Safe drone flight - assuring telemetry data integrity in U-Space scenarios

Summary

The Safe Drone Flight (SDF) project will investigate the security of flight surveillance systems and, in particular, the drone telemetry data they transmit. We pose the research question: How can the integrity of safety-critical, real-time telemetry data from insecure sources be assured? The work will investigate the integrity requirements and evaluate several proposed solutions. Developing a safety assured and cyber secure surveillance system is an important step in enabling U-Space services, supporting safe, efficient and secure access to airspace for large numbers of drones. This project is a collaborative effort between NATS and The Open University (OU).

The assurance of safety and security in a mixed crewed and uncrewed airspace user environment requires a high level of integrity of drone telemetry data across the Unmanned (air) Traffic Management (UTM) system. Forensic readiness requirements to address this challenge were investigated as part of *The Drone Identity – investigating forensic-readiness of U-Space services* Engage first wave catalyst fund project. That work, undertaken by the two entities supporting the SDF project, produced a prototype demonstrator that enables further investigation of safety goals and manages the trade-offs between them and other constraints through self-adaptation.

As guardians of UK airspace, NATS' primary focus is ensuring the safety of all airspace users. Achieving this requires safety-critical and related data, including location-based data which is crucial for building accurate and complete situational awareness. In a conventional, crewed aviation scenario, this data would typically be sourced from NATS' primary and secondary radar surveillance networks. In contrast, in a typical U-Space scenario, Air Navigation Service Providers (ANSP) may not have the capability to survey and locate all consumer drone-sized Uncrewed Aircraft (UA) using its surveillance assets and may need, instead, to source this data from distributed, untrusted sources, such as the drones themselves. This raises the challenge of assuring that the incoming data is secure – that it hasn't been maliciously or unwittingly changed – across a plurality of different U-Space scenarios.

In the current project, we aim to study concepts to mitigate vulnerabilities within U-Space and improve the overall global security of the Communications, Navigation, and Surveillance systems in Air Traffic Management (CNS/ATM). Our research is to investigate how distributed, multi-stakeholder data sources can be aggregated and assured in the context of NATS' tools and systems. The SESAR Engage KTN catalyst funding will enable engagement, knowledge exchange, and collaborative research between the ATM industry member (NATS) and the academic member (OU). The project will involve creating a set of U-Space use cases and scenarios, ascertaining requirements on a flight surveillance system and evaluating solutions, including the prototype demonstrator.