Report on fallback communication system

Deliverable 2.4

Work package: **WP2**
Dissemination level: **SEN**
Lead partner: INESC
Authors: **Hugo Miguel Silva, Helder Fontes (INESCTEC)**
Due date: **28** / 02 / 2025
Submission date: **25**/ **03** / **2025**

The OVERWATCH project has received funding from the Horizon Europe call "HORIZON-EUSPA-2021", topic HORIZON-EUSPA-2021-SPACE-02-52, under agreement No. 101082320

Deliverable	Report on fallback communication system
Deliverable No.	D2.4
Work Package	2
Dissemination Level	SEN
Nature[1]	R
Author(s)	Hugo Miguel Silva (INESCTEC), Helder Fontes (INESCTEC)
Co-Author(s)	André Dias, João Jacob, André Moura, João Moura, Rúben Queirós, Guilherme Moreira (INESCTEC)
Date	08/02/2025
Status	Draft
Revision	13/02/2025
Reviewed by (if applicable)	Edoardo Arnaudo (LINKS)
Information to be used for citations of this report	Silva H. and Fontes H. (2025): Fallback Communication System, D2.4, OVERWATCH. Horizon Euspa Space 2021 Grant Agreement No 101082320,

Deliverable abstract	The OVERWATCH Fallback Communication System (FCS) is a robust solution designed to ensure reliable and continuous communication during disaster scenarios where conventional infrastructure is compromised. Utilizing a tethered drone-based system, the FCS provides an autonomous, resilient, and rapidly deployable network, critical for maintaining operational connectivity and situational awareness. The system integrates a high-endurance UAV platform, modular communications payload, and redundant power supply to support real-time data relay. The FCS operates through advanced software for flight control and seamless integration with OVERWATCH's systems, ensuring minimal latency and adaptive data transmission. Thorough testing has demonstrated the system's reliability under challenging conditions, reinforcing its capability to support mission-critical operations. The system's future development will focus on increasing autonomy, expanding communication range and available bandwidth, and enhancing performance through AI-driven analytics.

[1] Nature of the deliverable: **R** = Report, **P** = Prototype, **D** = Demonstrator, **O** = Other

Keywords	Tethered drone, satellite backhaul, communications, disaster areas.

Table of Content

Figures

Tables

Document revision history

Version	Date	Modification reason	Modified by
1	10/02/2025	First draft	Hugo Silva (INESTEC)
2	13/02/2025	Internal Review	Edoardo Arnaudo (LINKS)
3	28/02/2025	Deliverable complete	Hugo Silva (INESCTEC)
4	07/05/2025	Review with integrations	Helder Fontes (INESCTEC)

List of authors, contributors and reviewers

No.	Name	Role	Organization
1	Hugo Silva	Author	INESCTEC
2	Helder Fontes	Author	INESCTEC
3	André Dias	Author	INESCTEC
4	João Jacob	Author	INESCTEC
5	Andre Moura	Author	INESCTEC
6	João Moura	Author	INESCTEC
7	Rúben Queirós	Author	INESCTEC
8	Guilherme Moreira	Author	INESCTEC

Abbreviations

CH Chapter
C2 Command & Control
D Deliverable
FCS Fallback Communication System
FRD Forward-Right-Down
IMU Inertial Measurement Unit
ISP Internet Service Provider
LEO Low Earth Orbit
LTS Long Term Support
NED North-East-Down
OGC Open Geospatial Consortium

ROS	Robotic Operating System
RTT	Round Trip Time
TCP	Transmission Control Protocol
TRL	Technological Readiness Level
UDP	User Datagram Protocol
WP	Work Package

Executive Summary

In disaster scenarios where conventional communication infrastructure is compromised, maintaining reliable connectivity is critical for maritime security operations. The OVERWATCH Fallback Communication System (FCS) is designed to provide an autonomous, resilient, and rapidly deployable communication solution to ensure uninterrupted data flow between OVERWATCH operational assets and command centers. By leveraging a tethered drone-based system, the FCS offers a robust contingency plan to enhance situational awareness and operational coordination in disaster environments. Where maintaining communications is critical for performing successful mapping operations.

The primary objective of the OVERWATCH FCS is to establish a rapid, reliable, and self-sustaining communication network in the event of primary system failure and allow other OVERWATCH sub-systems to operate even with primary systems communication blackout.

The FCS is centered around two primary components:

1. **Tethered Drone System**: A high-endurance, tethered aerial platform providing persistent aerial connectivity.
2. **Communications Module**: A modular system integrated within the drone to facilitate real-time data relay and ensure network stability.

The FCS hardware architecture is designed to provide seamless and resilient operation under challenging conditions. Key hardware elements include:

- **Tethered UAV Platform**: Provides continuous flight capability, powered through a ground-based tethering system.
- **Power and Data Tether**: Supplies constant power and ensures low-latency, high-bandwidth data transmission.
- **Communication Payload**: Houses multiple connectivity solutions, including LTE, SATCOM, and mesh networking.
- **Ground Control Station (GCS)**: Manages drone flight operations and network configurations.
- **Redundant Power Supply**: Ensures system stability in case of primary power source failure.
- **STARLINK Connectivity**: Ensures internet connection through satellite link.

The software architecture of the FCS is designed for real-time performance, security, and adaptability. It includes:

- **Autonomous Flight Control System and Tethered drone User interface**: Manages take-off, hovering, altitude adjustments, and landing operations.
- **Interoperability Layer**: Ensures seamless integration with OVERWATCH's systems, namely the integration of ROS with the project-level message bus, RabbitMQ, to send/receive messages between the FCS and OVERWATCH C2.

To ensure secure and effective operations, the FCS tethered drone system follows strict operational protocols:

- **Pre-Deployment Checklist**: Verifies hardware integrity and network readiness.
- **Automated Flight Path Management**: Adjusts altitude and positioning based on environmental conditions and operational needs.
- **Failsafe Procedures**: Automatic descent in case of system failure or adverse weather conditions.

- **Data Transmission Optimization**: Ensures minimal latency and adaptive routing based on real-time network analysis.

The FCS tethered drone system has undergone rigorous flight testing to validate its performance and reliability in disaster applications. Key flight tests include:

- **Stability and Endurance Trials**: Evaluating continuous flight duration and resistance to winds and weather.
- **Communication Performance Testing**: Assessing data transmission quality across various connectivity scenarios.
- **Integration with OVERWATCH Systems**: Transmit flight data from the FCS to OVERWATCH C2 through the internet.

The OVERWATCH Fallback Communication System (FCS) is a critical component in ensuring resilient communication for disaster scenarios. By integrating a tethered drone-based system with advanced hardware and software architecture, the FCS enhances operational resilience, maintains real-time situational awareness, and ensures uninterrupted connectivity in disaster scenarios. Future advancements will focus on increasing system autonomy, expanding communication range, and further integrating AI-driven analytics to optimize performance.

The selection of Starlink as the satellite backhaul provider is justified by its superior uplink and downlink throughput, low latency, and widespread availability, as confirmed by the Portuguese National Authority for Communications (ANACOM) and by the long-term performance evaluations (see Section 2.3). Starlink was the only satellite-based ISP offering uplink speeds above 25 Mbit/s with stable RTTs around 28 ms, meeting the demanding data transmission requirements of OVERWATCH's C2 integration and enabling real-time situational awareness. Additionally, Starlink's mobility support allows the FCS to operate in varied field locations without requiring fixed infrastructure or installation addresses.

1. Introduction

1.1. Goals and Links with the Project Objectives

Disaster response scenarios often present significant challenges in maintaining effective communication networks, especially when terrestrial infrastructure is damaged or unavailable. Tethered unmanned aerial systems (UAS) equipped with satellite backhaul capabilities provide an innovative solution for bridging connectivity gaps. These systems can act as persistent communication hubs, facilitating high-speed data transmission and reliable network access for drone operators and first responder teams in disaster environments. The tethered design (power cable plus fiber optical link) on these drones ensures uninterrupted power delivery and secure data transfer through a physical link, allowing for extended operational endurance and consistent communication performance. By incorporating satellite backhaul functionality on the ground, tethered drones can establish direct connections to satellite networks, offering broadband connectivity to remote or communication-deficient areas, supporting emergencies and first responders' actions on the field. This capability is vital for ensuring real-time coordination between field operators and central command centers, especially in situations that require rapid decision-making and situational awareness. In OVERWATCH, the satellite backhaul provided by tethered drones guarantees continuous control and data relay to the drone operators base stations during reconnaissance, surveillance, and search-and-rescue missions. Similarly, first responder teams benefit from enhanced communication reliability, enabling the seamless exchange of voice, video, and data, between the command & control center and the Overwatch assets in the field which is essential for efficient disaster response operations. The scientific and operational advantages of tethered drones with satellite backhaul capabilities position them as transformative assets for disaster management, meeting the critical need for resilient and scalable communication infrastructure in emergency situations. The system can also be customized to work with other legacy communication infrastructures.

1.2. Overwatch Architecture

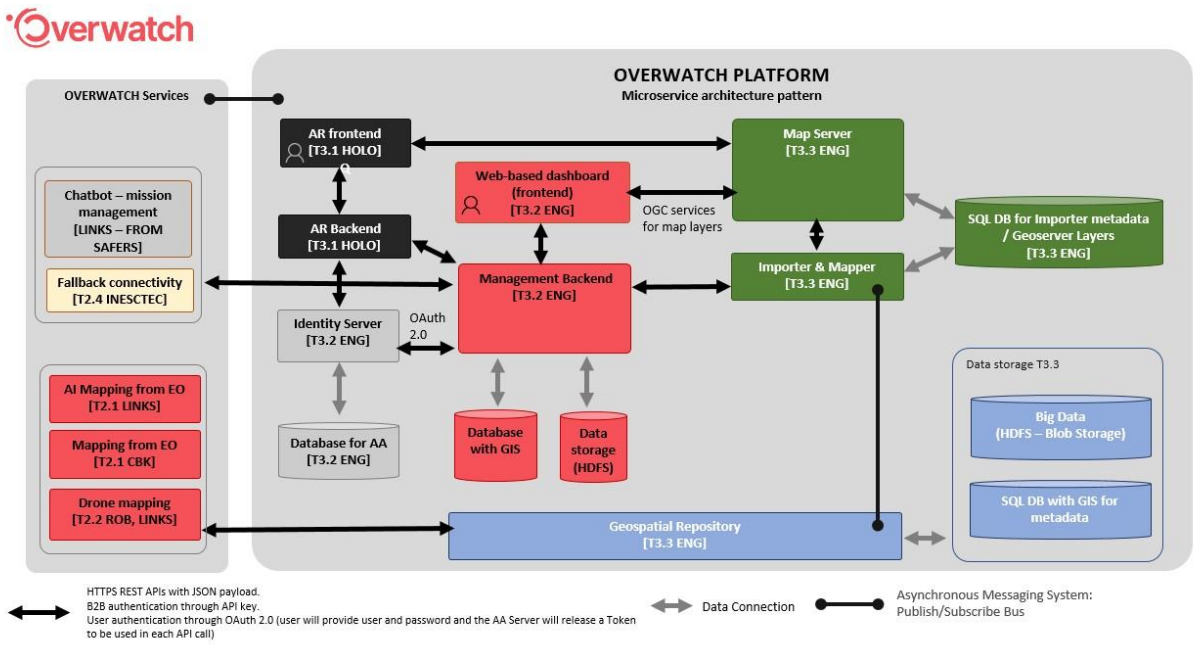

Figure 1. The Overwatch architecture in a nutshell

OVERWATCH system architecture, see Figure 1 is structured into two main components. The first component focuses on generating actionable data derived from imagery sourced through satellite Earth observation, drone acquisitions, or legacy systems. The second component consolidates this information and delivers processed results to the end user. Concerning data ingestion and processing GIS layers and imagery serve as the foundational data sources of the architecture, necessitating a standardized and efficient processing pipeline. Initially, these data are ingested using a Big Data storage solution, which interfaces with a **Geospatial Repository**. This repository operates in an event-driven manner, employing a message broker to signal operations. This design maintains loose coupling between the data-providing and consuming components, ensuring modularity and flexibility.

Once ingested, the storage infrastructure triggers a processing phase that harmonizes the raw data into map layers. During this phase, the system performs operations to standardize, organize, and integrate the data. This process includes cataloguing and querying the imported data alongside associated metadata, utilizing **OGC-compliant services** such as GeoServer to facilitate seamless geospatial data management.

The processed information is made accessible through a robust management system that supports querying and visualization. By leveraging OGC services, the system delivers geospatial data and maps in formats optimized for client applications, enabling easy rendering on various devices and platforms. These platforms include augmented reality (AR) interfaces and web dashboards, offering users an intuitive and interactive way to interact with the data.

The two architectural components are interconnected using technologies and mechanisms designed to ensure robust and reliable communication. Recognizing the critical importance of **network**

connectivity in operational scenarios, the architecture incorporates fallback connectivity systems to mitigate potential disruptions.

Disruptions such as network outages, hardware failures, or environmental factors—common in crisis or remote settings—are addressed through backup and alternative connectivity solutions. These measures ensure continuous interaction between system modules, preserving overall functionality and minimizing downtime even in adverse conditions.

This design philosophy ensures that the system remains resilient, adaptable, and capable of delivering high-quality geospatial insights to end-users under a wide range of operational circumstances as illustrated in Figure 2 .

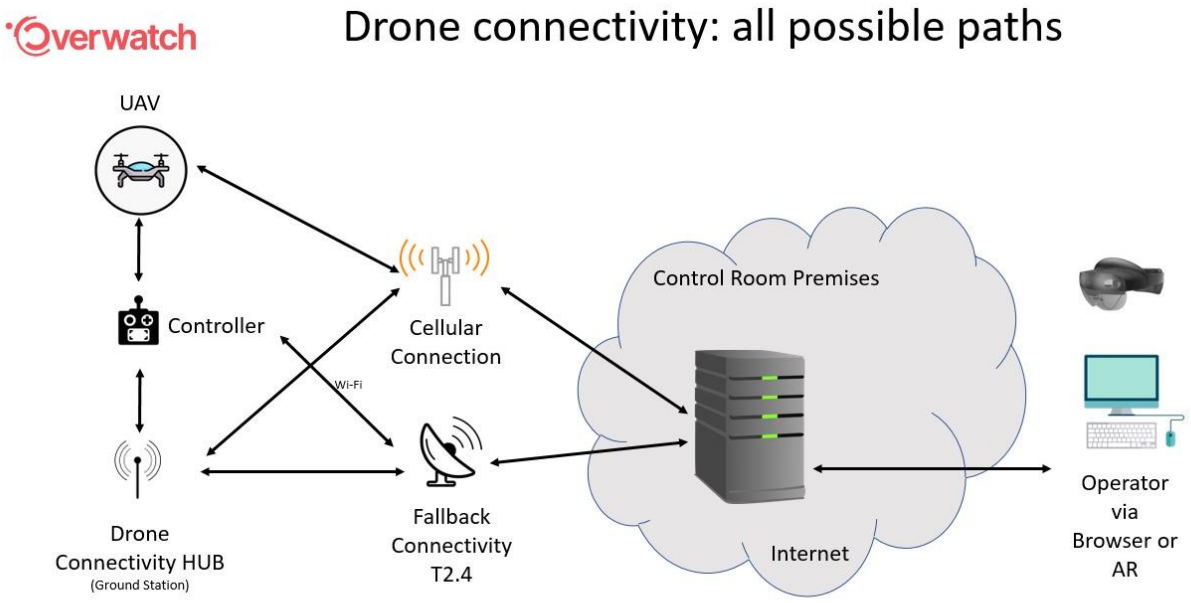

Figure 2. Overwatch Drone Connectivity Pathways

1.3. End-User Requirements concerning FCS

The **Fallback Communication System (FCS)** is a critical component of the Overwatch architecture, designed to provide reliable communication capabilities when primary networks are disrupted or unavailable in operational scenarios. It addresses the challenges of maintaining connectivity between OVERWATCH assets in remote locations, supporting the system's overall resilience and operational continuity. It's of key importance to maintain redundancy since through Wi-Fi satellite backhaul using Starlink can provide internet connection between, for example, Drone Ground Stations and OVERWATCH Command & Control Station. From the interviews and co-design to draw requirements from the end-users in Task 1.1, which originated the deliverable D1.1 the following requirements, shown in Table 1, that were specified by the end-users.

Table 1. End-User Functional Requirements concerning the design of the fallback communication system

IDENTIFIER	DESCRIPTION
FCS-FM-000	The OVERWATCH must support C2 in coordinating emergency response efforts by providing redundant communication channels using a fallback communications system with a tethered drone
FCS-FM-010	The fallback communications system must integrate with the emergency communication system to facilitate communication between C2 and all other emergency responders in blackout regions.
FCS-FM-020	The drone must maintain a stable and reliable connection to the GCS to ensure uninterrupted communication with emergency responders
FCS-FM-030	The drone must carry a payload to support Wi-Fi communications and make use of a satellite broadband communication link for providing fallback communication hotspots in case of infrastructure damage or network outages
FCS-FM-040	The ground control station system must be able to receive and process data transmissions from the tethered drone in real-time
FCS-FM-050	The tethered drone must be able to remain airborne for an extended period, providing continuous communications coverage for emergency responders, provided that they are within the communications range capabilities of the wireless technologies used
FCS-FM-060	The ground station control system must have a user-friendly interface that is easy to use and navigate by emergency responders
FCS-FM-070	The system must provide high-speed data transfer capabilities for sharing critical information such as maps, photos, and other data
FCS-FM-080	The tethered drone must land safely whenever it loses connection to the GCS
FCS-FS-000	The AIMS should be able to identify communication blackouts and automatically deploy tethered drones to maintain communication coverage
FCS-FS-010	The ground station control system should have the ability to provide remote access for authorised personnel to monitor the GCS.
FCS-FS-020	The ground station control system should be able to log all activity for post-incident analysis and reporting
FCS-C-000	The FCS could have the ability to integrate with other communication networks, such as cellular networks, e.g., 5G, to provide redundant communication coverage
FCS-C-010	The system could have the ability to provide encrypted communication for the secure transmission of sensitive information
FCS-W-000	The system won't have the ability to operate without the tethered connection to the GCS
FCS-W-010	The system won't be able to provide communications coverage beyond a certain distance from the GCS
FCS-W-020	The tethered drone won't be able to operate in extreme weather conditions, such as heavy rain or strong winds

FCS-W-030	The system won't be able to operate and provide communication coverage in areas where drones are prohibited by law or regulation

Concerning end-user requirements the main aspects that are set, are related to the capabilities of the FCS provide network coverage throughout extended periods of time, to carry a payload that can support wi-fi communications in the disaster area, to have an easy and accessible user interface and integrate with other legacy communication systems than can be already in use by the end-users in their emergency field operations, as illustrated in Table 2.

Table 2. End-User Non-Functional Requirements concerning the design of the fallback communication systems

IDENTIFIER	DESCRIPTION
FCS-AVT	The system should be highly available, with minimal downtime and quick recovery in case of failure
FCS-COMP	The system should be compatible with a range of communication equipment (Wi-Fi), allowing for flexibility in deployment and use
FCS-INT	The system should integrate with other communication systems used by emergency responders, allowing for seamless communication between teams
FCS-MNT	The system should be easy to maintain and update, with clear documentation and a straightforward maintenance process
FCS-PERF	The system should have high performance, with minimal latency and fast data transfer rates
FCS-REL	The system should have a high level of reliability, ensuring that it can function in harsh environments and under extreme weather conditions without failure
FCS-RES	The system should be designed to withstand disruptions and failures, ensuring that it can continue to function in the event of an emergency
FCS-SCA	The system should be scalable, allowing for easy expansion as the emergency response network grows
FCS-SEC	The system should be secure, with measures in place to protect data and prevent unauthorised access to the network
FCS-USBT	The system should be easy to use, with intuitive interfaces that require minimal training

1.4. Functional Requirements concerning FCS

The **Fallback Communication System (FCS)** is an essential component of the Overwatch architecture, designed to ensure the continuity of communication in scenarios where primary networks are disrupted. Reliable communication is critical for maintaining real-time monitoring, data exchange, and decision-making processes, particularly in challenging maritime environments or during crises.

To achieve this, the FCS must fulfill specific functional requirements that enable it to support seamless connectivity across diverse operational scenarios. These requirements encompass redundancy, scalability, interoperability, security, and performance. By addressing these aspects,

the FCS ensures that Overwatch maintains its operational integrity even under adverse conditions, safeguarding critical infrastructure and enabling uninterrupted system functionality.

The following section depicted in Table 3 outline the functional requirements of the FCS, focusing on its ability to provide robust and adaptive communication capabilities for various use cases and operational contexts.

Table 3. Functional Requirements concerning the design of the fallback communication systems

IDENTIFIERS	FUNCTIONAL REQUIREMENTS	END USER REQUIREMENTS	DESCRIPTION END USER REQUIREMENTS
FCS-FR-1	Provide external connection with other OVERWATCH sub-modules and legacy systems (namely C2)	FCS-FM-000 FCS-FM-010	Provide external connection between the fallback connectivity and other Overwatch sub-modules, C2 and other legacy systems
		FCS-FS-010	
FCS-FR-2	Provide Connectivity (network and Internet access) to other systems	FCS-FM-030	The fallback connectivity system must be able to provide support for reliable communications e.g, Wi-Fi, Ethernet and (if available) 5G to provide redundant communications coverage to nearby local systems, allowing them to communicate locally and to the Internet (e.g. upload and download data from the cloud systems).
		FCS-C-000	
FCS-FR-3	Tethered drone GCS functionalities	FCS-FM-020	These requirements relate to the functional requirements of the tethered drone GCS and capabilities to system a reliable and functional system. Namely capability to ensure communications, user-friend interface, log all activities and be able to receive data.
		FCS-FM-040 FCS-FM-060 FCS-FM-070 FCS-FM-080 FCS-FS-020	
FCS-FR-4	Tethered drone functional capabilities	FCS-FM-050	The tethered drone must remain airborne for extended periods of time and land safety whenever it loses connection to GCS
		FCS-FM-080	

2. Fallback Communication System Architecture

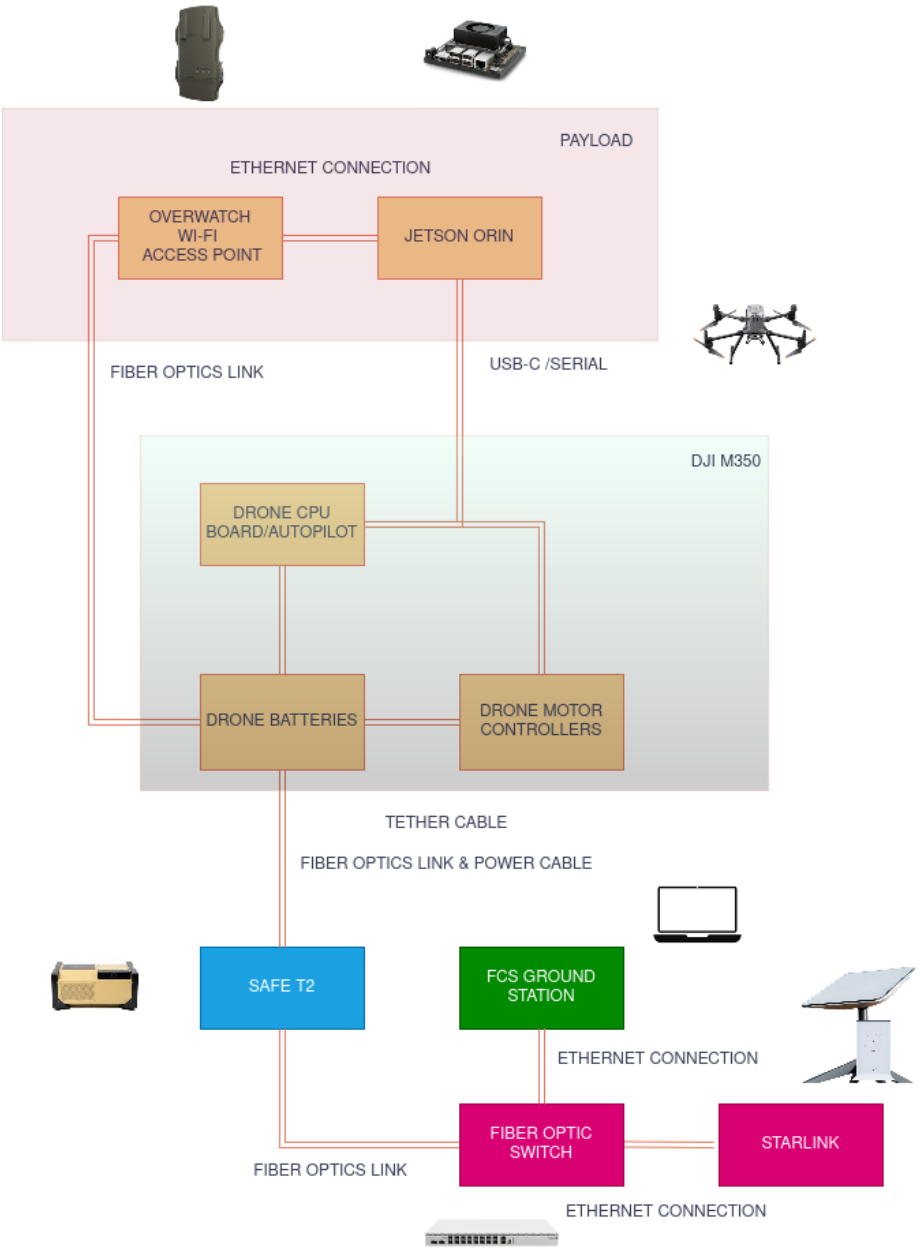

Figure 3. Fallback Communication System Components.

In Figure 3 are depicted the main components on which the fallback communication system solution for OVERWATCH is based upon. The fallback communication system consists of hardware components that are located on the ground or in the air modules of the drone: (1) on the ground, we will have the ground control of tether drone (SAFE-T2), the FCS ground station (a portable laptop) that is receive the data streaming information being dispatched by the aerial components of the FCS. Also on the ground there is the satellite backhaul through STARLINK connection;(2) concerning the aerial component, we have the customized tether drone system that will have dedicated CPU/GPU

to process and stream the data, as well as a Wi-fi access point that will act as a mobile altitude antenna for providing connectivity to drone and/or operators on the ground.

2.1. Tether Drone

In the context of the OVERWATCH project, the solution for the design and development of the FCS that was deemed more feasible based on the available development time and final system high TRL objective, was to integrate a tethered system that can provide power and fiber optical link as well as servo-controlled tether cable with a INESCTEC customized DJI drone. A tethered solution like the SAFE-T2[2] provides continuous power, allowing the DJI M300 drone to stay airborne for extended periods of time. The solution is not optimal since the tethered system only provides power to the motors and not to the other payload that is required in OVERWATCH but assures still uninterrupted operation for extended periods of time up to 4 hours based on approximations and initial testing, making it ideal for long-duration missions.

In OVERWATCH the drone will be equipped with communication payloads such as Wi-Fi or 5G nodes or mesh networking devices, the M350 can serve as a stable and persistent communications relay. This is especially useful in areas where ground-based infrastructure is unavailable or damaged. Operating at height, the tethered M350 overcomes line-of-sight issues and terrain obstacles, delivering seamless communication across large areas critical for effective monitoring and coordination.

The tethered system is portable and quick to set up, after having followed a pre-plan detailed procedure, making it ideal for time-sensitive deployments. The M350 compatibility with various payloads adds versatility, enabling it to perform dual roles such as surveillance and communication relay, which reduces the need for additional assets.

The tethered system minimizes interference or disruptions during operations—key requirements for critical missions by providing a consistent power supply and stable data link. Moreover, this approach is a cost-effective alternative to traditional solutions like fixed antennas, mobile carriers or temporary communication towers, optimizing resource allocation for OVERWATCH operations.

a. SAFE T2

The SAFE-T2 by Elistair is an advanced tethering system designed to provide continuous power and secure data transfer for various drone operations. The information depicted in Table 4 summarizes SAFE-T2 main characteristics.

Table 4. SAFE-T2 Specifications and main characteristics.

Feature	Specification
Micro-Tether Length	Up to 100 meters (328 feet)
Micro-Tether Weight	16 g/m, 20 g/m, or 25 g/m
Tensile Strength	150 daN
Operating Temperature	-10°C to 45°C (14°F to 113°F)
Maximum Continuous Power	2200 W continuous; peak at 2800 W

[2] https://elistair.com/solutions/tethering-station-safe-t/

Data Communication	Dual secure communications: Broadband over Power Lines (BPL) and optional Fiber Optic
Wi-Fi Connectivity	2.4 GHz frequency; supports WEP/TKIP/AES encryption
Power Supply Requirement	200-250 VAC, 50-60 Hz, minimum 3 kW
Ingress Protection Rating	IP54
Dimensions	603 mm x 408 mm x 261

In OVERWATCH FCS, the SAFE T2 system (see Figure 4) provided by ELISTAIR was selected, due to the fact that it can provide up to 100 meters of cable length, it has power and fiber optical cables connected through a single wired cable and can provide 2200w continuous power, which is sufficient to power the DJI 350 motors continuously. It also comes with an integrated API for smooth configuration through web or mobile devices. In OVERWATCH this feature will not be used since the SAFE T2 is directly connected to the onboard payload in the DJI M350 Jetson Orin, and the network utilized will be the one provided by OVERWATCH wi-fi access point that will be on board the drone and connected to the ground control station laptop through fiber optical link.

Figure 4. Safe-T2 and DJI M350 drone systems

b. DJI M350–INESCTEC

Figure 5. DJI M350 customized with Jetson Orin.

INESCTEC as partner responsible for T2.4 and given the OVERWATCH project timeframe, decided to use the DJI M350 (see Figure 5), as the drone platform for developing tethered drone solution. The use of the DJI M350 provides some advantages, namely, already a high TRL flight platform that has extended flight hours and, therefore, is highly reliable i.e. DJI interfaces and command & control are straightforward to execute, meaning that most drone-certified pilots and even amateur or hobbyist pilots can fly a DJI drone. Even though this is not a hard requirement, the fact that the drone is easy to fly can be an advantage for emergency teams that can train their pilots in smaller, cheaper drones. Another advantage is the fact that in the context of the OVERWATCH we can access all DJI motors, controllers, autopilot and navigation information, which allows us to develop a fully customized solution taking advantage of the already well-established and flight-proven platform.

In the context of OVERWATCH, an onboard computer was utilized for interfacing and controlling in case of need the flight and reading the sensors measurements from the DJI M350 RTK drone. The onboard computer utilized was based on a Nvidia Jetson Orin AGX board running Ubuntu 20.04 LTS and ROS Noetic. In this section, we present the ROS implementation on this board, presenting user guiding Tables associated with the usage of ROS topics for reading sensors measurements, the usage of ROS services for performing simple tasks, and the usage of ROS actions to perform more advanced tasks.

Concerning the documentation regarding ROS message structure, ROS topic publication and subscription, ROS services and ROS actions, the reader can find the information with the following links:

- ROS std_msgs: http://wiki.ros.org/std_msgs;
- sensor_msgs and geometry_msgs:http://wiki.ros.org/common_msgs?distro=noetic;
- simple publisher and subscriber: http://wiki.ros.org/ROS/Tutorials/WritingPublisherSubscriber;

- ROS services: http://wiki.ros.org/Services;
- ROS actions:https://wiki.ros.org/actionlib;

Table 5. ROS Topics

ROS TOPIC NAME	Description	Message Type
/dji_m350/altitude	Provides aircraft's fused data for altitude above sea level, in m.	std_msgs/Float64.msg
/dji_m350/battery/b1	Provides battery information for the battery 1 (capacity, voltage, current, and battery percentage).	sensor_msgs/BatteryState.msg
/dji_m350/battery/b2	Provides battery information for battery 2 (capacity, voltage, current, and battery percentage).	sensor_msgs/BatteryState.msg
/dji_m350/battery/whole	Provides battery information for the full battery system (capacity, voltage, current, and battery percentage).	sensor_msgs/BatteryState.msg
/dji_m350/cameras/fpv	Provides 1080p30 image from the FPV camera video stream.	sensor_msgs/Image.msg
/dji_m350/cameras/main	Provides 1080p30 image from the main camera video stream (wide, zoom, or thermal).	sensor_msgs/Image.msg
/dji_m350/cameras/ main/camera_params	Provides the main camera source (wide, zoom, or thermal) and the current main camera zoom factor.	Jetson_m350/Camera_params .msg Header header uint8 camera_source float64 zoom_factor
/dji_m350/compass	Provides aircraft's magnetometer reading, fused with IMU and GPS. This reading is the magnetic field recorded by the magnetometer in x,y,z axis.	geometry_msgs/ Vector3Stamped.msg
/dji_m350/display_mode	Provides a granular state representation for various tasks/flight modes from DJI PSDK E_DjiFcSubscriptionDisplayMode.	std_msgs/UInt8.msg
/dji_m350/flight_status	Provides drone flight status:	std_msgs/UInt8.msg

	0 - Aircraft is grounded and motors are still 1 - Aircraft is grounded but motors are spinning 2 – Aircraft is in the air	
/dji_m350/gimbal	Provides gimbal pitch (x), roll (y), yaw (z), in degrees	geometry_msgs/ Vector3Stamped.msg
/dji_m350/gps	Provides fused GPS position with latitude, longitude and altitude.	sensor_msgs/NavSatFix.msg
/dji_m350/gps/nsats	Provides the number of visible satellites.	std_msgs/UInt16.msg
/dji_m350/ homepoint_altitude	Provides altitude of the homepoint, in m.	std_msgs/Float64.msg
/dji_m350/obstacle	Provides distance from obstacles in all the available obstacle sensor directions and health state of each sensor: 0 - not healthy or 1 – healthy. Custom message based on T_DjiFcSubscriptionAvoidData DJI PSDK message type	jetson_m350/Obst.msg Header header float32 down float32 front float32 right float32 back float32 left float32 up uint8 downHealth uint8 frontHealth uint8 rightHealth uint8 backHealth uint8 leftHealth uint8 upHealth uint8 reserved
/dji_m350/quaternion	Provides aircraft body frame (FRD) to ground frame (NED) rotation, in degrees.	geometry_msgs/Quaternion.msg
/dji_m350/ relative_altitude	Provides the difference between the drone altitude and homepoint altitude, in m.	std_msgs/Float64.msg
/dji_m350/velocity	Provides aircraft's velocity in a geometry_msgs/ ground-fixed NEU frame, in m/s. This velocity data is a fusion output from the a	geometry_msgs/ Vector3Stamped.msg
/dji_m350/velocity/health	Provides the health state of aircraft velocity data. It can be 0 (healthy) or 1 (not healthy).	std_msgs/UInt8.msg
/dji_m350/vo_position	Provides aircraft's position in a Cartesian frame, in m. Based mainly on visual odometry and	geometry_msgs/ Vector3Stamped.msg

	IMU. without the need for GPS.	

Table 6. ROS Services

ROS Service Name	Description	Request and Response
/dji_m350/camera/cont_zoom	Allows to start and stop continuous zoom in or zoom out with the main camera.	Request: int8 direction # 0 - stop zoom # 1 - zoom in # -1 - zoom out Response: bool success
/dji_m350/camera/record_video	Allows to start/stop the recording of video from the main camera.	Request: bool start # 0 - stop #1 - start Response: bool success
/dji_m350/camera/stream	Allows to select the main camera stream source and start/ stop stream (IR, ZOOM, WIDE, or OFF).	Request: string state # “IR” - thermal stream # “ZOOM” - zoom stream # “WIDE” - wide stream # “OFF” - camera off Response: bool switched
/dji_m350/camera/zoom	Allows to set the main camera zoom factor value.	Request: float64 zoomFactor #desired zoom factor Response: bool success
/dji_m350/gimbal/mode	Allows to select the main camera gimbal mode: 0 - Free mode: fix gimbal attitude in the ground coordinate, ignoring movement of aircraft; 1 – FPV mode: only control roll and yaw angle of gimbal in the ground coordinate to follow aircraft; 2 - Yaw follow mode: only	Request: uint8 gimbalMode # 0 - free mode # 1 - fpv mode # 2 - yaw follow mode Response: bool success

	control yaw angle of gimbal in the ground coordinate to follow aircraft.	
/dji_m350/gimbal/move	Allows to control the main camera gimbal movement in roll, pitch, and yaw, in both relative and absolute angle modes.	Request: float64 roll float64 pitch float64 yaw # desired gimbal roll, pitch, and yaw angles bool relative # 0 - absolute angles # 1 - relative angles Response: bool success
/dji_m350/photo/mode	Allows to set the number of photos from the main camera to be captured with /dji_m350/photo/shoot and the time interval between them.	Request: uint8 captureCount # number of pictures uint16 timeInterval # interval between pictures Response: bool success
/dji_m350/photo/shoot	Allows to start capturing photos from the main camera.	Request: bool start # 0 - stop # 1 - start Response: bool success

Table 7. ROS Actions

ROS Action Name	Description	Goal, feedback an result
dji_m350/actions/takeoff	Allows to start drone takeoff and move to a desired altitude.	Goal: bool climb # 0 - don't climb # 1 - climb after takeoff float64 height # desired height for the climb, in meters Feedback: int32[] stage # stage of takeoff value, for debug Result: bool tookoff # 0 - didn't take off # 1 - took off

		int32 error_code # error code value, for debug
dji_m350/actions/land	Allows to start drone landing.	Goal: #no goal Feedback: int32[] stage # stage of takeoff value, for debug Result: bool landed # 0 - didn't land # 1 - landed int32 error_code # error code value, for debug
dji_m350/actions/rotate	Allows to perform a drone yaw rotation of a certain angle, in degrees.	Goal: float64 yaw_in_degrees # desired yaw value, in degrees Feedback: float64 diff_in_degrees # difference between drone current yaw and desired yaw Result: bool rotated # 0 - didn't rotate # 1 - rotated int32 error_code # error code value, for debug
dji_m350/actions/motors	Allows to turn on/off the motors.	Goal: bool spin # 0 - motors stop # 1 - motors spin Feedback: Result: bool spinning # 0 - motors are stopped # 1 - motors are spinning int32 error_code # error code value, for debug
dji_m350/actions/moveby	Allows the drone to move by a desired amount in the 3D directions (x, y, z), in m.	Goal: float64 x float64 y float64 z # desired amount for x, y and z movement, in meters

		Feedback: int32 progress # percentage of movement completed Result: int32 error_code # error code value, for debug bool success
monitor	Handles the interation between the GUI and the monitor action server. Allows the user to send a control frame and monitor the Safe-T system status.	Goal: string frame - ”standard”, ”V0”, or ”V1” uint8 power - 0x00: OFF - 0x01: ON - 0xFF: Determined by physical button uint8 torque - 0..10: For ”standard” or ”V0” - 0..254: For ”V1” - 0xFF: Determined by physical button Feedback: string status - Provides updates such as ”Control frame sent successfully.” or ”Waiting for response.” Result: bool success - Indicates success or failure of the monitoring action string message - Error or success message (e.g., ”Timeout: no response received.”, ”Monitoring data published.”).

2.2. Communications Payload

The selection of the Communications Payload considered constraints including a maximum weight limit of 2 kg, compliance with Wi-Fi standards of 802.11ax (Wi-Fi 6) or higher, an ingress protection rating of IP65 or above to endure heavy rainfall without experiencing any adverse effects, and the capability to support optical fiber connectivity with a minimum data transfer speed of 1 Gbit/s. Additionally, it had to be compatible with the drone's tether fiber optic specifications, including an LC simplex connector and single-mode 9/125 optical fiber.

An initial market survey revealed that identifying an access point (AP) capable of meeting these constraints while staying within the maximum weight limit would be more challenging than anticipated. Either the APs were too bulky and heavy, did not support the latest communications standards, did not support power over DC jack, or did not even have an onboard medium converter with Ethernet switching capabilities. An initial design consisted of an AP and separate medium converter with Ethernet switching and PoE capabilities to power the AP. This design was then updated to consider a final simpler, lightweight and IP66-rated AP that had all these features integrated. The performance validation tests presented below were focused on the final solution, since it was the one fully compliant with all the requirements and constraints, was lighter, and presented lower intregration complexity and potential points of failure. This enabled more accurate and realistic testing of the network throughput, jitter, and packet loss under simulated field conditions.

The first design architecture is depicted in (Figure 6, Table 8). We proposed and included a Wi-Fi 6 AP (Engenius ECW260), a four-port switch (PLANET IGS-624HPT), and an SFP transceiver (FS: Cisco GLC-BX-D Compatible). The switch was required because the AP lacked an SFP connector, and an extra Ethernet port was needed to connect the NVIDIA Jetson to the network. While this design addressed most requirements, it had notable drawbacks: the switch lacked an IP-rated enclosure, the payload mounting process was complex, and the switch only offered Gigabit Ethernet ports, which limited the use of the AP's 2.5 Gbit/s Ethernet port capacity.

Table 8. Initial Communications Payload Design.

Equipment	
Access Point	Engenius ECW260
Antennas	Included
SFP Transceivers	FS: Cisco GLC-BX-D Compatible
	FS: Cisco GLC-BX-U Compatible
Onboard Switch	PLANET IGS-624HPT

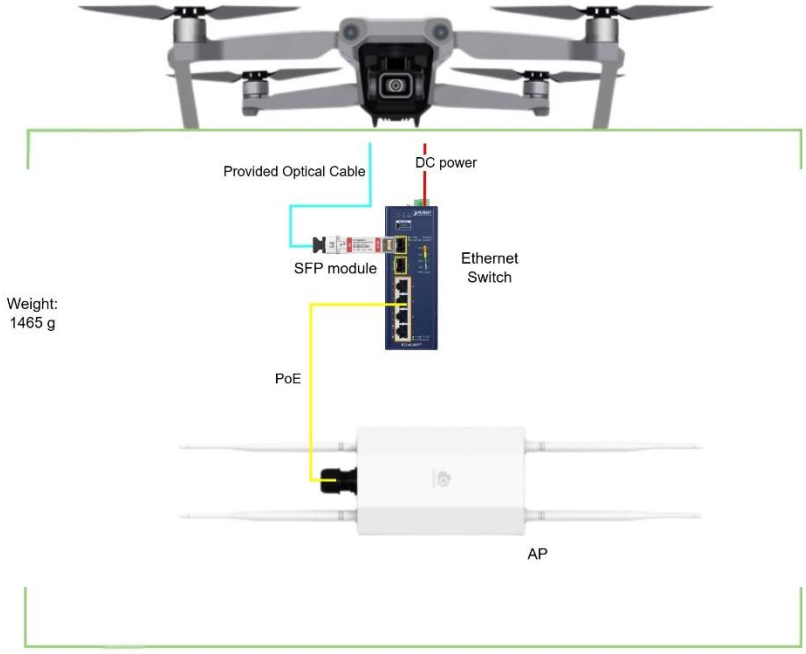

Figure 6. Initial Communications Payload Design.

The final design (see Figure 7, Table 9) utilized a Wi-Fi 6 AP (Mikrotik NetMetal AX) with an SFP cage capable of achieving 2.5 Gbit/s, enabling a direct fiber optic connection to the ground station switch. This AP also featured a Gigabit Ethernet port for bridging the NVIDIA Jetson, an IP66 rating, and a total weight of only 810 g, effectively meeting all constraints while being significantly less complex to be integrated and powered by the drone. Additionally, it was necessary to replace the SFP transceivers with models capable of supporting 2.5 Gbit/s (FS: S+23LC10D) to fully take advantage of the AP's performance capabilities.

Table 9. Final Communications Payload Design.

Equipment	
Access Point	MikroTik NetMetal AX
Antennas	Mikrotik HGO-antenna-OUT
SFP Transceivers	FS: S+23LC10D D
	FS: S+23LC10D U

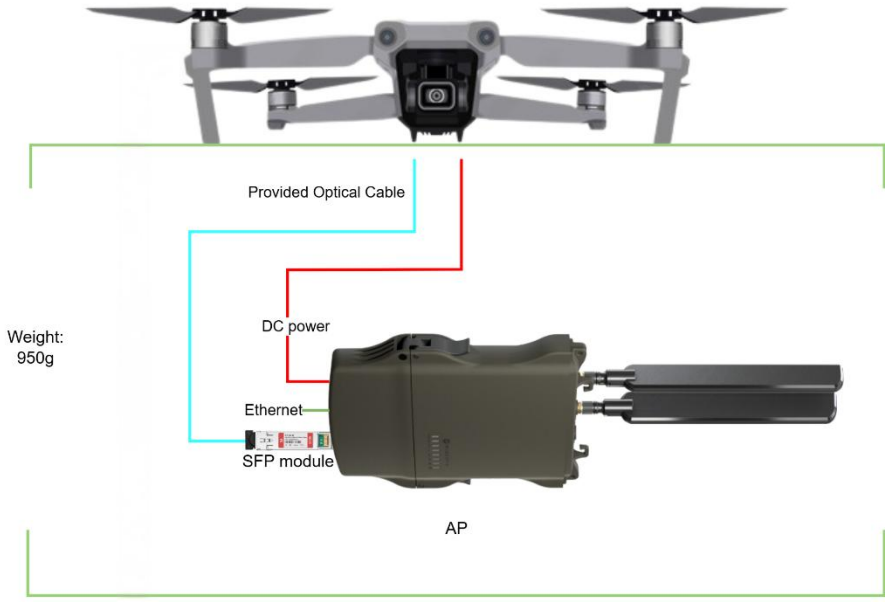

Figure 7. Final Communications Payload Design.

Lab experiments shown in Table 10, were conducted to evaluate the Final communications payload design by performing multiple performance tests using the iPerf3 tool. The tests measured performance between two user devices using the Final design, analysing both the 2.4 GHz and 5 GHz frequency bands with 1, 4, and 10 concurrent traffic streams. These tests were conducted using UDP, with each test running for a duration of two minutes. No bitrate limits were imposed, exceeding typical capacity constraints and revealing the AP's true performance under heavy load.

The 5 GHz band achieved 847 Mbit/s (10 streams), while 2.4 GHz peaked at 130 Mbit/s (4 streams), limited by bandwidth constraints and congestion. Jitter was significantly lower on 5 GHz (~0.163 ms) compared to 2.4 GHz (1.172 ms), ensuring more stable performance for real-time applications.

The high packet loss on 2.4 GHz (85–87%) is expected due to its limited bandwidth, which causes excessive drops when pushed beyond practical limits. In contrast, 5 GHz maintained a much lower packet loss (9-17%), benefiting from wider channels and less congestion. It is important to note that this high packet loss ratio is expected because the UDP protocol, used to test the maximum throughput of the AP, does not have any intrinsic congestion control mechanism and we were generating traffic above the capacity of the link to saturate it. In real operation we expect a much lower packet loss ratio, since most network applications use TCP that has an integrated congestion control mechanism, or UDP for real-time but low-bitrate network flows.

Table 10 - Lab experiments results.

iPerf3 UDP Results	**Bitrate (Mbits/s)**			**Jitter (ms)**			**Packet Loss ratio (%)**		
	Streams			Streams			Streams		
Frequency	1	4	10	1	4	10	1	4	10
2.4 GHz	115	130	129	0,117	0,34	1,172	87	85	86
5 GHz	625	814	847	0,014	0,096	0,163	17	9,7	9

2.3. Communications Ground Components

a. Starlink Satellite Backhaul

In this section we will discuss the hardware selection for the satellite backhaul link, which is directly tied to the selection of the Low Earth Orbit Internet Service Provider (ISP). Furthermore, a long-term performance analysis of the link performance is also presented, so that we have an estimate of the uplink and downlink speeds, as well as the round-trip time (RTT) experienced when using the LEO Internet Access link.

First, we started by consulting the website of the Portuguese National Authority for Communications (ANACOM), since they keep track of all ISPs operating in Portugal, including a list of the satellite providers and their expected performances. Figure 8 shows a screenshot of ANACOM's website, listing the 6 satellite ISPs available in Portugal, as well as the expected downlink and uplink average speeds for such services. Right away it became evident that the service provided by Starlink seemed to be the most adequate to the OVERWATCH FCS due to the much higher announced upload capacity of 25 Mbit/s, which would accommodate much better the upload of data captured from the OVERWATCH on-site systems, such as drones, to the cloud infrastructure (OVERWATCH Platform), to be then processed and later consumed by its users (e.g., Commander using the Augmented Reality System for improved and comprehensive situational awareness). Furthermore, the announced average downlink capacity of 220 Mbit/s was also the best of all the LEO ISP providers.

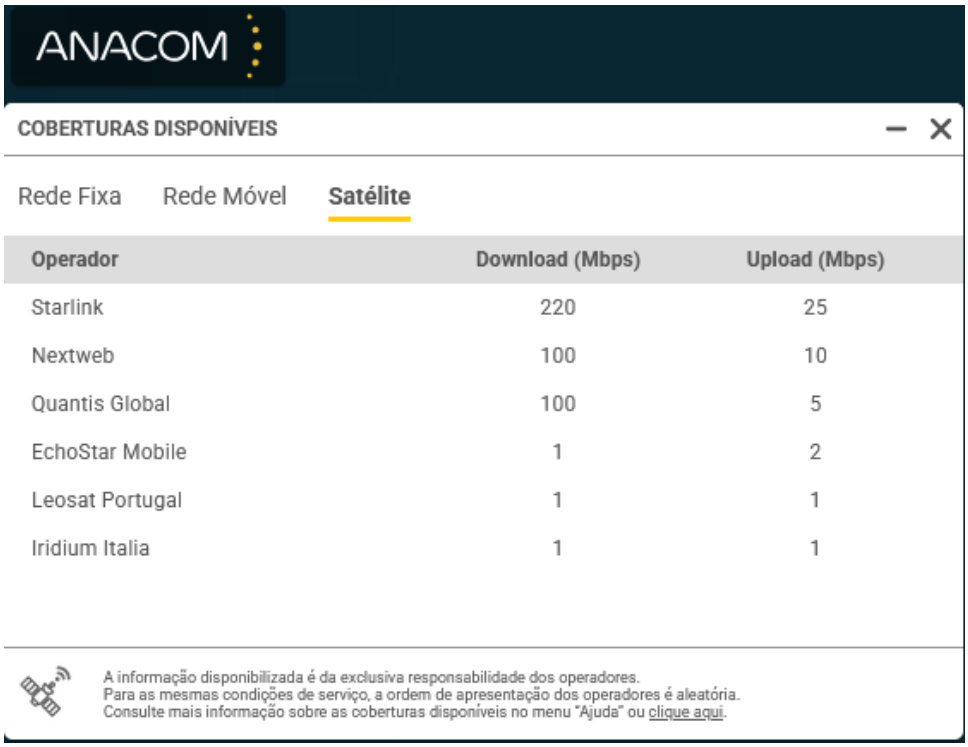

Figure 8. Screenshot of the ANACOM Website, the Portuguese National Authority for Communications, showcasing the list of satellite Internet Service Providers available in Portugal, as well as the expected average downlink and uplink speeds in Mbit/s.

We purchased the Starlink Internet Access hardware, subscribing to the plan with unlimited Internet traffic and without a fixed installation address, as we needed the system to be operatable anywhere in the world with Starlink coverage. The exception was the maritime environment in which the Starlink *geolocks* the service and only allows the operation of specific subscription plans and hardware prepared to be installed on vessel and operated while moving and under unstable conditions.

We installed the Starlink system on the rooftop of INESC TEC (see Figure 9 and Figure 10), connected it to a PC acting as an Internet client, to test its operation performance and stability over

several months. This way we could be certain about its expected performance in the field, including the OVERWATCH field trials.

Figure 9. Antena of the Starlink system installed on the rooftop of INESC TEC's building, in Porto.

Figure 10. Modem Router and Gigabit Ethernet adapter of the Starlink system.

Figure 11. Modem Router and Gigabit Ethernet adapter of the Starlink system.

From August 2024, until the end of January 2025, we had the system operating 24/7, taking consecutive measures, with a period of 10 minutes, of the uplink and downlink throughput in Mbit/s, and the round-trip time (RTT) in milliseconds. In what follows, we present the statistical analysis of those results for three performance metrics, aggregating them per month (since August 2024 until January 2025), per week (since November 2024 until January 2025), per day (since the 24th of December until the 23rd of January), per weekday (since August 2024 until January 2025), and per hour-of-the-day (since August 2024 until January 2025).

The boxplots represent the 25th, the 50th (median) and 75th percentiles, with the lower and upper whiskers representing the 5th and the 95th percentiles. A red color represents the median getting lower (worse throughput, but better RTT), comparatively to the previous interval, while the green color represents the median getting higher (better throughput, but worse RTT). For the plots aggregating the results per weekday and per hour-of-the-day, while the graphical representation is not a box, the percentiles are the same (5th, 25th, 50th, 75th and 95th).

Performance results aggregated per month

Figure 12, Figure 13 and Figure 14 present the monthly throughput and RTT performance results of the Starlink system. We can observe that the performance has been improving over time, which is related to the Starlink LEO expansion (more density of satellites) together with the introduction of technology improvements that increases the multi-hop throughput between LEO satellites in space (now many of them use free space optical link interconnections in space, instead of just relying on RF). It is important to note that while the number of Starlink clients may have increased over this period, the network improvements more than compensated for the possible extra load on the network, resulting in increased throughputs and decreased delays (RTT).

In January 2025, Starlink was achieving a median downlink throughput of 180Mbit/s, a median uplink throughput of 35 Mbit/s, and a median delay (RTT) of 28 ms, which is very good for a LEO satellite link, and fits the expectations and requirements of the OVERWATCH project.

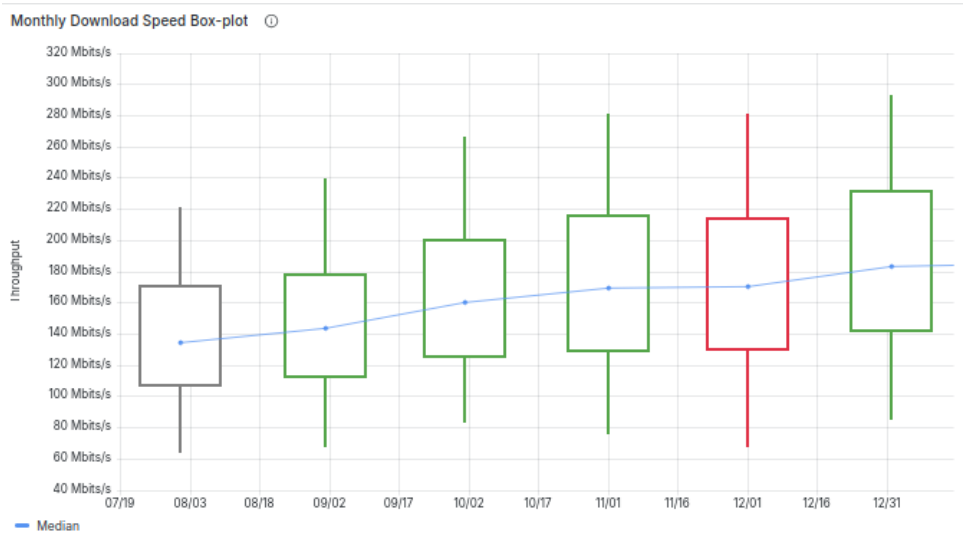

Figure 12. Monthly (from August 2024 until January 2025) Downlink speeds of the Starlink system in Mbit/s.

Figure 13. Monthly (from August 2024 until January 2025) Uplink speeds of the Starlink system in Mbit/s.

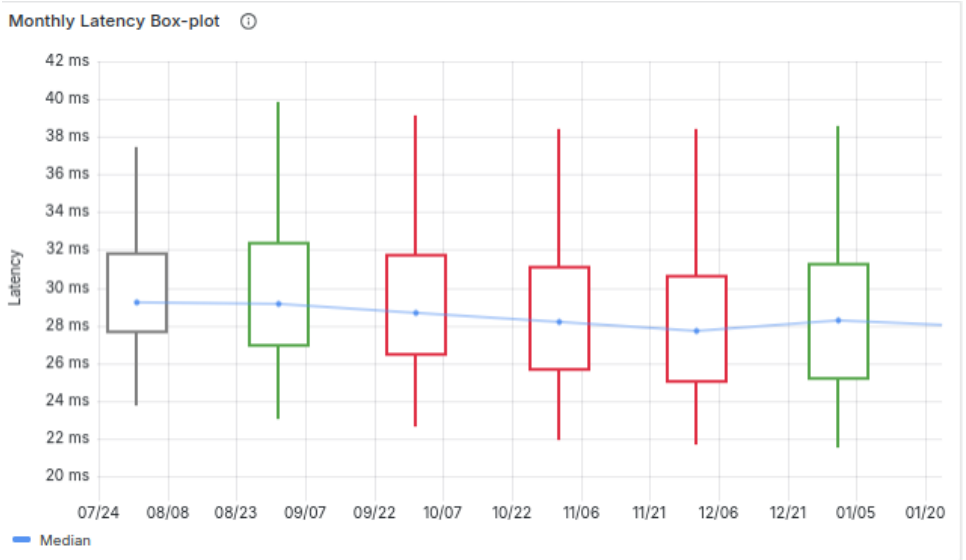

Figure 14. Monthly (from August 2024 until January 2025) Latency (RTT) of the Starlink system in milliseconds.

Performance results aggregated per week

Figure 15, Figure 16 and Figure 17 present the weekly throughput and RTT performance results of the Starlink system. We can observe the similar positive evolution trend of the throughput, and reduction of the RTT, also present in the monthly statistics.

Near the end of January 2025, Starlink was achieving a median downlink throughput of 210Mbit/s, a median uplink throughput of 44 Mbit/s, and a median delay (RTT) of 28 ms, which are very good results, as stated previously.

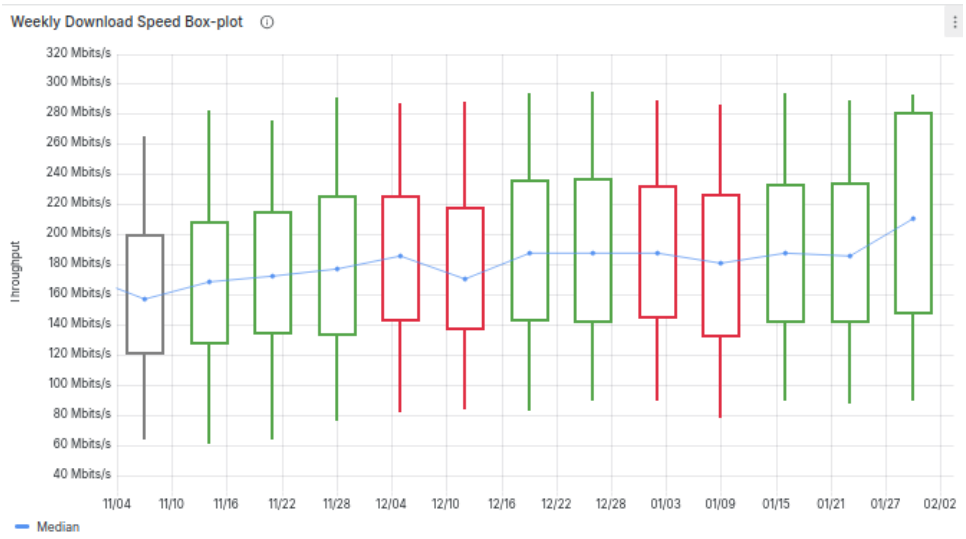

Figure 15. Weekly (since November 2024 until January 2025) Downlink speeds of the Starlink system in Mbit/s.

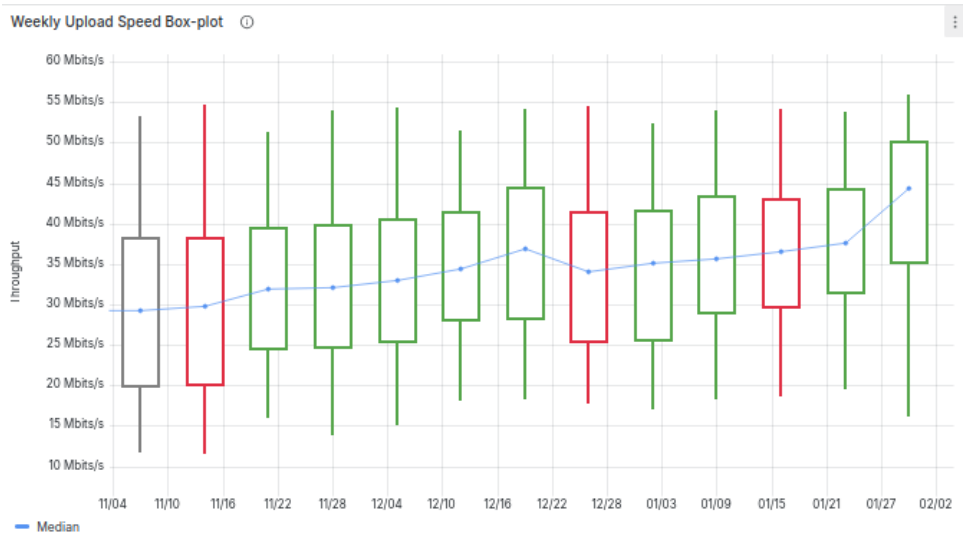

Figure 16. Weekly (since November 2024 until January 2025) Uplink speeds of the Starlink system in Mbit/s.

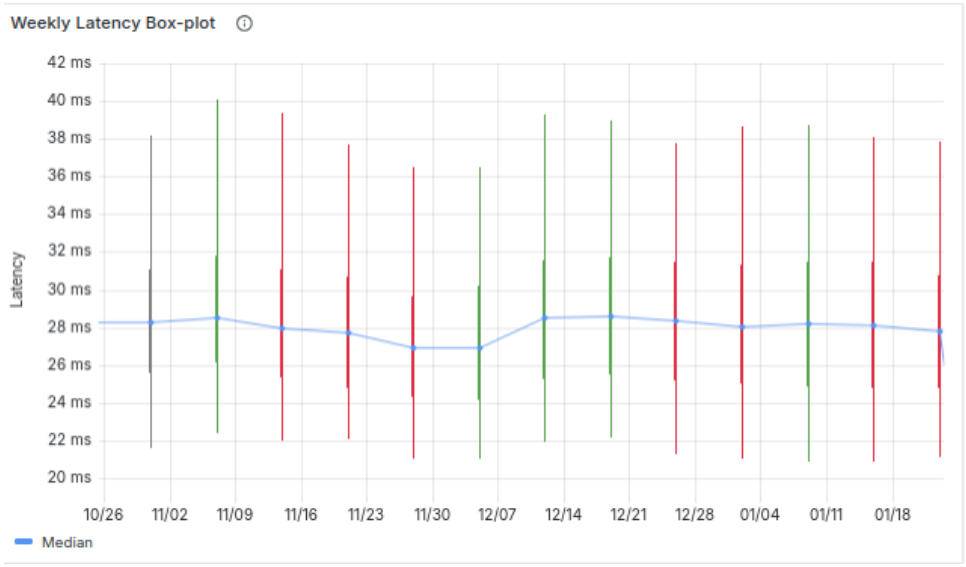

Figure 17. Weekly (since November 2024 until January 2025) Latency (RTT) of the Starlink system in milliseconds.

Performance results aggregated per day

Figure 18, Figure 19 and Figure 20 present the daily throughput and RTT performance results of the Starlink system. We can observe that the throughput and RTT remain more-or-less stable during the days. Nevertheless, we will present a more detailed analysis in this report, aggregating the results per weekday and per hour-of-the-day, to see what the expected performance is over workdays and weekends, as well as in the Internet rush hours and off-peak times.

On the 23rd of January 2025, Starlink achieved a median downlink throughput of 220Mbit/s, a median uplink throughput of 45 Mbit/s, and a median delay (RTT) of 26 ms, which are very good results, as stated previously.

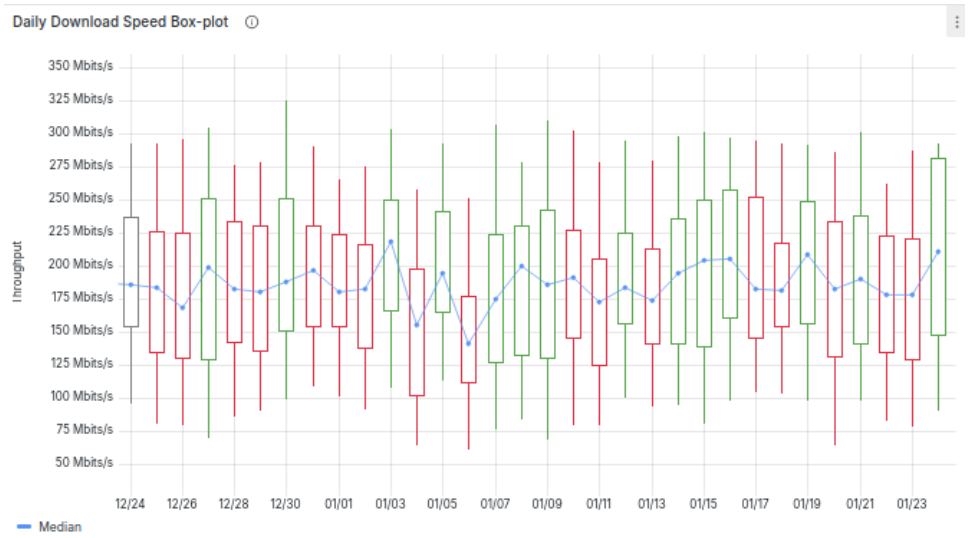

Figure 18. Daily (from the 24th of December until the 23rd of January) Downlink speeds of the Starlink system in Mbit/s.

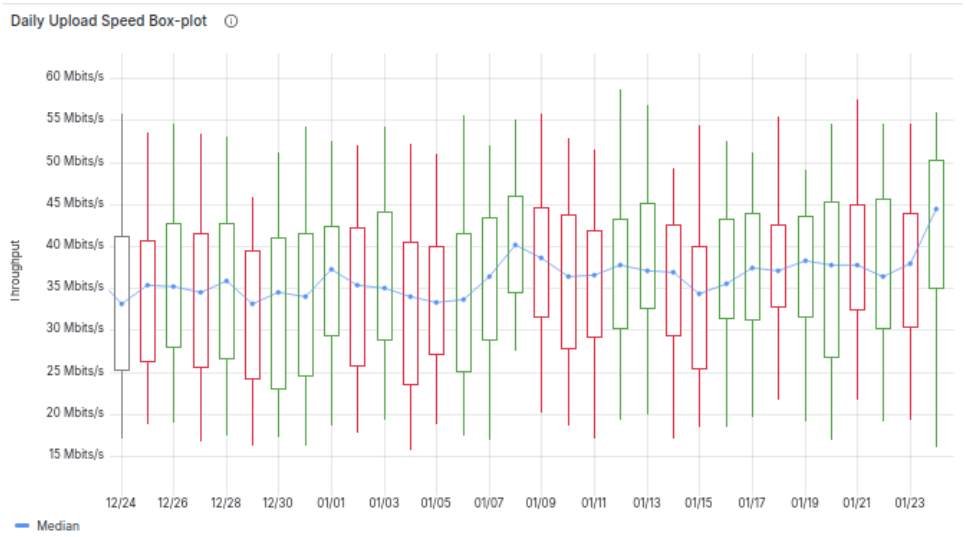

Figure 19. Daily (from the 24th of December until the 23rd of January) Uplink speeds of the Starlink system in Mbit/s.

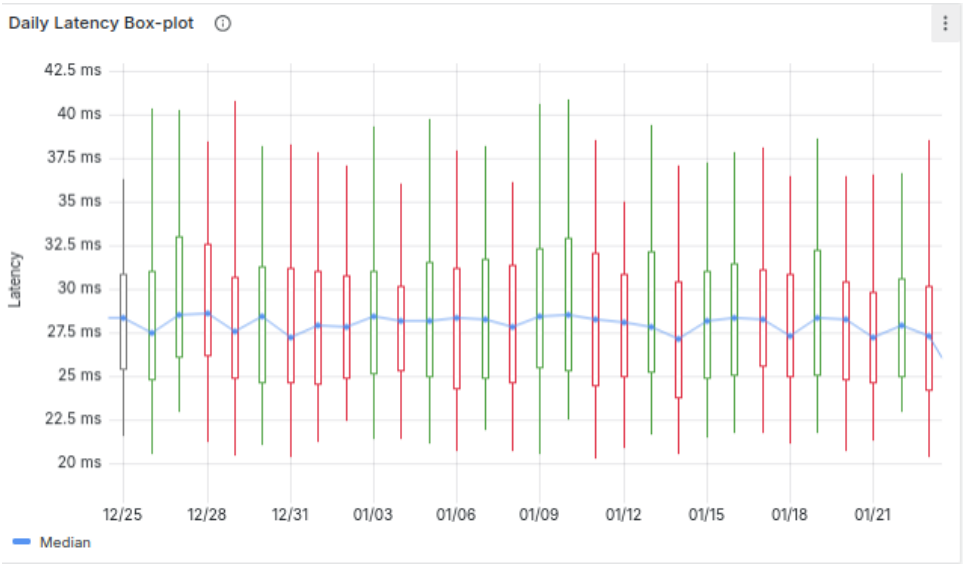

Figure 20. Daily (from the 24th of December until the 23rd of January) Delay (RTT) of the Starlink system in milliseconds.

Performance results aggregated per weekday

Figure 21, Figure 22 and Figure 23 present the throughput and RTT performance results of the Starlink system aggregated per weekday (from Monday until Sunday). The objective of this analysis was to see if a major difference was observed between the usual workdays (Monday to Friday) and the weekend (Saturday and Sunday).

We can observe that the throughput and RTT remain more-or-less stable during the days, independently if it is a regular workday or the weekends, which shows a good indication that the Starlink system is well dimensioned, i.e., the capacity of the installed network infrastructure is capable of handling the normal traffic demand, not showing any alarming signs of congestion such as a systematically high throughput and RTT degradation over certain days.

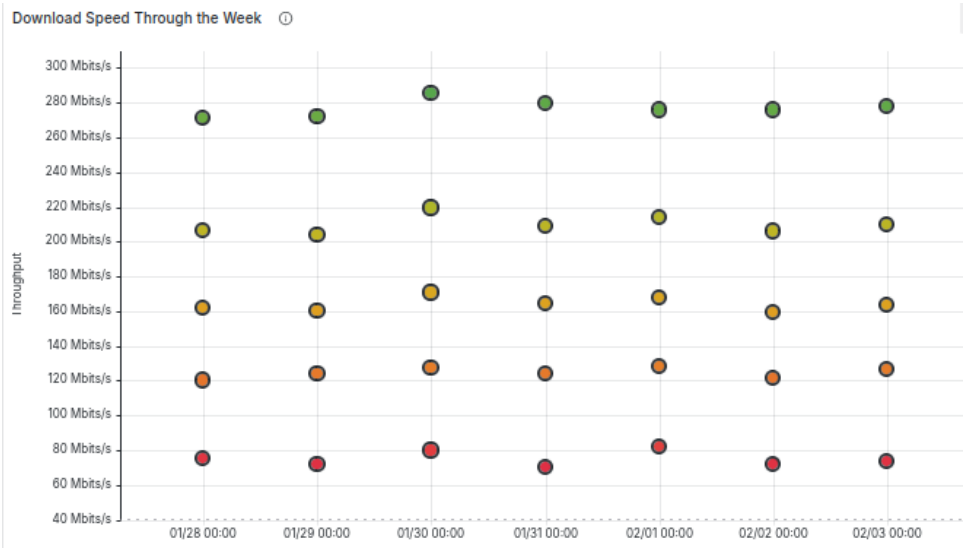

Figure 21. Downlink speeds of the Starlink system in Mbit/s per weekday (Mon, Tue, Wed, Thu, Fri, Sat, Sun).

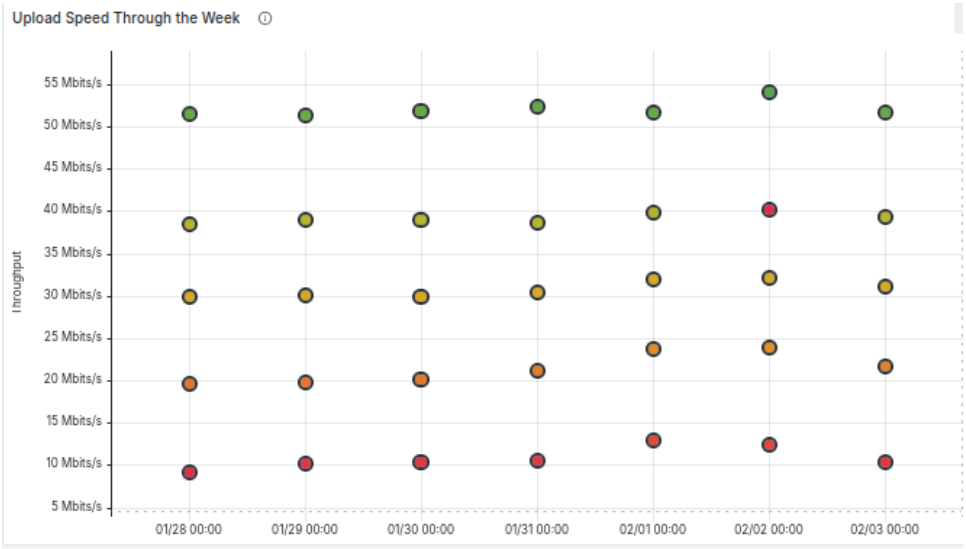

Figure 22. Uplink speeds of the Starlink system in Mbit/s per weekday (Mon, Tue, Wed, Thu, Fri, Sat, Sun).

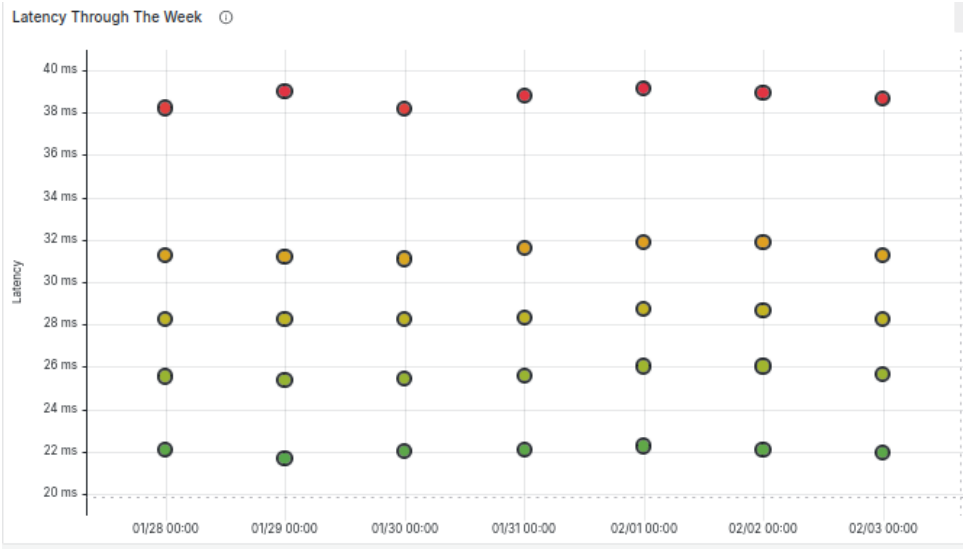

Figure 23. Latency (RTT) of the Starlink system in milliseconds per weekday (Mon, Tue, Wed, Thu, Fri, Sat, Sun).

Performance results aggregated per hour-of-the-day

Figure 24, Figure 25, and Figure 26 present the hourly throughput and RTT performance results of the Starlink system (from 0:00 to 23:59). The objective of this analysis was to see if a major difference was identified between the usual Internet rush hours and off-peak times.

We can observe, as expected, that the throughput and RTT are a little worse, especially during the afternoons and mainly between 15:00 and 21:00. This is even more evident on the RTT curves, where a spike in delay is clearly observed from 15:00 until 21:00.

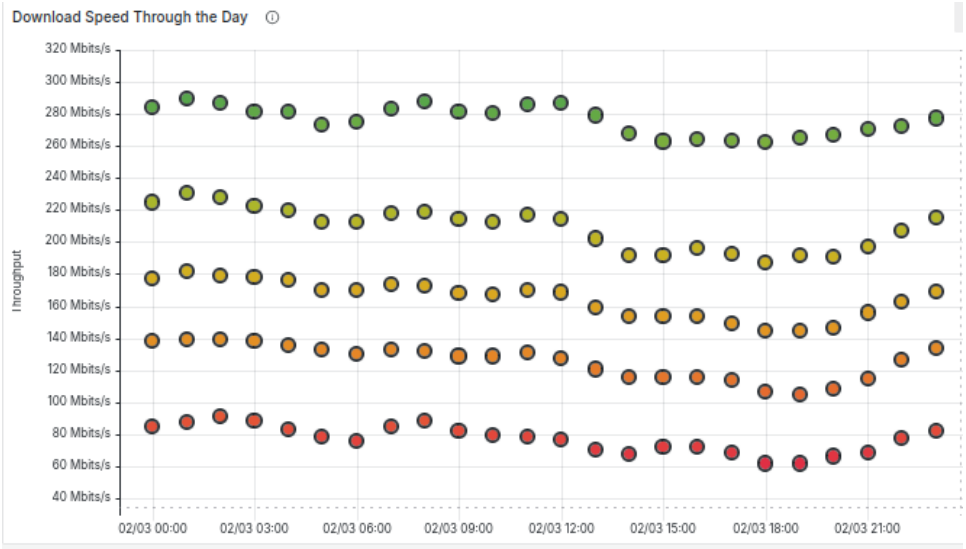

Figure 24. Hourly Downlink speeds of the Starlink system in Mbit/s.

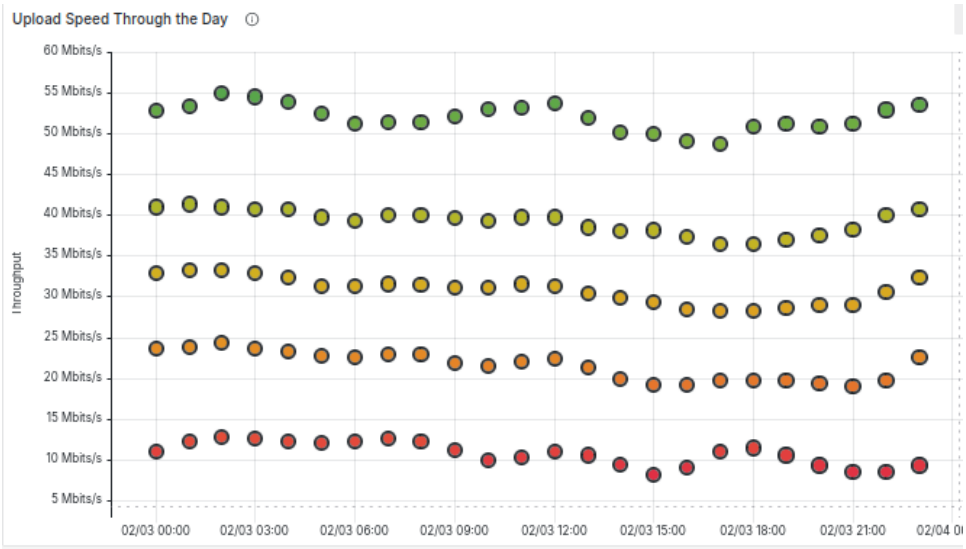

Figure 25. Hourly Uplink speeds of the Starlink system in Mbit/s.

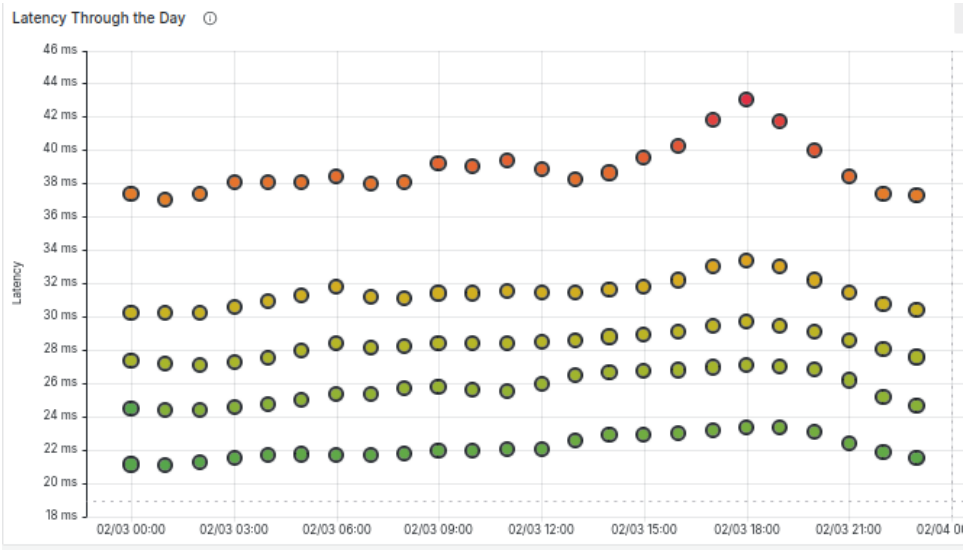

Figure 26. Hourly Delay (RTT) of the Starlink system in milliseconds.

In conclusion, the Starlink performance exceeded the expectations, showing that the system continues to improve along the time, and that its performance remains stable along all the weekdays, only showing a little expected degradation during the period of 15:00 until 21:00. Nevertheless, we don't expect any difference in the Quality of Experience of the end users, since the throughput and RTT values remain in the same order of magnitude, and very similar to the values of the off-peak hours.

b. Ethernet and Fiber Optics Switch

The selection of the Ethernet and Fiber Optics Switch considered constraints such as an ingress protection rating of IP65 or higher to withstand heavy rainfall without adverse effects and the capability to support optical fiber connectivity compatible with both the drone's fiber optic specifications and the AP's SFP transceiver. Additionally, it needs to provide a minimum data transfer speed of 2.5 Gbit/s to fully utilize the AP's maximum performance capabilities.

Based on these requirements, we consulted Mikrotik's SFP compatibility list and evaluated available switches that met the minimum IP65 rating and supported a fiber optic speed of 2.5 Gbit/s. As a result, we selected the Mikrotik RB5009UPr+S+OUT, which features an IP66 rating, seven Gigabit Ethernet ports, one 2.5 Gbit/s Ethernet port, and a 10 Gbit/s SFP+ port.

Figure 27 - Mikrotik RB5009UPr+S+OUT.

2.4. Software Architecture and Integration with OVERWATCH Platform

The DJI M350 onboard computer is an NVIDIA Jetson Orin AGX Dev Kit running Ubuntu 20.04. The interface between the UAV and the onboard computer is made using the DJI E-Port Dev Kit, which allows for sending commands to the UAV from the onboard computer and receiving sensor data.

The onboard computer runs multiple ROS software modules based on the DJI SDK, which is responsible for interfacing data received and commands sent to the UAV with the ROS framework. This results in several ROS topics with messages such as camera video streams, gimbal data, flight status, UAV pose, GPS data, battery status, and the time on the onboard PC2, as well as makes available topics in which command messages can be published and are then converted to the appropriate format using the SDK.

The ELISTAIR SAFE-T2 tethering system, in addition to providing continuous power to the UAV, also provides an optical fiber connection that is used to connect the onboard PC with the tethering system. Furthermore, a ground station computer is connected to the tethering system via ethernet, which, in addition to making the ROS topics from the UAV-onboard PC connection available, also allows to publish additional messages to ROS with data collected from the ELISTAIR system, including tether cable tension, voltage and current of the UAV power connection, the current cable length, temperature of the tethering system, torque applied to the tether cable, and current flight time of the UAV.

The ground station computer is also responsible for interfacing ROS with RabbitMQ, transporting topics from ROS to Rabbit MQ regarding GPS data, relative altitude, flight status, and onboard PC time. RabbitMQ is then used to transport data from the FCS to OVERWATCH dashboard.

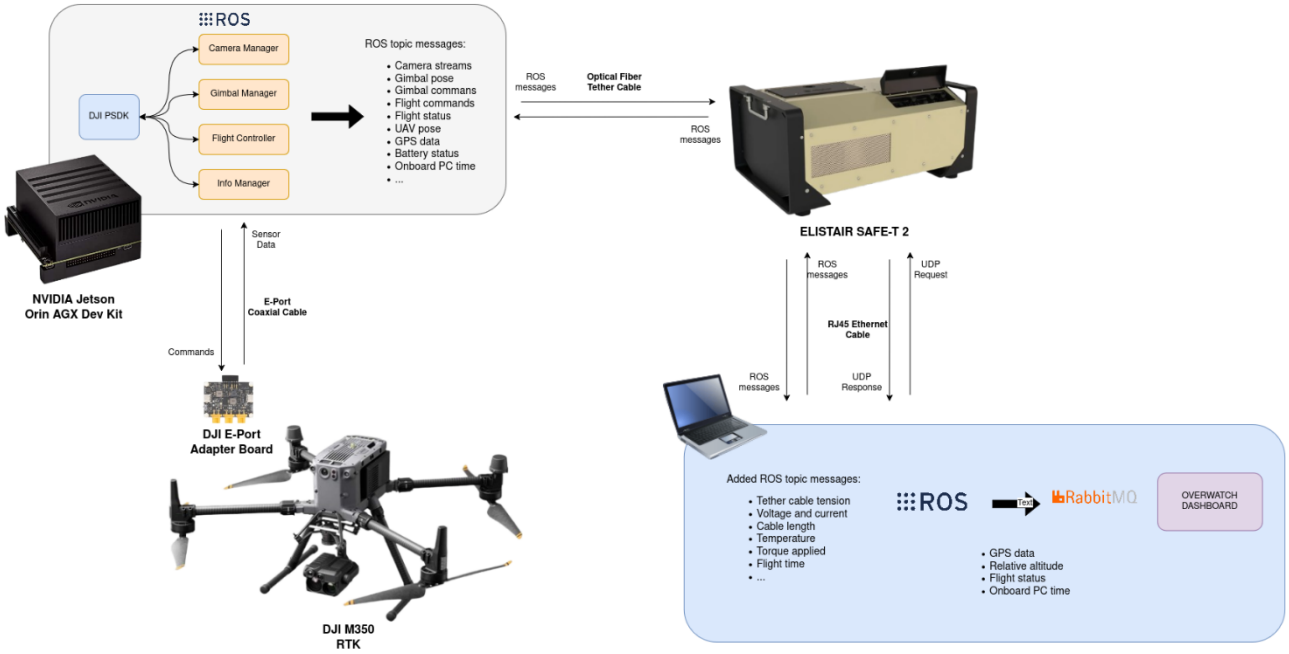

Figure 28. Tethered Drone Software Architecture.

In Figure 28 is depicted the tethered drone software architecture. The ground station computer subscribes the "*/dji_m350/gps*" and "*/dji_m350/relative_altitude*" ROS topics, mentioned in Table 5 and sends the status message with the format detailed in Table 12 periodically, every 3 seconds with the most recent data available from ROS.

Table 11. Format of status message sent through Rabbit MQ.

VARIABLE	Description	Data Type
altitude	UAV above ground level, relative altitude	float
coordinates	Array with UAV longitude and latitude	[float, float]
name	UAV Name	string
droneID	UAV Unique Identifier	string
owner	UAV partner owner	string
status	UAV current status (UP, DOWN, IDLE)	string
timestamp	Onboard PC current timestamp	String(YYYY-MM-DD T HH:mm:ss Z)

Finally, Figure 29 and Figure 30 validate the correct operation of this communication between ROS and the OVERWATCH dashboard.

```
(ow) ubuntu@overwatch:~/overwatch-code$ python rabbitmq_snippet.py
Sent Data
{'altitude': 79.37528228759766, 'coordinates': [-8.607622245084118, 41.178995926662594], 'name': 'Fallback_Connectivi
ty_Drone', 'droneId': 'TBD', 'owner': 'INESCTEC', 'status': 'TBD', 'timestamp': '2025-01-30T11:50:43.008052Z'}
Sent Data
{'altitude': 79.3541488647461, 'coordinates': [-8.607621581126043, 41.17899595848798], 'name': 'Fallback_Connectivity
_Drone', 'droneId': 'TBD', 'owner': 'INESCTEC', 'status': 'TBD', 'timestamp': '2025-01-30T11:50:46.011811Z'}
Sent Data
{'altitude': 79.38585662841797, 'coordinates': [-8.60762101057302, 41.17899618480149], 'name': 'Fallback_Connectivity
_Drone', 'droneId': 'TBD', 'owner': 'INESCTEC', 'status': 'TBD', 'timestamp': '2025-01-30T11:50:49.015665Z'}
Sent Data
{'altitude': 79.30130004882812, 'coordinates': [-8.607621203738898, 41.17899640857132], 'name': 'Fallback_Connectivit
y_Drone', 'droneId': 'TBD', 'owner': 'INESCTEC', 'status': 'TBD', 'timestamp': '2025-01-30T11:50:52.019475Z'}
Sent Data
{'altitude': 79.30130004882812, 'coordinates': [-8.607621298896149, 41.17899679357186], 'name': 'Fallback_Connectivit
y_Drone', 'droneId': 'TBD', 'owner': 'INESCTEC', 'status': 'TBD', 'timestamp': '2025-01-30T11:50:55.023157Z'}
Sent Data
{'altitude': 79.3092269897461, 'coordinates': [-8.607622154543742, 41.17899790497604], 'name': 'Fallback_Connectivity
_Drone', 'droneId': 'TBD', 'owner': 'INESCTEC', 'status': 'TBD', 'timestamp': '2025-01-30T11:50:58.027093Z'}
```

Figure 29. Ground station computer sending ROS data periodically, through RabbitMQ connection.

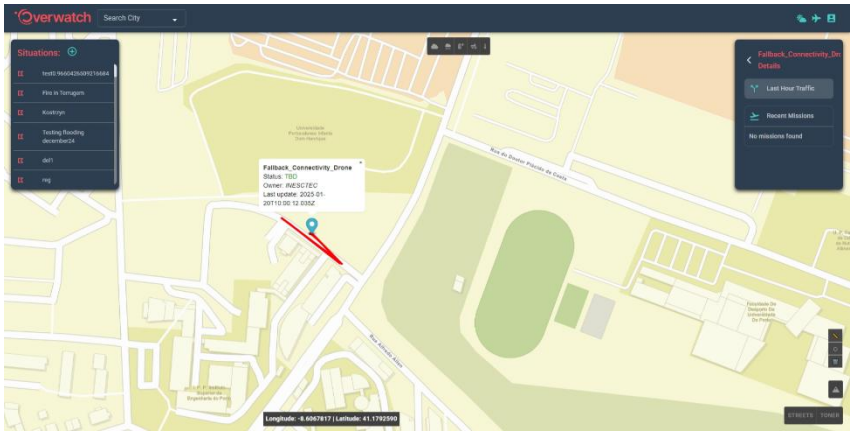

Figure 30. INESCTEC Fallback Connectivity Drone represented in OVERWATCH dashboard.

2.5. INESCTEC Tethered System Graphical User Interface

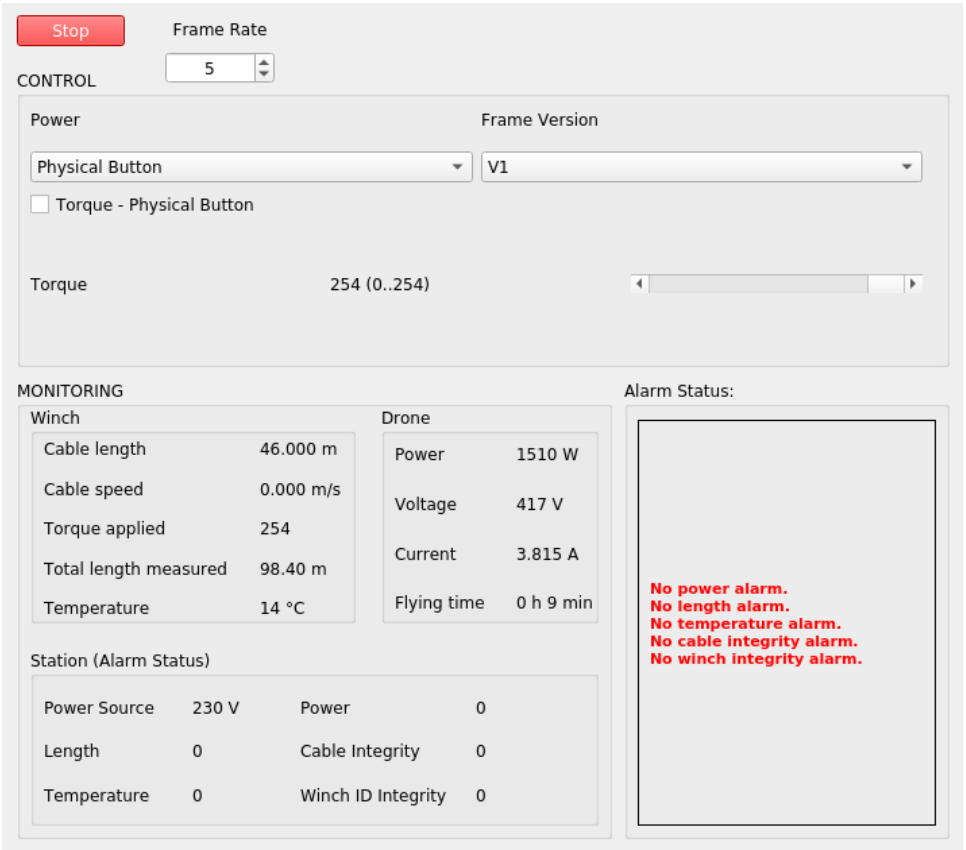

Figure 31. INESCTEC Tether System Graphical User Interface, with data acquisition during a tethered drone flight.

Figure 31 shows the **RQT SAFET GUI**, which serves as a graphical user interface for controlling and monitoring the SAFE-T2 GCS system. Below is an explanation of its key components:

Control Section:

- **Frame Rate**: Allows the user to set the update rate for monitoring data, displayed in frames per second.
- **Power Control**
- Dropdown menu to select the power mode (e.g., "Physical Button").
- Checkbox and slider to adjust the torque manually, within a range of 0 to 254.
- **Frame Version**: Dropdown menu to select the specific version of the communication frame being used.

Monitoring Section:

- **Winch Parameters**
- **Cable Length**: Displays the length of the deployed cable in meters.
- **Cable Speed**: Indicates the speed at which the cable is moving (m/s).
- **Torque Applied**: Shows the amount of torque being applied to the winch.
- **Total Length Measured**: Displays the total length of the cable used in the current operation.
- **Temperature**: Monitors the winch system's temperature in degrees Celsius.
- **Drone Parameters**:
- **Power**: Displays the current power consumption in watts.
- **Voltage**: Shows the current voltage supplied to the drone.
- **Current**: Indicates the current draw (amperes).
- **Flying Time**: Tracks the total flight duration of the drone.
- **Station (Alarm Status)**:
- Monitors various system parameters like power source voltage, total power consumption, cable length, temperature, and the integrity of the winch or cable.

Alarm Section:

- Displays the status of potential alarms related to the system's operation:
- **Power Alarm**: Indicates issues with power supply.
- **Length Alarm**: Alerts if the cable length exceeds limits.
- **Temperature Alarm**: Monitors for overheating.
- **Cable Integrity Alarm**: Detects any faults in the cable.
- **Winch Integrity Alarm**: Alerts on winch-related malfunctions.
- In the figure, all alarms are shown in **red text**, indicating that no alarms are currently active, which is normal.

Stop Button:

- A **red button** at the top left corner allows the operator to halt operations immediately if needed.

This GUI provides a centralized interface for real-time control and monitoring of both the winch and the drone systems associated with SAFE-T2 GCS. It allows the user to adjust operational parameters, track system performance, and respond to alarms efficiently.

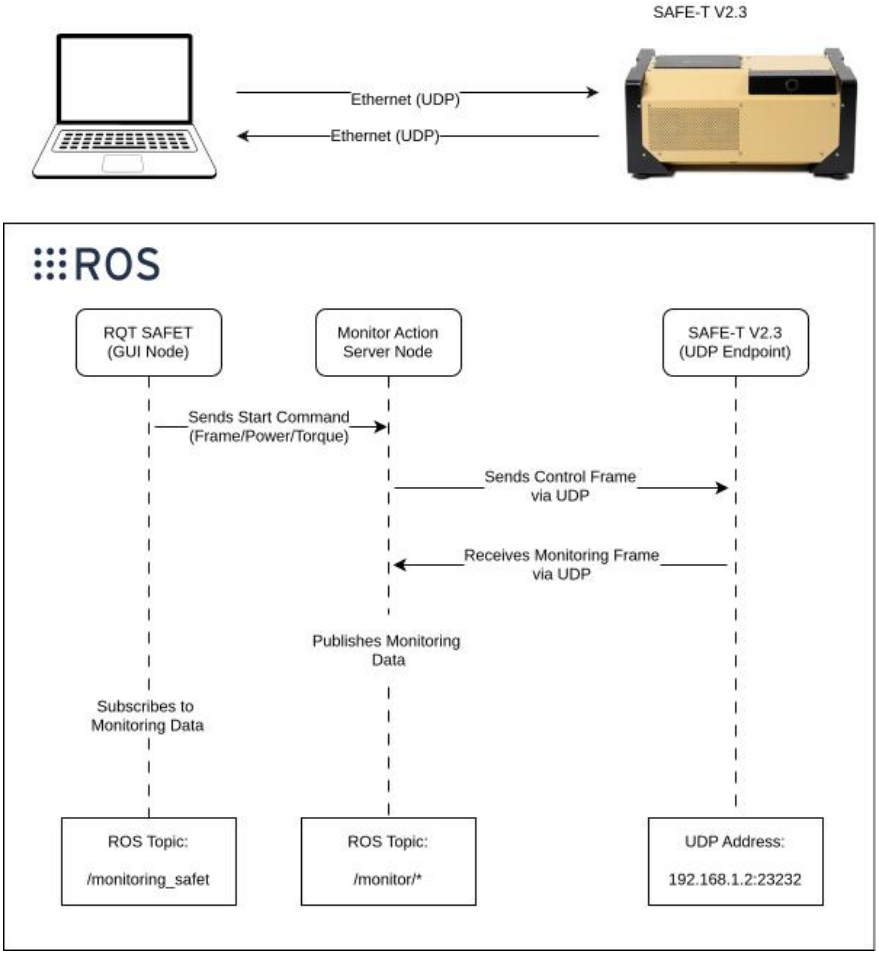

Figure 32. ROS interface between the Communications Laptop and SAFE-T2 GCS.

Figure 32 illustrates the integration of a SAFE-T2 GCS system with ROS (Robot Operating System) for monitoring and control purposes, using UDP-based Ethernet communication. The system consists of the following components, workflow and ROS TOPICS:

SAFE-T2 GCS Hardware:

- Acts as a UDP endpoint that sends and receives monitoring and control data.
- Operates at the IP address 192.168.1.2 on port 23232.

ROS Nodes:

- **RQT SAFET (GUI Node)**:
- Provides a graphical user interface for controlling and visualizing the monitoring data.
- Sends start commands to initiate the monitoring process, specifying parameters like frame, power, and torque.
- Subscribes to the ROS topic /monitoring_safet to receive real-time monitoring data.
- **Monitor Action Server Node**:
- Handles communication between the RQT SAFET GUI and the SAFE-T2 GCS system.

- Sends control frames via UDP to the SAFE-T2 GCS.
- Receives monitoring frames from the SAFE-T2 GCS and publishes the data to the ROS topic /monitor/*.

Communication:

- The GUI node sends commands to the Monitor Action Server Node, which translates them into control frames.
- The control frames are transmitted to the SAFE-T2 GCS hardware via UDP.
- The SAFE-T2 GCS sends monitoring frames back to the Monitor Action Server Node over UDP.
- The Monitor Action Server Node publishes the monitoring data to ROS topics for visualization and analysis.

Key ROS Topics:

- **/monitoring_safet**: Subscribed to by the GUI Node for accessing real-time monitoring data.
- **/monitor/**: General topic pattern where monitoring data from the SAFE-T2 GCS system is published.

3. Tethered Drone Protocols

3.1. Tether Drone Installation Procedure

The SAFE-T2 system includes two components: (1) the ground control station that is responsible for controlling the winch mechanism and being able to provide cable length (power and fiber optic) to the drone, (2) the air-module that is connected to the batteries of the drone and can provide power to the drone. One of the drawbacks of such a connection is that currently, the Air-Module, see Figure 33 and Figure 34, provides power to the drone motors and not to all the drone payload, which will provoke a decay in the drone autonomy for a period of time, currently estimated in about 2 to 3 hours' time. Therefore, this will require landing the drone and exchange batteries without disassembling the drone payload, a procedure that takes around five minutes to execute.

Figure 33. Tethered Drone Air Module

Figure 34. Tethered Drone Air Module connection to batteries and tether cable.

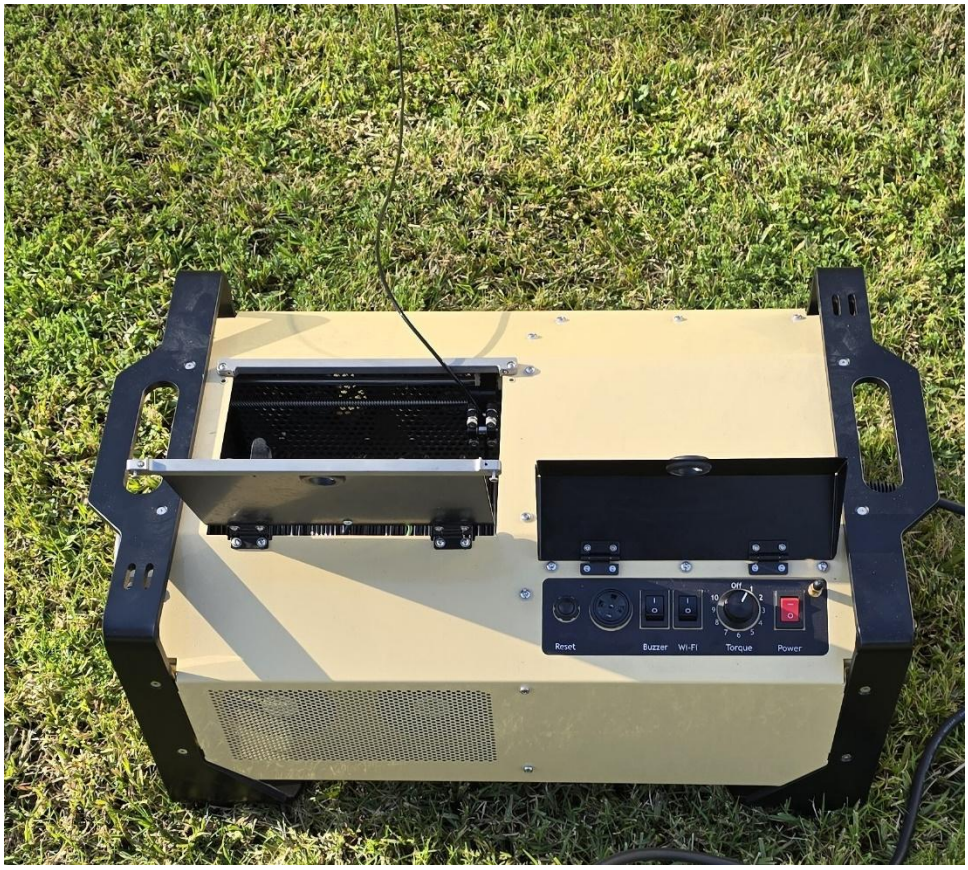

Figure 35. SAFE-T2 ground control systems and tether cable.

3.2. Tether Drone Initialization and Take-off Procedure

The SAFE-T2 requires to follow a setup initialization procedure to power up the Air Module and allow the DJI-M350 to take-off, namely:

- The drone batteries will have to be fully charged at the time of take-off procedure (with Min:95% charge and Tension Voltage higher than 50V).
- The tethered cable power must be switched off prior to the take-off.
- The batteries on the DJI-drone will have to be inserted into the drone, before the air module is connected.
- Afterwards, the tethered cable can be connected to the Air Module.
- Only then, can the tethered ground station be turned on, and also the drone. After this procedure the AIR module led will turn red.
- Turn on the micro cable at the SAFE-T2 ground control station. Wait for 6 seconds, the Air Module LED should turn on to green light. In case of malfunction please repeat the procedure.

Figure 36. Tethered Drone positioned and ready prior to Take-off.

As soon as the drone starts the take-off procedure as displayed in Figure 36, it should follow a straight trajectory upwards. The flight trajectory should have an upward velocity of up to 2m/s so the tethered cable stretches in the right direction without exceeding maximum tension.

During the flight the drone altitude should be adapted to the wind conditions, in case an alert appears in the DJI controller module. If, for some reason, the energy drops below 200 Watts, this means that the drone will be running on batteries and not being powered by the tethered system.

When landing the trajectory should be slow, so the tethered cable enrolls in a proper manner. At 1 meter from the ground, the trajectory should be diagonal, to try that the tethered cable stays stuck below the drone, and it's not damaged by the drone propellers.

After the landing, the SAFE-T2 ground station should turn off the power cable before powering off the drone, in order to avoid damage to the Air Module. Afterwards, the drone can be powered off. After 2 min all tethered drone systems can be powered off completely.

4.Field Tests and Validation

The system was fully assembled and tested on the ground in a laboratory environment. After all systems were validated both hardware and software it was tested in flight. The DJI customized drone is fully capable of carrying the payload and all the systems worked. In the following link, https://drive.inesctec.pt/s/LmLKbFHAkEAde3X there is a video of the drone flying in full payload working mode at ISEP. The drone was tested at about 50 meters altitude, which is the maximum altitude the drone can fly to in the designed locations. The drone was tested at ISEP premises, see Figure 37 and also at FADEUP campus, see Figure 38. Video from the flight is available in the following link https://drive.inesctec.pt/s/JynNopnYyaSxjW2.

The tests consisted of testing all the FCS systems and subsystems and the connectivity link between the drone and Overwatch C2 through the satellite backhaul. This was achieved with success, concluding the work related to the development of OVERWATCH FCS. Now in future work and in WP4 developments additional tests are now being planned in remote locations, for preparing OVERWATCH pilot in Portugal. The additional tests will focus on improving the available bandwidth of the system and checking the endurance and the autonomy of the drone during the flight. The take-off procedure takes 5 minutes after having arrived and deployed all the necessary equipment at the site. The drone autonomy is not directly affected by the wind-speed, despite the motors will consume more current, since the motors are always powered by the tether system, But is affected by the power consumption of the drone payload that runs on the drone batteries. This is a current limitation of the SAFE-T2 system but also works as an assurance that the end-user does not forget the drone in the air. The estimated flight time is currently 3 to 4 hours, with 5 min landing and take-off time to put on new batteries on the drone.

The endurance of drone currently is limited by the DJI-M350 flight conditions.

Figure 37. Tethered Drone in flight at ISEP Campus.

Figure 38. Tethered Drone in flight at FADEUP campus.

5. Conclusions

The Fallback Communication System **(FCS)** has demonstrated its effectiveness in providing a **resilient, redundant, and rapidly deployable** communication solution for emergency response. By integrating **tethered UAVs, advanced communication payloads, and satellite backhaul**, the system ensures continuous connectivity, even in areas with compromised infrastructure.

The results from field tests confirm that the **FCS is reliable, scalable, and capable of maintaining high-speed data transmission** under challenging operational conditions. The system's seamless integration with the **OVERWATCH platform** further enhances real-time monitoring, decision-making, and coordination among field teams and command centers.

This deliverable details the development of the **Fallback Communication System** within the **OVERWATCH** project. The report provides an in-depth description of the system components at both the hardware and software levels, with a particular focus on the **tethered drone system**. The system is divided into two major modules: (1) **Ground Module:** Incorporates the **SAFE-T2 system**, responsible for controlling the drone. The SAFE-T2 system is connected via a power and fiber optic link to the air module of the drone; (2) **Air Module:** This is the aerial component of the tethered system, which supplies power to the drone's batteries during flight, thereby significantly extending its operational endurance.

To enhance the autonomous control of the drone, a **ROS-based framework** was developed within the **OVERWATCH** project. This framework allows seamless control of both the SAFE-T2 system and the drone, improving the transparency of drone operations for the user. Additionally, software was developed to translate ROS commands into **RabbitMQ messages**, facilitating communication between the drone's tether system and the **OVERWATCH dashboard**.

During validation flights, the **tethered communication system** successfully transmitted data remotely while operating in **Porto, Portugal**, with the **Command and Control (C2) dashboard** located in **Sicily, Italy**. This was achieved by leveraging **Starlink connectivity**, which enabled seamless internet access. The system also includes an onboard Wi-Fi **access point**, providing emergency communications for other systems within a disaster-stricken area.

The system has been validated in-flight and is fully operational. Future work will focus on **enhancing autonomy, improving reliability, and increasing data throughput** by integrating new antennas onboard the drone to optimize communication performance.

References

References included as hyperlinks in the text.