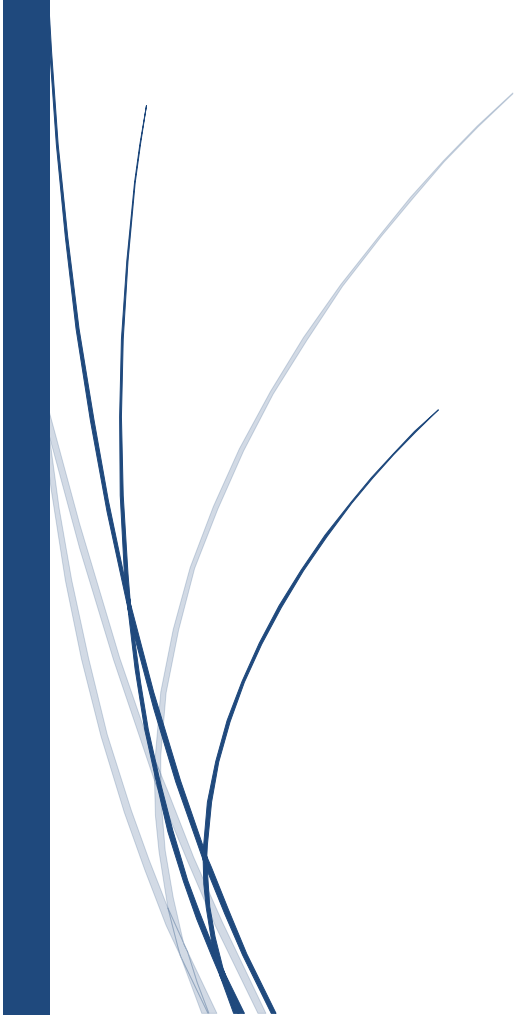
2018-1-31

CAAC

Low-Altitude Connected Drone Flight Safety Test Report



CONTENTS

Foreword

With the rapid development of drones, the topic of supervision has drawn enormous public attention while emerging as a serious challenge for the civil aviation and transportation industry. Supervision bodies of the civil aviation sector urgently need to study drones' operating characteristics and supervision options to launch appropriate, efficient, and feasible technological management solutions. Under the guidance of the Civil Aviation Administration of China (CAAC), the CAAC Information Centre combined available resources, and teamed up with technology companies to carry out technological tests on the supervision of connected drones. These tests focused on the feasibility and effectiveness of cellular networks in drone supervision. Such efforts provided researchers with mastery over core technologies and related intellectual property rights. The test results will help spur the rapid and healthy development of the drone industry, while promoting the expansion of innovative low-altitude digital industries.

I. Development of the Drone Industry

Since 2015, major investment and consulting agencies have released a series of analysis and expectations for the drone industry.

- In 2015, research institute EVTank forecasted that in 2020, global drone sales will reach 4.33 million and the market space will hit a record high of US $25.9 billion.
- In 2016, Goldman Sachs estimated that the market space of commercial drones will reach US $20.6 billion by 2020, while that of civilian drones will reach US $14 billion.
- In May 2016, PwC stated that the total value of business and labor that may be potentially replaced by drone powered solutions will reach US $127 billion.

The drone-related industry chain is also rapidly growing with the rise of a new diverse range of companies. These include DJI, Ehang, TopXGun, Ewatt, Zerotech, 3DR, Parrot, SkyCatch, and DroneDeploy.

Civilian drone technologies are quickly developing. Drones today are getting increasingly better at automatic driving, hovering, obstacle avoidance, and video processing. Non-line-of-sight applications are gradually emerging, adding to the previous line-of-sight ones. In addition, drones are not only seen in the domain of consumption, but are also playing a greater role in inspection, agriculture, logistics, and security.

The prosperity of the drone industry sets out new requirements for communication links. For example, real-time and reliable connected flight safety management must be available for drones at 1000 m and below. When drones are flying at an altitude of 300 m and under, the uplink must support 50 Mbps real-time image transmission and remote control latency must be within 50 ms. Industry forecasts indicate that the combination of drones and mobile communications will generate a tenfold increase in business growth opportunities.

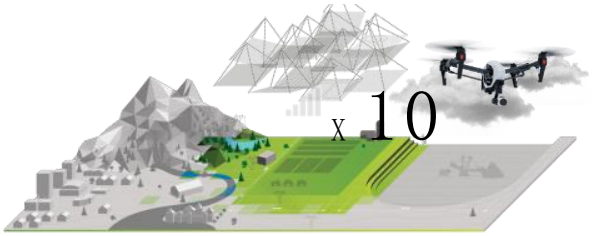


Figure 1 Mobile communication promoting drone industry's development

A. Urgent Need for Ensuring Flight Safety

As the drone industry and related technologies rapidly mature, a great number of civilian and consumer-level drones are put into use. However, this has unfortunately led to an increase in improper drone usage.

a. Currently, civilian drones in the market use open-standard GPS modules. Ground stations and drones interact with each other via the point-to-point communication mode, and such a mechanism is prone to incur following risks:
   - Tampering of GPS data/modules
   - Simulation of stronger false GPS signals

- Cracking of the air interface protocol between drones and controls
- Cracking of the drone application software (to lift no-fly zone restrictions)

In June 2017, a company seeking to circumvent restrictions openly sold drones with anti-fence features, allowing drones to breach governments' no-fly zones. Two months later, a branded agent directly sold drones with modified GPS modules.

b. In April 2017, Chengdu Shuangliu International Airport encountered multiple drone disruptions. Many flights were diverted to other airports in Xi'an, Chongqing, Guiyang, and Mianyang. Flights were forced to return and tens of thousands of passengers were stranded at airports, with no resource.

This series of incidents has adversely led to a negative influence, highlighting the issues associated with this technology. A well-rounded drone safety mechanism must be set up as soon as possible to ensure that drones can be seen, managed, and tracked. This will ensure airspace safety, give drone users greater freedom, and promote the healthy development of the drone industry.

B. Gradual Improvement in Drone Regulations

Government authorities have published multiple guidance documents to initiate special actions to tackle the series of drone-related safety issues.

➢ **Registration Management**

In May 2017, Aircraft Airworthiness Certification Department of CAAC issued *Provisions on the Administration of the Real-name Registration of Civil Unmanned Aircraft*. Civilian drones weighing 250 grams and above must be registered under real names starting from June 1, 2017.

➢ **Operation Management**

In November 2015, CAAC released the *Provisions for the Operation of Light and Small Unmanned Aircraft (for Trial Implementation)*. Drones weighing over 7 kg and beyond visual line of sight (BVLOS) drones of less than 7 kg must be connected with the drone cloud in real time. This system will sound alarms when drones fly into an electric fence.

Class	Net Weight (kg)	Take-off Weight (kg)
I	0 < W ≤ 1.5	
II	1.5 < W ≤ 4	1.5 < W ≤ 7
III	4 ≤ W ≤ 15	7 < W ≤ 25
IV	15 < W ≤ 116	25 < W ≤ 150
V	Plant protection (agriculture/crop-related) drones	
VI	Unmanned airship	
VII	BVLOS Class I and II	
XI	116 < W ≤ 5700	150 < W ≤ 5700
XII	W > 5700	

Figure 2 Drone classification standards

In October 2017, CAAC published *Fence of Unmanned Aircraft System* and *Interface Specifications of*

Unmanned Aircraft and Cloud System to ensure the orderly management of the drone system.

Two months later, Ministry of Industry and Information Technology (MIIT) of China issued the *Guidance of Promoting and Normalizing Commercial Unmanned Aerial Vehicles' Development*. The Guidance proposed the research and introduction of drone digital identification rules and technical solutions (specifying that each drone shall have a dedicated ID). Enterprises are encouraged to add communication modules for civilian drones to implement identification, monitoring, and management.

- **Standard System**

In August 2017, the Office of Standardization Administration of the People's Republic of China issued *Guideline on Building a Standard System for Unmanned Aircraft*[1]. The guideline elaborated upon the objectives and development stages required to establish a standard system for the drone industry.

Phase one (from 2017 to 2018) aims to meet market requirements of the drone system. This includes support for drone industry supervision demands, the preliminarily setup of the drone standard system, and a key focus on developing key standards (that are in urgent need if markets are to support supervision).

Phase two (from 2019 to 2020): aims to gradually promote the establishment of the drone standard system. It is expected that by 2020, a standard system for the drone industry will be appropriately supplemented and complete, with the formulation and revision of more than 300 drone system standards. These standards will cover all basic, management, and technical standards and conform to industry application requirements.

C. Survey on Drone Flight Safety Requirements

Based on the customer survey of drone flight safety policies and markets, a clear set of requirements have been proposed. It is growing increasingly apparent that customers are urging for the close supervision of drones. This is especially targeting the flight management of low-altitude, low-speed, and lightly weighted drones (that account for a high percentage).

Table 1 Major requirements of drone flight safety

No.	Requirement	Description
1	Simplified flight approval	The period of applying for a drone flight plan and flight airspace is excessively long. Therefore, application processes need to be simplified by level and classification. As for drones capable of real-time network connectivity reporting (particularly small-size civil drones), users do not require flight plans, or applications can be quickly approved.
2	Convenient real-name registration	Convenient operations and real-time online verification are supported. Users must manually register on the CAAC website or use related apps to

[1] 《无人驾驶航空器系统标准体系建设指南》

No.	Requirement	Description
		enter accurate information (such as the drone owner identity, contact information, and drone information).
3	Dynamic fence update and notification	Drone fences are updated in real time before departure to provide prompt and on-demand services. Drones cannot take off if the update fails. Fence locations are visible to users to ensure orderly flying. Detection and alarm reporting of drone fence locations are also supported.
4	Reliable geographic verification	Inaccuracy issues related to self-reporting of drone locations are resolved. Potential issues include unreliable drone locations due to terrain-caused instability or perhaps fractured GPS signals and drone takeoff failure due to unsuccessful geographic verification.
5	Reliable real-time communication link	QoS guarantee for drone management links (different classes and categories), status data, and management commands are provided. Additionally, the report interval must be under 1s and the latency must be under 1s as proposed in *Provisions for the Operation of Light and Small Unmanned Aircraft*.
6	Wide-range low-cost safety management	The requirement of civil drones (especially consumer-level drones), for flights at anytime and anywhere is met with low cost. Additionally, overall security in terms of service data and management are ensured with the help of technical means for preventing intrusive system damage or personal injury.

Table 2 Requirements on communication link specifications for drone flight safety

Link Description	Rate	Cellular Network Latency	End-to-End (E2E) Latency	Reliability	Coverage Height
Uplink status information	30–50 kbit/s	50–100 ms	< 1s	10^{-3}	0–1000 m
Downlink management instructions	5–10 kbit/s	20–50 ms	< 300 ms	10^{-3}–10^{-6}	

II. Concepts of Drone Flight Safety

Connected drones indicate a connection to a cellular network. Upon connection to the cellular network,

convenient real-name registration, reliable geographic verification, and real-time reliable data transmission are supported for drones. Moreover, pre-event warning, in-event control, and post-event tracing are facilitated on the basis of secure overall services using integrated comprehensive management processes, as well as encryption and authentication.

Figure 3 Drone flight safety architecture shows the drone flight safety architecture.

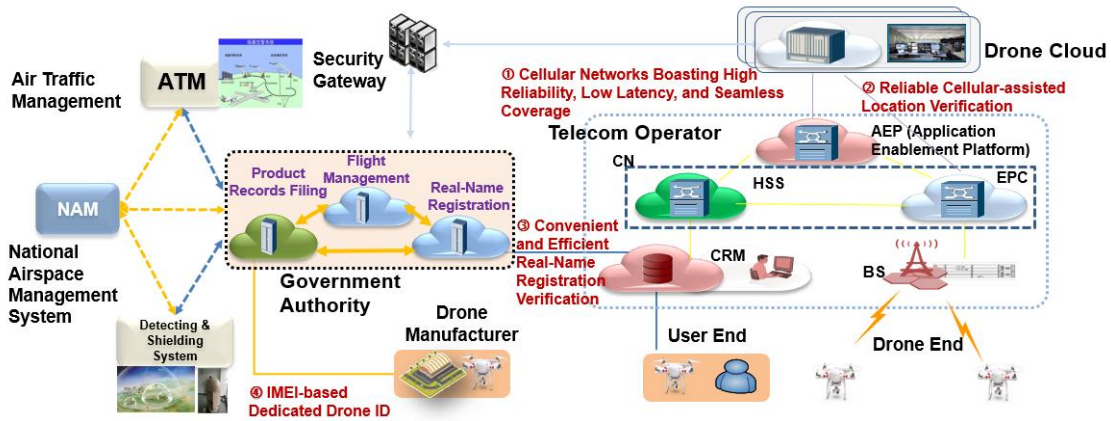


Figure 3 Drone flight safety architecture

Figure 4 shows the connected drone flight safety service flow.

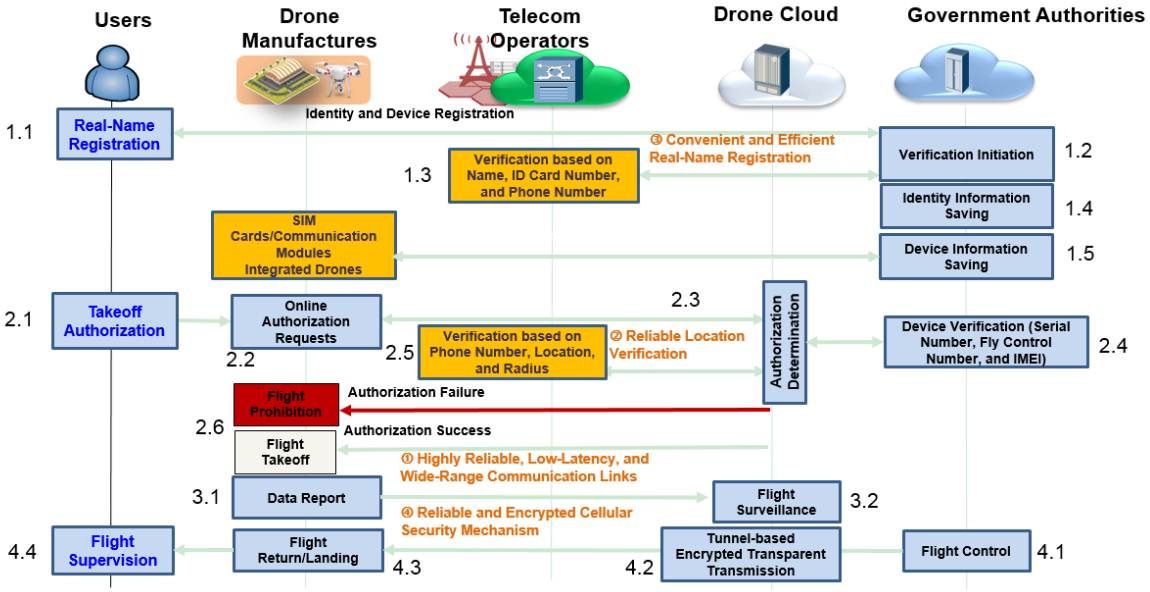


Figure 4 Connected drone flight safety service flow

a. **Cellular Network-based Real-Time, High-Reliable, and Low-Cost Drone Communication Links**

By the beginning of 2017, more than 200 telecom operators in more than 150 countries have deployed 4G networks. In October 2017, the MIIT official website announced that by September 2017, a total of 6.041 million base stations have been constructed across China. However, this type of wide-range communication for drones

consists of 4.471 million 3G and 4G base stations and 3.8 million 4G base stations.

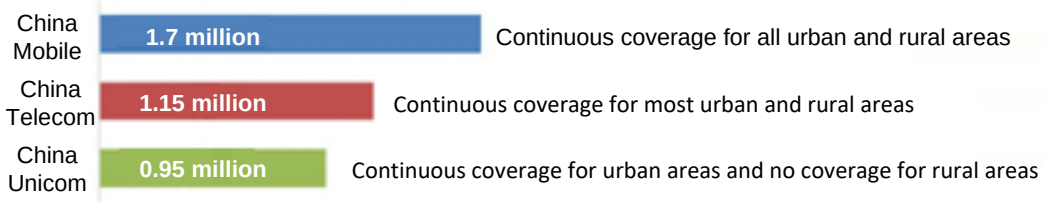


Figure 5 4G base station scale by September 2017

According to live-network tests, a mobile cellular network meets the majority of drone application requirements at an altitude below 120 m. Requirements on service links in most airspace areas below 300 m (see **Table 2 Requirements on communication link specifications for drone flight safety**) can also be fulfilled. Air-to-ground convergence cellular communication supports full coverage of 4G networks below 300 m and 5G networks below 1000 m, and dedicated air-to-air cellular communication supports coverage of specific airspace areas below 10,000 m.

Based on national cellular mobile communication networks (via 4G/5G technologies), an efficient and low-cost flight safety system is constructed for the drone industry to achieve continuous drone management for different levels, types, and regions.

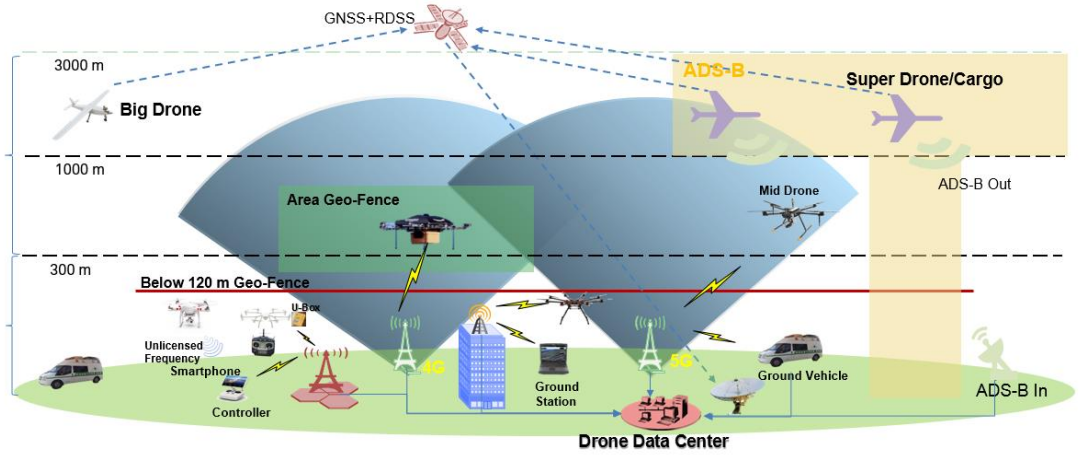


Figure 6 Concepts of drone flight safety

In extreme cases (such as signal interference and weak coverage), cellular communication quality can be ensured by optimizing antenna configuration, uplink and downlink power control, AI-based automatic interference cancellation, coordination of multiple base stations, and site addition.

4G cellular networks currently provide real-time data transmission to contribute to drone flight safety. This involves the calculation of data by a granularity of reported 100-byte data packet based on channel interference and location of the cell where a drone is located. These locations are referred to as the near point, middle point, far point,

and height. The E2E data latency spans 50–300 ms, within which the air interface latency spans 8–50 ms. **Figure 7 Distribution of data transmission latency of a cellular network** shows related latency details.

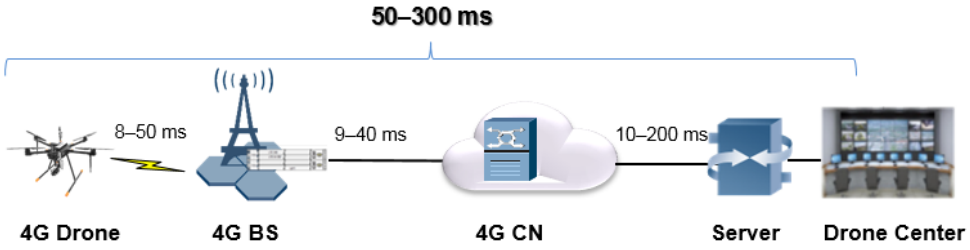


Figure 7 Distribution of data transmission latency of a cellular network

QoS guarantees for cellular networks are classified into Guaranteed Bit Rate (GBR) and non-GBR. Both provide GBR connections with multiple QoS guarantees for drone management links and reserve fixed bearer bandwidths. A drone provides differentiated QoS guarantees for diversified data types, such as management heartbeats, uplink data reports, and downlink management instructions. A cellular network provides QoS class identifiers (QCIs) 1 to 9, further meeting level- and type-specific link management requirements for drone flight safety.

Table 3 QoS levels

QCI	Resource Type	Priority	Packet Latency Budget	Packet Error Loss	Suggestion
1	GBR	2	100 ms	10^{-2}	
2		4	150 ms	10^{-3}	Heartbeats and uplink data reports
3		3	50 ms	10^{-3}	
4		5	300 ms	10^{-6}	Downlink management instructions
5	Non-GBR	1	100 ms	10^{-6}	
6		6	300 ms	10^{-6}	
7		7	100 ms	10^{-3}	
8		8	300 ms	10^{-6}	
9		9			

b. **Location Reliability Using Cellular Network Auxiliary Positioning**

According to *Fence of Unmanned Aircraft System* released by CAAC on October 20, 2017, the drone fence LBS service is aimed at obtaining geographic information of mobile terminal users through a cellular radio

communication network provided by a telecom operator. Moreover, Level 4 capability of the drone cloud must pass an LBS verification test. Telecom operators are expected to provide APIs for reliable geographic verification with the help of the network capability openness platform to provide drone cloud services.

According to the current flight safety survey, drones take off from the ground to solve the problem of inaccurate or fraudulent GPS information. Therefore, drones only meet the specified requirements if reliable geographic verification has been performed prior to takeoff.

In most cases, drone fences are used to isolate and protect specified areas by a coarse granularity of kilometer. In this situation, cell IDs are sufficient for positioning. Cell-ID-based positioning operates on a single base station. Specifically, the location of a mobile terminal is represented according to the location of a cellular base station that serves the mobile terminal. The positioning precision depends on the radius of a cell served by a cellular base station (R = 1/2 inter-site distance, referring to Figure-9 xxx). Given that a drone can be located in a handover area of a cell, the precision is 1.54-fold (calculated by the formula 763/500) R, as shown in xxx. In general, cell radius R is approximately 300–1000 m in urban areas and 2000–4000 m in rural areas.

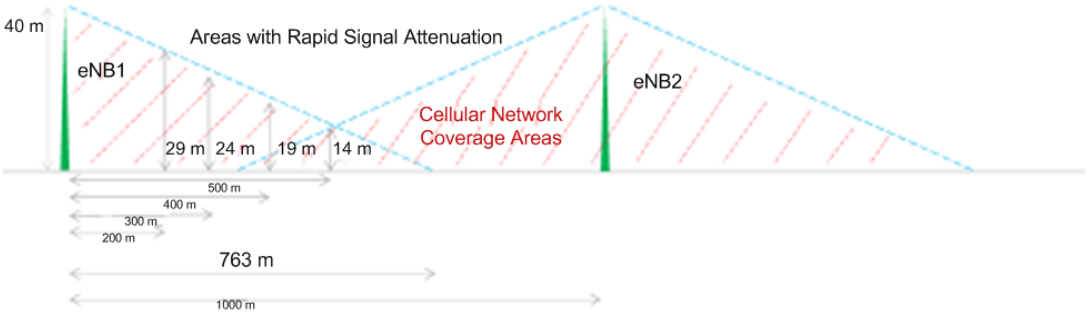


Figure 8 Precision calculation of coarse-granularity cell-ID-based positioning

Figure 9 Cellular network-based location verification shows the location verification design of cellular auxiliary networks provided by a telecom operator.

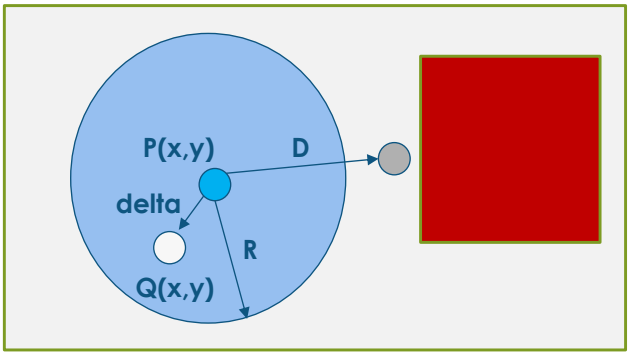


Figure 9 Cellular network-based location verification

In the preceding figure, P (x, y) is the GPS location reported by a drone, and Q (x, y) is the location of the base station that serves the drone. R shows the cell radius, and D indicates the take-off location threshold for verification, namely, the kilometer-level fence protection threshold. R is smaller than D.

The calculation algorithm is as follows: Delta = |P (x, y) – Q (x, y)|.

If Delta ≤ D, the geographic verification is passed. Otherwise, the geographic verification fails.

c. **Real-Name Drone Registration Using Fast and Convenient Real-Name Registration on Mobile Phones**

Drone owners must provide both drone and personal information (including the owner name, ID card number, phone number, and address). Currently, telecom operators have registered real identity information of mobile phone users. Additionally, the network capability openness platform provides an API for real-name identity verification to enable online validation of such information as name, ID card number, and phone number of a drone owner. This ensures convenient, credible, and efficient real-name registration.

For privacy protection purposes, the network capability openness platform must request for security authorization from the app before verifying the identity of a potential owner.

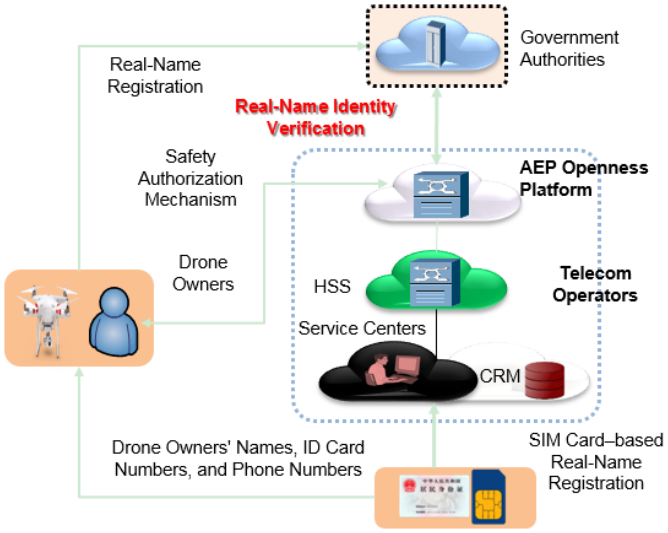


Figure 10 Workflow of real-name drone authentication

d. **A well-established management process and encryption and authentication technologies ensure the overall service security.**

Drone flight safety faces security challenges in terms of terminals, networks, platforms, and E2E management. Therefore, the following three security-ensuring technologies and a well-established management process are critical for drone services.

Figure 11 "Three Technologies+ One Management Process" to ensure service security

i. Terminal security

In 2016, Huawei introduced the integrated Secure Element (inSE) technology, which is applied to Kirin 960 and Kirin 970 chipsets. In October 2017, Huawei realized the commercial launch of this technology in cooperation with China Construction Bank. All mobile phones equipped with the Kirin 960 or 970 chipset support China Construction Bank's personal banking shield function and can complete mobile payments without any need for physical media.

The inSE security module supports encryption and decryption algorithms such as CRT-RSA, RSA, DES/3DES, and AES, and implements cloud-based key management to improve terminal security. This module can also be integrated into future drones. A shield authenticated and authorized by competent government bodies will be recorded on a drone during its registration. In this case, a drone cannot be modified or used without a user name and password even if irretrievable (due to loss or damage).

ii. Network security

The following technologies are the key to ensuring 4G network security:

- Physical and environmental security is ensured through the proper distribution of base stations, regular optimization, continuous watch-out, and periodic inspection.
- Network access security is ensured through temporary identity, two-way authorization, and confidentiality and integrity protection technologies. They help prevent security risks such as user identity leaks, identity masquerading, eavesdropping, and signaling tampering.
- Network and management device security is ensured through network device authentication, intranet IP address isolation, intranet firewall, and security audit technologies. These mechanisms are introduced to prevent data eavesdropping, tampering, or thwart attempts to disguise or attack data during transmission over the network.

iii. Cloud security

Cloud computing solutions are combined with following technologies to ensure cloud security and contribute to drone flight safety.

- Terminal access security technologies (GBA and whitelist)

- Network security (firewall, VPN, and Anti-DDOS)
- Software security (virus scanning and port detection)
- Device security (virtual terminal, device isolation, and data backup)
- Application security (security sandbox, encryption protocols, access control, and security auditing)
- Management security (key management and vulnerability scanning)

At present, Huawei cloud computing solutions have obtained five security certifications from authoritative organizations both at home and abroad. These include C-STAR, information protection (the Ministry of Public Security, China), ISO27001, security review (Cyberspace Administration of China), and Trusted Cloud Service certifications. Huawei solutions have since gained wide industry recognition and are used throughout finance, electric power, and logistics sectors. Large-scale applications are seen in financial institutions with high security requirements (Industrial and Commercial Bank of China, China Construction Bank, China Merchants Bank, and China Everbright Bank).

iv. Process management security

An E2E process involving all stakeholders is set up to achieve overall supervision and management of drones. This includes aspects such as drone product records filing, real-name registration upon purchase, pre-flight online authorization, in-flight real-time data reporting/heartbeat keep-alive/control commands, and post-flight data reporting/inquiries. A process such as this helps to achieve synergy among all functions, connecting government authorities, drone clouds, drones, and drone users and owners. It also ensures overall E2E security and prevents data errors and signaling attacks.

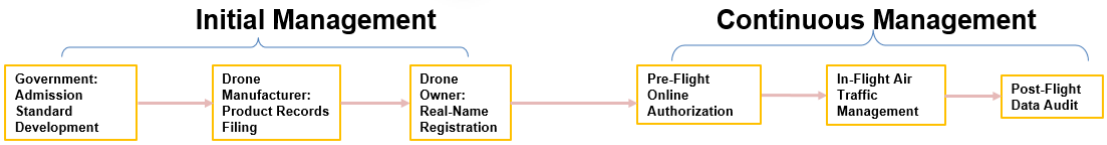


Figure 12 E2E safety assurance for drones

5G networks feature high openness and connection among things. This brings about new challenges to network security. 5G networks incorporate the following technologies to ensure overall security for drone services, robotics, and other vertical industries.

i. **Network functions virtualization (NFV):** Software and hardware are decoupled, universal hardware redundancy is used, and virtual operating systems are deployed to virtualize software and hardware resources to implement dynamic resource deployment and scheduling. Security isolation and redundancy backup are implemented for each telecom network function to enhance the security and reliability of devices and meet the security requirements of vertical industries such as drones, robots, and industrial manufacturing.

ii. **Network slicing:** Each slice (for drones of different classes and categories) is configured with a particular level of security protection to realize slice security as a service (SSaaS). This enables

telecom operators to provide differentiated and customizable security packages (including encryption algorithms, parameters, blacklist and whitelist configuration, authentication methods, and isolation strength). Vertical industries are also able to monitor the performance of security packages, make timely adjustments, delete a number of auxiliary devices (if necessary), and reconfigure resources to prevent external attacks and improve E2E service security.

iii. **Security application enable platform:** In addition to network capabilities, 5G offers security capabilities for vertical industries, eliminating the need for identity authentication, registration authentication, and key management. The security functions in 5G networks are modularized and can be easily invoked through required interfaces. By combining different security functions, security capabilities can be quickly provisioned to meet the E2E security requirements of diverse services.

III. Drone Flight Safety in Practice

In 2017, CAAC collaborated with China Mobile, Ehang, U-Cloud, TopXGun, and Huawei to conduct low-altitude cellular network coverage tests and the overall service feature tests in several cities across China (Nanjing, Guangzhou, Hangzhou, and Shanghai). **Table 4 Tested items on the flight safety of drones and test results** lists the test items and results.

Table 4 Tested items on the flight safety of drones and test results

No.	Test Item	Test Description	Test Result
1	Owner identity registration	The owner registers his/her identification with the government authority through the drone manufacturer's app. The identification includes the owner's name, ID card number, phone number, and address. The government authority can obtain the owner identity information from the telecom operator in real time.	Pass
2	Drone registration	The owner registers the drone's information with the government authority through the drone manufacturer's app. The information includes drone registration code, drone serial number, flight control serial number, and IMEI.	Pass

No.	Test Item	Test Description	Test Result
3	Electric fence update	Before a drone can take off, it obtains the latest electric fence information from the government authority over the drone cloud on the cellular network. If the latest fence fails to be obtained, the drone cannot take off.	Pass
4	Pre-flight device check	Before a drone can take off, it obtains the drone registration code, drone serial number, flight control serial number, and IMEI from the government authority over the drone cloud to conduct a consistency check. If the verification fails, the drone cannot take off.	Pass
5	Pre-flight location verification	Before a drone can take off, it conducts location check over the drone cloud on the cellular network of the telecom operator based on its real-time GPS position. If the verification fails, the drone cannot take off.	Pass
6	Flight heartbeat keepalive	After a drone is powered on and passes authentication, it periodically sends heartbeat messages to the drone cloud to keep heartbeat links alive. If the heartbeat is lost, the drone performs a return or landing.	Pass
7	Real-time flight data reporting	After a drone is powered on and passes authentication, it periodically reports data such as its location, altitude, and status to the drone cloud.	Pass
8	Flight management command transmission	A drone is connected to the drone cloud at all times to receive commands from the government authority in real time and act accordingly (return, landing, or other actions).	Pass
9	Fence alarm detection and warning	The drones and the drone cloud support drone fence alarm detection and warnings.	Pass

a. Despite a small number of coverage holes, the low-altitude cellular network can meet drone flight safety requirements.

In 2017, CAAC collaborated with China Mobile and Huawei to conduct low-altitude network quality tests on 4G live networks. The tests were carried out in different scenarios across multiple cities, covering urban areas, industrial parks, and suburban areas. The inter site distance (ISD) ranges from 180 m to 2000 m. TDD-LTE D band

(2575–2635 MHz) and F band (1885–1915 MHz) are used. The altitude ranges from 50 m to 300 m. Downlink reference signal received power (RSRP), downlink signal to interference plus noise ratio (SINR), and other indicators that are closely related to drone flight safety (uplink service rate, latency, and offline rate) are measured.

Table 5 Low-altitude cellular network coverage test scenarios

	A Stadium in the Urban Area	A Park in the Urban Area	Industrial Park	A School in the Suburban Area	Suburban Area
ISD	Approx. 180 m	Approx. 300 m	Approx. 400 m	Approx. 1000 m	Approx. 2000 m
Ambient characteristics	Lots of buildings	Open area with lakes and lots of woods	Lots of low-rise buildings	Open and plain ground in the center, with buildings around it	Open ground with mountains and woods at distance

i. The signal quality test shows that the RSRP ranges from –80 dBm to –90 dBm when drones are at an altitude of 50 m to 300 m. This indicates healthy 4G network signal strength and coverage. However, the base stations along the flight route are designed to serve ground terminals. Drones at altitude are out of the coverage of antenna lobes. The signals are disordered and drones have no primary service cells. These result in severe downlink interference. In a small number of areas, demodulation is prone to fail and disconnection occurs. In these cases, drones flying for an extended period of time must land or return. The RSRP and SINR distribution in different scenarios is shown in the following figures.

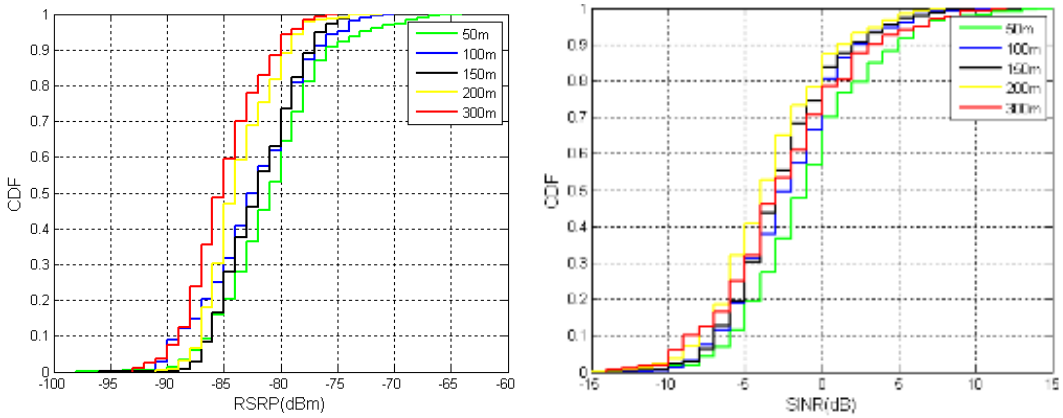


Figure 13 Low-altitude cellular network coverage test results

ii. The test also shows that the average uplink TCP service rate is over 5 Mbps when drones' altitudes range from 50 m to 300 m. In more than 70% of cases, the rate is higher than 5 Mbps. In approximately 1% of the cases, the rate is lower than 1 Mbps. Such performance meets the flight safety requirements for

communication and the collection of status information (30–50 kbps). In areas where drone connection is intact, flight safety can be ensured with 5–10 kbps downlink rate. However, in areas with excessive interference where connection with the drones is lost, it is challenging to transmit commands in the downlink. Drones flying in such areas for long periods of time are prone to land or return.

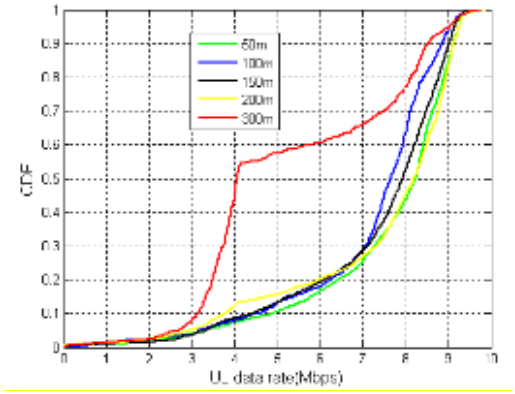


Figure 14 Low-altitude cellular network speed test results

iii. Ping packets (32 bytes) and TCP packets (100 bytes) are used to test the network latency. The result shows that the latency is 200 ms to 300 ms under most circumstances. When drones are at an altitude of 300 m, the latency ranges from 500 ms to 600 ms.

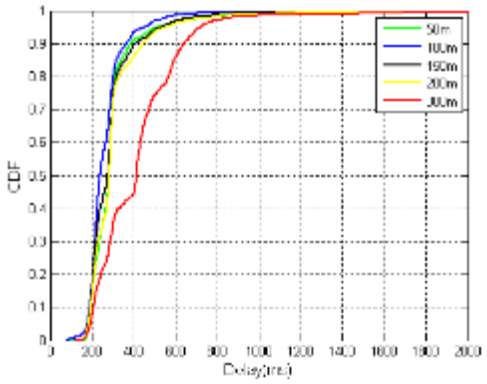
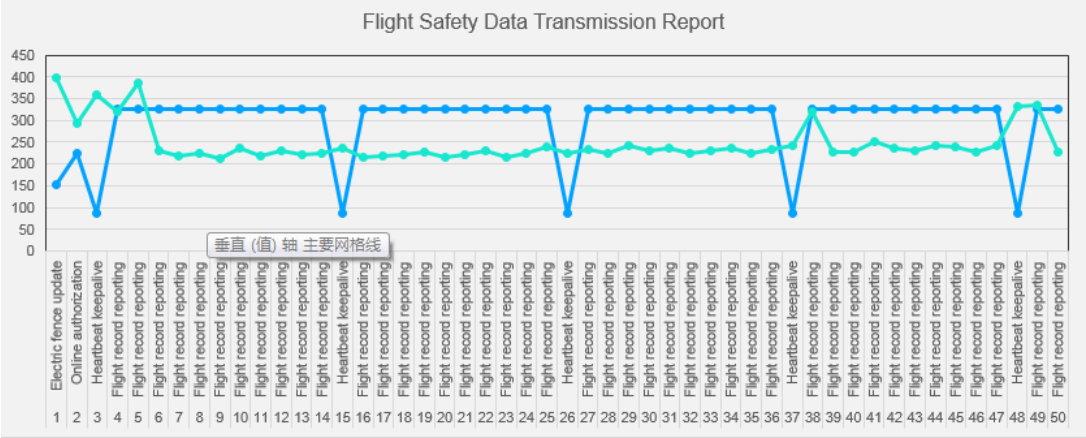


Figure 15 Low-altitude cellular network latency test results

In December 2017, field tests on the uplink data of drones were conducted in Zhejiang, China. The figure below shows the test results.



Item	Packet Length (Byte)	Description	Latency (ms)
Electric fence update	154	Average latency	399
Online authorization	226	Average latency	293
Heartbeat keepalive	87	Average latency	279
		Maximum latency	360
		Minimum latency	226
Flight record	325	Average latency	239
		Maximum latency	386
		Minimum latency	214

Figure 16 Flight data reported in tests

According to the test results, when drone are being powered on, the latency for electric fence update and online authentication message processing is 399 ms and 293 ms, respectively. The average heartbeat keepalive latency is 279 ms and the average flight record latency is 239 ms. These figures indicate that data transmission is stable after the drone takes off and the latency depends mainly on the quality of the network. In addition, when heartbeat keepalive messages are sent, the flight record latency fluctuates, indicating a direct relationship between concurrent uplink packets.

The test results in

Table 2 Requirements on communication link specifications for drone flight safety show that the E2E latency can meet the requirements for the collection of uplink status information. When drones are flying under 300 m, the latency for commands transmission is satisfactory (300 ms). However, the latency is unfortunately larger for drones at altitudes higher than 300 m.

The low-altitude coverage test shows that current networks can support low-altitude (300 m and lower) drone services that are not extremely sensitive to data rate and latency.

The signal coverage strength below 300 m is satisfactory, but the current mobile network is mainly designed for ground terminals. When drones at altitude are beyond the main coverage of the base stations' antenna, the

downlink interference is large. In a number of areas, disconnection may occur for a short while. In addition, downlink interference affects the speed and latency of drone monitoring services. Therefore, networks in these areas must be optimized. The specific procedures include joint processing and neighboring relation optimization.

Radio communication in the air is different from that on the ground in that it suffers from more sources of interference, irregular cell coverage, and complex neighbor relationships. All this adds further complexity to low-altitude coverage and invalidates mobility management. 5G networks can be a solution to these issues by introducing new technologies such as Massive MIMO/3D-MIMO and enhancing existing technologies such as joint processing and automatic neighboring relation optimization.

b. Reliable cellular-assisted location verification complements GPS to boost accuracy and prevent GPS-related fraud.

Five tests were performed at each test point. **Table 6 Location verification test results**lists the urban coverage test results.

Table 6 Location verification test results

	Distance to the Base Station (m)	Location Verification Threshold (m)		
		500	1000	2000
Test point 1	700	N/A	Fails five times	Succeeds five times
Test point 2	400	N/A	Fails five times	Succeeds five times
Test point 3	600	N/A	Fails five times	Succeeds five times
Test point 4	150	Fails once and succeeds four times	Succeeds five times	Succeeds five times

Over 100 tests were conducted based on randomly constructed GPS values. The location verification reliability reaches 100%.

The location verification threshold is recommended to be twice the cell radius (ISD) based on the distribution of base stations across China Mobile's networks and the configuration of drone fences (see **Figure 9 Cellular network-based location verification**).

Table 7 Suggestions on the location verification threshold

	City	Suburb	Rural Areas
Maximum cell radius (m)	1000	2000	4000
Threshold (m)	2000	4000	8000

c. Enhanced cellular network identity authentication enables convenient and efficient real-name drone

registration.

The real-name authentication service provided by telecom operators now enjoys wide application throughout the field of Internet finance. The CAAC Information Centre and China Mobile are now benefiting from the open application platform interface (API). Field tests indicate that the app can detect incomplete and inconsistent personal information in real-time (within 1 second). The detection accuracy reaches 100%. The app also reminds users to enter the correct identity information, which ensures efficient and convenient real-name drone registration.

Table 8 Test results of real-name registration identity authentication

	Case	Information	Test Result	Conclusion
1	Authentic identity information	a. Phone number: 1502441XXXX b. ID card number: 310231987110XXXXX c. Name: XXX	The identity information is matched.	Pass
2	Incorrect phone number	a. Phone number: 1502441XXXX b. ID card number: 310231987110XXXXX c. Name: XXX	The identity information is incorrect.	Pass
3	Incorrect name	a. Phone number: 1502441XXXX b. ID card number: 310231987110XXXXX c. Name: XXX	The identity information is incorrect.	Pass
4	Incorrect ID card number	a. Phone number: 1502441XXXX b. ID card number: 310231987110XXXXX c. Name: XXX	The identity information is incorrect.	Pass

d. Cellular-network-based information security ensures drones' overall service security.

Currently, the drone cloud and drones only process data link messages on drone flight safety (see **Table 1 Major requirements of drone flight safety**), including electric fence update, online authorization, real-time data reporting, command management, and heartbeat keepalive.

Downlink management commands and heartbeat response sent by the rogue drone cloud constitute the main risks to drones' flight safety. At present, management commands and the heartbeat messages only involve two operations: return and landing. No serious incident will occur in the case of intrusion.

Table 9 Flight safety control test results

Item	Function Description	Test Result
Management	Drones receive and identify	**Pass**: Drones correctly follow the return/landing

commands	management commands from the government authorities, perform corresponding operations, and reject commands from other sources.	instructions. Drones do not follow illegal instructions or obey other commands (such as posture control) in management links.
Heartbeat message	Drones periodically receive and send heartbeat messages. If no heartbeat keepalive response is received within a specified period, drones perform the established return operation.	**Pass:** Drones' heartbeat keepalive function is normal. Drones do not respond to unidentified or incorrect heartbeat messages. Drones return if no heartbeat response is received within a specified period.
Network security	The mobile network security test verifies the signaling processes of mature security technologies. The processes include air interface encryption, device authentication, user authentication, IP address isolation, and cloud security audit.	**Pass:** China Mobile's information security projects are tested by communications administrations twice a year and by MIIT once per year (test dates vary each year). The projects have passed periodic security audit and information security authentications (such as NSFOCUS and security reviews Cyberspace Administration of China).

The following figures show the key drone flight safety test results.

Figure 17a Performing a return operation according to the management command

Figure 17b Performing a return operation in the case of heartbeat disconnection

IV. Vision for Drone Flight Safety

Drone's flight safety requires joint efforts of all social sectors:

a. Government authorities: Formulate drone admission standards and management standards, and provide product databases.

b. Drone cloud: The cloud must coordinate with drones to enable real-time flight management. It must also assist government authorities with drone management and support interconnection and interworking between drones.

c. Drone manufacturers: Produce connected drones that comply with national standards. Documents about all drones must be filed before sale.

d. Telecom operators: Provide reliable communication connections, real-time service assurance, real-name registration, and location verification for drones.

As a critical body in ensuring drones' flight safety, CAAC will team up with more communications equipment vendors and telecom operators such as China Mobile and Huawei. The aim is to help construct a future intelligent air traffic management system featuring broadband, low latency, and reliable communications offered by 4G and 5G technologies. This system will ensure efficient, orderly drone transportation management, allowing drones to fly safely and freely without violating airspace regulations. It will also contribute to the Digital Sky Initiative and promote the prosperity of low airspace economy.

Figure 18 Digital sky

Appendix

1. Agencies and companies participating in this research (in no particular order)

a. CAAC Information Centre/Flight Standard Department/Aircraft Airworthiness Certification Department
b. Equipment Institute of Center for Information Industry Development (CCID), MIIT
c. Aircraft Owners and Pilots Association of China (AOPA-China)
d. Huawei Wireless X Labs
e. 5G Joint Innovation Centre of the China Mobile Communications Research Institute
f. Beijing U-Cloud Aviation Technology Co., Ltd.
g. Shanghai TopXGun Robotics Co., Ltd
h. Guangzhou Ehang Electronic Co., Ltd.

2. References

a. CAAC, AC-91-FS-2015-31, *Provisions for the Operation of Light and Small Unmanned Aircraft*
b. CAAC, AC-61-FS-2016-20R1, *Air Traffic Management Regulations for Civilian Unmanned Aircraft System*[2]
c. CAAC, MH/T 2008-2017, *Fence of Unmanned Aircraft System*
d. CAAC, MH/T 2009-2017, *Interface Specifications of Unmanned Aircraft and Cloud System*
e. CAAC, AP-45-AA-2017-03, *Provisions on the Administration of the Real-name Registration of Civil Unmanned Aircraft*
f. CAAC, CCAR-118TM, *China Civil Aviation Radio Management Regulations*[3]
g. Office of the Standardization Administration of the People's Republic of China, Jun. 2017, *Guideline on Building a Standard System for Unmanned Aircraft*
h. MIIT, Dec. 2017, *Guidance of Promoting and Normalizing Commercial Unmanned Aerial Vehicles' Development*
i. 3GPP, TR 22.891 V14.2.0, *Feasibility Study on New Services and Markets Technology Enablers*
j. 3GPP, TR 36.777 V0.0.1, *Study on Enhanced LTE Support for Aerial Vehicles*
k. 3GPP, TSG-SA WG1 Meeting #71, *SMARTER: Modifications to use case for UAV Remote Control*

[2] 《民用无人驾驶航空器系统空中交通管理办法》

[3] 《中国民用航空无线电管理规定》