OPEN TOOLS FOR TRUSTED FLIGHT AND UTM RESILIENCE

Hrishikesh Ballal,[*] Govind Singh,[†] and Rhythm Chopra[‡]

This paper covers two crucial aspects of digital security in the context of drone flights and advanced (e.g. Beyond Visual Line of Sight (BVLOS)) operations. Trusted Flight is a set of software services that provide a security layer to operators and manufacturers to conduct flight operations using the mature and well-tested Public Key Infrastructure and commonly available identity and authentication standards. We will cover the concept of "trusted flights" and its open implementation in Ardupilot and PX4, two popular open-source flight controllers, and the Aerobridge Management server to help with the automation of the security workflow.

In the second part of the paper, we focus on Unmanned Traffic Management (UTM) and the activities within the Global UTM Association (GUTMA) and Dronecode Foundation. Specifically, we introduce the UTM Adapter working group and the contributions to ensure that UTM services are cyber safe from the get-go. Additionally, some of the authors led a taskforce within GUTMA on UTM cybersecurity and resilience to provide an industry perspective for security and open implementations for UTM services. The GUTMA task force aimed to address the cybersecurity aspect within the context of certification / validation of UTM systems. The task force provided a cyber security risk assessment template framework as a starting point for UTM service provider certification efforts in the European Union.

INTRODUCTION

Security in the context of drone flights requires a holistic approach covering cyber-physical systems. We will build a holistic perspective on cybersecurity and the related activities in the context of flight operations and Unmanned Traffic Management (UTM) to enable secure operations and cyber security from the get-go. The common theme between these concepts is the open implementations developed to enable them. Trusted Flights enable drone operators to provide a security layer via digital flight permissions (e.g. one time permission (OTP)) and flight log signing and management within the organization for post-flight audit and security. The trusted flight system allows operators to generate a permission object as a JSON web signature that is downloaded from its digital infrastructure and must be transferred to the drone and the flight controller in order to conduct the mission. The Flight controller is designed so that it can only arm the drone once the

[*] Founder / Project Maintainer, OpenUTM + Aerobridge Server, Openskies Aerial Technology, Dublin, Ireland
[†] Principal Engineer, Secure Systems Research Center, Technology and Innovation Institute, Abu Dhabi, United Arab Emirates
[‡] Software Engineer, Independent Contributor, Prague, Czech Republic

https://doi.org/10.52202/075106-0005

validity of the token has been verified. In addition, features like public key rotation and flight log signing by the flight controller ensure post-flight checks and verification assurances. We cover the technical mechanism and the benefits of trusted flight management to add security in drone operations in this paper.

On the UTM side, we will cover the activities within the Global UTM Association (GUTMA). From December 2023 till March 2024 GUTMA members co-led by Openskies Aerial Technology and Technology Innovation Institute (TII) (authors of this paper) around cyber-proofing UTM services. Some members of GUTMA are undergoing or considering EU Certification and this task force was aimed at helping the membership build understanding and knowledge base so that the UTM services are cyber-proof from the get-go. We will cover the content of the Technical White Paper that not only delves into the findings, insights, and recommendations derived from the analysis within the task force. This white paper also provides a template to build a threat-based risk assessment and mitigation measures of the identified security challenges in UTM operations. This white paper will serve as a crucial reference for industry stakeholders seeking to enhance the security posture of UTM systems and help with UTM validation / certification efforts. Finally, we share the open-source implementation of the security concepts and verification tools for UTM providers to validate their systems.

Together this builds a comprehensive and holistic framework for flight security and provide opensource tools for verification and deployment within a operators internal environment.

TRUSTED FLIGHT

In the context of this work, trust in drone flight operations focuses on the provision of digital infrastructure and workflows to ensure that only authorized (by an organization) flight plans, vehicles, personnel, and software can conduct a mission. These workflows cryptographically ensure that only the approved flight plan can be executed. The stack ensures that the arming of the vehicle will be disallowed if the cryptographic and other checks fail by building the mechanism in the flight controller itself. This means that UAV hardware manufacturers or operators control what software can and cannot run by refusing to run unsigned / untrusted flight plans. Hardware and software are not only secured for its owner but also secured against its owner. Specifically, this stack covers four specific aspects of drone flight operations:

1. Who is flying the drone? If there is an identity and authentication layer available for the operator across, only personnel and GCS authorized by the company can be allowed to fly.
2. Where is the drone hardware and software made? Who built the hardware and flight controller software / firmware for the aircraft and how to make sure that it is associated with the identity of the company operating the aircraft. This means that the operators can get a remote “kill switch” to prevent any personnel or vehicle from arming the drone.
3. How was the flight plan approved? Is there a mechanism to associate the flight plan with a “permission to fly” for the aircraft, operator, and the vehicle. In other words, without a digital permission linked to the flight plan and the vehicle no flying / arming is allowed.
4. Did the drone fly the approved flight plan? Once the flight plan is validated and executed, the specified drone fly only the specified flight plan.

Together these systems form a holistic trusted flight mechanism where confidence and assurances can be made to ensure security of the drone system. There are other important / major considerations for drone flight security e.g. C2 link encryption and others, but we cover those aspects in another paper. For this work, we will cover the four aspects listed above with a specific focus on

https://doi.org/10.52202/075106-0005

open tools being developed in Ardupilot and PX4, two of the most popular open-source flight controllers for UAVs and other open source projects developed by the authors.

Trusted Flight Components

Figure 1 below shows the main components of this trusted flight system. They operate together, and are linked, however they are not dependent on each. The authors have developed open-source implementations for these concepts; however, these can be swapped as necessary with own proprietary software if they adhere to the openly published API specifications.

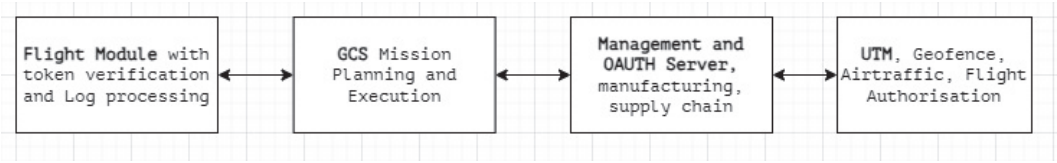

Figure 1. Trusted Flight Components

- *Flight Permission Token:* This is the central component of the trusted flight system; this is a token represented as a JSON Web Token (JWT) issued by the management server once the mission is approved and is transferred to the vehicle. This token has information about the flight plan, the pilot etc. and serves as cryptographic time limited proof of permission to fly / perform the operation.
- *Flight Module:* This is a specialized version / build of a flight controller / auto pilot software that is linked to the company's domain. This flight controller contains the public key of the company's domain and the root certificate. This ensures that only tokens signed by the company's domain are processed and approved. This flight controller uses publicly available Public Key Infrastructure to validate and verify the tokens and subsequently allow arming and other pre-flight checks. This is the most critical cyber-physical system that digitally links the vehicle to the company and its digital infrastructure.
- *Ground Control Station:* The Ground Control Station is a communications mechanism that mainly deals with moving the permission token issued by the management server to the vehicle. We have implementations in QGCS that mainly use Mavlink to send the token to pre-defined locations in the flight controller. In some cases, it will interact with the UTM system to offer UTM services e.g. air-traffic information etc.
- *Management Server:* A optional but a crucial component of automating / performing operations at scale. This component helps in managing the permission artifacts and interactions with the GCS and storing records and keys. While all of this can be done manually, having a management server or extending the fleet management server to accommodate this security layer will ensure at-scale operations.
- *UTM:* For advanced operations, a UTM system must be able to exchange the flight plans and operational intents with peer UTM providers and perform UTM services like strategic deconfliction or remote ID tracking etc.

Trusted Flight Data and Workflow

To understand how the system works together, we consider a simple case of an operator building a flight plan on QGCS and then submitting the plan to the drone to fly. Without the Trusted flight system, this can simply be achieved with the following steps:

1. Connect the drone to the GCS
2. Use the Ground Control system interface to build a flight plan
3. Send the plan to the vehicle
4. Arm the drone and conduct the mission

This workflow has many security-related issues that are introduced at the beginning of the paper. Crucially, the presented above workflow assumes that there is a trust in the pilot and the pilot flies the mission that he is supposed to fly. The trusted flight system provides a security layer for the operators to ensure that only the approved vehicles and flight plans are processed, and appropriate digital logging is provided.

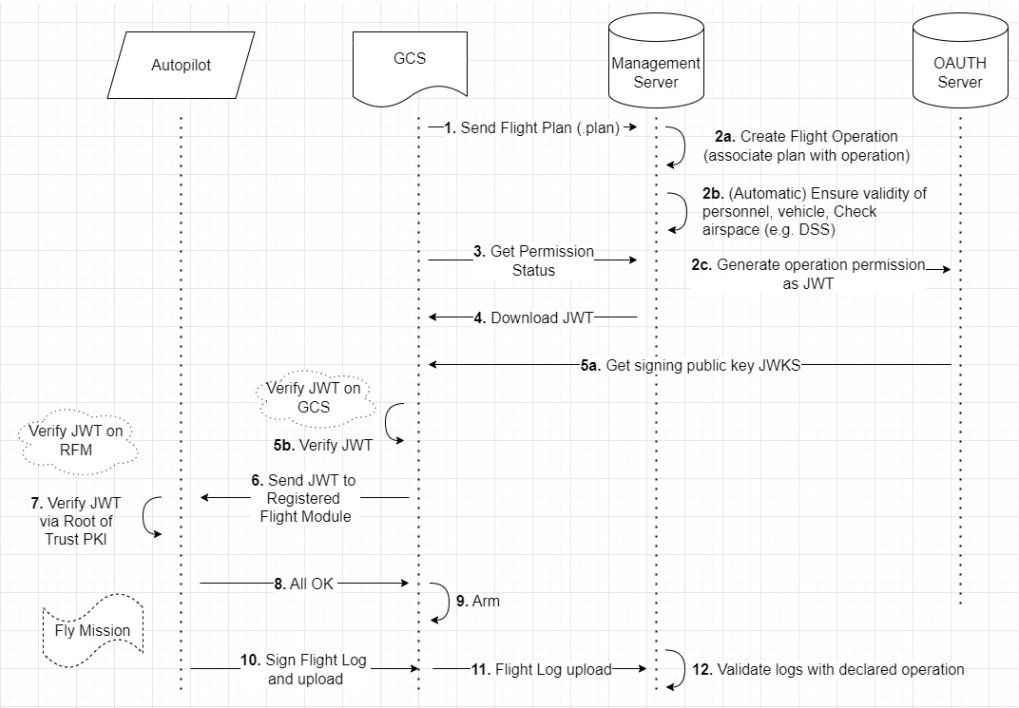

Figure 2. Trusted Flight workflow

To understand how this workflow will work in the context of trusted flights, we use the workflow depicted in Figure 2. A step-by-step depiction of the process is below, these steps will be largely automated in a digital context and assumes integration with the GCS, Management server and the UTM system:

- *Step 0:* Custom firmware is flashed on the vehicle that includes the root certificate and issuer name embedded in the firmware and stored / loaded from read-only memory.
- *Step 1:* The operator builds a flight plan (or loads a flight plan that is already stored in the management server).
- *Step 2a:* The management sever processes the flight plan and creates an operation i.e. associates this plan with a vehicle and person in the organization.
- *Step 2b:* The management server performs additional checks e.g. interaction with the UTM system etc. to ensure de-confliction.

https://doi.org/10.52202/075106-0005

- *Step 2c:* Once the initial checks are complete, the Management server contacts the OAUTH server of the organization to generate a permission artifact as a JWT, see the permission token details for the claims and sample token.
- *Step 3 and 4, 5:* The GCS then downloads the permission token and verifies the artifact.
- *Step 6:* Once the permission token is validated, the token is sent to the vehicle and the mission is also sent to the vehicle.
- *Step 7:* The flight controller verifies the token is valid and checks against the public key in ROMFS and the claims to ensure that the permission is granted for the vehicle, also if a plan file hash is provided, the firmware hashes the loaded file and cross checks against the provided has in the token.
- *Step 8:* The GCS sends the commands to arm if the Step 7 is executed properly
- *Step 10:* Once the flight is completed the flight controller signs the flight log and sends it to the management server, the management server verifies the signature since it has the public key of the flight controller.

This "full cycle" flow ensures that the objectives of the security system are met, and a digital proof and verification system is in place to ensure security audits.

Trusted Flight Permission Token

The permission token is expressed as a JWT and has the following claims, Figure 3 shows a decoded permission token issued by the management server. Using JWT ensures that we utilize existing tools and libraries to validate and parse the data. In addition to the standard claims provided by JWT, we can also add additional claims that can be verified by the flight controller.


```
{
  "iss": "https://id.openskies.sh/",
  "exp": 1640024322,
  "iat": 1640020722,
  "sub":
"g37lXifAQoBfVuQZxT3VJFjXIMgdfXIOpa2LdWBQ@clients",
  "scope": "",
  "typ": "Bearer",
  "flight_plan_id": "12818e87-4c96-4e4c-8c63-
82b8e12c3b73",
  "flight_operation_id": "3408bce9-dbab-4665-abfc-
8ea03b0ad871",
  "plan_file_hash":
"a2a201efa111dde5aaa8f42b7b46d17b595e39d850500dbacd9f79a
ef0bbf68e"
}
```


Figure 3. Flight Permission token claims

We first ensure that the token is decoded and validated correctly and then additionally perform the following computation:

- Utilize the *plan_file_hash* to compute the hash of the flight plan loaded on the flight controller to ensure that the same plan is loaded on the vehicle.
- The *flight_plan_id* and *flight_operation_id* establishes the link between the token and the plane and operation on the management server for auditing.

- The *sub* claim can be used to establish the link between the vehicle / RFM to the flight plan.

Flight Controller Modifications

The core of the trusted flight system consists of modifications to the autopilot to enable additional checks in the pre-arming system.

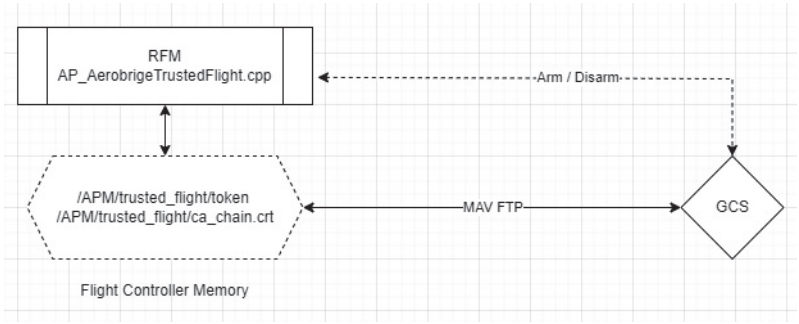

Figure 4. Flight Controller Architecture (Ardupilot implementation)

In the context of Ardupilot, we implemented a new module (AP_AerobridgeTrustedFlight) for handling all the operations and validations related to Trusted Flight. It is wired into the existing pre-arm checks to ensure these validations are performed before arming and cannot be by-passed even with forced arming, given the Trusted Flights feature was enabled during the ardupilot build for RFM. AP_AerobridgeTrustedFlight module expects the certificate chain and JWT token to be available on the filesystem path (/APM/trusted_flight/) as depicted in the Figure 4, failing which the pre-arm checks for the RFM will fail during arming preventing any unauthorized operation to execute.

OPEN IMPLEMENTATION OF TRUSTED FLIGHT

This section provides details about the opensource tools available to enable at-scale automation of the trusted flight system. These contributions are made by the authors to the community as pull requests to opensource projects. And in some cases, this additional security layer provided by these tools will ensure reliable and safe operation of drones in the airspace powered by mature, publicly available cryptography tools and systems. These tools provide an easy on ramp for operators and manufacturers to ensure an elevated level of operational security and data assurance.

https://doi.org/10.52202/075106-0005

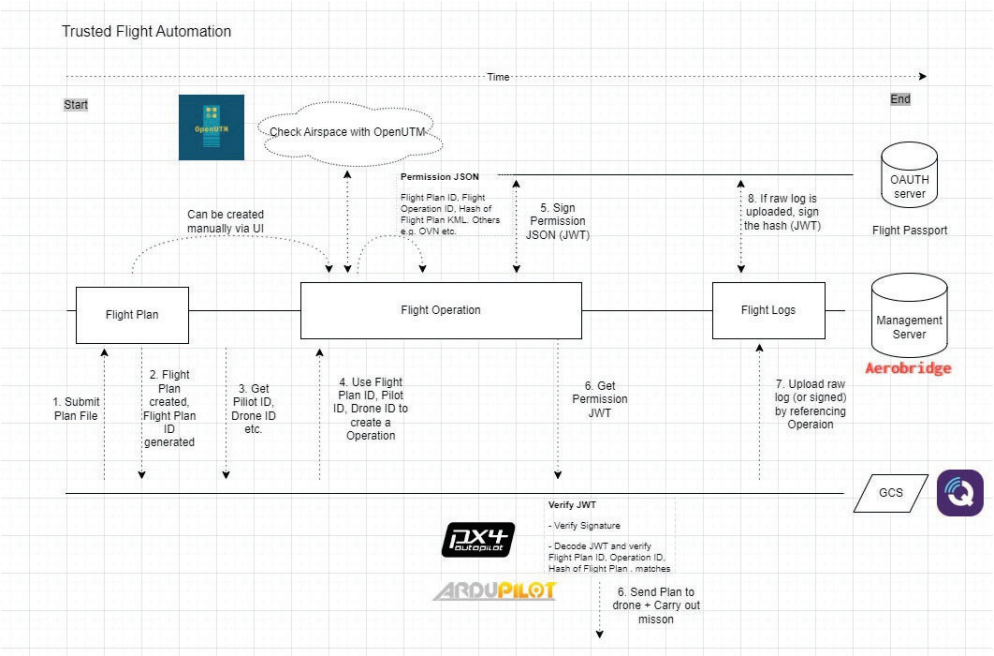

Figure 5. Trusted Flight Components implemented with Management Server and Auto-pilots

The authors have built open-source implementations for this in various projects. The PX4 and Ardupilot software repositories have existing pull requests with the trusted flight module. The Management server is implemented as Aerobridge[*] management server and can help an organization manage its flight permissions process and issuance of JWT tokens. There are additional features in the Aerobridge management server that ensure the trackability of the components, the provision of signed firmware etc. The QGCS is an opensource ground control station that has integrations and support for the UTM and the management server. Finally, the UTM system is implemented in OpenUTM[†] to ensure a standard compliant UTM system that utilizes the latest standards e.g. the ASTM standard for strategic de-confliction.

CYBER SECURE UTM

In the rapidly evolving landscape of aviation, the need for robust cybersecurity measures within Unmanned Traffic Management (UTM) systems has never been more critical. As drones become increasingly integrated into airspace operations for various applications, from delivery services to surveillance and beyond, ensuring the integrity, confidentiality, and availability of UTM services is paramount.

At the heart of this necessity lies the imperative to protect against a myriad of cyber threats that could compromise the safety, efficiency, and reliability of unmanned aerial vehicles (UAVs) and

[*] Aerobridge Management Server, available at: https://www.github.com/openskies-sh/aerobridge

[†] OpenUTM, available at: https://github.com/openutm

https://doi.org/10.52202/075106-0005

the airspace they navigate. From malicious intrusions seeking to disrupt operations to unauthorized access attempts aimed at stealing sensitive data, the potential risks are diverse and ever-present.

To address these challenges, regulatory bodies such as the Federal Aviation Administration (FAA) and the European Union Aviation Safety Agency (EASA) have issued comprehensive recommendations, outlining stringent security requirements for UTM systems[*†]. These guidelines emphasize the importance of implementing robust security controls across all facets of UTM infrastructure, including USSP (U-space Service Provider), CISP (Communication and Information Service Provider), and operator systems. FAA's Near-Term Approval Process (NTAP) and the UTM Pilot Program, along with the EU Regulation 2021/664 on U-Space and accompanying AMC/GM, recommend information security using some generic standards like ISO27001.

All regulatory requirements and recommendations necessitate a comprehensive framework from industry bodies responsible for implementing and deploying UTM services. Recognizing this gap, the authors, co-led a task force[‡] within GUTMA, a UTM industry association, on Secure and Resilient UTM. This task force aimed to explore the implications for UTM service providers regarding security considerations for UTM services deployment. Because of the task force's findings, there emerged a need to create comprehensive, updated tools capable of verifying compliance against a specific class of ever-evolving cybersecurity threats.

UTM Adapter Project

The UTM adapter[§] project seeks to mitigate the fragmentation observed between operators and UTM Service Providers (UTMSPs) in the UAS Traffic Management (UTM) ecosystem. Operators often utilize diverse Ground Control Stations (GCS) and operational procedures to communicate data to the UTM systems. This leads to inconsistencies and interoperability challenges when interfacing with UTMSPs. The UTM adapter project serves as a middleware solution that can be plugged into any GCS, bridging the gap between these heterogeneous operator systems and the standardized interfaces expected by UTMSPs. This project provides a standardized interface for operators to connect with UTMSPs, the adapter eliminates fragmentation and streamlines data exchange, ensuring seamless integration into the broader UTM network. Ultimately, the UTM adapter enhances operational efficiency, promotes interoperability, and facilitates the adoption of UTM services across diverse operator platforms.

Additionally, As depicted in Figure 6, this approach enables harmonized security measures across the UTM ecosystem. By standardizing the interface between operators and UTM Service Providers (UTMSPs) through the UTM adapter, security protocols and mechanisms can be uniformly enforced and monitored. This harmonization ensures consistent implementation of cybersecurity measures, such as authentication, encryption, and access control, across all interactions within the UTM network. As a result, the UTM adapter not only addresses interoperability

[*] https://www.faa.gov/uas/advanced_operations/traffic_management
[†]https://www.easa.europa.eu/en/document-library/acceptable-means-of-compliance-and-guidance-materials/amc-and-gm-implementing
[‡] GUTMA secure-and-resilient-utm Taskforce, available at: https://www.unmannedairspace.info/latest-news-and-information/gutma-launches-members-task-force-on-secure-and-resilient-utm/

[§] Dronecode UTM Adapter, available at: https://github.com/Dronecode/utm-adapter.

https://doi.org/10.52202/075106-0005

challenges but also strengthens the overall security posture of UTM operations, promoting trust, resilience, and confidence in the system.

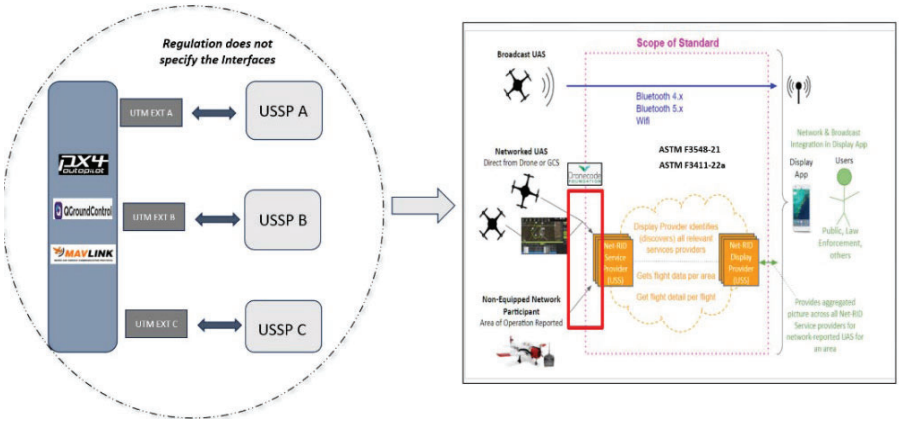

Figure 6. UTM Adapter Conceptual Diagram

UTM Service cyber-security verifier

A new project was created* to address the need for a suite of tools for UTM service providers to verify their compliance against the latest cyber security threats. The goal of the UTM cyber-security verifier project is to provide a toolset that can be run against the UTM services to monitor conformance and response to security threats. This initiative aims to address cybersecurity concerns of regulators associated with certification and validation of UTM systems by establishing a robust security framework grounded in industry standards and developed by a community. The findings and tools developed through this initiative will be published for wider dissemination within the industry.

This projects ultimately aims to bolster UTM security using Confidentiality, Availability, and Integrity cybersecurity principles as shown in Figure 7, they aim to enhance the resilience of UTM services against potential cyber threats and ensure their continued reliability and safety. These tools provided by this project play a vital role in assessing, validating, and continuously monitoring the cybersecurity posture of UTM systems, enabling stakeholders to detect and mitigate vulnerabilities effectively. By aligning with EASA recommendations and leveraging advanced cybersecurity solutions, the aviation industry can confidently navigate the complexities of UTM security, ensuring the seamless and secure integration of drones into our skies.

* UTM Cyber security verifier, available at: https://github.com/tiiuae/UTM-Security-Verifier

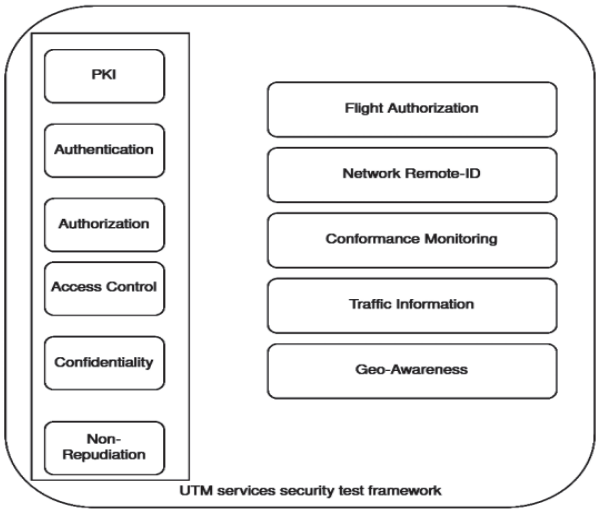

Figure 7. UTM Cybersecurity Attributes.

The UTM cyber security verifier project aims to verify the security features within individual UTM (UAS Traffic Management) services, aiming for a comprehensive assessment of cybersecurity measures across the UTM ecosystem. This initiative focuses on evaluating the effectiveness and resilience of these measures, with the goal of enhancing the overall security posture of UTM systems. The deliverables of this project include a test framework, tailored for examining the functional specifications of UTM adapters to ensure compliance with adapter specifications. Additionally, a security test framework for UTM services is developed, encompassing the creation of test cases as depicted in Figure 8, to validate each security feature against specified requirements and the documentation of verification results, including audit logs. These deliverables are designed to be applicable to any Ground Control Station (GCS) and UTM provider, facilitating the implementation of robust security measures across the UTM landscape.

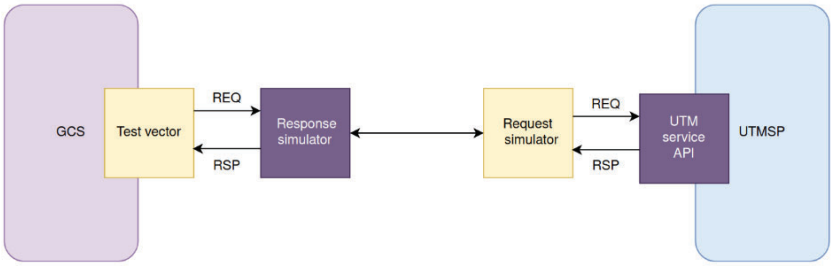

Figure 8. UTM Security Verification Framework

CONCLUSION

In this paper we introduced the concept of trusted flight and shared a series of open tools that are available for the community to ensure safe and secure integration of drones in the airspace.

https://doi.org/10.52202/075106-0005

ACKNOWLEDGMENTS

The authors acknowledge the contributions of the Ardupilot, PX4, OpenUTM, Aerobridge and UTM Adapter community in developing and refining these concepts. In addition, India's No Permission No Takeoff policy inspired early thinking around development of mission security and the operations management server.