The drone identity – investigating forensic-readiness of U-Space services

Executive summary

The Drone Identity (DI) project has analysed the existing UK Airprox incidents and surveyed the literature about autonomous unmanned systems. We compared various UAV scenarios and the taxonomy of safety requirements that require forensic investigation (Task 1). With our industry partner NATS, we elicited forensic-readiness requirements for identity management, and mapped the LiveBox reference architecture to the services of UTM in the U-space project (Task 2). Furthermore, we implemented some of these requirements on three commonly considered scenarios: organ delivery, safe landing, and air lifting and tested these conceptual implementations through a preliminary simulator, dragonfly, which supports the cautious adaptation of the controller software behaviours (Task 3.1), experimenting with distributed ledger technology and smart contracts for capturing evidence (Task 3.2). Finally, we have evaluated the forensic-readiness of Drone Identity features through drone delivery and surveillance scenarios using a DJI drone demonstrator in a controlled environment (Task 4).

As far as we can, through research outputs (RO1-RO8), we have answered a number of research questions through technical and experimental studies with clear success criteria, these are included in the following table.

Research Questions and Success Criteria

Research Questions	**Success Criteria**
How much data bandwidth is necessary and sufficient to capture, store, and transmit live boxes of UAVs to the cloud / ground station?	A reduction ratio compared to the full transmission of all sensory data [RO1, RO8].
How many features in the existing research methods are able to cover safety requirements for AUS, which are also applicable to the UAV?	A good coverage of the literature through systematic literature mapping study [RO4].
How to modify the software behaviours of UAVs when their original functionality cannot satisfy global security requirements?	The improvement of failure rates comparing legacy off-the-shelf UAV systems to the adapted ones [RO3].
How to simulate the favourable and adversarial environmental conditions and test the failure rates of UAVs with, or without the wrapper?	The number of contextual variables which can be simulated [RO2].
How to preserve or retain the integrity of flight data records so that the risk of tampering is minimised?	Surviving massive injection attacks in the network for the resilience of the integrity using distributed ledger technology [RO1].
How to design a smart contract that can achieve forensic soundness in terms of integrity and efficiency?	A smart contract-based system has been developed to demonstrate logging of interactions between drones and witnesses (pedestrians and vehicles) and their corresponding geolocation data using Ethereum's DLT [RO5].
How to make real-time trade-offs between various live requirements of drone' including safety, security, privacy, timeliness and responsiveness, etc?	A demonstrator of requirements-driven design of motion planning tool has been created and evaluated with respect to the real-time trade-offs [RO6-7].

This project has received funding from the SESAR Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement No 783287.