International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.677

(03/2020)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

OSI networking and system aspects – Naming, Addressing and Registration

Identification mechanism for unmanned aerial vehicles using object identifiers

Recommendation ITU-T X.677

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	
Services and facilities	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalling and switching	X.50–X.89
Network aspects	X.90–X.149
Maintenance	X.150–X.179
Administrative arrangements	X.180–X.199
OPEN SYSTEMS INTERCONNECTION	
Model and notation	X.200–X.209
Service definitions	X.210–X.219
Connection-mode protocol specifications	X.220–X.229
Connectionless-mode protocol specifications	X.230–X.239
PICS proformas	X.240–X.259
Protocol Identification	X.260–X.269
Security Protocols	X.270–X.279
Layer Managed Objects	X.280–X.289
Conformance testing	X.290–X.299
INTERWORKING BETWEEN NETWORKS	
General	X.300–X.349
Satellite data transmission systems	X.350–X.369
IP-based networks	X.370–X.379
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	
Networking	X.600–X.629
Efficiency	X.630–X.639
Quality of service	X.640–X.649
Naming, Addressing and Registration	**X.650–X.679**
Abstract Syntax Notation One (ASN.1)	X.680–X.699
OSI MANAGEMENT	
Systems management framework and architecture	X.700–X.709
Management communication service and protocol	X.710–X.719
Structure of management information	X.720–X.729
Management functions and ODMA functions	X.730–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	
Commitment, concurrency and recovery	X.850–X.859
Transaction processing	X.860–X.879
Remote operations	X.880–X.889
Generic applications of ASN.1	X.890–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	X.1000–X.1099
SECURE APPLICATIONS AND SERVICES (1)	X.1100–X.1199
CYBERSPACE SECURITY	X.1200–X.1299
SECURE APPLICATIONS AND SERVICES (2)	X.1300–X.1499
CYBERSECURITY INFORMATION EXCHANGE	X.1500–X.1599
CLOUD COMPUTING SECURITY	X.1600–X.1699
QUANTUM COMMUNICATION	X.1700–X.1729

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.677

Identification mechanism for unmanned aerial vehicles using object identifiers

Summary

Recommendation ITU-T X.677 analyses the requirements for full life-cycle management and operating identity recognition of unmanned aerial vehicles (UAVs) with security considerations. It also specifies an identification mechanism for UAVs using object identifiers (OIDs), including detailed specifications of assignment rules and registration procedures of OIDs used for UAVs.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T X.677	2020-03-08	17	11.1002/1000/14039

Keywords

Identification, OID, unmanned aerial vehicle (UAV).

[*] To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T X.677

Identification mechanism for unmanned aerial vehicles using object identifiers

1 Scope

This Recommendation analyses the requirements for full life-cycle management and operating identity recognition of unmanned aerial vehicles (UAVs) with security considerations. It also specifies an identification mechanism for UAVs using object identifiers (OIDs), including detailed specifications of assignment rules and registration procedures of OIDs used for UAVs.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.660] Recommendation ITU-T X.660 (2011) | ISO/IEC 9834-1:2012, *Information technology – Procedures for the operation of object identifier registration authorities: General procedures and top arcs of the international object identifier tree.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 international object identifier tree [ITU-T X.660]: A tree whose root corresponds to [ITU-T X.660] and whose nodes correspond to Registration Authorities responsible for allocating arcs from a parent node.

3.1.2 object identifier (OID) [ITU-T X.660]: An ordered list of primary integer values from the root of the international object identifier tree to a node, which unambiguously identifies that node.

3.1.3 primary integer value [ITU-T X.660]: A primary value of type integer used to unambiguously identify an arc of the international object identifier tree.

3.1.4 primary value [ITU-T X.660]: A value of a specified type assigned to an arc of the OID tree that can provide an unambiguous identification of that arc within the set of arcs from its superior node.

3.1.5 registration [ITU-T X.660]: The assignment of an unambiguous name to an object in a way which makes the assignment available to interested parties.

3.1.6 registration procedures [ITU-T X.660]: The specified procedures for performing registration and amending (or deleting) existing registrations.

3.1.7 relative object identifier [b-ITU-T X.680]: A value which identifies an object by its position relative to some known object identifier.

3.1.8 secondary identifier [ITU-T X.660]: A secondary value restricted to the characters forming an (ASN.1) identifier (see Rec. ITU-T X.680 | ISO/IEC 8824-1), assigned either in an ITU-T Recommendation, an International Standard or by some other Registration Authority to an arc of the OID tree.

NOTE – An arc of the international object identifier tree can have zero or more secondary identifiers.

3.1.9 secondary value [ITU-T X.660]: A value of some type associated with an arc that provides additional identification useful for human readers, but that does not in general unambiguously identify that arc, and is not normally included in computer communications.

3.1.10 Unicode label [ITU-T X.660]: A primary value that consists of an unbounded sequence of Unicode characters that does not contain the SPACE character (see clause 7.5 of [ITU-T X.660] for other restrictions) used to unambiguously identify an arc of the OID tree.

NOTE 1 – Unicode labels are always case sensitive for matching purposes and when determining unambiguity. However, all Unicode labels from a given OID node shall be distinct after normalization.

NOTE 2 – An arc of the international object identifier tree can have multiple Unicode labels.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 physical object: A material object existing in the world or the mirror object of this material object acting in a network.

3.2.2 UAV identification: The ability to establish the identity of a specific unmanned aerial vehicle (UAV) and its associated owner and pilot.

3.2.3 UAV identity: A data set that can be traced to a unique unmanned aerial vehicle (UAV), its owner and/or operator.

3.2.4 unmanned aerial vehicle (UAV): An aircraft operated without the possibility of direct human intervention from within or on the aircraft.

3.2.5 virtual object: Any object that is not covered by the definition of a physical object, such as a data module or a security module.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AIDC	Automatic Identification and Data Collection
E-id	Electronic identifier
GCS	Ground Control Station
ICT	Information Communication Technology
MCS	Monitoring and Control Station/Server
NVM	Non-Volatile Memory
OID	Object Identifier
PKI	Public Key Infrastructure
RA	Registration Authority
RFID	Radio Frequency Identification
UAV	Unmanned Aerial Vehicle
WORM	Write Once Read Multiple

5 Conventions

None.

6 General requirements of OIDs for unmanned aerial vehicles (UAVs)

6.1 Overview

There are many different types of unmanned aerial vehicles (UAVs) using a wide variety of technologies. The lack of standardized monitoring procedures does not permit effective supervision of product quality and operation activities of UAVs. The quality assurance and identification of the owner/operator of a UAV are of greatest concern to regulatory authorities. To achieve this goal, this Recommendation proposes to associate object identifiers (OIDs) of UAV devices not only with all stages of the UAV life-cycle (manufacturing, marketing, repairing and scrapping), but also with the owner/user personal information through regular registration procedures.

Figure 1 shows some key elements in identity management of UAVs such as the UAVs themselves, ground control stations (GCSs) and the owners/users.

Figure 1 – Key elements in identity management of UAVs

6.2 Characteristics of OIDs for UAVs

– Identifying anything in the ICT infrastructure:

In order to enhance the identification and monitoring of UAVs, series of data related to UAV activities need to be shared in real time and processed correctly. It is necessary to associate OIDs with many objects related to a UAV to enable correct locating and real time handling of these objects.

– Communication between things:

OIDs [ITU-T X.660] can be used to identify objects in the information communication technology (ICT) environment, especially objects that represent physical entities. OIDs would also enable UAVs to communicate with people and other objects using various technologies.

– Independence of different network technologies and devices:

In ICT environments, numerous devices may connect with each other using different networking technologies. OIDs [ITU-T X.660] are independent of networking technologies and have been widely used to identify objects related to UAVs even in different networking scenarios.

6.3 Identity classification and storage

6.3.1 Identity classification

Two tamper-resistant identifiers are used to identify a UAV. The first identifier is a physical identifier, which is recommended to be always used. In addition, there is a second identifier, the electronic identifier (E-id), which is optional.

The physical identifier is similar to a vehicle identification number. The physical identifier is produced by the manufacturer in accordance with coding rules at the production stage and is printed or pasted onto the surface of the UAV. It can be a string or combination of digits and letters and it can also be coded in a two-dimensional code. It is recommended to use an OID as the physical identifier and to make it both electronically and physically readable.

The electronic identifier (E-id) is similar to a vehicle license plate number. While regulatory authorities have the right to define their own E-id regulations, it is recommended that regulatory authorities adopt OIDs as the UAV E-id directly. In this case, the owner/user obtains an E-id from the regulatory authority when registering the UAV. The E-id should be used to uniquely identify a UAV in its operating period, be continuously available in near-real time and be electronically readable.

Different countries may have different requirements for UAV management. OID or E-id may be required to be identified remotely. When an OID or E-id is required to be used remotely, the OID or E-id should be written into the safe storage area of the UAV by the owner/user.

6.3.2 Identifier storage

Identifier storage is shown in Figure 2.

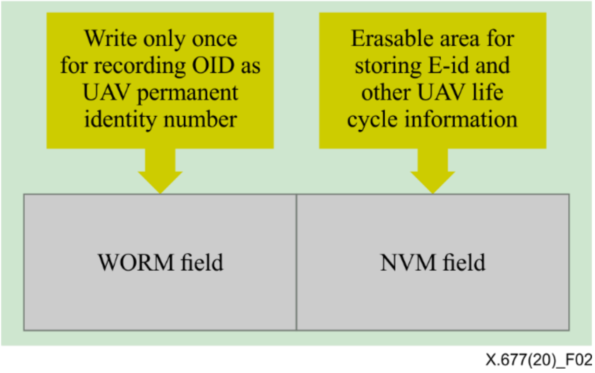

Write only once for recording OID as UAV permanent identity number
Erasable area for storing E-id and other UAV life cycle information
WORM field
NVM field
X.677(20)_F02

Figure 2 – Identifier storage

To be electronically readable, it is suggested that the OID should be written into the UAV device using Write Once Read Multiple (WORM) technology during the manufacturing period.

For E-id storage, E-id could also be written into the non-volatile memory (NVM) of the UAV device. The NVM is erasable and may be subsequently updated.

7 Full life-cycle management and OID assignment rules

7.1 Full life-cycle management scenario of UAVs

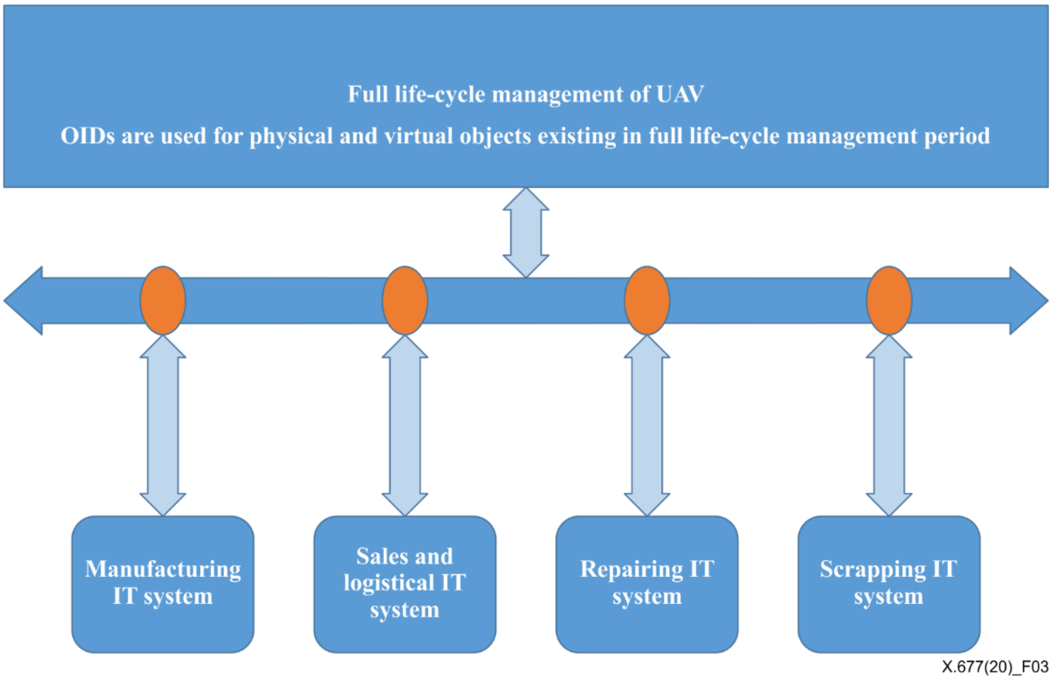

Full life-cycle management of UAV
OIDs are used for physical and virtual objects existing in full life-cycle management period
Manufacturing IT system
Sales and logistical IT system
Repairing IT system
Scrapping IT system
X.677(20)_F03

Figure 3 – Full life-cycle management of UAV

Figure 3 shows a typical full life-cycle management scenario of UAV. Figure 4 shows a description of this full life-cycle management scenario in six stages with more details below:

There are six stages in a full life-cycle management:

Stage 1: Identity encoding and distribution

Regulatory authorities are responsible for the development of OID coding rules and allocation of numbering segments. OIDs are used to define both physical and virtual objects, with considerations of encoding and storage rules for OID encoded structure, data compaction rules, processing of data presentation and capture, data modules of exchange information, etc. A feasible and efficient OID distribution mechanism should be built.

Stage 2: Manufacturing

The manufacturer is responsible for writing and/or setting the OID on a UAV cover, to aid recognition of the UAV identity when radio technologies do not work.

Stage 3: Circulation

Sales and logistical companies shall record data related to UAVs, according to standardized data modules identified by OID.

Stage 4: Registration

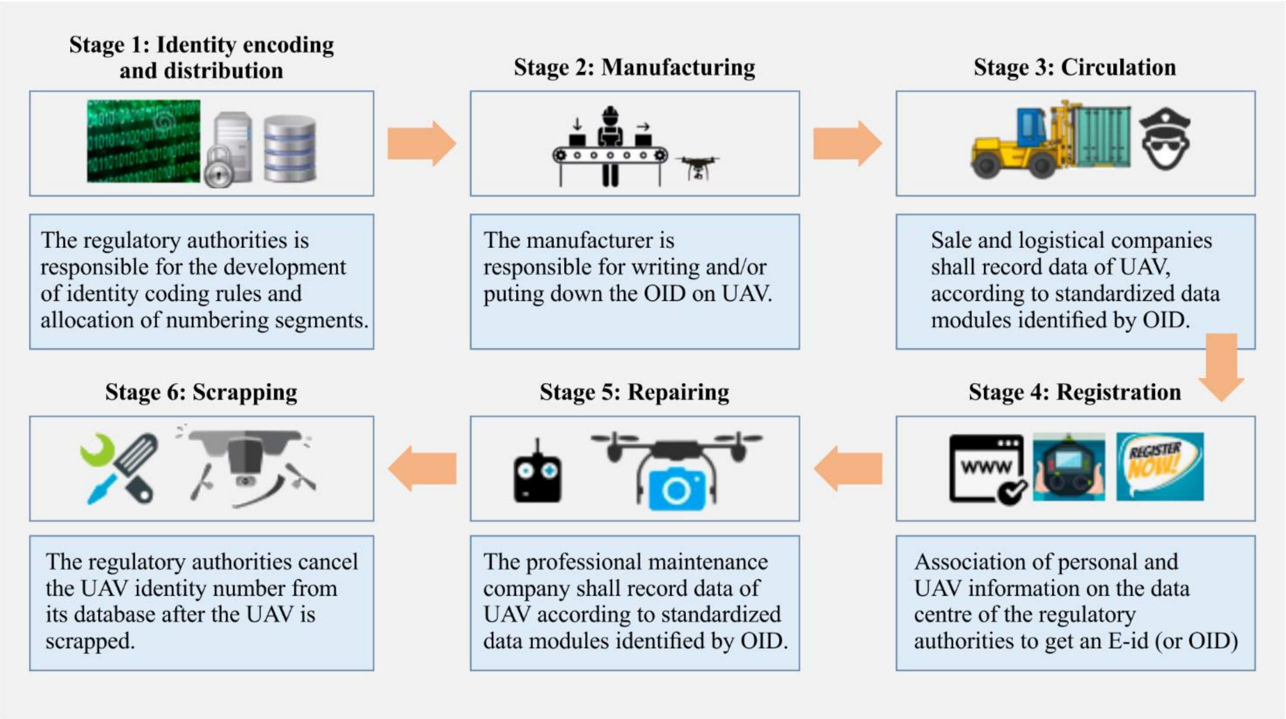
An association of both personal information and UAV information should be registered on the data centre of the regulatory authorities in order to obtain a unique identity number.

Stage 5: Repairing

Professional maintenance companies shall record data related to UAVs during the maintenance period, according to standardized data modules identified by OID.

Stage 6: Scrapping

Scrapping agencies shall inform the regulatory authorities about the scrapping work of a UAV. The regulatory authorities can cancel the UAV identity number from its database and inform the end users.



Stage 1: Identity encoding and distribution

The regulatory authorities is responsible for the development of identity coding rules and allocation of numbering segments.

Stage 2: Manufacturing

The manufacturer is responsible for writing and/or puting down the OID on UAV.

Stage 3: Circulation

Sale and logistical companies shall record data of UAV, according to standardized data modules identified by OID.

Stage 4: Registration

Association of personal and UAV information on the data centre of the regulatory authorities to get an E-id (or OID)

Stage 5: Repairing

The professional maintenance company shall record data of UAV according to standardized data modules identified by OID.

Stage 6: Scrapping

The regulatory authorities cancel the UAV identity number from its database after the UAV is scrapped.

X.677(20)_F04

Figure 4 – Scenario description for the full life-cycle management of a UAV

7.2 OID assignment rules and usage

7.2.1 Dedicated UAV OID

The OID [ITU-T X.660] dedicated to the identification of UAVs is `{joint-iso-itu-t(2) uav(52)}`. Information about the registration authority for this UAV OID can be found in the jointly administered registers which can be downloaded from the ITU-T SG17 web page[1].

7.2.2 OID assignment rules

This Recommendation defines OID assignment rules for both physical and virtual objects under the dedicated UAV OID as follows.

The assignment rules for OIDs are listed in Table 1.

Table 1 – OID arcs for both physical and virtual objects of UAVs

OID arc	Objects
{joint-iso-itu-t(2) uav(52) 1}	UAV devices
{joint-iso-itu-t(2) uav(52) 2}	Ground control stations
{joint-iso-itu-t(2) uav(52) 3}	Monitoring devices

[1] The jointly administered registers can be downloaded directly from http://www.itu.int/go/x660.

Table 1 – OID arcs for both physical and virtual objects of UAVs

OID arc	Objects
{joint-iso-itu-t(2) uav(52) 4}	Data modules for the full life-cycle management of UAVs
{joint-iso-itu-t(2) uav(52) 5}	Security modules

According to [b-ITU-T X-Sup.31], the OID assignment rules for UAV devices, GCS and monitoring devices are as listed in Table 2, and consist of an OID arc for the UAV or GSC or monitoring device and a physical serial number. Each constituent part is considered as a relative OID. The coding rules are shown in detail in Annex A.

Table 2 – OID arcs for UAV devices, GCS and monitoring devices

OID arc	Physical serial number (as relative OIDs)		
{joint-iso-itu-t(2) uav(52) 1}	Manufacturer's ID	Category ID	Entity ID
{joint-iso-itu-t(2) uav(52) 2}	Manufacturer's ID	Category ID	Entity ID
{joint-iso-itu-t(2) uav(52) 3}	Manufacturer's ID	Category ID	Entity ID

The OID assignment rules for data modules for the full life-cycle management of UAVs are listed in Table 3.

Table 3 – OID arcs for data modules for the full life-cycle management of UAVs

OID arc	Object
{joint-iso-itu-t(2) uav(52) 4 1}	Data modules of a manufacturing system
{joint-iso-itu-t(2) uav(52) 4 2}	Data modules of a sales and logistical system
{joint-iso-itu-t(2) uav(52) 4 3}	Data modules of a repairing system
{joint-iso-itu-t(2) uav(52) 4 4}	Data modules of a scrapping system

7.2.3 OID usage

The OID of a UAV should be continuously available in near-real time, electronically and physically readable, tamper resistant and easily accessible.

According to [b-ITU-T X-Sup.31], an OID should act as the unique identifier of a UAV during its full life-cycle management period and should be combined with several automatic identification and data collection (AIDC) technologies in order to be physically readable:

– OID and manufacturer's logo information can be engraved on the UAV's fuselage cover directly or can be generated as a unique two-dimensional code engraved on the UAV's fuselage cover using laser etching or spraying technology.

– OID can be written into a radio frequency identification (RFID) chip attached on the UAV's fuselage cover and readable by mobile phone or other smart devices.

7.3 Security, encryption and authentication

According to the general requirements in clause 6, it is recommended to use a public key infrastructure (PKI) mechanism where the subject components of the certificates are OIDs.

8 Operating identity recognition and OID assignment rules

8.1 Identity recognition scenario of operating UAVs

As shown in Figure 5, there are three possible solutions to identity recognition of operating UAVs: local non-cellular broadcasting, GCS network multicasting and GCS/cellular monitoring station network multicasting. Regulatory authorities of different countries can choose different solutions according to national regulations. For example, a country might only select a local non-cellular broadcasting solution, while another country might require a local non-cellular broadcasting along with, optionally, GCS network multicasting.

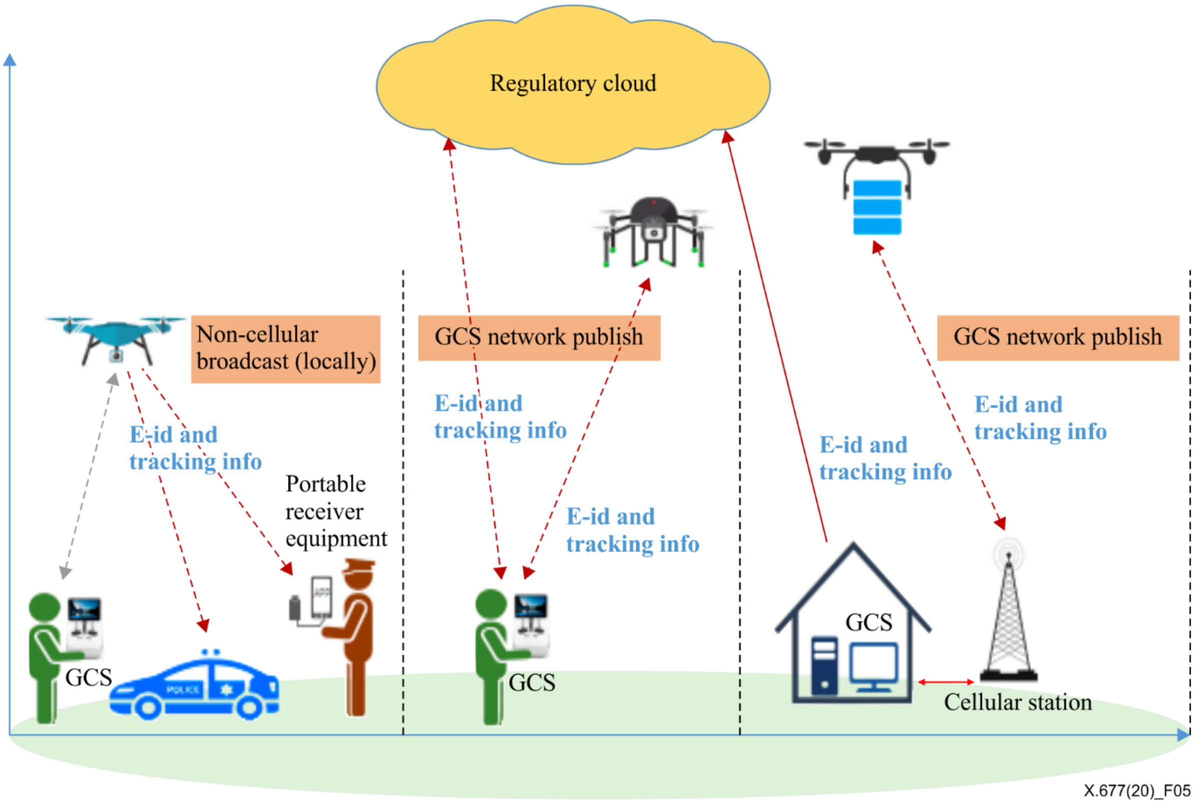


Figure 5 – Identification recognition scenario of operating UAVs

The composition of the identity recognition mechanism of operating UAVs is shown in Figure 6.

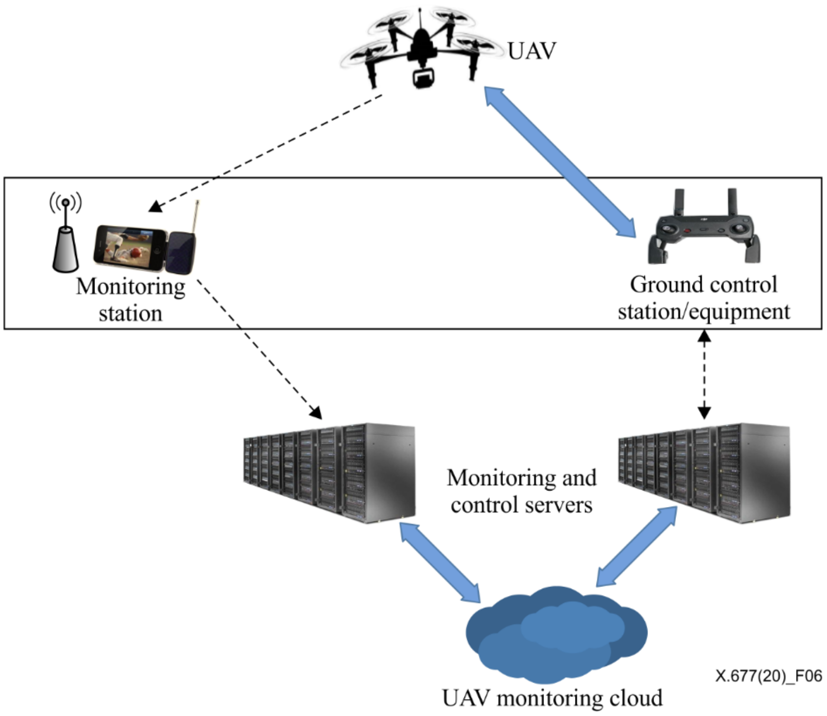

UAV
Monitoring station
Ground control station/equipment
Monitoring and control servers
UAV monitoring cloud
X.677(20)_F06

Figure 6 – Composition of identity recognition mechanism of operating UAVs

The identity recognition mechanism of operating UAVs includes the following components:

- Unmanned aerial vehicle (UAV) device
- Ground control station (GCS)/equipment
- Monitoring station
- Monitoring and control servers (MCSs)
- UAV monitoring cloud

The working flow of operating identity recognition is as follows:

- Flight of UAV is controlled by GCS.
- UAV should broadcast, at a suitable frequency and slot time, its real-time information including: E-id (or OID), location information with a time stamp (location of UAV and location of GCS) and parameters of flight conditions (optional): flight plan, UAV status, etc.
- The monitoring station should keep searching for real-time information of the UAV, demodulating the information after detection and reporting it to the MCSs.
- The MCSs complete the identity authentication process and make a record of related flight data. The flight data record should have integrity non-repudiation properties.
- Different MCSs and GCS could be connected together in a UAV monitoring cloud.

8.2 OID assignment rules and usage

8.2.1 OID assignment rule

When a UAV is operating, there may be new virtual objects that need to be identified such as data modules being used in the UAV system, GCS system, MCS system, UAV monitoring cloud system, etc.

The assignment rules of OIDs used for operating identity recognition of a UAV are listed in Table 4.

Table 4 – OID arc for operating identity recognition of UAVs

OID arc	Objects
{joint-iso-itu-t(2) uav(52) 6}	Data modules for identity recognition of UAV

The OID assignment rules for data modules of operating identity recognition are listed in Table 5.

Table 5 – OID arcs for data modules of operating identity recognition

OID arc	Objects
{joint-iso-itu-t(2) uav(52) 6 1}	Data modules of UAV systems
{joint-iso-itu-t(2) uav(52) 6 2}	Data modules of UAV GCS systems
{joint-iso-itu-t(2) uav(52) 6 3}	Data modules of UAV MCS systems
{joint-iso-itu-t(2) uav(52) 6 4}	Data modules of UAV monitoring cloud systems

8.2.2 OID usage

Besides used as an UAV's broadcasted identity, E-id (or OID) could also be reported to MCS through mobile communication network. This would achieve effective regulation of commercial UAVs across the world through authentication of UAVs based on OIDs together with their broadcast pattern or mobile communication network pattern.

8.3 Security, encryption and authentication

Figure 7 shows a sequence diagram of the communication between a UAV, a receiver device and a database centre. The database centre consists of GCS, monitoring station and UAV monitoring cloud.

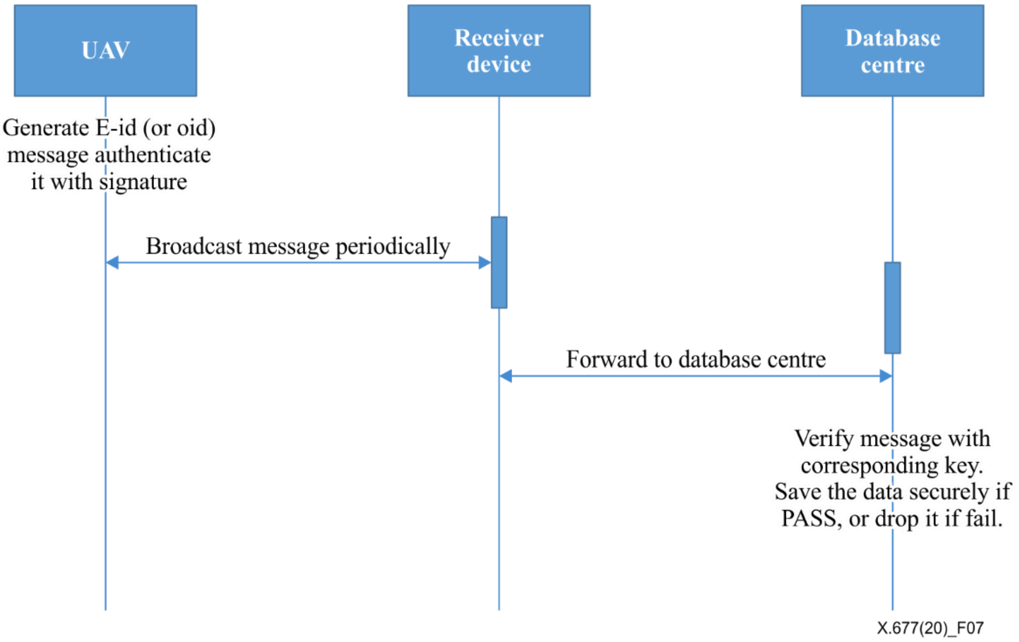

UAV
Receiver device
Database centre
Generate E-id (or oid) message authenticate it with signature
Broadcast message periodically
Forward to database centre
Verify message with corresponding key.
Save the data securely if PASS, or drop it if fail.
X.677(20)_F07

Figure 7 – UAV communication and security, encryption and authentication

If the broadcast message does not carry sensitive personal privacy or key confidential data, it does not need to be encrypted.

The broadcast message shall be protected against unauthorized modification, which must be authenticated by an UAV unique symmetric or asymmetric key.

Authentication algorithms could use any open industry standard in order to meet general requirements in clause 6.

9 Registration procedures for the UAV OID

9.1 General

When receiving an application for an OID from a manufacturer or related IT service provider, the registration authority (RA) for the UAV OID (see clause 7.2.1) will assign a subsequent OID. The applicant is then responsible for the allocation of further subsequent arcs in compliance with [ITU-T X.660].

9.2 Registration application

Applicants should submit the following information:

a) Name of the organization that submits the application;

b) Name, postal address, e-mail address and optionally telephone numbers for the contact point within the requesting organization;

c) Identification of the person submitting the application;

d) Description of the usage of the OID planned to be allocated;

e) (optionally) Any desired secondary identifier(s);

f) (optionally) Any desired Unicode label(s);

g) (optionally) Assignment rules for subsequent OIDs of the OID planned to be allocated.

Applicants should also transmit any supporting documents if requested.

9.3 Verification and acceptance

The application is checked on the basis of the submitted information and supporting documents.

An application should be accepted if judged by the registration authority of the UAV OID that the requested OID will identify typical and common objects.

In response to a notice of rejection, the applicant can submit, to the ITU-T study group responsible for the maintenance of this Recommendation, a supplement to its original application that responds to the reason(s) for rejection.

The appeal shall be resolved by the ITU-T study group responsible for the maintenance of this Recommendation.

NOTE – At the time of approval of this Recommendation, the study group responsible for the maintenance of this Recommendation is ITU-T SG 17.

9.4 Registration announcement and notification

Once the application is accepted, a notification of registration is sent to the applicant. It includes at least the following information:

a) The primary integer value assigned;

b) Any confirmed secondary identifier(s);

c) Any confirmed unicode label(s).

If the registration is not accepted, a notification of rejection is sent to the applicant. It includes at least the following information:

a) The reason of rejection.

9.5 Change of registration information

Organizations identified by an allocated OID shall not change from the original application, but supporting information, such as the information provided in clause 9.2 b), may change from time to time. It is necessary to update the registration information, maintaining an audit trail of earlier information.

9.6 Fees

The organization providing the registration authority (RA) of the UAV OID should do so on a cost-recovery basis. The fee structure should be designed to recover the expenses of operating the RA, to cover web publication of registrations (which is strongly encouraged), to support enquiry requests, and to discourage frivolous and multiple requests.

The fee values should be determined by the RA, subject to the approval of the ITU-T study group responsible for the maintenance of this Recommendation. Fees can apply to:

a) registration;

b) response to inquiry;

c) update/maintenance of registration information.

Fees should be independent, subject to the exchange rate fluctuations of the country where the application is made from.

Once the fee associated with an initial application has been charged, there should be no further charges for the maintenance of that entry or its web publication.

Annex A

OID coding rules for UAV devices

(This annex forms an integral part of this Recommendation.)

According to [b-ITU-T X-Sup.31], there are several key factors that should be considered as constituent parts of a new OID assignment scheme, such as registration authority ID, category ID, entity ID, etc. A complete OID would be a combination of these key factors.

Detailed information of OID constituent parts is given in Table A.1.

Table A.1 – Detailed information of OID constituent parts

Constituent part	Mandatory/ optional	Hierarchical layers recommended	Interpretation
Registration authority ID	M	Consistent with actual management	Registration authority ID (could include a country ID or a combination of a country ID, a province or region ID, if applicable, and a city ID). Each level of registration authority ID should be allocated by the upper level registration authority.
Category ID	O	One or more layers	Category (and subcategories) of an object in application field, such as people, departments, standards, etc.
Entity ID	M	One layer	Unique number allocated to an entity (usually as a combination of batch number and product)

Thus, it is recommended that the physical serial number of a UAV device should also consist of three parts: manufacturer's ID, category ID and entity ID, where each part is encoded as follows:

1) Manufacturer's ID

The manufacturer's ID is a 6-digits number where the first digit is not zero.

The manufacturer's ID is assigned by the RA of the UAV OID (see clause 7.2.1) and could be obtained by manufacturers through regular procedures (see clause 9.2).

2) Category ID

The category ID is a 4-digit number, which shall be assigned and maintained by the manufacturer.

3) Entity ID

The entity ID is a series number with maximum 16 digits. It is generated by the manufacturer. The first two digits represent the number of digits in the entity ID (including the first two digits themselves).

Bibliography

[b-ITU-T X.680] Recommandation ITU-T X.680 (2015) | ISO/IEC 8834-1:2015, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*.

[b-ITU-T X-Sup.31] Supplement 31 to ITU-T X-series Recommendations (2017), *ITU-T X.660 – Supplement on guidelines for using object identifiers for the Internet of things*.

[b-OID handbook] ITU-T Handbook Object identifiers (OIDs) and their registration authorities, https://www.itu.int/pub/T-HDB-LNG.4-2010

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2020