SESAR Engage KTN – catalyst fund project final technical report

Project title:	Safe Drone Flight - Assuring telemetry data integrity in U-Space scenarios ('SDF')
Coordinator:	NATS, UK
Consortium partners:	Open University, UK
Thematic challenge:	TC1 Vulnerabilities and global security of the CNS/ATM system
Edition date:	27 July 2021
Edition:	1.0
Dissemination level:	Public
Authors:	Jacob Blamey / NATS
	Anthony Rushton / NATS
	Gavin Moir / NATS
	Robert Westerberg / NATS
	Danny Barthaud / OU
	Yijun Yu / OU

The opinions expressed herein reflect the authors' views only. Under no circumstances shall the SESAR Joint Undertaking be responsible for any use that may be made of the information contained herein.

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.

1 Abstract and executive summary

1.1 Abstract

The Safe Drone Flight (“**SDF**”) project was led by NATS in collaboration with The Open University (OU) and funded by the SESAR Engage Knowledge Transfer Network (KTN) catalyst. The project investigated the security of unmanned flight surveillance systems and, in particular, the drone telemetry data they transmit. 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 matured a prototype blockchain-based drone surveillance system taking a U-space scenario-based approach to simulate several drone operations and validate the concept’s suitability. Cyber security and safety assurance related research was conducted to determine data integrity-related design and performance requirements on the solution respectively.

1.2 Executive summary

The SDF project was set in the context of a wider thematic challenge to mitigate the safety and security vulnerabilities of future Communications, Navigation, and Surveillance systems in Air Traffic Management (CNS/ATM).

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, manned 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 other words, the assurance of safety and security in a mixed 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 the safety and security challenges associated with drone surveillance systems 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 the *LiveBox* prototype that enabled further investigation of safety goals and managed the trade-offs between them and other constraints through self-adaptation.

The aim of the SDF project was to develop the *DroneBox* novel drone surveillance system, a predecessor to the *LiveBox* prototype, but rather than considering forensic data, the focus of this research was real-time drone telemetry data. The SDF project sought to mature the DroneBox prototype through industrial application while also understanding requirements on drone surveillance systems in terms of assuring the integrity of drone telemetry data and the mechanisms and system design principles that may be employed to do so.

The SDF project had three research activities:

1. Concept and prototype assessment

2. U-space scenario planning
3. Evaluation and validation activities

Through collaboration between NATS and the OU, all three activities have been carried out, resulting in a number of reports, the results and conclusions of which have been summarised in the following sections.

Notable outcomes include:

- **Capability study** that confirmed the prototype met the requirements to perform the validation activities as part of the project
- **Suitability assessment** which established that a blockchain-based solution using mobile drone witnesses was suitable for short surveillance operations in lower VLL airspace in urban environments
- A set of U-space BVLOS drone **use cases and scenarios**
- A set of cyber security mechanisms for **assuring digital trust**, commentary on their applicability to drone telemetry data, and an architectural design requirement on drone surveillance systems to have multiple embedded layers of security controls
- **Services and use case hazard assessments** which resulted in the deduction of the allowable data integrity failure probabilities, setting minimum requirements on the quality of the drone data needed for the provision of U-space services

Two SDF workshops were held over the course of the project which were attended by key internal and external stakeholders and both were very well received.

The intention is to publish a paper on the DroneBox prototype, seek future grant opportunities to further mature the concept, and disseminate the findings even wider through an upcoming conference.

This project brought together and leveraged the academic expertise from the OU with the industrial application and aviation knowledge from NATS. Doing so brought the early-stage DroneBox prototype closer to industrial application while identifying new research avenues to explore.

2 Overview of catalyst project

2.1 Operational/technical context

Drones represent an exciting development in aviation technology and offer new opportunities for emergency services, businesses and individuals in the UK and across the globe (NATS, 2021). Indeed, the drone market is expected to contribute £42bn to the UK economy alone by 2030 with 76,000 drones in use across UK skies by this time (PwC, 2021).

The capability to detect non-cooperative manned aircraft such as by radar, allows for safe and expeditious use of airspace. A similar capability to detect unmanned aerial vehicles (UAVs), particularly in congested or shared-use airspace, is needed to provide safe and reliable services that will enable emerging drone use cases. The physical characteristics and flight profiles of UAVs differ greatly with manned aircraft to the extent that surveillance systems and technologies built to detect manned aircraft are not suitable to detect UAVs.

It has been shown that communication between a drone and its controller can be detected using wireless signal packet analysis. A network of devices with such detection capability, appropriately positioned over an area of interest, could provide a reliable detection network. However, the creation and installation of such infrastructure is unlikely to be practical. Hence, there is a need to develop an alternative solution which solves these challenges and enables ATC visibility of drone locations while assuring that the drone telemetry data is created, transmitted and recorded safely and securely; to a high level of data integrity.

The operational environment considered in this project is one in which BVLOS drone operations are conducted in UK airspace that has been delegated as U-space airspace. The U-space airspace definitions are as per the CORUS ConOps (CORUS, 2019). A set of use cases and scenarios were developed as part of this project which describe the operational flow, the airspace structure and the actors involved.

2.2 Project scope and objectives

The project was set in the wider context of mitigating vulnerabilities and improving the global security of the Communications, Navigation, and Surveillance systems in Air Traffic Management (CNS/ATM). Under this Thematic Challenge, the SDF project investigated the requirements on the safety and security of real-time drone telemetry data while developing and maturing a novel drone surveillance system concept and prototype through industrial application and validation activities.

As per the overarching goals of the SESAR Engage KTN programme, this project enabled engagement, knowledge exchange and collaborative research between the partners involved in the project – an ATM industry member (NATS) and an academic member (The Open University) – and also sought involvement and interaction with other key external stakeholders.

The objectives as set out at the start of the project were to **decide** which U-space services are dependent on drone telemetry data, **develop** operational scenarios, **perform** an assessment on the prototype developed by the OU, **provide** feedback as required and finally, **evaluate** the performance and capability of the concept and prototype.

2.3 Research carried out

The section below provides a description of the concept and prototype central to this SDF project. The methodology employed over the course of this 12-month project to develop the prototype and further understand how to mitigate safety and security vulnerabilities associated with drone telemetry data is also explained.

2.3.1 Concept

Detailed descriptions of the DroneBox concept can be found in the DroneBox Paper (Barthaud, et al., 2021) and the DroneBox Capability Study (Blamey & Barthaud, SDF DroneBox Capability Study, 2021).

At a high-level, the DroneBox concept is a drone surveillance system that satisfied the aforementioned challenges associated with providing an alternative, unmanned surveillance system. It is based on two key elements:

1. **Distributed ledger technology (DLT)**; specifically blockchain, to enable drone surveillance data from a plurality of sources to be recorded and stored on a virtually tamper-proof, decentralised ledger while embedding security features and mechanisms to assure a high level of data integrity.
2. **Opportunity-based**; using mobile phones as portable drone detectors to provide low-altitude drone surveillance coverage without the need for widespread, impractical, and potentially unfeasible ground infrastructure.

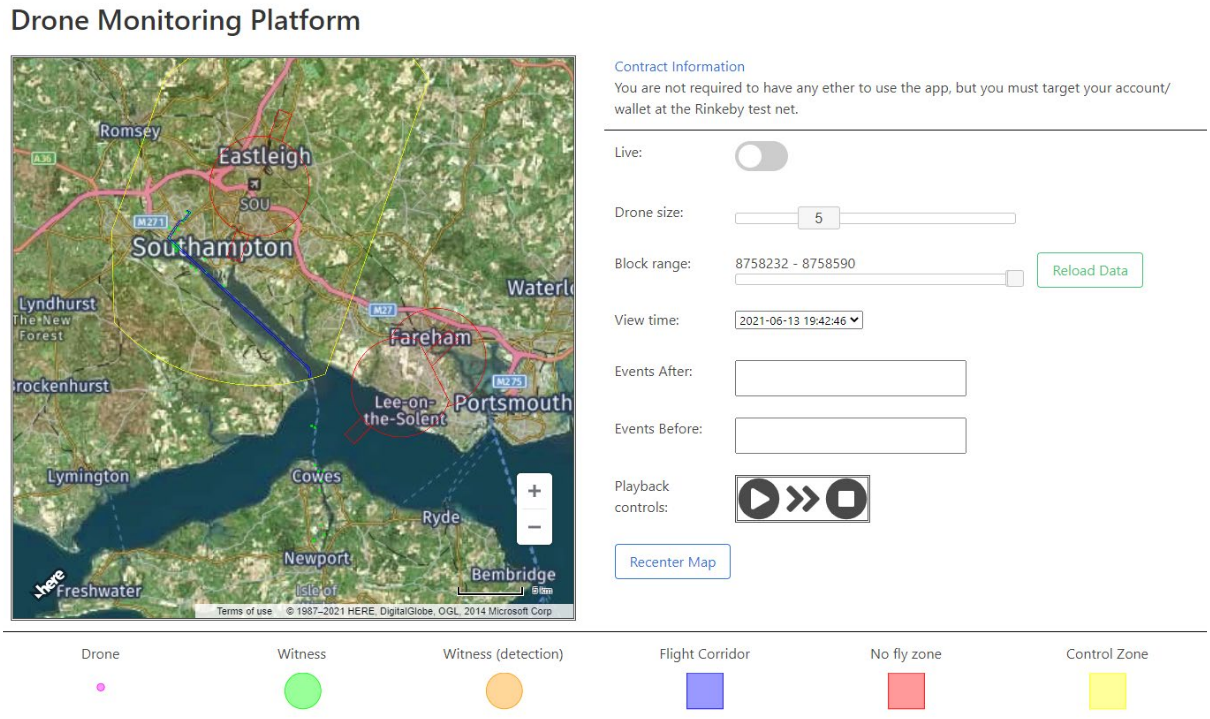
2.3.2 Prototype

One of the fundamental aims of the SDF project was to develop and mature the DroneBox prototype.

A detailed description of the DroneBox prototype can be found in the DroneBox Paper (Barthaud, et al., 2021) and the DroneBox Capability Study (Blamey & Barthaud, SDF DroneBox Capability Study, 2021). Visualisations of the simulation outputs can be found in the DroneBox Suitability Assessment (Blamey, SDF DroneBox Suitability Assessment, 2021) as well as in the Session 2 Final Workshop Slides (Blamey, Barthaud, Neale, & Yu, 2021).

At a high-level, the DroneBox prototype comprises:

1. **Simulator**; simulates the U-space operational environment including drones, drone detectors/“witnesses” and airspace structures. As drones pass within range of the witnesses, and the witness conducts a search, a detection is made and recorded.
2. **Blockchain**; utilises smart contracts to store the drone telemetry data.
3. **Data visualisation tool**; extracts data from the blockchain and displays it on a geographical map as illustrated in Figure 1.



Drone Monitoring Platform

Contract Information

You are not required to have any ether to use the app, but you must target your account/ wallet at the Rinkeby test net.

Live:

Drone size: 5

Block range: 8758232 - 8758590

Reload Data

View time: 2021-06-13 19:42:46

Events After:

Events Before:

Playback controls:

Recenter Map

Drone	Witness	Witness (detection)	Flight Corridor	No fly zone	Control Zone
●	🟢	🟠	🟦	🟥	🟨

Figure 1: Screenshot of the DroneBox prototype visualisation tool

2.3.3 Methodology

The process flow for the research carried out in this project is illustrated in Figure 2. The elements - research activities, tasks and outputs – have been mapped out with the interdependencies between the elements denoted by the directional arrows. The colour and shapes within the flow indicate the type of element (see flow key in the top right of the diagram).

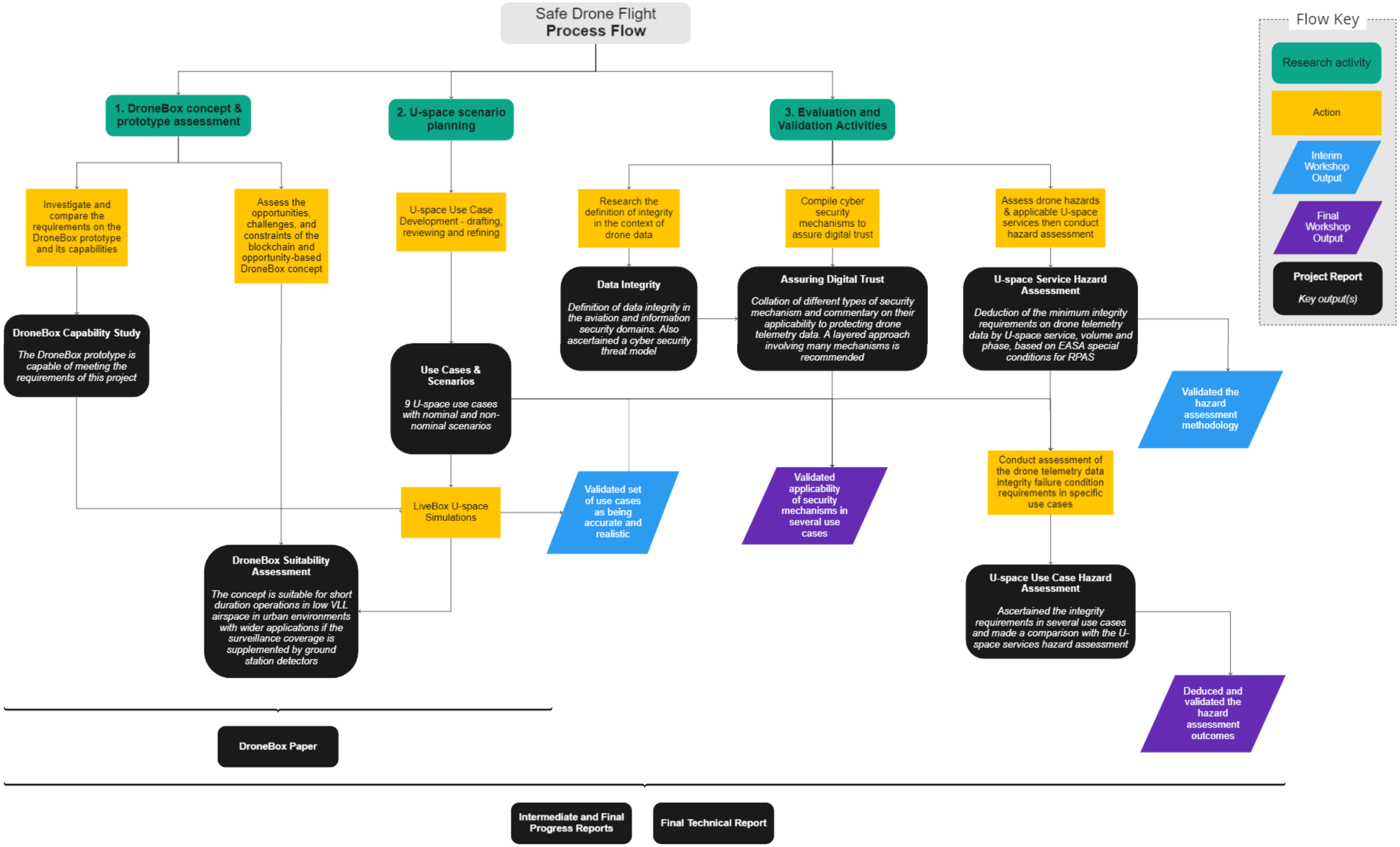

Safe Drone Flight Process Flow
1. DroneBox concept & prototype assessment
2. U-space scenario planning
3. Evaluation and Validation Activities
Investigate and compare the requirements on the DroneBox prototype and its capabilities
Assess the opportunities, challenges, and constraints of the blockchain and opportunity-based DroneBox concept
U-space Use Case Development - drafting, reviewing and refining
Research the definition of integrity in the context of drone data
Compile cyber security mechanisms to assure digital trust
Assess drone hazards & applicable U-space services then conduct hazard assessment
Data Integrity
Definition of data integrity in the aviation and information security domains. Also ascertained a cyber security threat model
Assuring Digital Trust
Collation of different types of security mechanism and commentary on their applicability to protecting drone telemetry data. A layered approach involving many mechanisms is recommended
U-space Service Hazard Assessment
Deduction of the minimum integrity requirements on drone telemetry data by U-space service, volume and phase, based on EASA special conditions for RPAS
DroneBox Capability Study
The DroneBox prototype is capable of meeting the requirements of this project
Use Cases & Scenarios
9 U-space use cases with nominal and non-nominal scenarios
Validated the hazard assessment methodology
Conduct assessment of the drone telemetry data integrity failure condition requirements in specific use cases
LiveBox U-space Simulations
Validated set of use cases as being accurate and realistic
Validated applicability of security mechanisms in several use cases
DroneBox Suitability Assessment
The concept is suitable for short duration operations in low VLL airspace in urban environments with wider applications if the surveillance coverage is supplemented by ground station detectors
U-space Use Case Hazard Assessment
Ascertained the integrity requirements in several use cases and made a comparison with the U-space services hazard assessment
Deduced and validated the hazard assessment outcomes
DroneBox Paper
Intermediate and Final Progress Reports
Final Technical Report
Flow Key
Research activity
Action
Interim Workshop Output
Final Workshop Output
Project Report
Key output(s)

Figure 2: Safe Drone Flight project research process flow

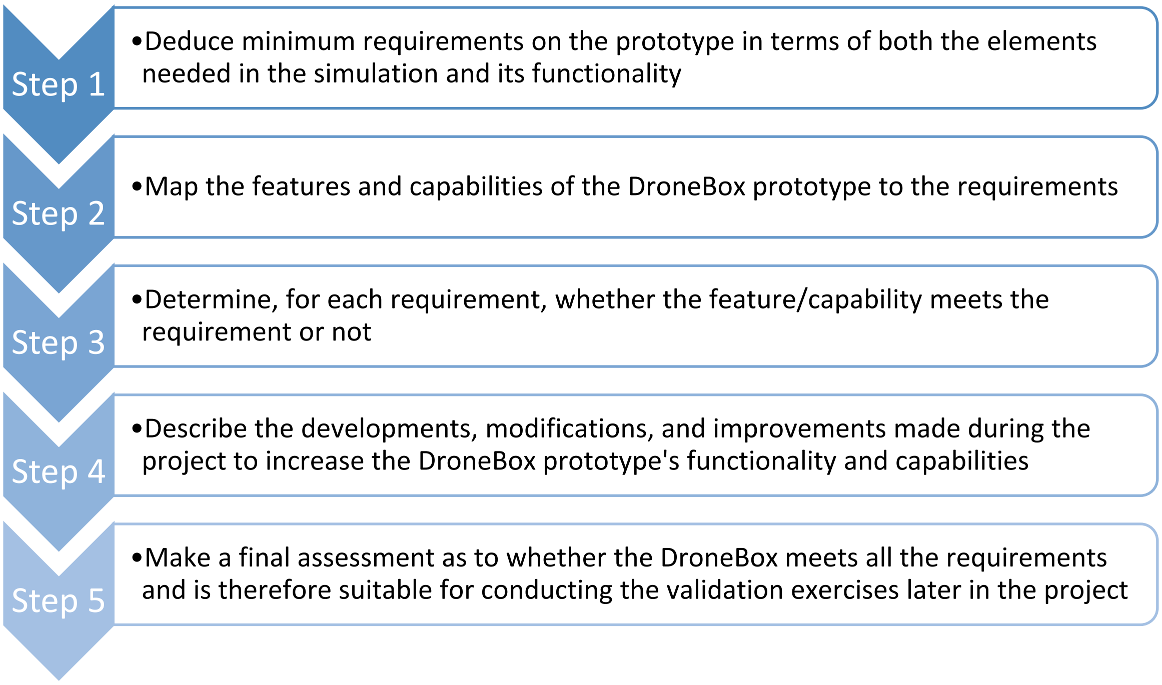
As shown in Figure 2, there were three research activities undertaken as part of the SDF project. The process followed for each of those activities is described below.

1. *DroneBox Concept and Prototype assessment*

This research activity involved two tasks each of this has been described in the subsections below.

DroneBox Prototype Capability Study

The step-by-step process undertaken for the capability study is described in Figure 3.



Step 1

- Deduce minimum requirements on the prototype in terms of both the elements needed in the simulation and its functionality

Step 2

- Map the features and capabilities of the DroneBox prototype to the requirements

Step 3

- Determine, for each requirement, whether the feature/capability meets the requirement or not

Step 4

- Describe the developments, modifications, and improvements made during the project to increase the DroneBox prototype's functionality and capabilities

Step 5

- Make a final assessment as to whether the DroneBox meets all the requirements and is therefore suitable for conducting the validation exercises later in the project

Figure 3: Capability study process

DroneBox Concept Suitability Assessment

The process for conducting an assessment of the suitability of the DroneBox concept is illustrated in Figure 4.

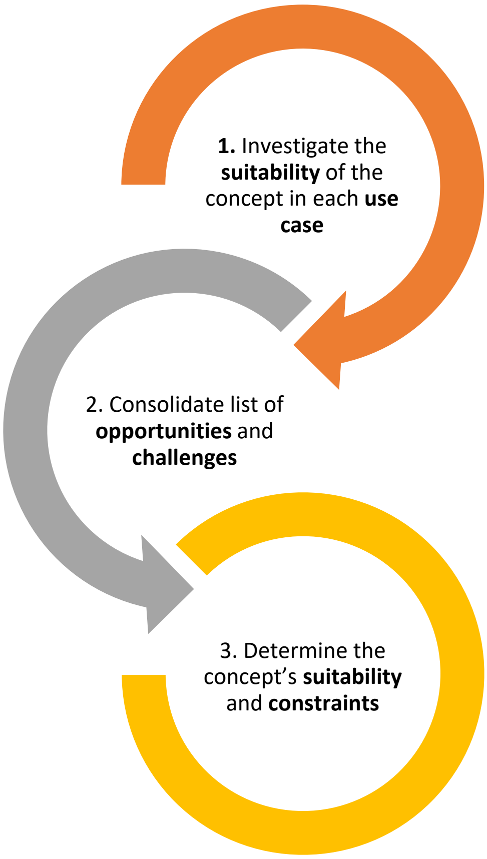

1. Investigate the **suitability** of the concept in each **use case**
2. Consolidate list of **opportunities** and **challenges**
3. Determine the concept's **suitability** and **constraints**

Figure 4: Suitability assessment process

Firstly, a qualitative assessment of the suitability of the opportunity and blockchain-based solution is performed using the three use case simulations. Along with the high level question "Is the concept appropriate for providing drone surveillance in this environment, under these conditions, in each case, the research question is posed "does the concept exhibit the three elements of the CIA triad (confidentiality, integrity and availability) of a secure data system?".

Secondly, a list of opportunities and a list of challenges was, each list categorised by the elements of the CIA triad.

Thirdly, the constraints on the DroneBox solution could then be ascertained from the opportunities and challenges. Finally, a conclusion could be drawn as to the suitability of the DroneBox solution in specific operational environments.

2. *U-space Scenario Planning*

A set of use cases were devised according to a common set of requirements, as listed below:

a. There is a BVLOS UA or PAV operation which, for at least part of the operation, takes place in UK controlled airspace.
b. A real-time telemetry feed is required to send data to the ATS provider to support one or more of the services ATC are providing.
c. Each use case is purposefully designed to be ambitious and challenging in order to deduce the most stringent requirements on an ANSP's systems. As such, use cases in U-space U1

development phase (as defined by the U-space Blueprint (SESAR Joint Undertaking, 2021)), which have a very restricted number of U-space services and don't have an ATM/UTM interface, have been excluded.

d. Each use case is designed to be realistic in the short to medium term and not too advanced as to seem unattainable with current technology. As such, use cases with a U-space U4 development phase have been omitted.

e. The use cases and scenarios are UAS technology agnostic, including the telemetry systems and aircraft equipage, to allow for a variety of different potential solutions.

The first step in the creation of the use cases was identifying existing or planned drone operations around the UK from which to take inspiration in addition to use cases developed for other SESAR and non-SESAR projects.

Leveraging the industrial knowledge and expertise from experts within NATS, the use cases were developed in line with the requirements above.

They were then validated as realistic by stakeholders in the Interim Workshop and used as the basis for many of the other tasks and outputs as shown in Figure 2.

3. Evaluation and validation activities

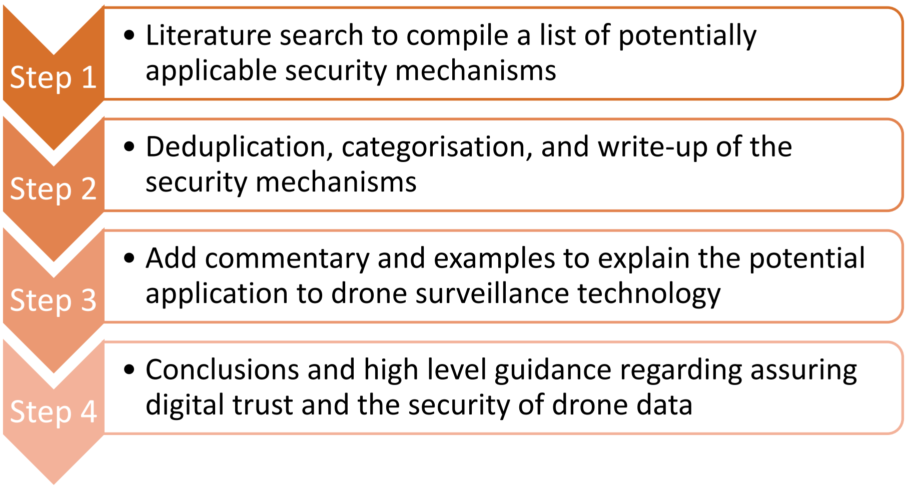
Data Integrity

This report was compiled to document background research carried out for this project which provided a common reference for the project team and fed into the other research tasks, most notably the Assuring Digital Trust report (Westerberg, Blamey, Ohler, McCullagh, & Whidborne, 2021). The aim was to define data integrity in the context of unmanned aviation and information security while also cataloguing the numerous threat vectors to data integrity.

This report was the result of a light-touch desk-based literature study, gathering input from multiple sources. Relevant extracts from those sources were consolidated and commentary was provided.

Assuring Digital Trust

To compile the report on assuring digital trust for drone surveillance systems, the process set out in Figure 5 was followed.



Step 1
- Literature search to compile a list of potentially applicable security mechanisms

Step 2
- Deduplication, categorisation, and write-up of the security mechanisms

Step 3
- Add commentary and examples to explain the potential application to drone surveillance technology

Step 4
- Conclusions and high level guidance regarding assuring digital trust and the security of drone data

Figure 5: Assuring digital trust process

Hazard Assessment

The purpose is to deduce and quantify the integrity requirements on drone telemetry data from a safety assurance perspective. This can be done in two ways – from a U-space services perspective and from a use case perspective. Both approaches were used and the steps involved are described in Figure 6.

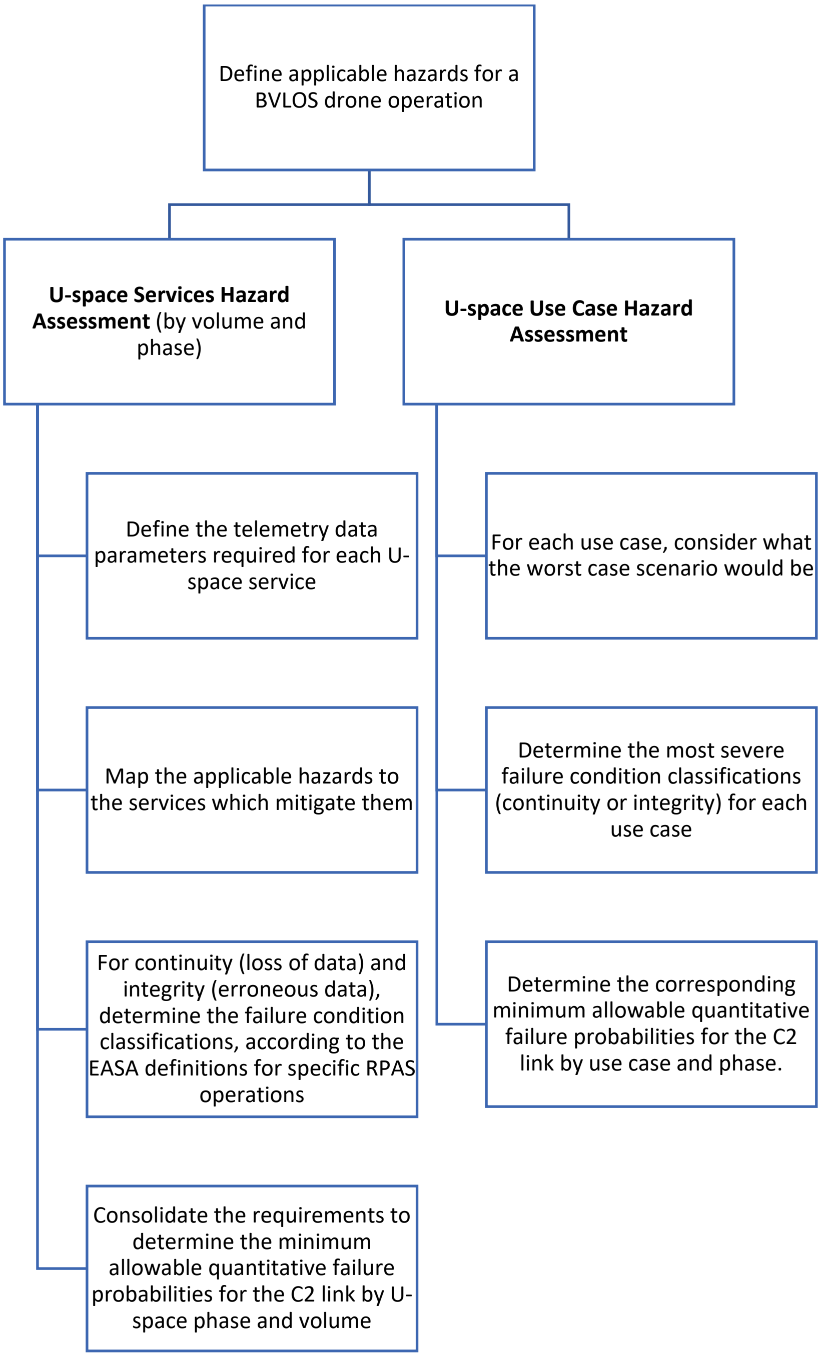

Define applicable hazards for a BVLOS drone operation
U-space Services Hazard Assessment (by volume and phase)
U-space Use Case Hazard Assessment
Define the telemetry data parameters required for each U-space service
Map the applicable hazards to the services which mitigate them
For continuity (loss of data) and integrity (erroneous data), determine the failure condition classifications, according to the EASA definitions for specific RPAS operations
Consolidate the requirements to determine the minimum allowable quantitative failure probabilities for the C2 link by U-space phase and volume
For each use case, consider what the worst case scenario would be
Determine the most severe failure condition classifications (continuity or integrity) for each use case
Determine the corresponding minimum allowable quantitative failure probabilities for the C2 link by use case and phase.

Figure 6: Hazard assessment process

After the two assessments were carried out, the outcomes from both assessments were cross-checked and used to validate the results.

Validation Activities

The validation activities carried out were as follows:

1. **Use case validation** – validate that the use cases were realistic, abided by the expected operational flow, and the set of use cases represented a wide spectrum of potential BVLOS drone operations in the UK.
2. **Security mechanism application validation** – validate that some or all of the security mechanisms in the Assuring Digital Trust report (Westerberg, Blamey, Ohler, McCullagh, & Whidborne, 2021) were applicable/suitable to be integrated into the DroneBox solution.
3. **Hazard assessment validation** – (a) validate the methodology and (b) determine the outcomes of the use case hazard assessment to validate the results of the U-space services hazard assessment.

2.4 Results

This section summarises the results from the respective reports from the SDF project.

2.4.1 DroneBox Capability Study

The following results have been obtained from the DroneBox Capability Study (Blamey & Barthaud, SDF DroneBox Capability Study, 2021). Please refer to that report for commentary and in-depth analysis.

The following table summarises the requirements on the prototype, the features and capabilities of the DroneBox prototype prior to any developments or modifications and an assessment as to whether the DroneBox prototype met the requirements.

Category	Requirement	Feature/capability of the prototype	Assessment outcome
Simulation elements (actors, objects, pointers, shapes, etc)	At least one drone per simulation	Simulator tested with up to 100 nodes (drones and witnesses) on a desktop PC	Met requirement
	At least 20 witnesses per simulation	Simulator tested with up to 100 nodes (drones and witnesses) on a desktop PC	Met requirement
	Geographical map of the simulation location	Simulation is overlaid on top of Here Maps	Met requirement
	Drone location indicator	Each drone's location is represented by a coloured circle on the visualisation	Met requirement
	Witness location indicator	Each witness's location is represented by a coloured circle on the visualisation	Met requirement
	Witness detection area indicator	The size of the circle visualising the location of the witness also represents the detection area, whose size can be independently adjusted on a witness-by-witness basis	Met requirement

	No Fly Zone (NFZ) size and shape indicator	A polygon shape comprised of lat-long coordinates can be manually entered to define a NFZ of any shape and size	Met requirement* *the capability is not scalable in its current form and is a potential area for future research and development
	Flight corridor size and shape indicator	Not currently possible to simulate with the prototype	Not met
	Control Traffic Region (CTR) size and shape indicator	Not currently possible to simulate with the prototype	Not met
Functionality	Ability to define the independent motion of each drone along a path across a defined geographical region	Lat-long coordinates could be manually entered to define the motion of each drone	Met requirement* *the capability is not scalable in its current form and is a potential area for future research and development
	Ability to move the witnesses independently along a defined path across a defined geographical region	Lat-long coordinates could be manually entered to define the motion of each witness, with variable flight speeds	Met requirement* *the capability is not scalable in its current form and is a potential area for future research and development
	Ability for the user to freely manoeuvre around the visualisation (translate, zoom in/out etc)	The prototype uses a static display. Manoeuvring around the visualisation is not currently possible.	Not met
	Ability to move through the simulation	An interactive timeline is provided which allows the user to specify where in the simulation (which part of the blockchain) is visualised. There is also the option to 'play' the simulation, progressing through the frames (blocks on the blockchain) at a predefined rate.	Met requirement
	Ability to share the prototype between the OU and NATS	The prototype is hosted by the OU on a private server and currently cannot be shared externally with NATS.	Not met

	Ability to change the witness scanning cycle	The witness detection cycle was fixed. Altering this is not currently possible.	Not met

Table 1: Requirements, capabilities and assessment outcome of the prototype prior to modifications

As is evident, prior to development within the SDF project, the DroneBox prototype did not have the capabilities needed to simulate the U-space use cases.

Below is a table of all the developments, modifications, and improvements made to the DroneBox prototype over the course of the project.

Feature / Capability	Before	After
Flight Corridors	It was not possible to simulate or visualise flight corridors.	A polygon shape input was defined in the simulator to enable flight corridors to be created and visualised. This prototype met the requirement following this change.
Control Traffic Region (CTR)	It was not possible to simulate or visualise CTRs.	A polygon shape input was defined (using the same format as the NFZs) in the simulator to enable CTRs to be created and visualised. This prototype met the requirement following this change.
Inputting scenario data	Creating a scenario was a manual, time consuming process involving entry of data points directly into the Python simulator code.	The simulator accepts Keyhole Markup Language (KML) files as the source of the scenario input data. This standardises and significantly speeds up the process of generating the necessary input data and importing it into the prototype.
Accessibility of the visualisation tool	The OU hosted the tool privately, meaning it was not initially accessible to external collaborators such as NATS. While it was possible to find alternative ways to capture the output of the tool and share it, this solution was time consuming and burdensome.	The online visualisation tool was made available via a web link. Access was enabled for both partners, the OU and NATS, who could access the tool and interact with it via their internet browsers. This development greatly improved the ability for both partners to independently analyse and investigate the outputs from each simulation.
Processing time	Previously, the simulations used to occur in real-time. For long-duration scenarios, this meant waiting a significant amount of time for the simulation data to become available on the blockchain.	The simulation can now pre-compute the events that take place in the scenario and then record them to the blockchain with the correct time stamps. The processing time has been de-coupled with duration of the real-time simulations. This has significantly increased the rate at which development of the prototype can take place.

Feature / Capability	Before	After
Adaptive witness algorithm	The witness' detection cycle was fixed.	It is now possible to change witnesses' detection cycle according to a specific algorithm. For instance, here are some examples of witness algorithms: (a) The witnesses detect for 1 second and rest for 2 seconds then repeating that cycle. (b) The witnesses scan for drones as per (a) until a drone is detected by the witness, at which point the scan and recording frequency increases. (c) The witnesses scan for drones as per (a) until a drone is detected by other witnesses in a given proximity, at which point the scan and recording frequency increases.

Table 2: Details of the improvements made to the DroneBox prototype during the SDF project

2.4.2 DroneBox Suitability Assessment

Full details of the suitability assessment including a description of all the continuity, integrity and availability related opportunities and challenges can be found in the DroneBox Suitability Assessment report (Blamey, SDF DroneBox Suitability Assessment, 2021). For concision, those have not been replicated here, but rather the resulting operational and technological constraints[1] have been reproduced.

Operational constraints

1. Surveillance altitude is restricted to lower VLL airspace only when using mobile phones as the detecting devices. The precise altitude limit needs to be determined through future research and technological development, simulations, and validation exercises.
2. Coverage for the mobile phone detectors are restricted to locations which are accessible on the ground.
3. This concept is likely to be suitable for surveillance of specific sites (e.g. airport, metropolitan park, industrial site).
4. There is a requirement for a high density of witnesses over the whole surveillance area to ensure coverage and resilience.
5. The witnesses must be trusted individuals (e.g. Police Officers, Airport staff etc).
6. The surveillance data from the witness' mobile phones is constrained timewise by the battery life of the mobile phones so the solution is better suited to shorter surveillance operations (lasting less than a day).

[1] These are not exhaustive, but aim to capture the key results from the assessment of the opportunities and challenges.

Technological constraints

1. The solution must use a private blockchain.
2. Security mechanisms must be employed including cryptography.
3. The mobile phones must be meet the technical requirements (yet to be determined) to execute the drone witness app.
4. The solution must be scalable.

2.4.3 Use Cases & Scenarios

Inspiration for the use cases was derived from: live trials either taking place or due to take place around the UK[2]; use cases devised for other SESAR Joint Undertaking projects including CORUS (CORUS, 2019) and GOF-USPACE (SESAR Joint Undertaking, 2020); and other ATM/UTM-related projects, namely the Connected Places Catapult (CPC) Open Access UTM project (CPC, 2019), the Airspace4All/NATS Drone Infringement Safeguarding project (Airspace4All, 2019) and the Risk-aware Automated Port Inspection Drone(s) (RAPID) project (CORDIS: EU Research Results, 2020).

The set of use cases was purposefully devised to encompass a range of UA applications, U-space volumes and U-space phases as detailed below.

Use Case	Title	Volume				Phase	
		X	Y	Zu	Za	U2	U3
1	State Surveillance	✓			✓		✓
2	Medical Supply Mission	✓			✓		✓
3	Offshore Inspection		✓		✓	✓	
4	Urban Air Mobility			✓	✓		✓
5	Coastguard Search and Rescue	✓		✓		✓	
6	High Altitude Platforms	✓			✓		✓
7	Port and Infrastructure Inspection		✓			✓	
8	Package Delivery			✓	✓		✓
9	Fire and Rescue Service			✓			✓

Table 3: Use case UA application, U-space volume, and U-space phase coverage

An accompanying nominal and non-nominal scenario was developed for each use case. For full descriptions of the 9 use cases please consult the Use Cases & Scenarios report (Blamey, Rushton, & Moir, SDF Use Cases & Scenarios V2.0, 2021).

[2] Where this is the case, a link to the live trial has been provided in the use case summary.

2.4.4 Data Integrity

One of the key results from the literature search into the meaning of the term ‘data integrity’ was the reference to it within the context of the CIA triad, which defines the three properties of a secure data system. Below are abbreviated versions of the definitions of those properties. For full descriptions, please see the Data Integrity report (Blamey & Westerberg, SDF Data Integrity, 2021).

Confidentiality

This is protecting data such that unauthorised users cannot access it. Processes and procedures should be put in place to ensure the drone telemetry data is made available only to authorised data users (e.g. ATC controllers).

Integrity

This is defined as the protection of data from unwitting or unauthorised, malicious changes to ensure it is reliable and correct. If there is a loss of data integrity, the consequences could be significant as decisions may be made on the basis of incorrect data which impacts safety and exposes users to more risk, both unintentionally and potentially unknowingly. Mitigating actions required include not only authentication and authorisation of information flows between U-space services and other actors such as ANSPs, but also continuous integrity verification of data(bases).

Availability

This means ensuring the data is available to the intended, authorised users while minimising disruption. Availability of the data to U-space services is essential for secure operations. Mitigations include duplication of essential services and systems for redundancy and resilience purposes.

Cyber Security Threat Model

Another key results from the Data Integrity report (Blamey & Westerberg, SDF Data Integrity, 2021) was finding the cyber security threat model in Figure 7, built upon the CIA Triad. Beneath each of the three concepts, potential threats are mapped out.

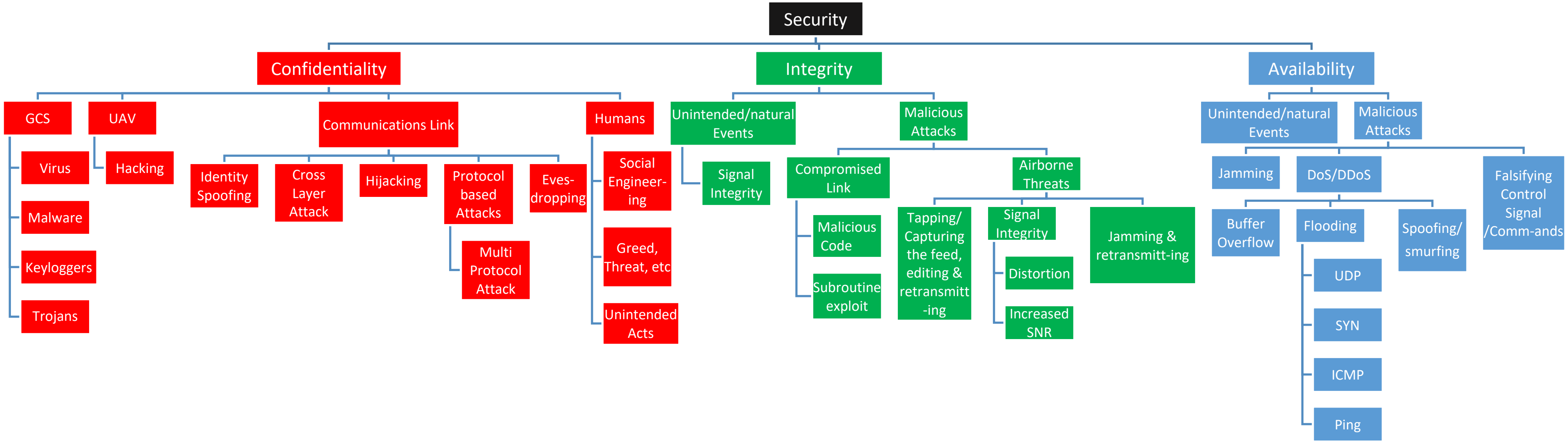
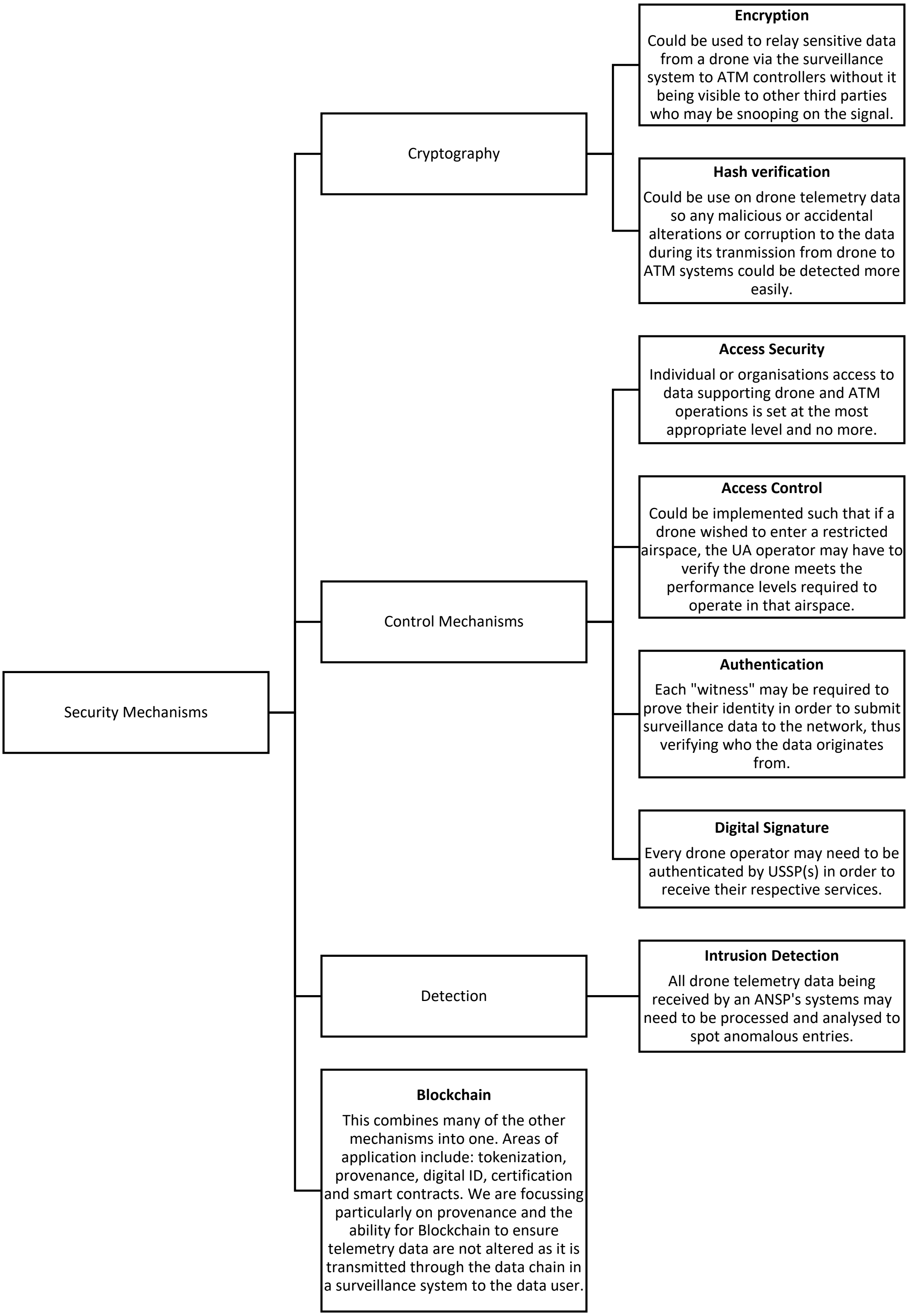


Figure 7: UAV System Cyber-Security Threat Model (Javaid, Sun, & Alam, 2016)

2.4.5 Assuring Digital Trust

A study conducted by the US Federal Aviation Administration (FAA, 2006) detailed many different forms of security mechanisms. This was the primary source upon which the security mechanisms detailed in the Assuring Digital Trust report (Westerberg, Blamey, Ohler, McCullagh, & Whidborne, 2021) were built. Please refer to that report for detailed descriptions of each security mechanism.

Table 8 summarises how each security mechanisms could potential apply in the context of drone surveillance systems and telemetry data.



Security Mechanisms

Cryptography

Encryption

Could be used to relay sensitive data from a drone via the surveillance system to ATM controllers without it being visible to other third parties who may be snooping on the signal.

Hash verification

Could be use on drone telemetry data so any malicious or accidental alterations or corruption to the data during its tranmission from drone to ATM systems could be detected more easily.

Control Mechanisms

Access Security

Individual or organisations access to data supporting drone and ATM operations is set at the most appropriate level and no more.

Access Control

Could be implemented such that if a drone wished to enter a restricted airspace, the UA operator may have to verify the drone meets the performance levels required to operate in that airspace.

Authentication

Each "witness" may be required to prove their identity in order to submit surveillance data to the network, thus verifying who the data originates from.

Digital Signature

Every drone operator may need to be authenticated by USSP(s) in order to receive their respective services.

Detection

Intrusion Detection

All drone telemetry data being received by an ANSP's systems may need to be processed and analysed to spot anomalous entries.

Blockchain

This combines many of the other mechanisms into one. Areas of application include: tokenization, provenance, digital ID, certification and smart contracts. We are focussing particularly on provenance and the ability for Blockchain to ensure telemetry data are not altered as it is transmitted through the data chain in a surveillance system to the data user.

Figure 8: Taxonomy of security mechanisms and their potential application to in the context of drone operations

2.4.6 U-space Service Hazard Assessment

Please consult the Hazard Assessment report (Moir & Blamey, SDF Hazard Assessment, 2021) for granular detail on the results from this assessment.

The first task – to identify the applicable hazards – resulted in the following list of hazards that BVLOS drone flights could experience:

- Loss of Control – Inflight (LOC-I)
- Mid-Air Collision (MAC)
- Low Altitude Operations hazard (LALT)
- Security Related (SEC)
- Loss of Visual Line of Sight (LVLOS)*

*This is a new hazard specific to UA operations.

Drone Telemetry Data Parameters

Table 4 summarises which drone telemetry data parameters are required by U-space phase and volume.

U-Space Phase / Volume	X	Y	Z
U1	Mandated: Identity, current position		
U2	Mandated: Identity, current position Optional: 3D state vector, intent, environment, collision avoidance, emergency, flight mode and equipage, emergency status	Mandated: Identity, current position, 3D state vector, intent, environment, collision avoidance, emergency, flight mode and equipage, emergency status	
U3			
U4	Mandated and optional future requirements are yet to be determined, but will be dependent on the U-Space services that will be available in U4		

Table 4: Telemetry data parameters required

The main takeaway from Table 4 is the expansion in the number of telemetry data parameters from U1 to U4 as more U-space services become available. Also, as Y and Z volumes represent airspace in closer proximity to crewed aviation and more populated ground features, a greater number of telemetry data parameters are mandated in these U-space volumes.

Allowable Data Integrity Failure Probabilities

The failure condition classifications, from ‘no safety effect’ through to ‘catastrophic’, as defined by the EASA special conditions for RPAS (EASA, 2015) were employed and deduced for each U-space service by volume. Using an EASA report on the Acceptable Means of Compliance for RPAS equipment and systems (EASA, 2015), it is possible to translate the failure classifications into allowable quantitative probabilities.

Table 5 displays the resulting minimum allowable failure probabilities for data integrity in each U-space phase and volume.

U-Space Phase / Volume	X	Y	Z
U1	Probable $< 10^{-3}$	Probable $< 10^{-3}$	Remote $< 10^{-4}$
U2	Remote $< 10^{-4}$	Remote $< 10^{-4}$	Extremely Remote $< 10^{-5}$
U3	Remote $< 10^{-4}$	Extremely Remote $< 10^{-5}$	Extremely Remote $< 10^{-5}$
U4	Remote $< 10^{-4}$	Extremely Remote $< 10^{-5}$	Extremely Improbable $< 10^{-6}$

Table 5: Allowable failure probabilities for telemetry data integrity, by U-Space phase and volume. The quantitative probabilities are average probabilities of failure per hour of operation.

2.4.7 U-space Use Case Hazard Assessment

Please consult the Use Case Hazard Assessment (Moir & Blamey, SDF Use Case Hazard Assessment, 2021) for a write up of the complete set of results from this assessment.

For this validation exercise, the same Failure Condition Classifications as seen in the U-space Services Hazard Assessment were assigned to each use case. For each one, a pre-mitigation hazard assessment was carried out, determining the likely outcome and its associated risks. Following this, mitigations to reduce the risks were identified and considered and the hazard assessment was carried out again. The results are provided in Table 6.

	U Space Phase		**Highest Allowable Probability of C2 Continuity / Integrity failure (per hour of operation)**	
Use Case	U2	U3	**Pre-Mitigation**	**Lowest Post-Mitigation**
1. State Surveillance		10^{-5}	10^{-6}	10^{-5}
2. Medical Supply Mission		10^{-5}	10^{-5}	10^{-4}
3. Offshore Inspection	10^{-5}	10^{-5}	10^{-5}	10^{-5}
4. Urban Air Mobility		10^{-6}	10^{-6}	10^{-5}
5. Coastguard Search and Rescue	10^{-5}	10^{-5}	10^{-6}	10^{-5} (See Footnote[3])
6. High Altitude Pseudo Satellite		10^{-5}	10^{-6}	10^{-5}
7. Windfarm Transit	10^{-4}	10^{-5}	10^{-6}	10^{-5}
8. Package Delivery		10^{-5}	10^{-6}	10^{-5}
9. Fire and Rescue Service		10^{-5}	10^{-5}	10^{-4}

Table 6: Allowable probabilities Use case hazard assessment

[3] This figure relates to when the Tactical Conflict Resolution service is available, (planned for introduction in U3). A lower (more onerous) allowable probability should be considered in the absence of the Tactical Conflict Resolution service.

3 Conclusions, next steps and lessons learned

3.1 Conclusions

The following subsections describe how the project helped to increase the maturity of the prototype while also furthering the understanding and knowledge of the safety and security of drone telemetry data.

3.1.1 DroneBox Capability Study

With the modifications that were made over the course of the project implemented, the conclusion was that the DroneBox prototype met all the requirements necessary and was therefore deemed capable of conducting the SDF simulation and validation activities. By making alterations prompted by airspace, ATM and U-space needs, the prototype increased in maturity towards applied/industrial research.

The capability study highlighted several potential areas of future research which would further improve the prototype:

a. **Automation**: Some aspects and features of the prototype, as commented on in Table 1 in section 2.4.1, are not currently scalable. Embedding more automation and batch processing into the prototype would help in this regard.
b. **Altitude**: Including altitude in the prototype, upgrading it from 2D to 3D would add more realism and widen the scope of the prototype simulations.
c. **Experimental validation**: Advance the maturity of the concept to an experimental proof of concept while testing and validating the accuracy and suitability of the prototype in different operational environments.
d. **Improved User Interface**: Improved/more user-friendly data viewer.
e. **Bulk data storage**: Enable larger storage of data in the prototype for larger scale simulations.
f. **High gain directional antenna**: Consider the inclusion of high gain directional Wi-Fi antenna in the surveillance network and assess how these might mitigate some of the challenges of the concept.

3.1.2 DroneBox Suitability Assessment

The following conclusion has been extracted from the DroneBox Suitability Assessment (Blamey, SDF DroneBox Suitability Assessment, 2021). For further details on this, please refer to that study and to the Session 2 Final Workshop Slides (Blamey, Barthaud, Neale, & Yu, 2021).

Taking into account observations from the U-space use cases, and recognising the limitations and constraints imposed by the opportunity-based solution, it is concluded that the DroneBox concept is suitable for providing surveillance information in particular operational environments. Namely, it could provide a suitable surveillance solution for short duration operations in lower VLL airspace in highly populated, urban environments where there are is a high density of ground witnesses. Use cases in this environment include: inner-city emergency service operations (police, fire and rescue, medical response); inspection and/or surveillance of high value or high sensitivity infrastructure (airports, tourist attractions, high-profile buildings); aerial monitoring during peak periods at train stations, bus stations, sports venues; and security operations at prisons, to name a few.

It was noted that by combining the opportunity-based solution (using witness' mobile phones) with larger detection range, stationary drone detectors, then the concept is suitable for a wider range of operational environments and use cases. For instance, it could then have application in settings such as: wind farms; power stations and grid networks; railway lines; airports; spaceports; and more.

3.1.3 Use Cases & Scenarios

The use cases and scenarios helped mature the prototype by providing the operational U-space environments and situations which formed the basis for the simulations and validation activities.

3.1.4 Data Integrity

This report helped develop an understanding of the central, underlying concept in this project, i.e. data integrity. The technical conclusions of the report were as follows.

Data integrity is critical for the security of U-space services insofar as it represents a key aspect of data quality specifications and constitutes the basis for key performance requirements for a UA surveillance system. Should there be a loss of data integrity then there is the potential for a risk to develop both to the U-space environment and those associated with it, such as manned aviation.

In order to protect itself from disruption it is vital that a data system is constructed and operated such that the key information security elements of confidentiality, integrity and availability are assured. Through this the system and the data within it can be utilised with the confidence that unauthorised users are unable to access it, that the data contained within it is reliable and correct, free from interference and that authorised users are able to access it in a timely and non-disrupted manner.

Any identified solution, such as the DroneBox, must respect the need for the integrity of aeronautical data from origination to distribution to the next intended user; and must contain procedures to mitigate the loss of data integrity depending on the criticality of the data.

3.1.5 Assuring Digital Trust

This report helped establish the cyber security mechanisms that ought to be embedded in the design of a drone surveillance system. The conclusions below contain requirements and considerations for the design of the DroneBox solution in its next phase of development.

When considering the various aspects of Digital Trust it must be remembered that none of these operate in a vacuum and therefore none are impervious to impact; at all stages elements such as poor cyber security hygiene and practices may impact the security of the network. As an example, whilst blockchain protocol has strong security, it can be attacked in a number of different ways including targeting vulnerabilities in the nodes and network that implement the distributed ledger which may enable an attacker to impact the operations and security of the blockchain and distributed ledger.

When designing and implementing Digital Trust systems, including future drone surveillance systems such as the DroneBox, it is essential to consider infrastructural requirements and preferably layers of security; not only must the nodes and networks be capable of receiving, carrying and processing large amounts of data, they need also to have built-in protections to minimize their vulnerability to attack. The correctly implemented multiple layers of security controls can reduce the impact and likelihood of a successful attack.

3.1.6 U-space Service Hazard Assessment

This assessment helped to increase the maturity of the prototype towards apply and industrial research as it led to the determination of which telemetry data parameters would be required in different U-space airspace and the quantification of drone telemetry data allowable failure rates. This, in turn, forms minimum requirements on the levels of data integrity on future drone surveillance concepts including the DroneBox.

Several trends in identified from the hazard assessment results are explained below.

In time, as the delivery of U-space progresses through phases U1 to U4, more U-space services will be implemented and provided to UA / PAVs. This will put more demands and higher levels of dependence on the C2 link and, in turn, its integrity. At the same time, the number of uncrewed aircraft in the skies is estimated to increase by several orders of magnitude, to the point where they are significantly more numerous that traditional, crewed aircraft. The higher dependency on the data and the higher density of traffic puts more demands on the CNS system while increasing the severity of a loss of data integrity. While the *severity* of a failure event will increase, in order to maintain an acceptable level of safety risk, the *likelihood* of a failure occurring must become less and less probable. Hence, as shown in Table 5 in section 2.4.6, a trend emerged from the hazard assessment results toward more stringent allowable failure probabilities with increasing U-space phase.

The *severity* of a failure event increases when moving from X to Y to Z volumes. This is because the volumes are intimately linked with the air and ground risks in those regions. Contributing risk factors might include: population density, presence of tall structures, hazardous industrial sites, presence of (high passenger number) airlines, unmanned and manned air traffic density and more. As a result, the likelihood of telemetry data integrity failures must be less likely in Z volumes than in Y volumes, and less probable in Y volumes than in X volumes.

3.1.7 U-space Use Case Hazard Assessment

The most onerous safety requirements for U-space services in U-space phases U2 and U3 were found to be Extremely Remote/$<10^{-5}$ per hour of operation.

The most onerous requirement, post-mitigation, for the 9 Use Cases assessed is also Extremely Remote/$<10^{-5}$ per hour of operation, with one exception – those Use Cases put into operational service in U2, that rely on Tactical Conflict Resolution service which is not planned to be available until U3. In this exceptional case, additional mitigations should be explored.

Therefore, provided the combination of mitigations employed for each use case are established to be greater than 90% effective, noting the exception above, the post-mitigation integrity and availability requirements for the C2 link that result from the use case hazard analysis are no more onerous than have already been determined for the hazard analysis of the relevant safety-related U-space services.

That is, the use case hazard assessment successfully validated the findings of the U-space services hazard assessment, bar one aforementioned exception.

3.2 Next steps

The research conducted in the SDF project will be taken forward in a number of different ways as outlined below. There are additional dissemination activities planned but these are covered in section 4.

3.2.1 Academic Publication

The DroneBox Paper (Barthaud, et al., 2021) was drafted during the course of the project on the subject of the concept and prototype. The OU have expressed their intention to further develop the DroneBox prototype during the summer in 2021, to gather more data from the simulations and to conduct analysis on that data. It is likely this research will revolve around the application of different adaptive witness algorithms (see Table 2 for more details) to deduce the relative (dis)benefits of each of them. Following this research, the aim is to write and submit, with support from NATS, an updated version of the DroneBox Paper to the International Conference on Software Engineering (ICSE) in late summer 2021.

3.2.2 Seek Grant Opportunities

Both NATS and the OU have signalled their willingness to continue collaborating together on developing, maturing and validating the DroneBox solution. Both partners will seek to find future calls for proposals to support that work.

In addition to the potential avenues of further work outlined in 3.1.1, it would be beneficial to understand the value proposition for the DroneBox concept. A simplistic example was shown in the Session 2 Final Workshop slides (Blamey, Barthaud, Neale, & Yu, 2021), however this is in need of refining in more rigorous detail.

3.2.3 Industrial Application

The methodology used for some aspects of this project and several outcomes from the project have value for other ongoing projects in the U-space / CNS domains. For instance, Use Cases & Scenarios has provided inspiration for some of the use cases being developed as part of Solution 2 of the AURA PJ.34 SESAR project (SESAR Joint Undertaking, 2021). The cyber security research questions raised during the Final Workshop are to be collated and followed-up with the cyber security team at NATS. In addition, the outcomes from the project will help guide the NATS data assurance policy for UAS and RPAS (more details in section 4.5).

3.3 Lessons learned

Below is a list of the lessons learned (positive comments and critical observations) with regards to the management aspects and how well the project worked.

- ✓ This Engage KTN project had light-touch management and a degree of flexibility with regard to the research activities. This allowed for more creative and less structured research which was very well suited to early-stage maturity concept development.
- ✓ The communication with the Project Coordinator at the University of Westminster has been excellent; very prompt and helpful.
- ✓ The size of the budget suited the scope of this type of project.

- For future Engage KTN projects, it would be useful to be provided with a brief on the scope and responsibilities of the project mentors to better utilise their input.
- Recommend slightly larger ‘next stage’ funding rounds (~€150k) for conducting small-scale validation exercises. These should preferably be open to partners who have already received prior Engage KTN funding.
- Would it be possible to create an Engage KTN network of contacts in key organisations (such as EASA, EUROCONTROL, certain ANSPs etc) who are willing to participate in Engage KTN workshops? This would reduce reliance on the partners’ own networks.
- Recommend making the templates for the progress and technical reports available from the start of the project so they can be developed during the course of the project.

4 Dissemination

4.1 Thematic Challenge 1 Workshops

On **10th November 2020**, slides (Blamey, SDF TC1 Workshop Project Slides, 2021) were presented at the TC1 Workshop by the OU on the purpose and the then progress of the project.

It has been agreed that an overview of the SDF project will be presented by NATS at the upcoming TC1 Workshop on **15th September 2021**.

4.2 Interim Workshop

An interim workshop was held on 11th January at the end of the first reporting period. The aim was to disseminate and validate some of the research findings from the first reporting period.

The overarching theme of this workshop was flight surveillance systems for drones and the security of real-time data those systems receive. Specifically, we were interested in how to assure the integrity and availability of drone telemetry data relayed by third-party sources.

4.2.1 Agenda

For the full workshop agenda document sent to invitees, please see the Interim Workshop Agenda document (Blamey & Rushton, SDF Interim Workshop Agenda, 2021).

9:30 – 11:00am	Session 1 Introduction to the **Safe Drone Flight** Engage Knowledge Transfer Network (KTN) project and the basic principles of U-space.
	Morning break
11:30 – 12:30pm	Session 2 Exploration of a set of **U-Space Use Cases** and Scenarios encompassing a range of UA BVLOS operations.
	Lunch break
14:00 – 15:00pm	Session 3 Explanation of how we used the Use Cases to conduct a **Hazard Assessment** to determine what the requirements are to assure the integrity of UA telemetry data.
	Afternoon break

15:30 – 16:30pm	Session 4 Discussion of potential **surveillance technology and digital trust solutions** including a blockchain prototype demonstrator.

4.2.2 Attendance

The meeting was attended by 29 stakeholders spanning the following organisations and institutes:

Industry
NATS
Direction des Services de la Navigation Aérienne (DSNA)
Heathrow Airport Holdings (HAL)
European Union Aviation Safety Agency (EASA)
EUROCONTROL
Academia
The Open University
University of Westminster
University of Belgrade
University of Kent

Table 7: Industry and academic organisations and institutes represented at the workshop

Workshop attendees had specialist knowledge and expertise in many relevant domains including: ANSP Research & Development, Unified Traffic Management, cyber security and information security, safety assurance, CNS systems, ANSP service architecture, transport and traffic engineering, aviation and air transport research, drone piloting, counter drone systems, drone software engineering and software development.

There was a high-level of engagement from the participants, prompted by a range of interactive workshop elements.

4.2.3 Overview & Takeaways

Session 1

- Introduction to project and aims of the workshop
- Discussions validated certain aspects of the methodology used in this project
- The participants posed many valuable questions which will help inform the research undertaken in the 2nd Reporting Period

Session 2

- The 8 Use Cases devised were validated in that there was consensus that they represented a broad, realistic set of Use Cases
- 2 new Use Cases suggested by a couple of the participants need to be added to fill gaps that were identified (this action to be taken in the 2nd Reporting Period)
- Discussion themes will be analysed and contribute towards the commentary around non-nominal threats and integrity level requirements

Session 3

- Safety-related definitions of ‘hazards’ and ‘data integrity’ were defined
- Discussions around the Use Case hazards identified key themes such as the elevated risks associated with UAM operations and those over dense populations
- A comparison between manned and unmanned aviation revealed many similar hazards exist

- The C2 link is of critical importance to the safety of U-space services, arguably more so than voice comms is to manned aviation
- There is a need to create a UA C2 link which has the same level (or better) resilience as the human voice

Session 4

- The Open University gave a live demonstration of the 'LiveBox' prototype by displaying two scenarios with UA flights being detected by witness and capturing their telemetry data on a blockchain
- This demonstration validated the applicability and functionality of the prototype in the case of two of the U-Space Use Cases

4.2.4 Feedback

Below are some of the remarks attendees made about the workshop:

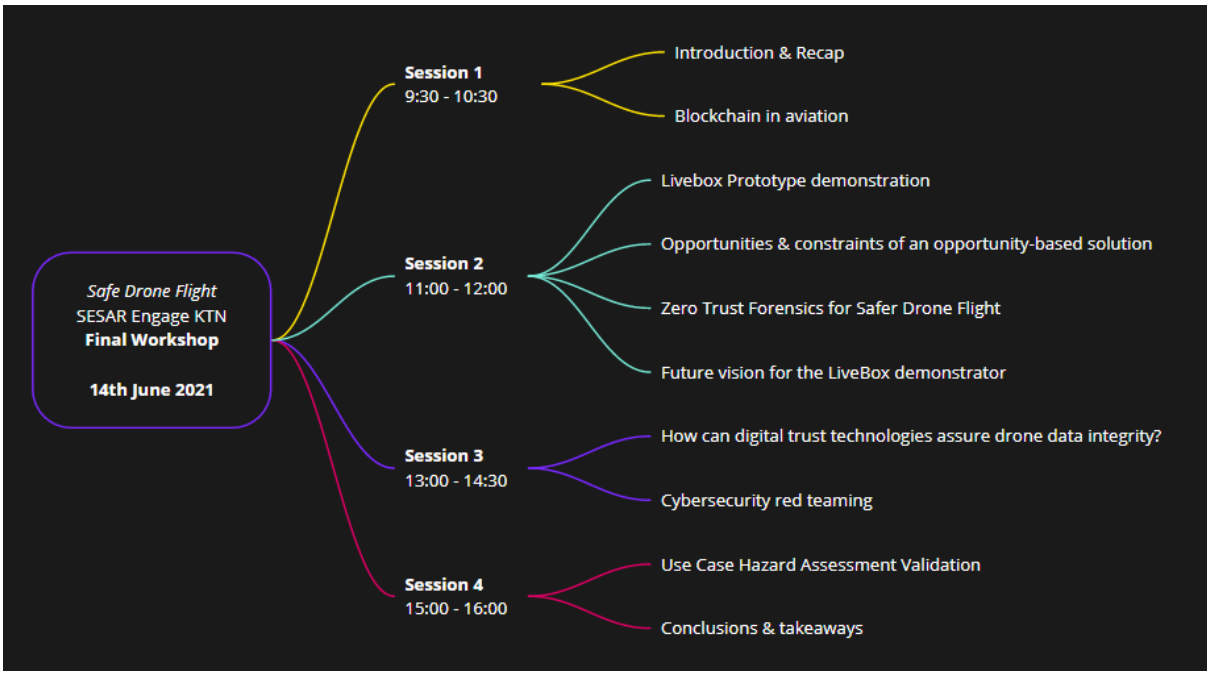
> "Great set of presentations. Fascinating."
> ***[name removed]**, Senior Systems Manager at NATS*
>
> "The workshops were excellent."
> ***[name removed]**, Head of UTM Programmes at NATS*
>
> "Insightful workshop."
> ***[name removed]**, Senior Lecturer in Software Engineering for Self-Adaptive Systems at the University of Kent*

4.3 Final Workshop

A final workshop was held on 14th June, near the end of the second reporting period. The purpose of the workshop was three-fold:

- **Participation**: Gather together a wide range of stakeholders to pool expert knowledge in a variety of different domains and disseminate the project findings to them, with an emphasis on the progress made in the second Reporting Period (RP2)
- **Engagement**: Promote and facilitate engagement, particularly between the academia and industry
- **Interaction**: Prompt interactions between the attendees to generate fruitful technical discussions and build and grow partnerships

4.3.1 Agenda



Safe Drone Flight
SESAR Engage KTN
Final Workshop

14th June 2021

Session 1
9:30 - 10:30
- Introduction & Recap
- Blockchain in aviation

Session 2
11:00 - 12:00
- Livebox Prototype demonstration
- Opportunities & constraints of an opportunity-based solution
- Zero Trust Forensics for Safer Drone Flight
- Future vision for the LiveBox demonstrator

Session 3
13:00 - 14:30
- How can digital trust technologies assure drone data integrity?
- Cybersecurity red teaming

Session 4
15:00 - 16:00
- Use Case Hazard Assessment Validation
- Conclusions & takeaways

4.3.2 Attendance

The meeting was attended by 25 stakeholders spanning the following organisations and institutes:

Industry
NATS
UK Civil Service
EUROCONTROL (ECTL)
Heathrow Airport Limited (HAL)
Neuron Innovations

Academia
The Open University (OU)
University of Westminster
University of Belgrade
University of Kent

Table 8: Industry and academic organisations and institutes represented at the workshop

Workshop attendees had specialist knowledge and expertise in many relevant domains including: ANSP Research & Development, Unified Traffic Management, U-space, cybersecurity and information security, safety assurance, digital forensics, CNS systems, transport and traffic engineering, aviation and air transport research, ATM market intelligence, drone software engineering, Distributed Ledger Technologies (DLT), and software development.

The slides and findings from the workshop were disseminated to 40+ stakeholders and the video recordings of the sessions were also shared where possible.

4.3.3 Overview & Takeaways

Session 1

- The project has progressed over the second reporting period and has taken on board many of the findings from the Interim Workshop.

- Many myths surround blockchain technology; it is a credible technology with many applications within ATM.
- Blockchain is a type of Distributed Ledger Technologies (DLT). DLT is an emerging technology. Its merits, drawbacks and suitability need to be assessed for each application on a case-by-case basis.

Session 2

- Demonstrated the Solent medical drone delivery use case using the LiveBox prototype which has improved functionality.
- LiveBox concept is principally suitable for short duration, lower VLL airspace operations in urban areas.
- Ascertained how the concept of 'Zero Trust' might be applied in the context of drone operations and surveillance system cybersecurity.
- Considered follow-on research and commercialisation opportunities for the LiveBox prototype.

Session 3

- Validated that various different types of security mechanisms can mitigate against the cyber risks in the use cases.
- Collated list of new research questions which need to be addressed.

Session 4

- Demonstrated use case hazard assessment aligns with the services hazard assessment.
- Use case corner cases warrant further investigation.

4.3.4 Feedback

Below are some of the remarks attendees made about the workshop:

> "The presentations were very interesting and informative, and the breakout sessions were very productive."
> ***[name removed]****, Research Analyst at NATS*
>
> "Really interesting day"
> ***[name removed]****, Information and Cyber security Analyst at NATS*

4.4 Research Collaboration Conference 2021

NATS is preparing to hold a Research Collaboration Conference in September/October this year. It will showcase in a virtual exhibition space the collaborative research that NATS is part of with universities and industrial partners.

The SDF project will feature in the conference with a collection of materials (which are currently being prepared) to engage a wide internal and external audience about the work that has been carried out.

- **Pre-recorded video** explaining what the SDF project is and the progress that was made, the contribution from each partner, and the benefits of the project
- **Webcast** panel discussion on a topic related to integrating new airspace users and assuring safety
- **Storyboard** focussing on integrity of the data chain for drone telemetry data

4.5 Blueprint on U-space Data Assurance

The project results will be disseminated to relevant stakeholders and key findings will potentially be integrated into a blueprint on U-space data assurance within NATS. The aim will be to leverage the knowledge gained and the research outcomes from the SDF project on the assurance of U-space data to guide the wider strategy.

Data assurance is considered at the core of the NATS ATM / U-space framework and supports the function of human roles within ATC; including consideration of Industry needs for pop-up and federated service provision through continuous development and integration.

U-space services are seen to require a data assurance level that shall allow U-space to enable:

- A greater diversity of users and data;
- Reduced human to machine workloads;
- Large volume data sharing; and
- On-demand provision of information and services

5 References

5.1 Project outputs

5.1.1 Research Documents/Reports

Barthaud, D., Yu, Y., Blamey, J., Rushton, A., Moir, G., Price, B., . . . Nuseibeh, B. (2021). *SDF DroneBox Paper: Automated Adaptive Collection of UAV Flight Data.*

Blamey, J. (2021). *SDF DroneBox Suitability Assessment.*

Blamey, J., & Barthaud, D. (2021). *SDF DroneBox Capability Study.*

Blamey, J., & Westerberg, R. (2021). *SDF Data Integrity.*

Blamey, J., Rushton, A., & Moir, G. (2021). *SDF Use Cases & Scenarios V2.0.*

Moir, G., & Blamey, J. (2021). *SDF Hazard Assessment.*

Moir, G., & Blamey, J. (2021). *SDF Use Case Hazard Assessment.*

Westerberg, R., Blamey, J., Ohler, C., McCullagh, H., & Whidborne, N. (2021). *SDF Assuring Digital Trust.*

5.1.2 Workshop Outputs

Barthaud, D., Yu, Y., & de Lemos, R. (2021). *SDF Interim Workshop Session 4 Slide Deck.*

Blamey, J. (2021). *SDF Interim Workshop Session 2 Slide Deck.*

Blamey, J. (2021). *SDF Interim Workshop Takeaways.*

Blamey, J. (2021). *SDF TC1 Workshop Project Slides.*

Blamey, J., & Rushton, A. (2021). *SDF Interim Workshop Agenda.*

Blamey, J., Barthaud, D., Moir, G., & Rushton, A. (2021). *SDF Final Workshop Takeaways.*

Blamey, J., Barthaud, D., Neale, C., & Yu, Y. (2021). *SDF Final Workshop Session 2 Slide Deck.*

Moir, G. (2021). *SDF Interim Workshop Session 3 Slide Deck.*

Moir, G., & Blamey, J. (2021). *SDF Final Workshop Session 4 Slide Deck.*

Rushton, A. (2021). *SDF Interim Workshop Session 1 Slide Deck.*

Rushton, A., Leoni, H., & Blamey, J. (2021). *SDF Final Workshop Session 1 Slide Deck.*

Westerberg, R., Ohler, C., & Whidborne, N. (2021). *SDF Final Workshop Session 3 Slide Deck.*

5.2 Other

Airspace4All. (2019, November 15). *Airspace4All/NATS Drone Infringement Safeguarding Report.* Retrieved from Airspace4All: https://airspace4all.org/wp-content/docs/20191115-Airspace4All-NATS-Drone-Infringement-Safeguarding-Report-V1.1.pdf

CORDIS: EU Research Results. (2020, July 11). *Risk-aware Automated Port Inspection Drone(s).* Retrieved from CORDIS: https://cordis.europa.eu/project/id/861211

CORUS. (2019, September 9). *SESAR Concept of Operations for U-Space.* Retrieved from SESAR Joint Undertaking: https://www.sesarju.eu/node/3411

CPC. (2019, September 30). *Open Access UTM.* Retrieved from Connected Places Catapult: https://s3-eu-west-1.amazonaws.com/media.cp.catapult/wp-content/uploads/2019/09/30150855/Towards-a-UTM-System-for-the-UK.pdf

EASA. (2015, October 12). *SC-RPAS.1309-01 Special Condition: Equipment, systrems, and installations.* Retrieved from EASA: https://www.easa.europa.eu/sites/default/files/dfu/SC-RPAS.1309-01_Iss02.pdf

Javaid, A. Y., Sun, W., & Alam, M. (2016, August 31). *Cyber Security Threat Analysis and Modeling of an.* Retrieved from ResearchGate: https://www.researchgate.net/profile/Ahmad_Javaid/publication/235676360_Cyber_security_threat_analysis_and_modeling_of_an_unmanned_aerial_vehicle_system/links/57c6db2908ae9d64047e4d5c/Cyber-security-threat-analysis-and-modeling-of-an-unmanned-aerial-vehic

NATS. (2021, July). *Drones: Enabling safe integration in our skies*. Retrieved from NATS: https://www.nats.aero/airspace/drones/

PwC. (2021, July). *The impact of drones on the UK economy*. Retrieved from PwC: https://www.pwc.co.uk/issues/intelligent-digital/the-impact-of-drones-on-the-uk-economy.html

SESAR Joint Undertaking. (2020). *U-Space: Consolidated report on SESAR U-Space research and innovation results.* Retrieved from SESAR JU: https://www.sesarju.eu/node/3691

SESAR Joint Undertaking. (2021). *PJ34-W3 AURA - ATM U-space Interface*. Retrieved from https://www.sesarju.eu/projects/aura

SESAR Joint Undertaking. (2021). *U-space Blueprint*. Retrieved from SESARJU: https://www.sesarju.eu/u-space-blueprint

6 Annex I: Acronyms

Acronym	Definition
ACAS	Airborne Collision Avoidance Systems
ADS-B	Automatic Dependent Surveillance-Broadcast
AF	Audio Frequency
ANSP	Aeronautical Navigation Service Provider
ATM	Air Traffic Management
ATC	Air Traffic Control
ATCO	Air Traffic Control Officer [‘Controller’]
ATS	Air Traffic Service
ATZ	Aerodrome Traffic Zone
BVLOS	Beyond Visual Line Of Sight

Acronym	Definition
CAA	Civil Aviation Authority
CAO	Coastguard Agency Officer
CAS	Calibrated Airspeed
CAT	Civil Air Transport
CFIT	Controlled Flight Into or towards Terrain hazard
CPC	Connected Places Catapult
CTA	Control Area
CTR	Controlled Traffic Region
C2	Command and Control
DAA	Detect And Avoid
DDoS	Distributed DoS
DoS	Denial of Service
EC	Electronic Conspicuity
ETA	Expected Time of Arrival
EVLOS	Extended Visual Line Of Sight
EVTOL	Electric Vertical Take Off and Landing
FCU	Flight Calibration Unit
FIMS	Flight Information Management System
FIS	Fight Information Service
FISO	FISO Officer
FMS	Flight Management System
FPV	First-Person View
GA	General Aviation
GCS	Ground Control Station
GPS	Global Positioning System
HAPS	High Altitude Pseudo-Satellite
HF	High Frequency
IAS	Indicated Airspeed
ICMP	Internet Control Message Protocol
ICT	Information and Communications Technology
IFR	Instrument Flight Rules
KTN	Knowledge Transfer Network
LALT	Low Altitude Operations hazard
LOC-I	Loss Of Control – Inflight hazard
LVLOS	Loss of VLOS
MAC	Mid-air Collision hazard
MCA	Maritime and Coastguard Agency
MCP	Mode Control Panel
MPS	Metropolitan Police Service
OFCOM	Office of Communications
OU	The Open University
PAV	Personal Air Vehicle
PKI	Public Key Infrastructure
PO	Police Officer
PSR	Primary Surveillance Radar
RPAS	Remotely Piloted Aircraft System
SA	Situational Awareness

Acronym	Definition
SEC	Security hazard
SESAR	Single European Sky ATM Research
SNR	Signal to Noise Ratio
SSR	Secondary Surveillance Radar
SVFR	Special VFR
SYN	Synchronise
TAS	True Airspeed
TOC	Top Of Climb
TOD	Top Of Descent
TI	Traffic Information
UA	Uncrewed Aircraft
UAM	Urban Air Mobility
UAS	Uncrewed Aircraft Systems
UDP	User Datagram Protocol
USS	UAS Service Supplier
USSP	U-Space Service Provider
USV	Uncrewed Surface Vehicle
UTM	UAS Traffic Management
VFR	Visual Flight Rules
VHF	Very High Frequency
VLL	Very Low Level
VLOS	Visual Line Of Sight
VMC	Visual Meteorological Conditions
WAM	Wide Area Multilateration

Term	Meaning
DroneBox	An automated system that enables the real-time detection and storage of drone data, based upon the LiveBox concept.
LiveBox	A self-adaptive forensic-readiness service for drones.