SESAR Engage KTN – catalyst fund project final technical report

Project title:	The Drone Identity
Coordinator:	The Open University (OU)
Consortium partners:	NATS
Thematic challenge:	TC1 Vulnerabilities and global security of the CNS/ATM system
Edition date:	30 June 2020
Edition:	1.0
Dissemination level:	Public
Authors:	Danny Barthaud / OU
	Yijun Yu / OU
	Blaine Price / OU
	Andrea Zisman / OU
	Arosha Bandara / OU
	David Bush / OU
	Bashar Nuseibeh / OU

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 Drone Identity project investigates *forensic-readiness requirements* of unmanned aerial systems (UAS), to help identify causes of safety and security related air traffic incidents. It is a collaborative effort between researchers at The Open University (OU) and NATS. The project contributes to addressing the vulnerabilities and global security of communications, navigation, and surveillance systems in air traffic management (CNS/ATM). The collection and use of forensic data associated with drones and surrounding physical contexts is key to effective investigation.
The research is conducted in the context of *U-Space*, focusing on the architecture and concept of operations for European unmanned traffic management (UTM), and the ability to preserve such vital information as evidence for forensic investigations The goals of such forensic readiness are to ensure that the root causes of incidents can always be analysed, facilitated by evidence collected during operation (drone flight). The project focuses on drone data, examining ways in which key drone characteristics can be determined and recorded soundly, if and when incidents involving the drone(s) occur. In particular, the key attributes that characterise and identify the drones, their operators, and their anomalous behaviours will be investigated. A prototype demonstrator has been developed, including a technical architecture, to illustrate and evaluate the proposed forensic readiness requirements for U-Space services.

1.2 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].

2. Overview of catalyst project

2.1 Operational/technical context

Drones are shaping an industry expected to be worth of £ 42 billion and 628,000 jobs for UK alone by 2030 [1]. However, they are also exerting huge pressure on existing safety air traffic infrastructures, increasing from 6K passenger aircraft flights to over 70K drone flights per day over the UK alone. Conflicts between manned and unmanned aircraft have already caused serious problems in safety and business operation of the international airports managed by ANSPs.

For aviation safety, drones are regulated by international (ICAO), European (EASA) and national aviation authorities (CAA in UK) [2]. Most drone-related incidents are unidentified (e.g., unknown pilots) and their root causes uncertain due to the lack of airmanship and lack of an infrastructure to preserve evidence [3][4]. This situation has led to a huge loss to the aviation industry (e.g., delays of thousands of flights in Gatwick and Heathrow airports), presenting great challenge to aviation authorities (CAA) and air traffic service providers (NATS).

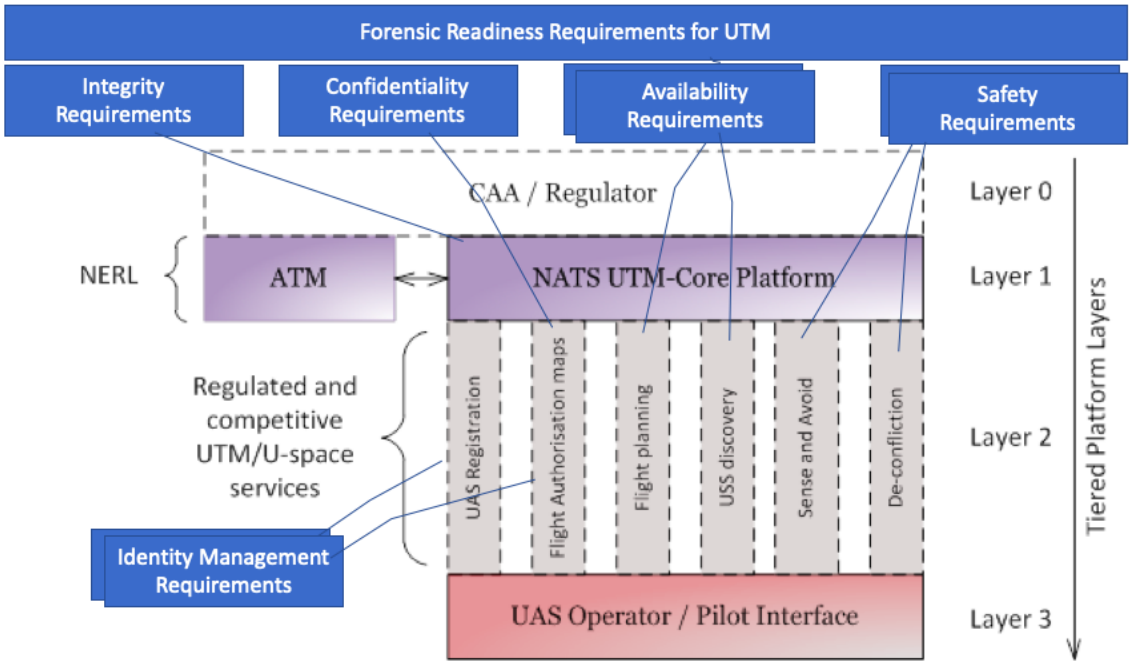

Figure 1. Drone Identity: Contextualising Forensic Readiness Requirements for UTM

Security and safety incidents in such 'systems of systems' are challenging to investigate, particularly given the diverse digital technologies and human behaviours involved, and the different degrees of automation involved. Unmanned aerial vehicles (or drones hereafter) are increasingly creating challenges for managing the safety of the aircraft that share the airspace with them. Recent high-profile incidents at airports arising from unidentified drones (such as those at Gatwick and Heathrow airport), underline the urgent need to investigate the risks and incidents in such managed airspaces.

The project contributes to addressing the vulnerabilities and global security of communications, navigation, and surveillance systems in the context of air traffic management (CNS/ATM). In particular, we considered the problem domains as illustrated by the architectural diagram of U-Services (see Figure 1).

To analyse the root causes of these incidents, forensic-readiness [5] is proposed as the capability to collect sound and timely evidence for subsequent investigations. In this proposed project, such readiness needs to be aligned to the architecture of Unmanned Traffic Management (UTM) in the context of SESAR U-space project.

2.2 Project scope and objectives

Forensic readiness entails that minimally relevant forensically sound evidence is collected, before and during flights, to identify any violation of regulations that led to an incident [5][6]. It needs to be supported by the UTM features such as drone/pilot registrations, geofencing, data records tracking, detect and avoid conflict resolution, and safe interoperation with manned aviation. Contributing towards more cyber-resilient systems, forensic readiness supports the following security, privacy, and trust properties:

- **Integrity:** *Tamper-proof immutable evidence* [12]: no one, including authorities, can change data;

- **Availability:** *Continuous live streaming* [13]: causality of logged events are made available at runtime;
- **Privacy:** *Adaptive minimality* [6]: accuracy in data is adapting to contexts sufficiently and minimal disclosure to the relevant parties [15];
- **Trust:** *Consensus on trust assumptions* [16]: evidence are made acceptable to multiple parties.

For forensic readiness, we have carried out the research to achieve the following objectives:

- We have investigated existing UAS incidents in order to understand their nature, frequency, and consequences, by analysing the reports on how the incidents happened and their reasons [1];
- We have developed an architecture with adaptive capabilities in order to collect relevant UAS incident data at the relevant time [1][5];
- We have evaluated that the data collection of UAS incidents is enables identifying their true causes [1][6].

2.3 Research carried out

We have conducted a number of research activities for the research questions set out within the scope of investigating forensic readiness requirements of UAVs and CNS/ATMs.

***RQ1**. How much data bandwidth is necessary and sufficient to capture, store, and transmit live boxes of UAVs to the cloud / ground station?*

For this we have simulated the transmission of sensory data for drone flights between hospitals in the Transport for London case study has evaluated the reduction ratio of over 46% when adaptive algorithms are used for sufficient forensic investigations to verify the hypothesis and validating the falsifiable forensic evidence [RO1, RO8];

***RQ2**. How many features in the existing research methods are able to cover safety requirements for AUS, which are also applicable to the UAV?*

In a literature mapping study published in [RO4], we have surveyed over 200 publications on the topic of safety requirements of unmanned autonomous systems, including UAVs, which demonstrated the need to have an adaptive reference architecture to such systems;

***RQ3**. How to modify the software behaviours of UAVs when their original functionality cannot satisfy global security requirements? How to simulate the favourable and adversarial environmental conditions and test the failure rates of UAVs with, or without the wrapper?*

We have introduced the concept of “cautious adaptation”, which prioritizes safety requirements as a global requirements of systems of systems over other local requirements of software components [RO3]. As such, we introduce the concept of “wrapers” to adapt the existing components when the satisfaction of their local requirements is in conflict with the global safety requirements. The improvement of failure rates comparing legacy off-the-shelf UAV systems to the adapted ones, and the number of contextual variables are further evaluated in the Dragonfly simulator [RO2];

***RQ4**. How to preserve or retain the integrity of flight data records so that the risk of tampering is minimised? How to design a smart contract that can achieve forensic soundness in terms of integrity and efficiency?*

Using the LiveBox reference architecture [RO1], we designed a system for recording and managing data from drones, pilots and witnesses.

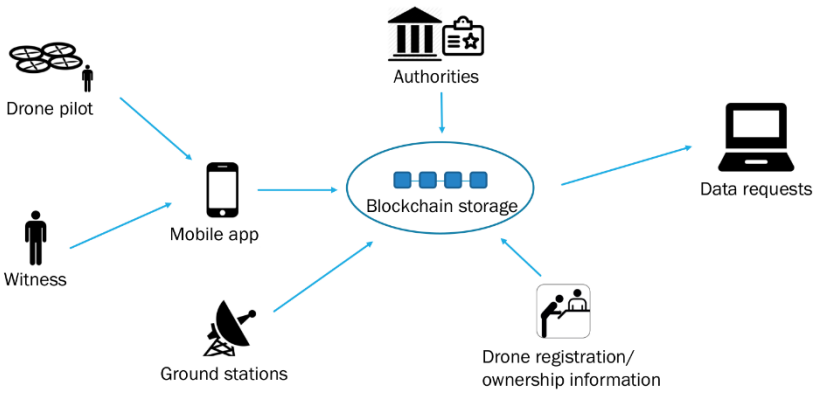

Figure 2. Drone Identity: An implementation of the LiveBox reference architecture [RO1]

We implemented a demonstrator based on this architecture that using smart contracts deployed on the Ethereum blockchain to record flight data records and drone detections made by witnesses (pedestrians and vehicles), [RO5], see Figure 2.

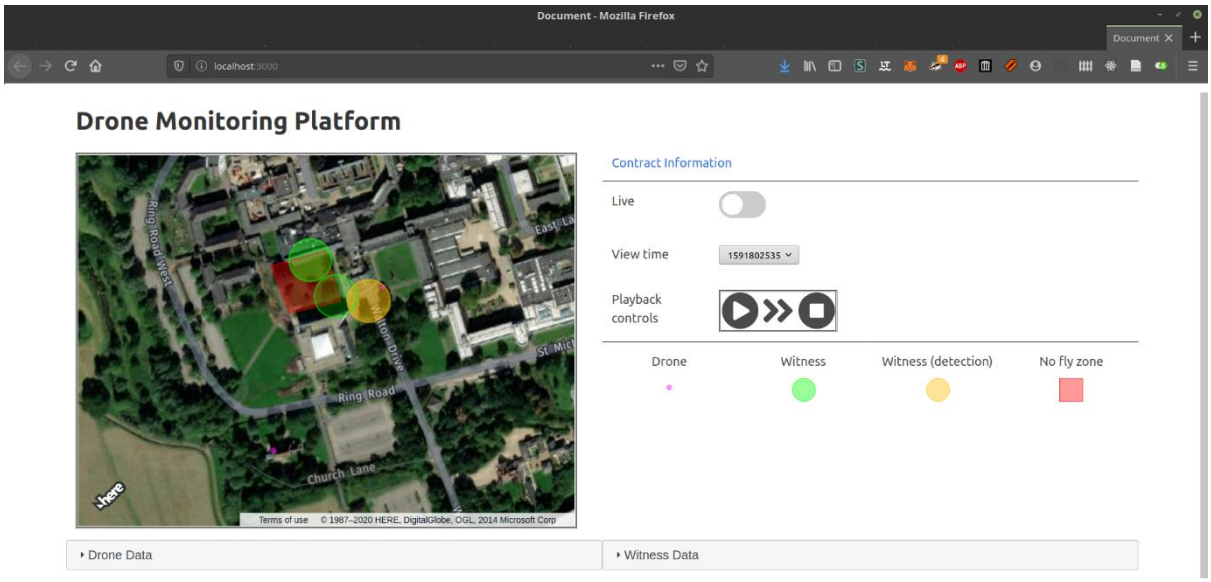

Figure 3. Visualization of our DLT-based implementation: forensically sound evidence have been captured and stored in blockchains efficiently. They can be queried to investigate a scene of forensic incident involving drones, witnesses (vehicles and pedestrians) in relation to no-fly zones [RO4]

The integrity of data stored on distributed ledger technology is guaranteed secure, against injection attacks on the network, by the proof-of-work consensus mechanisms provided by Ethereum protocols. Furthermore, the efficacy of such an implementation is provided through live and retrospective visualisations of the FDRs created in the demonstrator.

RQ5*. How to make real-time trade-offs between various live requirements of drones 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 between safety and privacy, security, timeliness, responsiveness requirements. [RO6-7]

2.4 Results

The contribution of LiveBox requirements, the cautious adaptation design method, and the taxonomy of AUS safety requirements have been shared to our industry partner NATS to design their next general air lifting scenarios, where drones served not only as vehicles for delivering goods, but also people. Therefore, the TRL in terms of safety and forensic integrity has been raised to increase the impact of the project. We have prototypes verified by simulations and scenarios that more closely resemble real-life, such as London Hospitals drone flight corridor in the UK, a urban city in US, a physical experiment in sports stadium in China, taking into account physical factors, etc.

3. Conclusions, next steps and lessons learned

3.1 Conclusions

The Drone Identity project has achieved the main objectives laid out a year ago, that is, to engage NATS to our research at the Open University to investigate on the real-life scenarios for forensic readiness requirements on CNS/ATMS systems. We have also demonstrated that forensic readiness of drone flight records for safety and security can be enhanced by a more resilient Livebox and Cautious Adaptation architectural features. An earlier evaluation through drone simulation and motion planning algorithms demonstrated the concepts could work for DJI drone flights. With NATS, we have met regularly and achieve the consensus that the demonstrators in our project outputs are ready for further investigations on realistic UTM datasets in the next stage.

3.2 Next steps

We have formalised the various forensic readiness safety and security requirements on FDR of UAVs. It is possible to extend this work further to UUVs and other autonomous transport systems in future work, as indicated by [RO6-RO7].

In the forthcoming TC1 Engage KTN event postponed due to COVID-19 uncertainty, we are preparing a talk by summarising the findings in the Drone Identity project based on earlier keynote talk [RO8]

We are going to continue working with NATS to achieve their goal of investigating Safe drone flight - assuring telemetry data integrity in U-Space scenario, which may further increase the TRL by leveraging part of the contribution to data integrity in this project with more realistic ATM datasets from NATS.

3.3 Lessons learned

- Tight industry engagement is what's required for the project to be successful. At the moment, we have mainly engaged with regulators with R&D of NATS. In the future we may consider engaging more with the manufacturers of UAVs and software engineers who are demonstrating the applications of UAVs.

- Identifying a common research goal between partners is key to the success of the project. We have two SESAR projects between NATS (U-services) and OU (this one) so that the reference architecture we proposed (LiveBox) could become a technical feature in NATS' U-services architecture.
- We would have hoped to get most of the technical architectures evaluated on real-world scenarios more. However, due to the COVID19, it affects our opportunity to engage with the partners of NATS. It is an area that we may need to encourage further engagement in the future.

4. References

4.1 Project outputs

[RO1] Yu, Yijun; Barthaud, Danny; Price, Blaine; Bandara, Arosha; Zisman, Andrea and Nuseibeh, Bashar (2019). LiveBox: A Self-Adaptive Forensic-Ready Service for Drones. IEEE Access. Vol. 7, pp. 148401 – 148412.

[RO2] Maia, Paulo; Vieira, Lucas; Chagas, Matheus; Yu, Yijun; Zisman, Andrea and Nuseibeh, Bashar. Cautious Adaptation of Defiant Components. In: The 34th IEEE/ACM International Conference on Automated Software Engineering (ASE 2019) (Lawall, Julia and Marinov, Darko eds.), 11-15 Nov 2019, San Diego, California, USA.

[RO3] Maia, Paulo; Vieira, Lucas; Chagas, Matheus; Yu, Yijun; Zisman, Andrea and Nuseibeh, Bashar (2019). Dragonfly: a Tool for Simulating Self-Adaptive Drone Behaviours. In: SEAMS '19 Proceedings of the 14th International Symposium on Software Engineering for Adaptive and Self-Managing Systems, IEEE pp. 107–113. file

[RO4] Luo, Yixing; Yu, Yijun; Jin, Zhi and Zhao, Haiyan (2019). Environment-Centric Safety Requirements forAutonomous Unmanned Systems. In: 27th IEEE International Requirements Engineering Conference (RE'19), 23-27 Sep 2019, Jeju, Korea, IEEE.

[RO5] Danny Barthaud, Yijun Yu (2020). A forensically sound demonstrator of LiveBox architecture for integrity of flight data records. To submit.

[RO6] Luo, Yixing; Yu, Yijun; Jin, Zhi; Li, Yao; Ding, Zuohua; Zhou, Yuan and Liu, Yang (2020). Privacy-Aware UAV Flights through Self-Configuring Motion Planning. In: International Conference on Robotics and Automation, 31 May - 4 Jun 2020, Paris, France.

[RO7] Luo, Yixing; Yuan Zhou; Tianwei Zhang; Liu, Yang; Zhao, Haiyan; Jin, Zhi; Danny Barthaud; and Yu, Yijun; Requirements driven Online Adaptation to Mitigate Runtime Uncertainty for Autonomous Unmanned Systems, submitted to IEEE Trans. On Software Engineering. (2020).

[RO8] Yu, Y. "The Drone Identity — Investigating Forensic-Readiness Requirements of Unmanned Aerial Vehicles", presented at the 3rd Canterbury Cyber Conference as a keynote, Jan 2020, Canterbury Christ Church University, UK.

4.2 Other

[1] PwC. “UK Drones Report”, PwC, Press Releases, May 29 2018.

[2] C. Stöcker et al., “Review of the Current State of UAV Regulations,” Remote Sens., vol. 9, no. 5, p. 459, May 2017.

[3] R. Clarke and L. Bennett Moses, “The regulation of civilian drones’ impacts on public safety,” Comput. Law Secur. Rev., vol. 30, no. 3, pp. 263–285, Jun. 2014.

[4] UK Airprox Board. https://www.airproxboard.org.uk/Reports-and-analysis/Statistics/Statistics.

[5] R. Rowlingson, “A Ten Step Process for Forensic Readiness,” Int'l J. Digital Evidence, vol. 2, no. 3, 2004, pp. 1–28.

[6] D. Alrajeh, L. Pasquale, and **B. Nuseibeh**, “On evidence preservation requirements for forensic-ready systems,” in Proceedings of the 11th Joint Meeting on Foundations of Software Engineering, Germany, 2017, pp. 559–569.

[7] Nurul Rahman, William Glisson, Yanjiang Yang, and Kim-Kwang Choo. “Forensic-by-Design Framework for Cyber-Physical Cloud Systems”, IEEE Cloud Computing 3(1):50-59, 2016.

[8] J. Cleland-Huang, M. Vierhauser, and S. Bayley, “Dronology: an incubator for cyber-physical systems research,” in ICSE (NIER) 2018, Gothenburg, Sweden, 2018, pp. 109–112.

[9] B. Nwachukwu, Securing and Networking Aircraft Live Flight Data for Real-Time Global Access. PhD. Thesis. 2017.

[10] R. Clarke, “The regulation of civilian drones’ impacts on behavioural privacy,” Comput. Law Secur. Rev., 30(3):286–305, Jun. 2014.

[11] **B. Nuseibeh**, C. B. Haley, and **C. Foster**, “Securing the Skies: In Requirements We Trust,” IEEE Comput., 42(9):64–72, 2009.

[12] G. Grispos, J. Garcia-Galan, L. Pasquale, and **B. Nuseibeh**, “Are You Ready? Towards the Engineering of Forensic-Ready Systems,” ArXiv170503250 Cs, May 2017.

[13] **Y. Yu**, M. Yang, and **B. Nuseibeh**, “Live Blackboxes: Requirements for Tracking and Verifying Aircraft in Motion,” in SCiA 2017 : 4th Software Challenges in Aerospace Symposium, 2017.

[14] P. Sommer, “Digital Footprints: Assessing Computer Evidence,” p. 19.

[15] M. Strohmeier, I. Martinovic, and V. Lenders, “A k-NN-Based Localization Approach for Crowdsourced Air Traffic Communication Networks,” IEEE Trans Aerosp. Electron. Syst., vol. 54, no. 3, pp. 1519–1529, 2018.

[16] **Yijun Yu**, Virginia N.L. Franqueira, Thein Than Tun, Roel J.Wieringa, and **Bashar Nuseibeh**. “Automated analysis of security requirements through risk-based argumentation”, Journal of Systems and Software, 106:102-116, 2015.

[17] Tony Kern. Redefining airmanship. McGraw-Hill (New York, USA), 1996.

[18] Kim, Alan, et al. "Cyber attack vulnerabilities analysis for UAVs", Infotech@Aerospace 2012. pp.24-38.

[19] DJI. Introduces new geofencing system for its drones. News, May 2015.

[20] Dutta, Raj Gautam, et al. "Estimation of safe sensor measurements of autonomous system under attack." Proceedings of the 54th Annual Design Automation Conference 2017. ACM, 2017.

[21] He, Daojing, et al. "Flight Security and Safety of Drones in Airborne Fog Computing Systems." IEEE Communications Magazine 56.5 (2018): 66-71.

[22] Han, Song, et al. "Intrusion detection in cyber-physical systems: Techniques and challenges." IEEE Systems Journal, 8(4) (2014): 1052-1062.

[23] Haque, Md Samsul, and Morshed U. Chowdhury. "A New Cyber Security Framework Towards Secure Data Communication for Unmanned Aerial Vehicle (UAV)." SecureComm 2017, Canada, October 22–25, 2017.

[24] Dursun, Mahir, and İsmet Çuhadar. "Risk based multi criteria decision making for secure image transfer between unmanned air vehicle and ground control station." Reliability Engineering & System Safety 178 (2018): 31-39.

[25] Lin, Chao, et al. "Security and Privacy for the Internet of Drones: Challenges and Solutions." IEEE Communications Magazine 56.1 (2018): 64-69.

[26] Webster, Matt, et al. "Formal methods for the certification of autonomous unmanned aircraft systems." International Conference on Computer Safety, Reliability, and Security. Springer, Berlin, Heidelberg, 2011.

[27] Oztekin, Ahmet, Cynthia Flass, and Xiaogong Lee. "Development of a framework to determine a mandatory safety baseline for unmanned aircraft systems." Journal of Intelligent & Robotic Systems 65.1-4 (2012): 3-26.

[28] Gonçalves, P., José Sobral, and L. A. Ferreira. "Unmanned aerial vehicle safety assessment modelling through Petri Nets." Reliability Engineering & System Safety 167 (2017): 383-393.

[29] Douglas Heaven. “Bitcoin for the biological literature”, Nature, Feb 2019, 566(7742):141-142.

[30] James Lockerbie, Neil Arthur McDougall Maiden, Jorgen Engmann, Debbie Randall, Sean Jones, **David Bush**: “Exploring the impact of software requirements on system-wide goals: a method using satisfaction arguments and i* goal modelling”. Requir. Eng. 17(3): 227-254 (2012)

[31] **David Bush.** “Modelling Support for Early Identification of Safety Requirements : A Preliminary Investigation”**,** In: 4th International Workshop on Requirements for High Assurance Systems (RHAS'05), Requirements Engineering, Paris, 2005.