs, as shown in Figure 4?
- Will the national aviation authority accept such a multi UTM landscape, which could mean handling a huge amount of data and several interfaces from each implemented UTM? If one or several service providers make their own proprietary interface solution that could prompt authorities to define new regulatory guidelines to address the UTM compliancy.

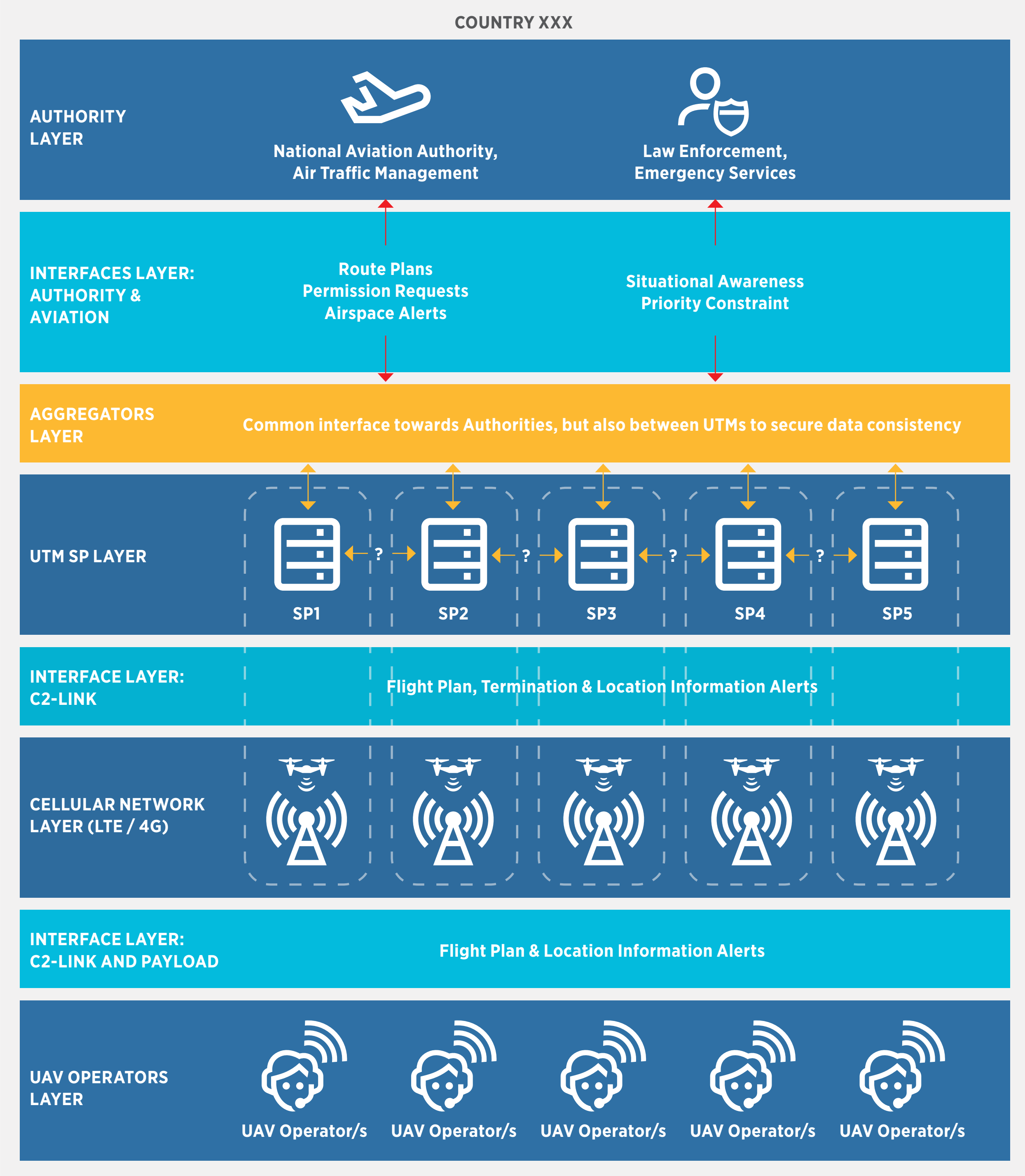

COUNTRY XXX
AUTHORITY LAYER
National Aviation Authority, Air Traffic Management
Law Enforcement, Emergency Services
INTERFACES LAYER: AUTHORITY & AVIATION
Route Plans
Permission Requests
Airspace Alerts
Situational Awareness
Priority Constraint
AGGREGATORS LAYER
Common interface towards Authorities, but also between UTMs to secure data consistency
UTM SP LAYER
SP1
?
SP2
?
SP3
?
SP4
?
SP5
INTERFACE LAYER: C2-LINK
Flight Plan, Termination & Location Information Alerts
CELLULAR NETWORK LAYER (LTE / 4G)
INTERFACE LAYER: C2-LINK AND PAYLOAD
Flight Plan & Location Information Alerts
UAV OPERATORS LAYER
UAV Operator/s
UAV Operator/s
UAV Operator/s
UAV Operator/s
UAV Operator/s

Figure 4: Multi UTM landscape

Such a scenario would require specific UTM-requirements to meet (or address) both information consistency between UTMs and the mechanisms through which aviation authorities interact with the various UTM solutions. Perhaps a simpler scenario would be to have a single UTM solution in each country to mitigate the complexities of multi UTM landscape. However, a single UTM solution would require a commitment from the national aviation authority (or another stakeholder) to host and maintain the single solution, as shown in Figure 5.

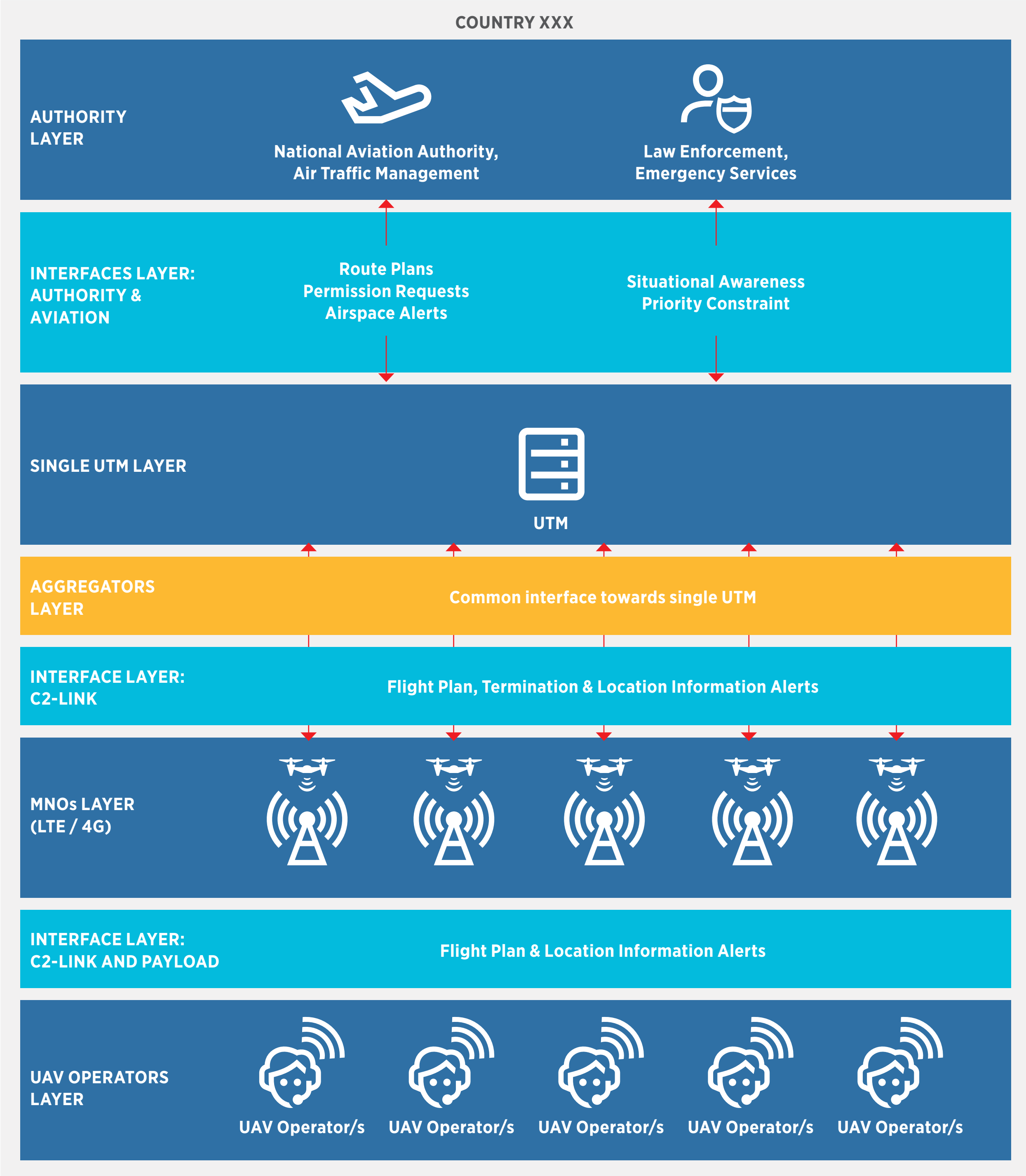

COUNTRY XXX
AUTHORITY LAYER
National Aviation Authority, Air Traffic Management
Law Enforcement, Emergency Services
INTERFACES LAYER: AUTHORITY & AVIATION
Route Plans
Permission Requests
Airspace Alerts
Situational Awareness
Priority Constraint
SINGLE UTM LAYER
UTM
AGGREGATORS LAYER
Common interface towards single UTM
INTERFACE LAYER: C2-LINK
Flight Plan, Termination & Location Information Alerts
MNOs LAYER (LTE / 4G)
INTERFACE LAYER: C2-LINK AND PAYLOAD
Flight Plan & Location Information Alerts
UAV OPERATORS LAYER
UAV Operator/s
UAV Operator/s
UAV Operator/s
UAV Operator/s
UAV Operator/s

Figure 5: Single UTM landscape

5. The Benefits of Using Mobile Networks

As mobile networks have already been deployed worldwide, they are well placed to support the rapid deployment of innovative UAS solutions, as well as underpinning new applications to improve the safety and data needs of UAS pilots and other stakeholders.

As discussed in the preceding sections of this paper, the growth trajectory of UAS means there will soon be a turning point where low altitude airspace will require some form of traffic management system to appropriately request, lodge and deploy UAS. With a significant increase in the volume of aircraft and a much higher level of automated operations, there will ultimately be an industrialisation of the (lower) airspace: flying robots will perform missions with different levels of autonomy, depending on the complexity of their tasks, and the flexibility and capabilities of the UAS. 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, UAS will need connectivity that meets the following requirements:

- **Scalable and suitable for the mass market:** Any solution must be able to support the rapid growth in UAS and to deliver a high level of capacity in the future.
- **High reliability and availability:** For safety reasons, a dependable solution is crucial for any implementation. A mobile network could enable UAS to be contextually aware of civil aircraft and/or other UA around the common airspace in near real-time.
- **Cost-effective and easy-to-integrate:** Industrialised solutions need to be efficient: 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, UAS 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:

- **The existing mobile networks can be reused without the need to deploy dedicated infrastructure for coverage in the air. Mobile networks support a standards-based approach and, therefore, offer a scalable connectivity solution:** Mobile networks take advantage of the harmonisation and standardisation of cellular technologies defined by the 3rd Generation Partnership Project (3GPP)[3]. Globally recognised, 3GPP continues to develop the capabilities of mobile networks.

[3] 3GPP http://www.3gpp.org/

- **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 could help national security and law enforcement agencies to identify and monitor UAS that may be of interest, by enabling the near real-time recording of UAS flight information in a UTM. Lawful intercept of communications from the UAS would also be available. Mobile operators can also provide independent verification of the location of the UAS for use by the UTM.
- **Identification capabilities through the SIM (Subscriber Identity Module) credentials and IMEI (International Mobile Equipment Identity):** The credentials established for mobile network authentication can meet the need for unique and trusted identification of UAS.

Figure 6 provides a high level representation of the potential interaction between mobile networks and the stakeholders involved in UTM.

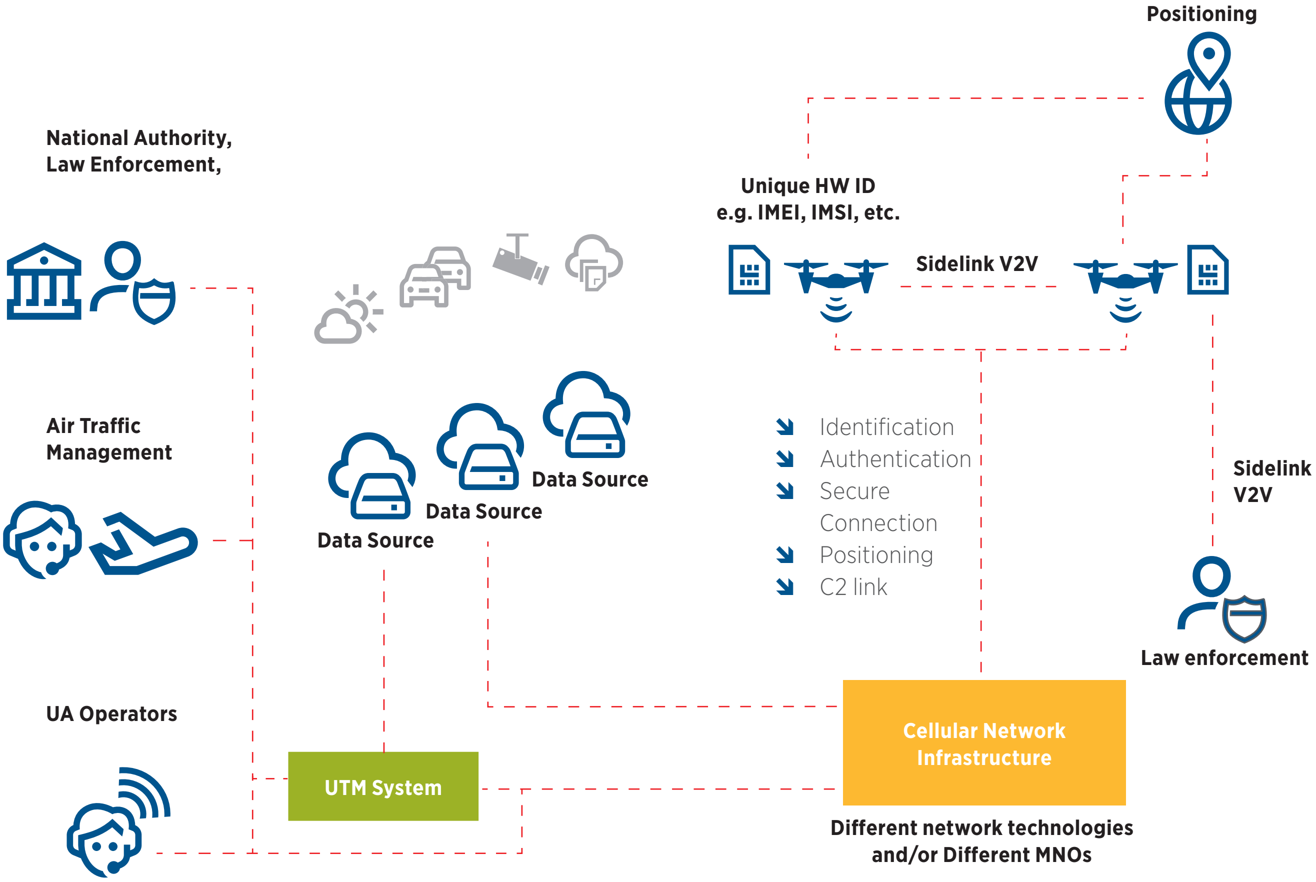


Figure 6: Scope of mobile networks for UTM and the wider ecosystem

Mobile networks are able to support UAS and UTM operations in four main interfaces, indicated in red in Figure 6:

- Between UAS for supporting V2V communication and collision avoidance, or to provide identification to law enforcement;
- Between UAS and UAS operators providing identification, authentication, secure connection for command and control (C2) link and payload, positioning and location verification, etc.
- Between UAS and the UTM system for supporting identification, positioning and location verification, secure connection for C2 link type of operation, such as establishing no fly zones or a change of flight path.
- For accessing various external data sources, both from UTM or UAS operators.

The next section of the paper describes in more detail the capabilities of mobile networks and how they support the various interfaces.

MOBILE CONNECTIVITY

In general, UAS are typically controlled using wireless connectivity in the unlicensed frequency spectrum in the Industrial, Scientific and Medical (ISM) bands. That limits the UAS and the pilot to short-range communications confined to the local area. Up to now, commercial UAS have not communicated with traffic management systems. However, in order to open the regulatory pathway towards BVLOS operation, UAS will need to have a communication channel to the traffic management systems and short-range technologies are not suitable to fulfil such a requirement.

Global, ubiquitous, scalable, secure and reliable, mobile networks can provide connectivity beyond the limited range that connectivity operating in the ISM frequencies can support: A UAS controlled over the mobile network will have the same range as the mobile network coverage (assuming the network can deliver the data rates required of the UAS). To ensure reliable communication, the mobile operator can control and monitor the quality parameters of the connection and provide appropriate service quality for supporting UAS. The extensive coverage of mobile networks allows for long distance flights, which would not be possible for UA communication using unlicensed spectrum. Although mobile phone users sometimes encounter coverage holes, UAS operators could plan flight paths based on the mobile network coverage and make sure that the flight is constantly in a coverage area.

The generic benefits of mobile connectivity for UAS are described in the Mobile-enabled Unmanned Aircraft paper [1]. While, this document focuses on the connectivity between the UAS and traffic management required to provide information, and command and control support, as described in the use cases. In essence, mobile networks can enable the monitoring of the UAS' position, altitude, speed, radio condition, camera footage and any other information, as well as enabling control of all operations from take-off to landing. UAS with built-in cellular connectivity can truly harness BVLOS. Furthermore, built-in connectivity allows for mobile network-based identification of the UAS, true end-to-end security, accurate and protected location information and support for law enforcement requirements (see subsequent sections).

Mobile networks will enable new services to proliferate for UAS. Once the UAS is cellular-connected, it will have access to real-time information communicated from the UTM, enabling innovation to develop and flourish. Moreover, the manual tasks that a UAS operator and UAS pilot have to do prior to a flight could be completed remotely via cellular connectivity.

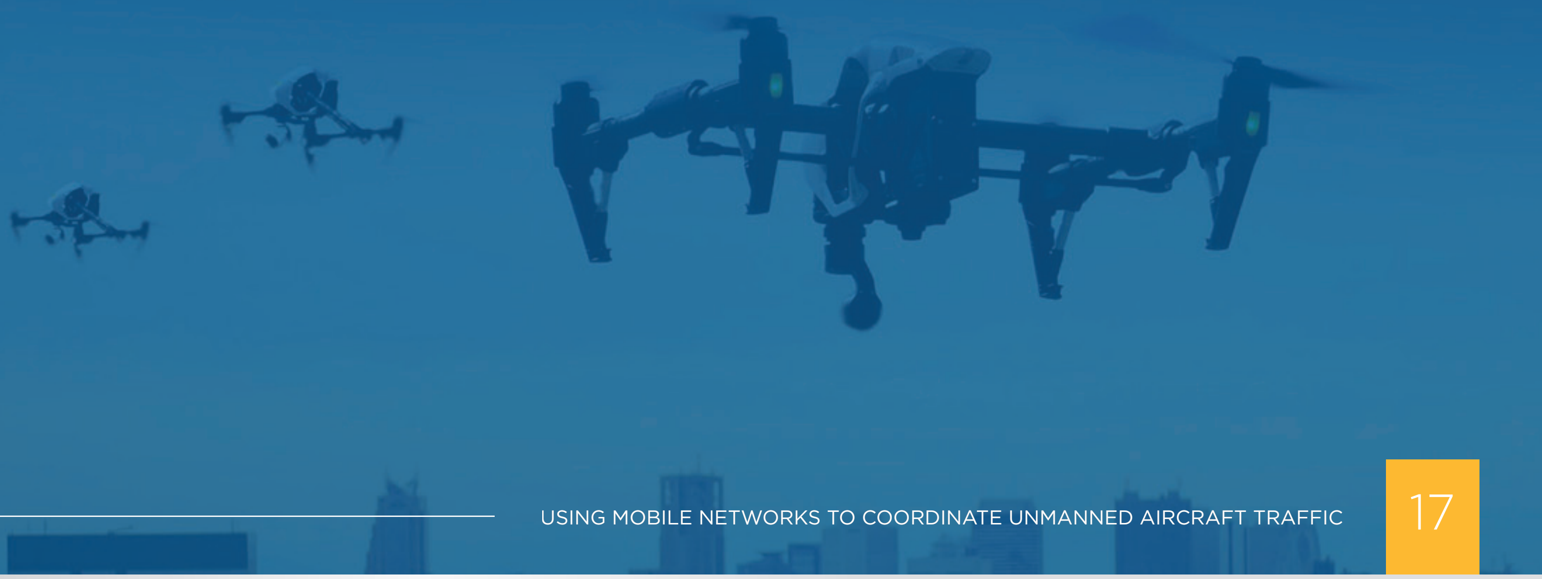
Mobile networks are constantly evolving to support the emerging services and needs of multiple industries. Most mobile operators already run 4G LTE (Long Term Evolution) networks, which can deliver high-bandwidth, low latency connectivity with an exceptional quality of service that is designed to scale.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

VEHICLE-TO-EVERYTHING (V2X) CONNECTIVITY

The 3GPP standards now support Vehicle-to-Everything (V2X) connectivity that enables real-time device-to-device communications. When applied to UAS, this approach can be used to provide sense and avoid capabilities. According to 3GPP, there are two main modes of operation: communication assisted by the network and direct communication.

- **A) Mobile network assisted:** a UAS is able to utilise the mobile network through the LTE Uu interface. This model, which is only possible within network coverage, potentially allows a vehicle to connect to a wide range of infra structure for providing and receiving a variety of information.
- **B) Direct communication:** a UAS can communicate to another UAS without needing the support of a mobile network. This model can also be used where there is no network coverage and it can be use with or without using a USIM. Using the new 3GPP radio interface “PC5”, a UAS is able to broadcast and receive information about the surrounding environment to be able to determine if there is another UAS nearby and make adjustments in the flight path to compensate and avoid mid-air collisions.

The cellular module (LTE or 5G) in the UAS can utilise both modes at the same time. An UAS is able to communicate directly with another approaching UAS and simultaneously receive useful information via the mobile network about traffic congestion, without competing for resources.



REAL-TIME DATA TRANSMISSION

Some examples of payload communications for UTM are:

- Location information (latitude, longitude, altitude, area).
- Sensor data for processing, analysis and decision-making mid-flight, command and control inputs in real-time, resulting in a safer, more reliable shared airspace.
- Dynamic no-fly zones and geo-fencing
- Alter existing flight plans, waypoints, and information about the horizontal and vertical velocity and bearing.
- Retrieve information about manned aircraft flights
- Allow for the review and approval of flights to be streamlined in areas of interest.
- External data source (e.g. weather information)
- SMS triggered services

Mobile networks provide a proven mechanism for storing the real-time data in a remote location, as required by the specific UAS service. The use of mobile connectivity to share real-time flight data online and to enable remote operators to interact with the UAS pilot and the UTM would lead to the emergence of many new use cases.

Whilst flying, mobile connectivity would enable the pilot to receive direct instructions on how to adjust flight paths, according to the current restrictions. These UTM instructions will give pilots a full picture of flying conditions, leading to safer and approved flights.

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 UAS world:

- **Identification of the hardware:** Cellular networks employ a global hardware identifier (the IMEI). This is the serial number that links the manufacturer to the device, and is stored on the electronics motherboard. For a UAS, some means would need to be found to tie such an identifier for the electronics pack age to the visible identifier of the airframe.
- **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 UAS, 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.

- **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 UAS 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.
- **User identification:** In telecommunications, 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 driver's license number, passport number, phone number, email address, etc. The GSMA is working to create a standardised identity extraction layer that can be employed 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 UAS and/or its current mission.

SECURITY

The UAS 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 UAS 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 UAS, 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. 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 preparation to the flight itself and the aftermath.

UAS manufacturers and UAS 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 and 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 its customers. The GSMA has published a comprehensive set of security guidelines [19] for the IoT that are also valid for UAS. 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* [19], which is a flexible framework that helps companies to provide secure Internet of Things solutions based on the GSMA IoT Security Guidelines.

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

- **Secure registration of pilots and their UAS:** The registration of pilots and their UAS 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 UAS with a pilot, just as a vehicle's license plate links it to a driver, so if the UAS goes off course, for example, the UTM can contact the pilot immediately.
- **Protection of sensitive data:** Sensitive data could include permitted flight boundaries (e.g. maximum altitude limits, distance from the take-off) or other data exchanged between the UTM and the UAS pilot, which could include commands or flight related information, such as the full flight traceability.

Mobile networks provide secure communication from the UAS and the network, while allowing for end-to-end encryption of the data. The *GSMA IoT Security Guidelines* [19] make several recommendations based on a risk assessment.

- **Seamless and secure connectivity:** For easy deployment worldwide, manufacturers need to be able to connect their UAS seamlessly and securely to networks in any country. Mobile networks provide secure connectivity around the world as explained in the earlier section on Mobile Connectivity.
- **Reliable UAS location:** Public authorities need to be able to identify UAS and locate them, anywhere and in real-time, reliably. UAS location data comprises digital IDs, such as serial numbers, and any related dynamic data (such as location and time), and this data must not be modified during the flight. Mobile networks can help to verify the information provided by the UAS, as described in the next section on Positioning and Location Services

POSITIONING AND LOCATION SERVICES

Many of the UAS flying today lack proper identification and are not supported by any form of traffic management (UTM) system coordinating flights. Many of these UAS have no mechanism by which they can be located, and rely on the UAS operator maintaining VLOS with the UAS. More advanced approaches have a built-in GNSS (global navigation satellite system) receiver, which can report the UAS' location, altitude and speed to a ground control system (GCS).

There are many UTM projects and initiatives being developed, but it will be some time before the first solutions are deployed. Clearly, all will require that the location of the UAS is known to the UTM. Whilst a separate GNSS could continue to be built-in to the UAS, most LTE chipsets now contain an integrated GNSS receiver, which can obtain position information with no additional weight penalty. The UAS can then report its location to the UTM or other ground systems via the LTE network. The UAS could report its position periodically or the UTM system could pull the information based on user request. 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 UAS 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 UAS. 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 [2] and [3]). 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 UAS using its Radio Positioning System (RPS) technology, which is a variant of the E-CID technique and hence independent of GNSS [4]. Although RPS is not widely used at the moment, given the ubiquity of GNSS receivers in LTE modems, this trial demonstrated that such techniques can be used to complement and verify any GNSS-based location information received from a UAS.

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

QUALITY OF SERVICE

4G LTE has been designed to support quality of service (QoS) capabilities, enabling mobile operators to prioritise data streams transmitted over the mobile network, which can be restricted to certain traffic. If QoS is not available, the data is delivered on a “best effort” basis, which would mean that the data might not be sent in real-time. QoS will be important if near real-time communications is required by the UTM.

LAW ENFORCEMENT SUPPORT

Mobile networks can help UAS 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 standardisation activities are looking to support to ensure international adoption of mobile-enabled UAS. LE needs this information to perform threat discrimination, determine nefarious intent associated with the use of a UAS, and perform UAS crash investigation. The ability to link a UAS operator to a UAS is also critical for LE.

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

Tracking solutions from an LE perspective must take into account both real-time (where is the UAS now, and where is the UAS operator now) and historical information:

- from where did the UAS take-off,
- where was the UAS operator upon UAS take-off,
- what was the flight path of the UAS,
- where was the UAS operator during the UAS flight,

- where did the UAS land or crash,
- where was the UAS operator when the UAS landed or crashed.

The preceding section on *Positioning and Location Services* describes how mobile networks help to verify the correct position of the UAS to UTM. From the perspective of LE, tracking a UAS has the following two aspects:

- Tracking the geographical coordinates, altitude, and time stamp of the UAS, and
- It is desirable (although not a strict requirement) to be able to access a flight plan for a UAS (if it exists).

Technical solutions for remote identification and tracking must take into account the needs of traffic control communities and the general public (see also [20]), as well as LE agencies.

Note, mobile networks do not provide identification and location information to LE agencies directly: mobile networks provide services for identifying and locating UAS to the authorised users, such as UAS operators and the UTM. It is then the responsibility of these users to provide the required information to LE. Lawful interception of communications to/from a UAS 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 [4], [5] and [6]. 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 UAS communications mechanisms.

NO-FLY ZONES

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

- The flight advisory area can be in the form of a geometric shape, such as a circle (single point defined with a radius) or a polygon (three to "n" coordinates defined), as shown in Figure 7.
- 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 UAS (examples are caution, turn around, or land immediately)
- UAS will receive the flight restriction broadcast and adjust its flight path.

Flight advisory zones can be static or ad hoc:

- Static – typically used for a fixed facility, such as an airport. However, 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 unauthorised UAS.

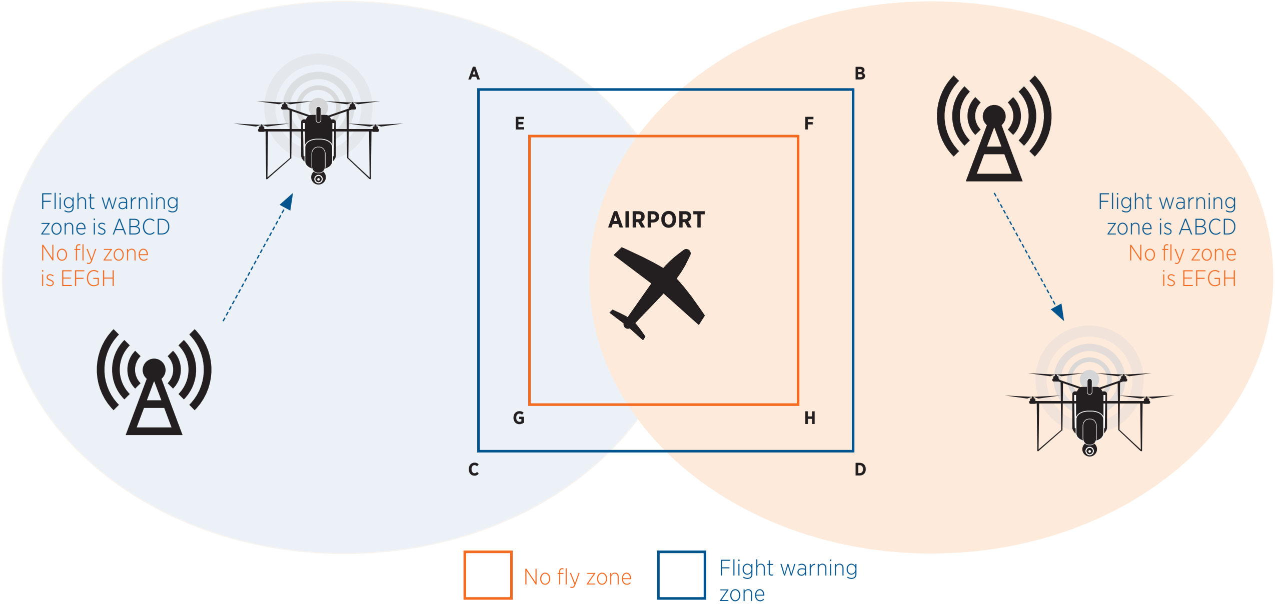


Figure 7: Communicating no fly zones and flight warning zones

An approved civil aviation authority, a local government official or government agency, such as NASA, may define the flight advisory areas. The UAS can validate the legitimacy of a received message by checking the certificate of the sending entity.

REGISTRATION

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 UAS registration.

MOBILE NETWORK EVOLUTION

Enhancements to the 3GPP standards have introduced features that improve the performance of UAS positioning in mobile networks. One of these features indicates whether the UAS is flying by introducing height measurement reports from the UAS, triggered by a threshold, thereby enabling the network to detect changes in the UAS' altitude. This can be useful in determining if the UAS is inflight and can enable features specific for UAS performance in the air.

Release 15 of the 3GPP standards addresses the radio aspects of communications with UAS.
In Release 16, 3GPP addresses support for UTM functions. Having completed a study on support of remote IDs for drones (SP-180781),[4] 3GPP recently agreed to a work item to extend the 3GPP architecture to better support UTM (SP-180771)[5]. Although the architectural specifics are not yet clear, the changes required are unlikely to be large. Support of UTM will draw heavily on the work 3GPP has already done for V2X. This includes, for example, how network capabilities and information can be exposed to external functions (such as UTM), reusing V2V capabilities for D&A (detect and avoid) and identity broadcasts.

Looking to the future, Release 17 of 3GPP will take into account the findings of a further study looking at any additional enhancements needed in either the radio or core network to support UAS (SP-180909)[6].

The evolution of cellular networks towards 5G [22] will bring a whole new set of capabilities that can be utilised for UAS operation and UTM operations, such as:

- Higher bandwidth, allowing enhanced payload data transmission capabilities, such as high resolution video.
- Lower latency, enabling faster C2 link and detect and avoid triggered by off-board data sources.
- Multi access edge computing [22], offloading detect and avoid compute from vehicles to lower the overall vehicle cost.
- Network slicing [23], allowing the creation of a dedicated virtual slice with optimised configuration for UAS and UTM operation support.
- Higher reliability.

[4] 3GPP (2018) SP-180781: *TR 22.825 on Remote Identification of Unmanned Aerial Systems*
[5] 3GPP(2018) SP-180781: Remote Identification of Unmanned Aerial Systems
[6] 3GPP (2018) SP-180909: Study on 5G enhancement for UAVs

6. Conclusion

Mobile network operators can play a key role in the emerging UAS and UTM ecosystem. The existing mobile network infrastructure, incorporating more than seven million base stations around the world, is the ideal starting point to deliver the required connectivity and service to support the majority of the use cases for UTM. The mobile industry connected more than 5 billion people to mobile services in 2017, supporting 8.4 billion connections, of which 700 million are M2M (machine to machine) and IoT [21].

Mobile network operators can play a key role in the emerging UAS and UTM ecosystem. The existing mobile network infrastructure, incorporating more than 7 million[7] base stations around the world, is the ideal starting point to deliver the required connectivity and service to support the majority of the use cases for UTM. The mobile industry connected more than five billion people to mobile services in 2017, supporting 8.4 billion connections, of which 700 million are M2M (machine to machine) and IoT [21].

Mobile networks deliver global interoperable and secure connectivity based on global 3GPP standards, which are designed to support a variety of capabilities and the quality of service required by most IoT applications. Moreover, the use of licensed spectrum enables mobile operators to better control the available resources. At present, mobile networks have sufficient capabilities to deliver connectivity, real-time data, security and identity management for supporting UTM requirements. As mobile operators maintain and upgrade their existing infrastructure to 5G, their networks' capabilities will expand further. While existing mobile networks are well suited to support the initial deployment of UAS, 3GPP is working on optimising cellular networks to further support UAS in future.

[7] GSMA (2017) How many global base stations are there anyway?

7. Appendix A

UTM PARADIGM AND ARCHITECTURES

UTM (UAS traffic management) is a global effort to introduce traffic management for UAS to address the following issues:

- Exponentially increasing number of vehicles, far exceeding conventional aircraft in both numbers and growth rate.
- Increasing incidents of sightings, near-misses, and even collisions between and conventional aircraft.
- Increasing sensitivity to the security risks posed by UAS (e.g., see [16]).
- Increasing variation in the types of vehicles in airspaces worldwide.
- Business demand – a large and growing UAS market, which could benefit from major cost reductions through automation.
- Public demand – to generate social acceptance among citizens of increasing numbers of UAS.

Approaches to UTM vary around the world, but there are some common elements.

Considerations for UTM architectures are shown in Figure 8 and Figure 9. These are, respectively, a system created by NASA showing a proposed architecture for the US, and a system from SESAR CORUS showing a proposed architecture for Europe ("U-space").

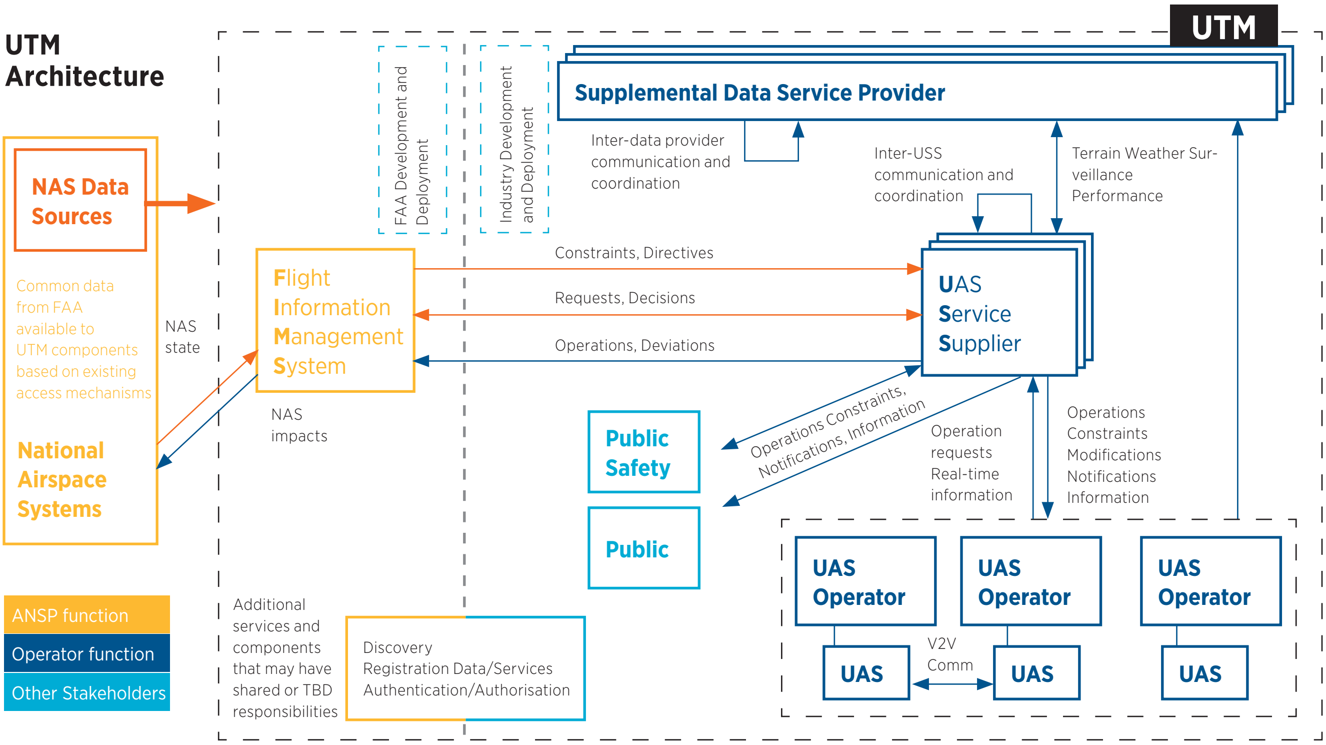

UTM Architecture
UTM
Supplemental Data Service Provider
FAA Development and Deployment
Industry Development and Deployment
Inter-data provider communication and coordination
Inter-USS communication and coordination
Terrain Weather Surveillance Performance
NAS Data Sources
Common data from FAA available to UTM components based on existing access mechanisms
National Airspace Systems
NAS state
Flight Information Management System
NAS impacts
Constraints, Directives
Requests, Decisions
Operations, Deviations
UAS Service Supplier
Operations Constraints, Notifications, Information
Operation requests Real-time information
Operations Constraints Modifications Notifications Information
Public Safety
Public
UAS Operator
UAS Operator
UAS Operator
UAS
UAS
UAS
V2V Comm
ANSP function
Operator function
Other Stakeholders
Additional services and components that may have shared or TBD responsibilities
Discovery
Registration Data/Services
Authentication/Authorisation

Figure 8: UTM Architecture – Source: NASA

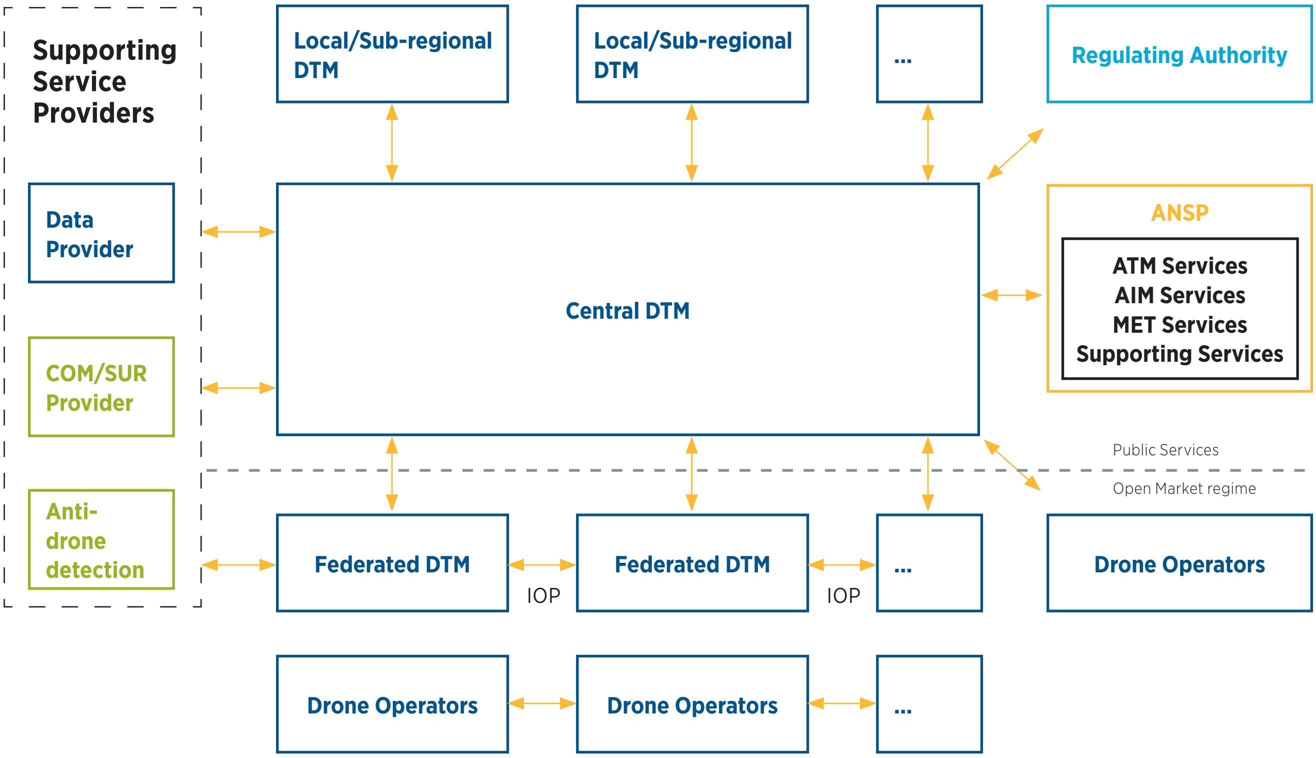


Figure 9: U-Space System – Source: CORUS

Other notable architectures are China's UOMS and Japan's JUTM. These and other emerging efforts worldwide are catalogued by GUTMA [18].

The typical operation of missions in Figure 8 is as follows[8]: A UAS operator (which may be a person or a flight-planning task in software) requests a route by providing a flight plan to its UAS Service Supplier (USS) (or DTM in Figure 9)[9]. This USS will consult with all other USS relevant to that flight plan, and provide feedback on whether the requested route will overlap with any other routes. If it is clear, the UAS can fly that reserved route. During flight, the UAS will report its status and position to the serving USS. In the case of problems or deviations from the planned route, the USS will coordinate with other USS (and their corresponding managed UAS) to re-route. Although the USS should ensure participating UAS avoid each other, each UAS must also perform local on-board tactical sense and avoid[10].

Certain changes in airspace status can be communicated from the CAA/ANSP (Civil Aviation Authority - Air Navigation Service Provider) to all USS, which will manage their served UAS. For example, an emergency event, such as a wildfire, may result in the creation of a temporary flight restriction. A notice of this event is sent by FIMS (Flight Information Management System) in Figure 8 (Regulating Authority/ANSP in Figure 9) to all the relevant USS, so that all affected UAS may act accordingly. Emergency vehicle missions may take priority over missions in progress, leading to dynamic rerouting directly by the UTM system.

As UAS and the UTM system may use a wide variety of data to optimise performance, these architectures both contemplate separate supporting data services (Supplemental Data Service Providers or SDSP in Figure 8 or supporting service providers in Figure 9). This may be data on weather, terrain, sense and avoid events, radio environment, or any other data. This may include shared/federated data from UAS themselves, or from other data sources.

Note, there is a public/private delineation in both Figure 8 and Figure 9, so that many traffic services are provided by private companies, offloading the Air Traffic Management (ATM) provider. This is also common worldwide.

Another nearly universal principle in UTM proposals is an emphasis on machine-to-machine communication. The traditional air traffic management system is, at its core, a person-to-person system. An increasing amount of data and automation have been introduced over the years, but the highest level decision makers and responsible parties are always (1) the pilot and (2) the air traffic controller. These people address all off-nominal conditions and have ultimate decision-making responsibility and authority.

While control by humans ensures a certain degree of common sense in the system, it also limits the complexity and density. With the growing number of UAS in the world, and the need for low-cost flights, there is widespread consensus that UTM must be largely machine-to-machine, ultimately with full autonomy.

[8] For brevity, a default term set is arbitrarily used throughout, and those terms are from NASA (Figure 8). References to corresponding CORUS terms (Figure 9) are in parenthesis when it is helpful to highlight common architectural elements.

[9] A common form is a set of 4D polygons, indicating 3D volumes and times those volumes will be occupied.

[10] This is for non-participating objects, or even participating objects in some conditions, such as off-nominal condition or planned overlap. Complete exclusivity in pre-flight de-confliction is a goal, but not a universal hard requirement in some proposed architectures. In general, de-confliction has multiple layers. The strate gic de-confliction is defined by NASA for operation between UAS that are subscribed to a UAS Service Supplier (USS) is a core function of a USS, see

Other commonalities between most UTM proposals worldwide are:

- UTM will first operate in regulated, but uncontrolled, airspaces not presently served by ATM. Objects under UTM and ATM must inevitably interact somewhat, but full integration of UTM/ATM is being pushed to later deployment phases, to the extent possible.
- UTM will provide pre-flight de-confliction[11] between all participating vehicles, so that a route is usually unique among participants. These routes can be at the resolution/timing of a machine, and so may be very dense.
    - However, de-confliction is always multi-layered, and UAS must be able to sense and avoid autonomously.
- UTM should have ability to make room, at short notice, for priority or emergency missions.
- UAS/USS should be continuously in touch and, therefore, able to identify and handle off-nominal situations quickly.
- UAS/USS should have a shared sense of perception, augmenting capabilities beyond what a single UAS could achieve.
- UAS must be capable of being identified by authorised parties.
- The UTM system should be able to create a "geofence" to permit or prohibit UAS activity in various airspaces.

There are also differences between views worldwide, for example on the topics of:

- Whether or not there should be a single USS, or multiple equivalent peers, or a combination of these (i.e., a central USS managing peer sub-entities, as in Figure 9).
- The roles of public/private entities.
- The method of reserving routes and synchronising between USS for de-confliction.
- Means for arbitrating airspace access between users.

Unlike cellular communications, there is, as yet, no definitive standards body for defining UTM. Some notable efforts are:

- ASTM F.38, which has groups for UAS-ID and UTM[12]
- Global UTM Association [18]
- SESAR/CORUS[13]
- NASA RTT and associated working groups[14]
- RTCA SC-228[15]
- ISO / TC 20 / SC 16[16]

[11] In the paper: "UTM Research Transition Team, Sense and Avoid Working Group Technical Work Package #2: UTM Conflict Management Model", tactical de-confliction refers to vehicle-to-vehicle operation without the involvement of USS.

[12] https://www.astm.org/Standards/F38.htm

[13] https://www.sesarju.eu/activities

[14] https://utm.arc.nasa.gov/docs/Rios_NASA-Tech-Memo-2017-219494.pdf

[15] https://www.rtca.org/sites/default/files/sc-228_jul_2017_agenda.pdf

[16] https://www.iso.org/committee/5336224.html

THE ROLE OF COMMUNICATIONS IN UTM

It is useful to divide UAS communications into two parts[17]:

- Command and Control (C2), which deals with actual flight and flight management[18].
- Payload, which refers to the mission-specific data being collected, such as inspection data.

There is no rigorous and universal definition[19] of C2 or its role. But broadly vehicles may be divided into two types:

1. Vehicles that are piloted from the ground, such that the C2 link carries flight commands. This is associated with terms, such as "remotely piloted aerial system" (RPAS).
2. Autonomous vehicles that pilot themselves using GPS or other cues to execute a predetermined flight plan. In this case, only minimal information will pass over the C2 link. This is sometimes referred to as "command, but not control."

Although this is a useful generalisation, in practice there are many options and varied approaches for defining the precise roles of the UAS, ground-based software and systems, and humans in the overall flight task, and the handling of off-nominal conditions. This leads to a wide variety in the purposes of, and therefore, requirements for C2. As the ability for an on-board sense and avoid system to operate independently with minimal interference or oversight increases, the system's overall reliance on a direct control link between the pilot or piloting system and aircraft decreases.

The absolute minimum C2 requirements of most UTM approaches are:

- Reverse link:
  - The vehicle should report its position periodically, such as once per few seconds.
  - The vehicle should also report certain off-nominal events.
- Forward link: The vehicle should be capable of receiving redirection due to dynamic conditions, which include at least:
  - making way for emergency / priority missions
  - reacting to dynamic restrictions imposed by the CAA/ANSP (such as a no-fly zone around the site of an accident, fire, or other condition).

In addition to this mandatory minimum, a C2 link may convey other information, such as

- Requests to re-route, or re-routing commands, for non-emergency reasons.
- Sharing of airspace-relevant data between UAS, USS, and SDSP that may improve overall system performance. This can include information on wind, weather, obstacles, terrain, non-cooperative aircraft, or other data of interest.
- Detailed flight commands (e.g., turn left, turn right), in a system where such detailed control is remote rather than on-board.

[17] Although these two parts are largely independent, with independent requirements in terms of reliability, economy, bandwidth, and latency, there may be some interplay between the two. For example, preliminary analytics on inspection data is used in real time to direct further information collection.
[18] In this document we use the definition of Command and Control as indicated by GUTMA in the "UAS Traffic Management Architecture" in section 9.2.1.
[19] Some architectures also refer to "C3", meaning Command, Control and Communications.

Thus, it is difficult to establish universal guidelines for C2 in general. It is highly dependent on the overall system design, including the UTM system and the UAS. The required latency, reliability, and bandwidth all need to be considered:

Latency: Although detailed vehicle control over a C2 link requires a low latency connection, the minimum requirement for a C2 link may be highly tolerant of latency. For example, initial NASA documents proposed a one second reporting period and one minute timer before a flight is declared rogue. Concepts of cloud-based or federated sense and avoid that might require low latency are not generally well developed in any UTM proposal worldwide, but it remains an active topic of research. In particular, this may prove a valuable tool for eventual UTM/ATM integration, since a key attribute of a machine-to-machine traffic system is its ability to react quickly, and across all vehicles in the system.

Reliability: this is often mapped to different concepts, such as:

- Coverage/availability: This is of paramount importance in aviation.
- Predictability: the ability of the UTM system to know a priori whether there is coverage or not. As explained in this paper (see the Mobile Connectivity section), the aerial channel may be highly predictable and this can be a critical advantage, largely compensating for holes in coverage.
- Packet loss rate while in coverage: The minimum requirement for a C2 link will be highly tolerant to packet loss rate, whereas detailed control will not be.

Bandwidth: Some systems may require a high bandwidth C2 link, particularly if live video is used as part of C2, which would correspond to a less automated operation. Telemetry data of almost any nature is small in comparison to live visual data.

The requirements for Payload are, of course, highly mission-specific. Note that there is a trade-off between the amount of inference or analytic intelligence on-board the UAS (resulting in shorter meta-data), versus the need to convey payload back down to the ground for terrestrial analysis. Even within one application, the requirements for payload can vary substantially based on the approach to analysis of that payload.

Moreover, some payload may be simply stored on the vehicle and retrieved by the pilot from a SD card after landing. Although this is a common approach for manual flight today, the advent of automated flight will require this manual step to be replaced with wireless transmission.

> “Mobile networks deliver global interoperable and secure connectivity based on global 3GPP standards, which are designed to support a variety of capabilities and the quality of service required by most IoT applications”

BEYOND UTM

Ubiquitous UTM requires a machine-to-machine system (UTM) to interface and co-operate with a person-to-person system (ATM): the "transition problem" facing automated driving is also true for aviation.

However, ATM was already facing challenges of its own. Even before the advent of UAS, the manned ATM system was struggling with congestion and overload in an increasing number of airports and routes. Efforts such as ICAO's Global Air Navigation Plan [11] or FAA's NextGen [7] are designed to cope with such congestion.

Clearly, the ATM system already needs to be more M2M-based.   This has led to discussion of "UTM-inspired ATM" as a solution for both problems (the congestion of ATM and integration with UTM). Thus UTM is not only the traffic management system for UAS, but may well be the inspiration and basis for all air traffic management in the longer term. This notion has introduced the concept of "Universal Traffic Management" for UTM that encompasses the new capabilities of UAS traffic management and the future evolution of ATM.

8. References

[1] Mobile-enabled Unmanned Aircraft, https://www.gsma.com/iot/wpcontent/uploads/2018/02/Mobile-Enabled-Unmanned-Aircraft-web.pdf

[2] 3GPP TS 23.271 - Functional stage 2 description of Location Services (LCS), https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=834

[3] 3GPP TS 36.305 - Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Stage 2 functional specification of User Equipment (UE) positioning in E-UTRAN, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2433

[4] 3GPP TS 33.106, Lawful interception requirements, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2265

[5] 3GPP TS 33.107, Lawful interception architecture and functions, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2266

[6] 3GPP TS 33.108, Handover interface for Lawful Interception, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2267

[7] https://www.vodafone.com/content/index/media/vodafone-group-releases/2018/iot-dronetracking.html#

[8] https://www.usatoday.com/story/news/2016/02/08/faa-drone-registration-eclipses-regularplanes/80002730/

[9] https://www.faa.gov/foia/electronic_reading_room/. See data item at “Reported Encounters with Unmanned Aircraft Systems (UAS)”

[10] https://www.dronebase.com/pilots

[11] ICAO: Capacity and Efficiency, 2016-2030 Global Air Navigation Plan, https://www.icao.int/airnavigation/Documents/GANP-2016-interactive.pdf

[12] NextGen plan https://www.faa.gov/nextgen/

[13] https://pdfs.semanticscholar.org/presentation/f6ec/1b0aac1b6ccadc8a7ae37de839252681deab.pdf

[14] https://www.utm.arc.nasa.gov/upp-industryworkshop/UPP_Industry_Workshop1_20180315_Final.pdf

[15] Reprinted with permission from CORUS_ConOps_1.0_approved.pdf, which is out for comment and will be published shortly.

[16] https://www.bbc.com/news/world-latin-america-45073385

[17] https://www.utmblueprint.com/

[18] https://gutma.org/map/Main_Page

[19] GSMA IoT Security Guidelines and Assessment, https://www.gsma.com/iot/iot-security/iot-securityguidelines/

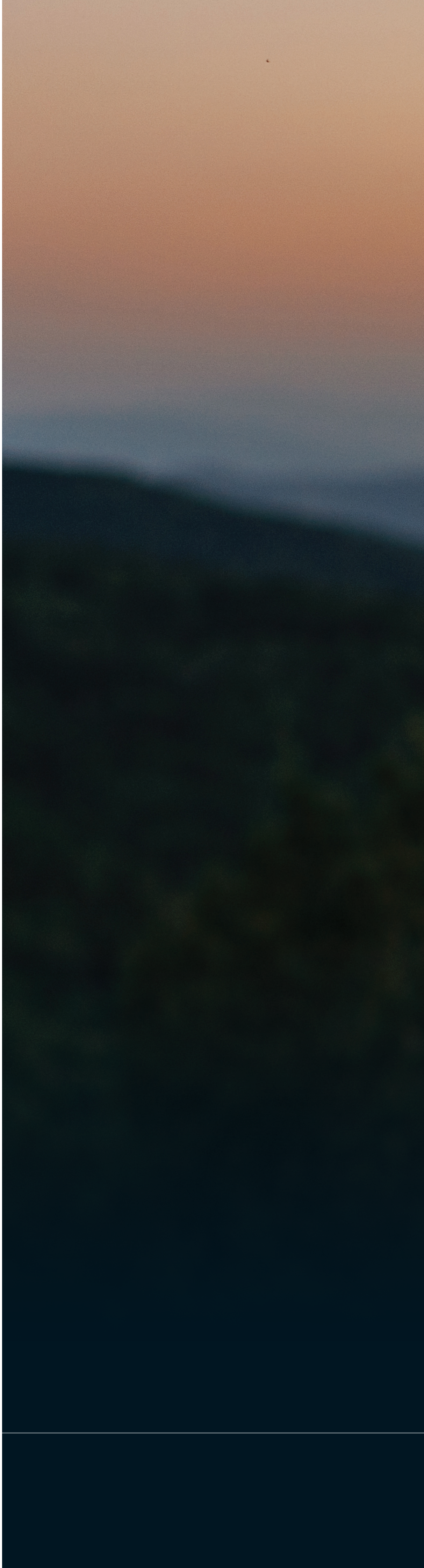
[20] UAS Identification and Tracking (UAS ID) - Aviation Rulemaking Committee (ARC); https://www.faa.gov/regulations_policies/rulemaking/committees/documents/media/UAS%20ID%20ARC%20Final%20Report%20with%20Appendices.pdf

[21] GSMA The Mobile Economy 2018 - https://www.gsma.com/mobileeconomy/wpcontent/uploads/2018/02/The-Mobile-Economy-Global-2018.pdf

[22] Unlocking Commercial Opportunities, section 4.3; https://www.gsma.com/futurenetworks/wpcontent/uploads/2017/03/704_GSMA_unlocking_comm_opp_report_v5.pdf

[23] Smart 5G networks: enabled by network slicing and tailored to customers' needs https://www.gsma.com/futurenetworks/wp-content/uploads/2017/09/5G-Network-Slicing-Report.pdf

For more information please visit:
www.gsma.com/IoT



GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601