2026

Safety committee– Topic 2

Director – Vincent Correia[1]

[1] This paper reflects the author's personal views and cannot be considered as the views of ICAO.

Mitigating the Safety Risks of Unmanned Aerial Vehicles (UAVs) in Shared Airspace

1. Background and Context

The rapid proliferation of unmanned aerial vehicles (UAVs), commonly referred to as drones, is one of the major structural changes in global airspace management since the commercial jet aviation era.

ICAO began addressing the regulatory challenges of UAV integration by developing the Remotely Piloted Aircraft Systems (RPAS) framework, introduced under Annex 2 and supported by the RPAS Manual (Doc 10019). But technological evolution has significantly outpaced global regulatory response and the absence of a comprehensive global framework creates safety gaps, particularly in low-altitude airspace where UAVs most frequently interact with manned general aviation, helicopter operations, and aircraft in the approach and departure phases of flight.

A series of well-publicized near-miss events has highlighted the need to establish clear standards for UAV registration, remote identification, operational restrictions, and integration within the general airspace.

The primary ICAO instruments relevant to this topic are:

- Annex 2 (Rules of the Air),
- Annex 6, Part IV (Operation of Aircraft — International Operations, Remotely Piloted Aircraft Systems),
- Annex 13 (Accident Investigation),
- Annex 19 (Safety Management),
- RPAS Manual (Doc 10019),
- Safety Management Manual (Doc 9859),
- ICAO UTM Common Framework, Edition 4[2]

2. Key Issues

Registration and Remote Identification

A crucial challenge in UAV safety management is establishing who is operating a drone and where it is operating. Many states have introduced national registration requirements, but these systems are inconsistent, non-interoperable, and non-applicable across borders.

[2] https://www.icao.int/sites/default/files/left-menu-pdfs/UTM%20Framework%20Edition%204.pdf

Remote Identification (Remote ID), i.e. the ability to broadcast a UAV's identity and location in real time, is considered by safety regulators to be a prerequisite for effective airspace management and law enforcement. However, regulators have adopted diverging approaches, thus increasing the risk of long-lasting discrepancies. For instance, while both the US and the EU require Remote ID for most drones weighing over 250 grams, key differences exist: the FAA registers the aircraft, while EASA registers the operator, and the two systems use different data-broadcast standards and compliance frameworks.

> **U.S. Regulatory Requirements**
>
> The FAA issued its Remote ID Notice of Proposed Rulemaking (NPRM) on 31 December 2019 which detailed the technical requirements for Remote ID on unmanned aircraft systems operation in the United States. During the 60-day public comment period, the FAA received more than 53,000 comments on the proposed rule. The final rule was published in the *Federal Register* on 15 Jan. 2021, with an original effective date of 16 March 2021. Corrections made to the rule and published in the *Federal Register* delayed the effective date to 21 April 2021. Changes included, for example, shortened manufacturer/operator compliance dates compared with the NPRM and the simpler opportunity for operators of non-standard remote ID drones to obtain a remote ID broadcast module and to retrofit the module to multiple drones that have the same registration number.
>
> In the FAA's final rule, drone pilots have the following choices:
>
> - Operate a standard remote ID drone, as noted, with built-in capability to broadcast its identification and location information about the drone and its control station/take-off point;
> - Operate a drone with a remote ID broadcast module, as noted, providing the add-on flexibility. Note: The remote pilots and other persons responsible must be able to see their drone at all times during flight; or,
> - Operate a drone without remote ID equipment only at FAA-recognized identification areas (FRIAs) sponsored by community-based organizations or educational institutions.

https://skybrary.aero/articles/uas-remote-identification

EASA Regulatory Requirements

The European Union's initial drone-identification regulations, which began to take effect in April 2019, introduced Direct Remote Identification requirements. If a UAS falls under these requirements and already has the specified built-in Direct Remote Identification broadcast function, that satisfies EASA. Otherwise, the operator must provide an equivalent add-on module that:

- "Allows the upload of the UAS operator registration number in accordance with Article 14 of Implementing Regulation (EU) 2019/947 and any additional number provided by the registration system. The system shall perform a consistency check verifying the integrity of the full [data] string provided to the UAS operator at the time of registration. In case of inconsistency, the system shall emit an error message to the UAS operator;
- Ensures, in real time during the whole duration of the flight, the direct periodic broadcast from the UA using an open and documented transmission protocol, of the following message elements, in a way that it can be received directly by existing mobile devices within the broadcasting range of at least the following data:
    - the UAS operator registration number and the verification code provided by the Member State of registration during the registration process unless the consistency check [noted above] is not passed;
    - the unique serial number of the add-on module compliant with standard ANSI/CTA-2063-A-2019, "Small Unmanned Aerial Systems Serial Numbers, 2019," affixed to the add-on and its packaging or its manufacturer's instructions in a legible manner;
    - the time stamp, the geographical position of the UA and its height above the surface or take-off point;
    - the route course measured clockwise from true north and ground speed of the UA; and,
    - the geographical position of the remote pilot or, if not available, the take-off point.
- Reduces the UA operator's ability to tamper with the functionality of the direct remote identification system; and,
- The add-on module will be placed on the market with manufacturer's instructions providing the reference of the transmission protocol used for the direct remote identification emission and providing instructions to install the module on the UA and to upload the UAS operator's registration number."

https://skybrary.aero/articles/uas-remote-identification

UTM (UAV Traffic Management) Systems

Conventional Air Traffic Management (ATM) was designed for traditional aircraft operating under instrument (IFR) or visual flight rules (VFR). It is not scalable to the volume, diversity, and low-altitude operations of UAVs: drone operators cannot interact with air traffic controllers or submit flight plans. To cope with this challenge, UTM seeks to provide automated, data-driven separation services for drones and onboard systems to avoid collisions ("detect and avoid") and organize the safe flow of drones.

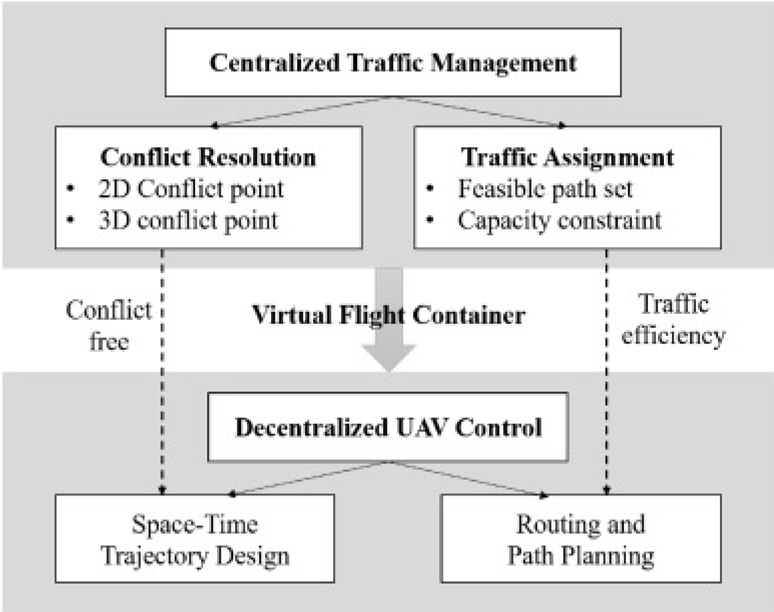
1.2. Centralized and decentralized approaches

Centralized control involves a single control center that manages and optimizes all UAVs within the controlled airspace, using global information for path planning, traffic flow management, and conflict resolution. For instance, Wu et al. (2021) addressed the challenge of managing a large number of UAVs in low-altitude airspace by resolving conflicts between pairs of UAVs and determining the optimal sequence for their operations. Pang et al. (2022) formulated a mixed-integer nonlinear programming (MINLP) problem to optimize control strategies for multi-UAV conflict resolution. To solve the MINLP efficiently, a meta-heuristic stochastic fractal search (SFS) algorithm is employed. Other methods, such as the ant colony optimization (ACO) algorithm (Hao et al., 2018), hybrid-metaheuristic algorithms (Islami et al., 2017), reinforcement learning techniques (Peng et al., 2021), first-come-first-served scheme (Dai et al., 2021), and simplified models (Tang et al., 2021; Zhu and Wei, 2019), have also been applied to solve complex UAV path planning and conflict resolution problems within centralized control framework.

Although centralized approaches can optimize path planning and conflict resolution for multiple UAVs within an integrated system, offering globally optimal solutions, they face significant challenges related to computational complexity. Heuristic models are commonly used to mitigate these issues, but they cannot guarantee optimal solutions for both conflict-free operations and traffic efficiency.

Decentralized control, by contrast, involves localized decision-making by individual UAVs or distributed controllers for path planning and conflict resolution. For instance, Seo et al. (2017) developed a geometry-based strategy for collision avoidance among UAVs, enabling efficient separation using a straightforward algorithm. Ho et al. (2018) introduced an adapted algorithm to allow each UAV to compute its own velocity adjustments in real time. A subsequent study by Ho et al. (2020) extended the multi-agent path finding (MAPF) framework to model conflict detection and resolution problems. Yang et al. (2019) employed the monte carlo tree search (MCTS) algorithm to solve the conflict-free flight problem online. Similarly, Mueller and Kochenderfer (2016) adopted partially observable MDP model for individual UAV modeling. Other decentralized methods are discussed in Bertram et al. (2021), Cao et al. (2019), Yang et al. (2023), Zhang et al. (2019), and Zhang et al. (2021).

Xiangdong Chen, Shen Li, Meng Li, "A hybrid centralized-decentralized traffic control framework for unmanned aerial vehicles in urban low-altitude airspace," Communications in Transportation Research, Volume 5, 2025



Xiangdong Chen, Shen Li, Meng Li, "A hybrid centralized-decentralized traffic control framework for unmanned aerial vehicles in urban low-altitude airspace," Communications in Transportation Research, Volume 5, 2025

UTM architectures are being developed across major aviation markets, but these systems use different technical standards and data protocols, creating interoperability challenges. They fundamentally rely on technological solutions, thus creating new potential risks:

- **Interface between unmanned and manned aviation**. If the safety of UAV operations is almost exclusively ensured by automation, how to ensure that traditional airspace users, most notably general aviation, are not at risk if their aircraft are not equipped with the same detection and identification technologies that make automated separation possible?
- **Cybersecurity vulnerabilities, GPS spoofing, and signal jamming**. Drone operations are expected to rely increasingly on connected technologies for remote control, communication, and data transfer. They will therefore be vulnerable to many of the same vulnerabilities of other connected systems. The dependence of small UAS on GPS signals makes them particularly vulnerable to jamming, spoofing, and signal interference.
- **System fragility and single points of failure**. A software outage, network disruption, or coordinated cyberattack could all at once ground drones flying over a commonly used airspace, strand them, or generate collisions.
- **Some advocate for more automation in the monitoring process**, to assess the new threats conveyed by automation itself, but it raises another question: what if the automated monitoring system fails to identify a risk before it happens?

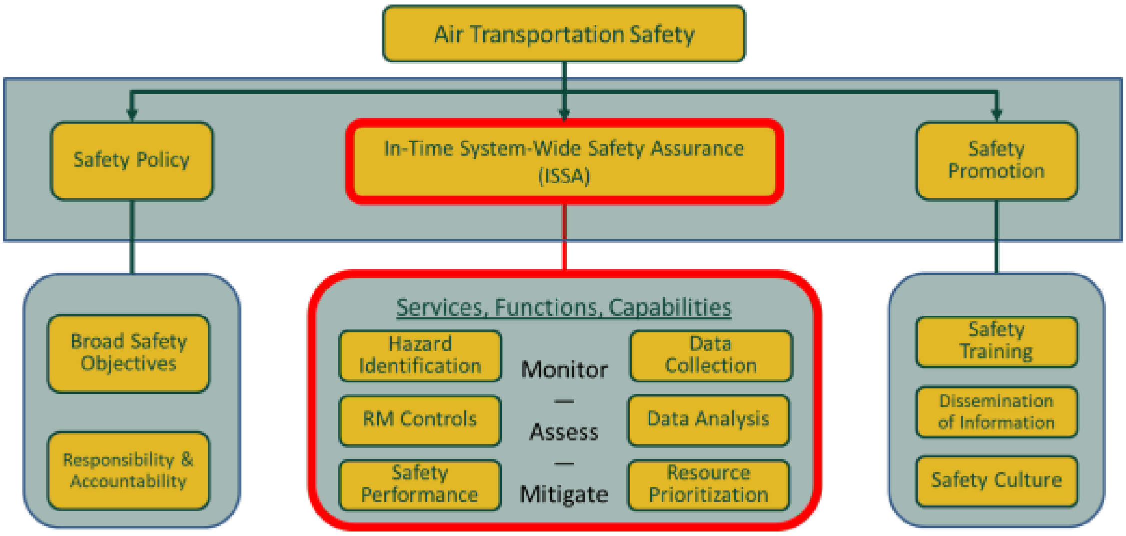


Figure I-4 - In-Time System-Wide Safety Assurance

ISSA replaces time-consuming manual steps with automated functions meant to monitor systems, assess issues, and mitigate risk. Monitoring can be passive (recording and watching the overall health of a system via metrics analysis) or active (looking at and analyzing the data going into, coming out of, and being used in a system). Identification of issues early facilitates quick assessment of issues and impacts. Mitigation can include standard design patterns already in use in UTM (e.g. communication of warnings with operators during emergency operations). This approach to safety management may help scale safety processes to suit the complexity of the UTM environment.

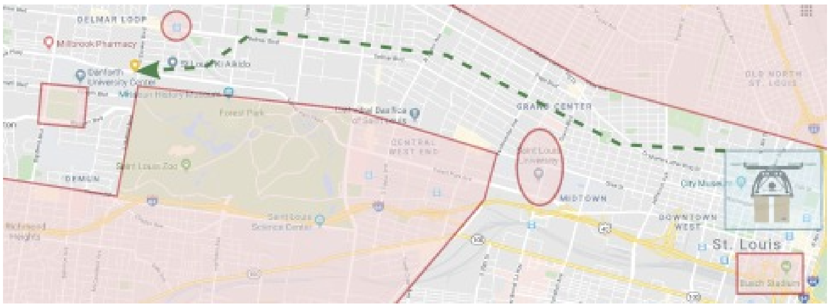
ICAO, Unmanned Aircraft Systems Traffic Management (UTM) – A Common Framework with Core Principles for Global Harmonization, Edition 4

Geofencing and Operational Restrictions

Geofencing technology restricts drone activity in sensitive regions (airports, airspace, and critical infrastructure) using GPS and pre-programmed geographic information. It is considered to be an essential safety measure, most notably to avoid collision with traditional aviation or the intrusion into prohibited/restricted areas.

22.2. UAV geofencing

Geofencing systems define virtual boundaries in a specific geographical area to keep UAVs away from any danger/collision. An illustration example is presented in Fig. 22.1, where a delivery UAV transports a package to the point shown by a star. The delivery UAV should not fly over the city stadium (Busch Stadium in this example), as there is an ongoing match and the UAV may collide with other UAVs that are recording the match. The delivery UAV should not fly over the campus (St. Louis University in this example) due to university regulations, and overcrowded places (the metro station in this example) should be avoided due to security rules. There are also some areas that the delivery UAV should not enter, as these areas are full of skyscrapers, are other UAVs' territories, or are classified as dangerous/illegal zones. Thus, we need a reliable navigation system that steers the UAV to the destination, while ensuring that the UAV flies in legal/safe zone at all times.



Mehdi Hosseinzadeh, "Chapter 22 - UAV geofencing: navigation of UVAs in constrained environments", in Anis Koubaa, Ahmad Taher Azar (eds.), In Advances in Nonlinear Dynamics and Chaos (ANDC), Unmanned Aerial Systems, Academic Press, 2021, pp. 567-594

The effectiveness of geofencing depends on manufacturers implementing consistent and accurate restricted zone databases, which in turn requires states to provide standardized, machine-readable aeronautical information.

Enforcement of operational restrictions also varies widely. In many developing states, enforcement capacity is limited even where regulations exist on paper, allowing unsafe UAV operations to continue unchecked near active airports and populated areas.

3. Key Questions for Delegates

- What should be the minimum global standards for UAV registration and Remote Identification? If ICAO cannot compel harmonization, what is the realistic minimum standard it can establish, and how long can fragmentation be tolerated?
- UTM architectures in the US, EU, China, and elsewhere are being built on different technical standards, creating a patchwork of systems that cannot communicate across borders. Is meaningful global interoperability still achievable and, if not, what is the fallback?
- Most drone-related incidents involve recreational operators, and enforcement is primarily a national responsibility. What could ICAO do to address a risk that sits largely outside its jurisdiction but could impact international civil aviation?
- How can ICAO design standards that raise the global safety baseline without simply formalizing a gap between states that can comply and those that cannot?