

CyTEF – Final Presentation



ESEC/REDU

09/2022

CyTEF Team

Summary



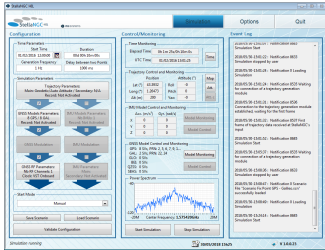
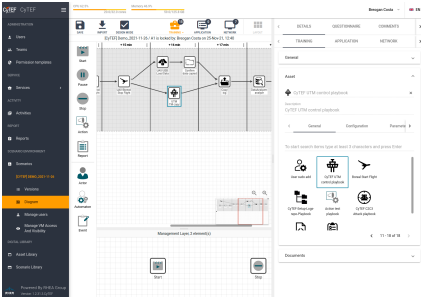
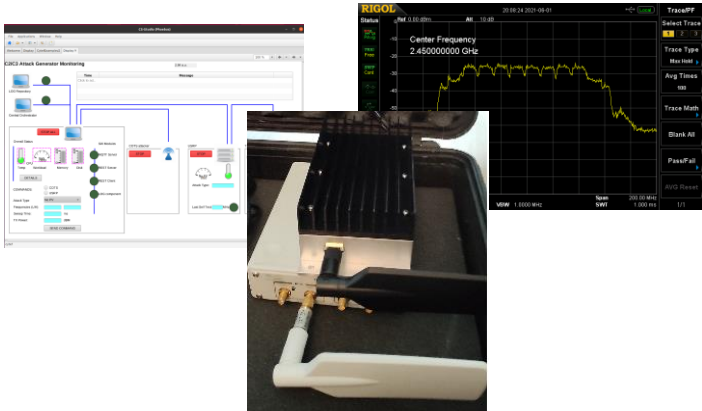
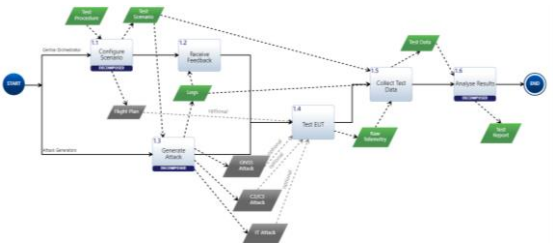
Time	Topic	Speaker
10:00-10:05	Welcome	R. Lucas Rodriguez, ESA NAVISP Technical Programme Office
10:05-10:10	Project Introduction	G. Caparra, Technical Officer, ESA
10:10-11:00	Project Implementation and Results	J. Torres, Project Manager, Telespazio Belgium
11:00-11:30	Question and Answers	Moderator: G. Caparra



Summary

- Project Implementation. (5 min)
- Overall System Architecture and Components. (25 min)
 - Central Orchestrator
 - C2/C3 Attack Generator
 - GNSS Attack Generator: Stella + COTS
 - IT Attack Generator
 - Data Analyser
- Proof of Concept: Systems Under Test and Premises (5 min)
 - Boreal Drone
 - AI Robot Drone and DJI Drones
 - Test Premises: RMA Chamber and DronePort
- Legal Framework for Jamming in Belgium (5 min)
- Achievements. Current and following steps. Business Model (5 min)

Consortium



Purpose and Rationale

✈️ Cyber Security Test and Evaluation Facility

✈️ Proof-of-concept for a Test Facility able to:

- ✈️ perform security and resilience tests on drones ...
- ✈️ against attacks in the
 - navigation,
 - RF communication and
 - cybersecurity domain.

✈️ Modular System:

- ✈️ Several attack generators
- ✈️ controlled by a central orchestrator
- ✈️ Post-analysis and report generation of the security assessment.

Purpose and Rationale

➤ Rationale for the project:

- Growing spread in the use of UAVs for civil and military applications
- Availability of low-cost RF equipment and Jammer and Spoofing COTS
- Increasing number of attacks and their impact

Examples:

"In May 2020, 17 drones crashed during a holiday performance in the southwestern city of Chengdu. Police later found out that employees from another drone company had caused the crash with drone jammers, after their own bid to carry out the performance was rejected."

Similar events have been repeated in June and October 2021 in Kanzhaji and Shanghai.

Project Implementation

WP1: Operational and Regulatory Requirement Definition

- Gathering of stakeholders needs
- Regulatory State-of-art analysis
- Formal User Requirement definition
- Completed by: 27/07/2020

WP2: Definition and Engineering

- Formal System Requirement definition
- Model Based System Engineering
- Test Methodology Definition (Common-Criteria)
- Completed by: 22/01/2021

WP3: Implementation

- Gathering of stakeholders needs
- Formal System Requirement definition
- Test Methodology Definition (Common-Criteria)
- Completed by: 04/03/2022

WP4: Service Demonstration

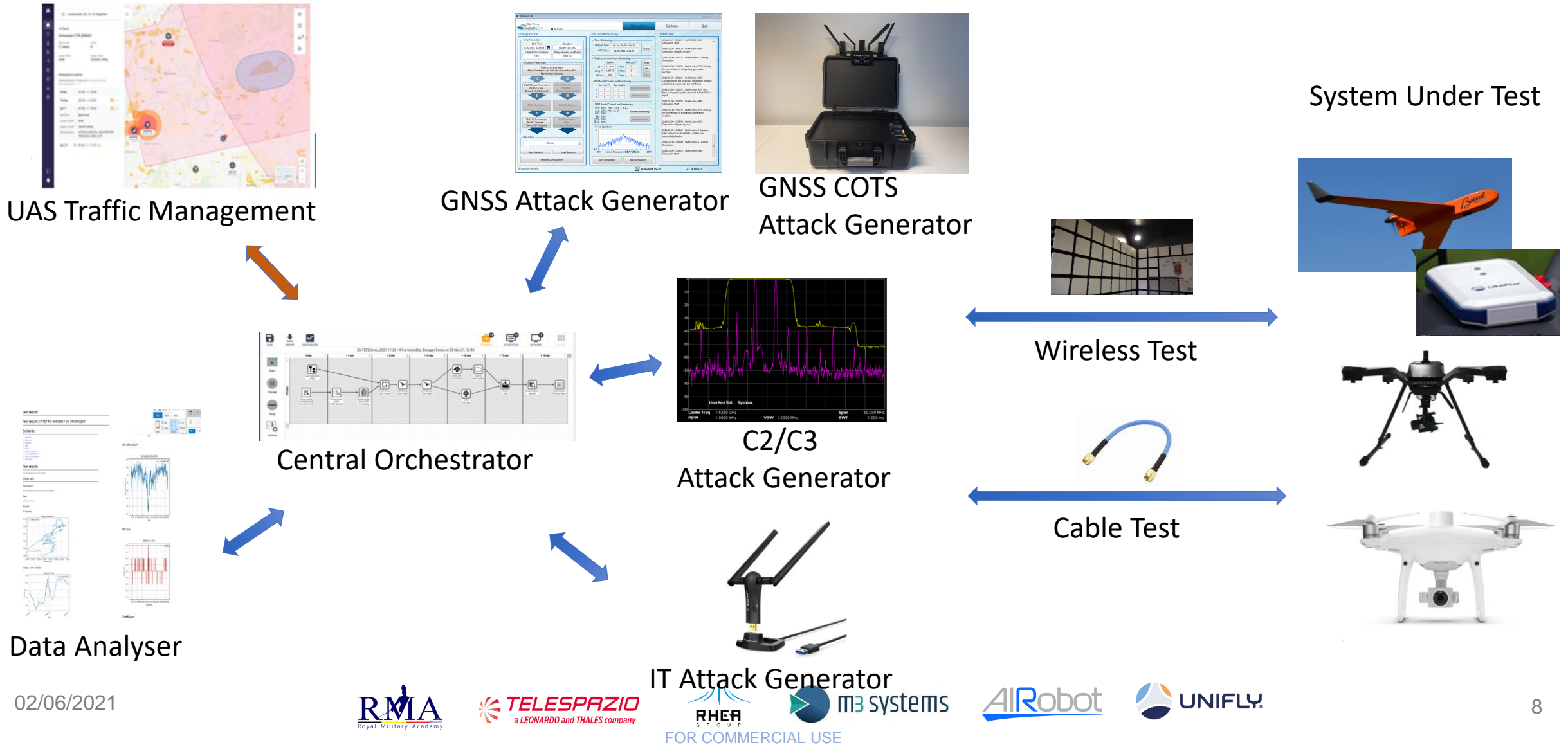
- PoC Demonstration
- Data Analysis
- Completed by: 13/04/2022



WP5: Dissemination

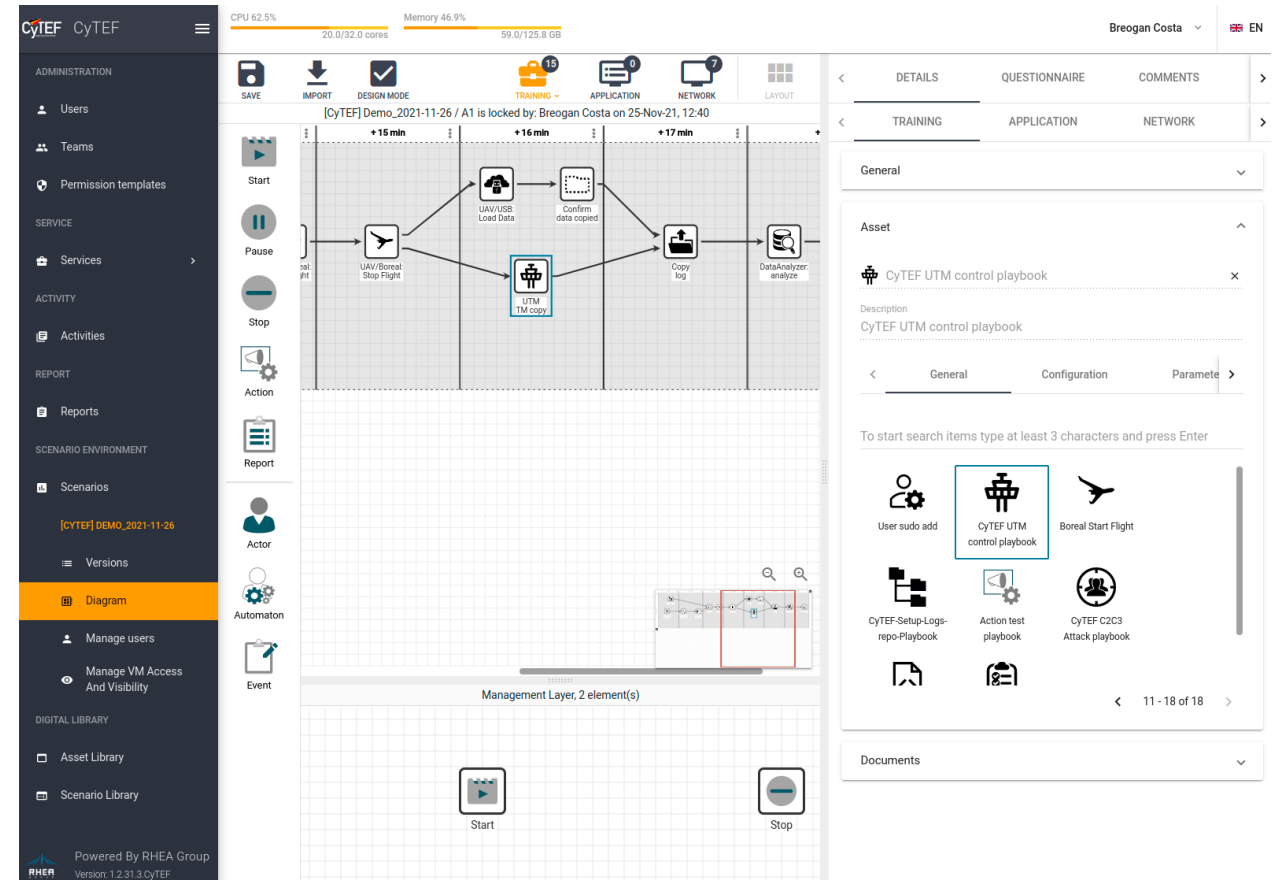
- Website, Events, etc

Overall View of the System




Central Orchestrator

- ✈ Orchestrates the subsystems
 - ✈ Supports AG deployed remotely
 - ✈ 2 protocols:
REST API and Ansible
- ✈ CITEF based
- ✈ Server deployed securely
- ✈ Central Repository of tests and test reports
- ✈ New scenarios created graphically



Central Orchestrator: Video


CyTEF

CPU 62.5%

20.0/32.0 cores

Memory 46.9%

59.0/125.8 GB

Breogan Costa

EN

ADMINISTRATION

Users

Teams

Permission templates

SERVICE

Services

ACTIVITY

Activities

REPORT

Reports

SCENARIO ENVIRONMENT

Scenarios

DIGITAL LIBRARY

Asset Library


Scenario Library

Report


Reports

Reports

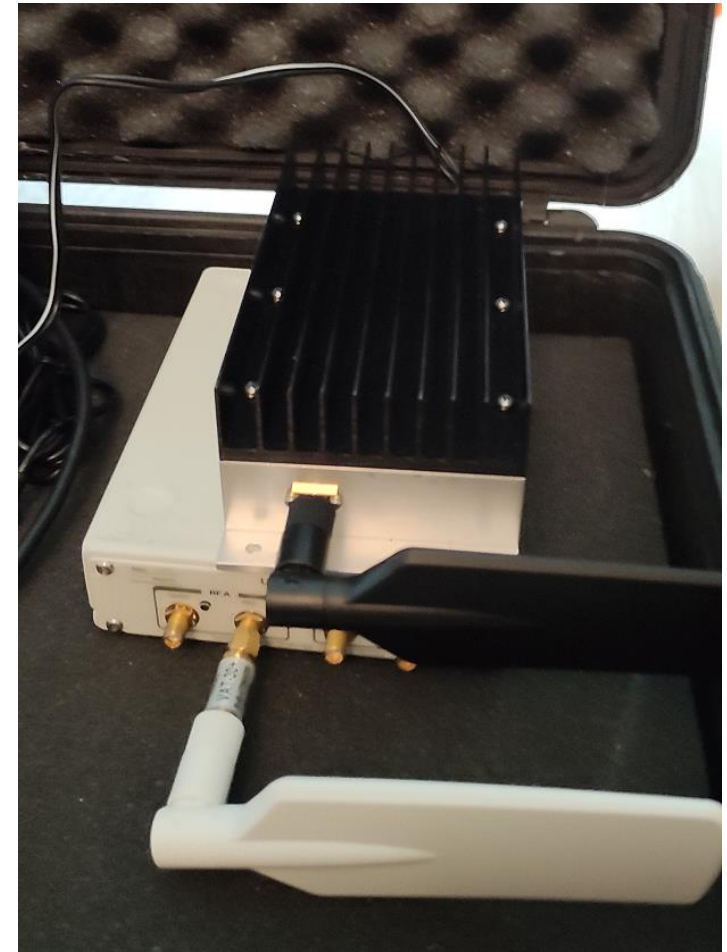
To start search items type at least 3 characters and press Enter

Name	Created	Scenario name	Actions
2021-11-02T19:59:50Z	02-Nov-21, 20:59	Report test	

1 total


Powered By RHEA Group
Version: 1.2.31.3.CyTEF

- The C2/C3 Attack Generator targets RF link between the UAV and Ground Station
- It supports the generation of multiple waveforms:
 - Chirp Waveform
 - OFDM (Wi-Fi) Waveform
 - GFSK (Bluetooth) Waveform
- Supported bands:
 - 5170-5251 and 5725-5851 MHz
 - 2400-2496 MHz Wi-Fi Band
 - 1610-1626 MHz Iridium Band
- C2/C3 Attack Generator supports advanced features:
 - Instantaneous Bandwidth up to 32 MHz (with 1 W peak power)
 - Random Frequency Hopping in milliseconds
 - Replay Attacking (Meaconing)
 - Self Testing and Monitoring of Hardware
- The C2/C3 Attack Generator is **very flexible** and can be adapted to **new needs**



C2/C3 AG: High level architecture

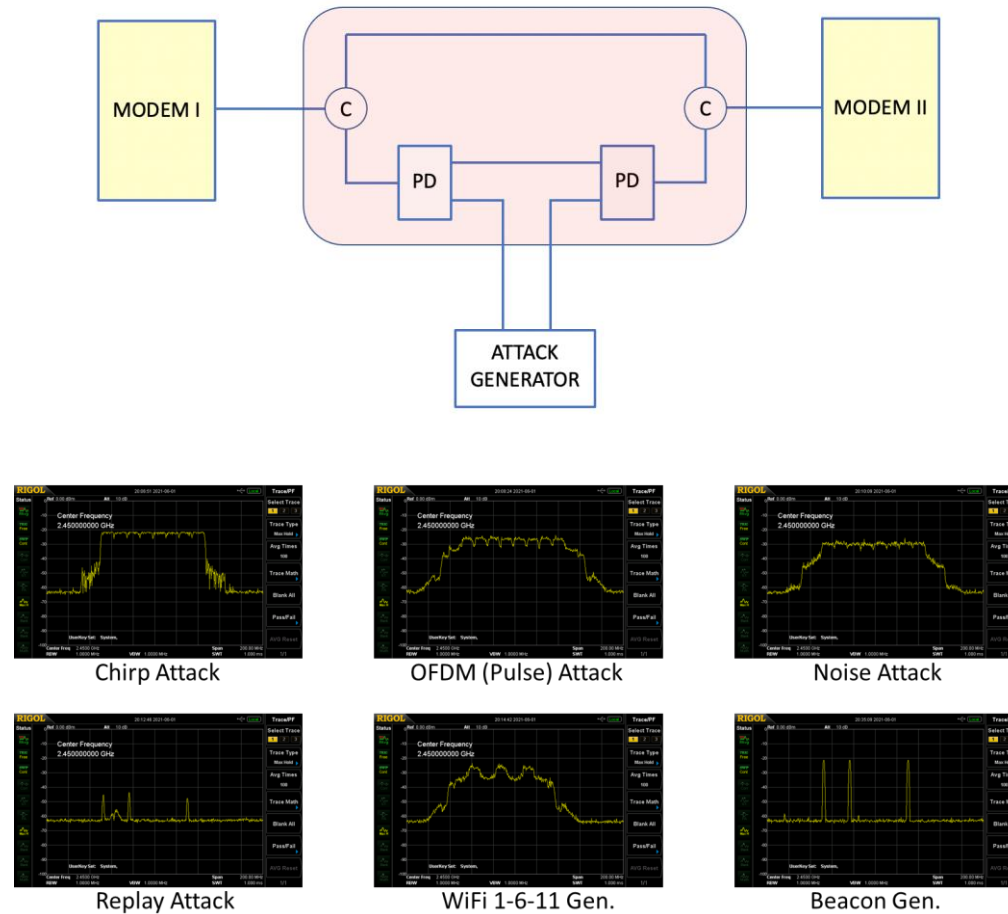
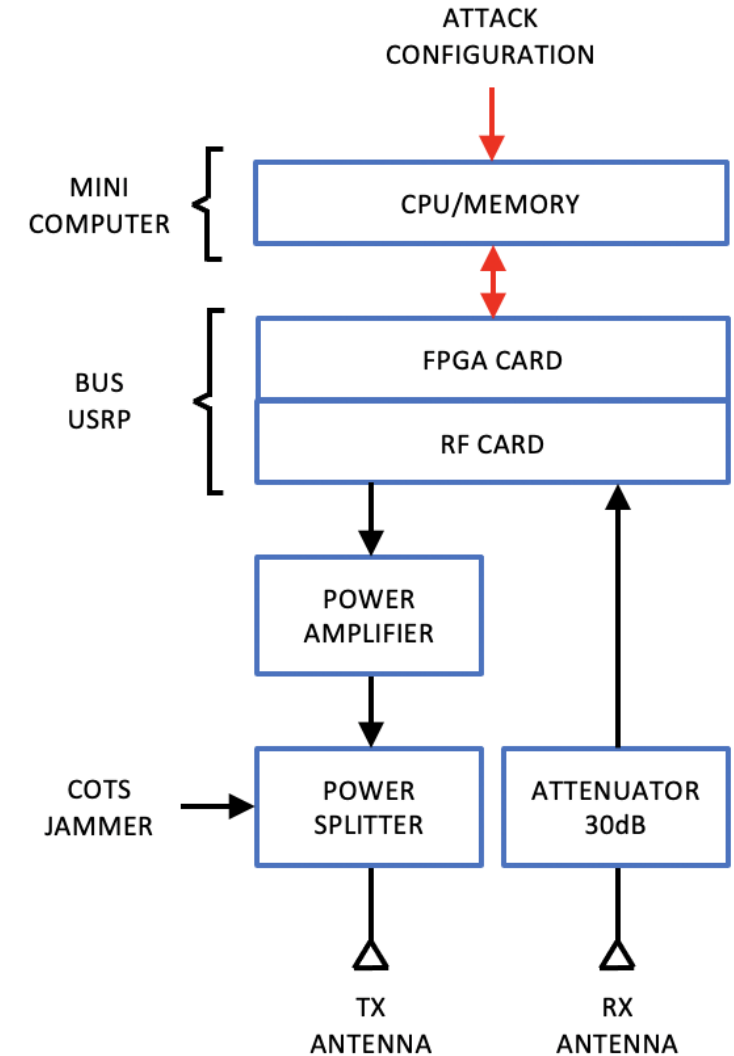


Fig 3. Max-hold spectrum analyzer results for different 2.4G attacks with 30 dB attenuator.



GNSS Attack Subsystem – STELLA SIMULATOR

► Characteristics

Highly Configurable GNSS Model

- Multi Constellation, Multi frequency GNSS (GPS, Galileo, GLONASS, Beidou, QZSS)
- Model Configuration (Satellite motion, broadcasted data, atmosphere perturbations, antenna management, power budget)

Real Time Trajectory Simulator

- Open Loop / Closed Loop

Open Real Time Data Flow

- Intermediate Data (IQ samples, Raw GNSS Data)

Easy to use GUI

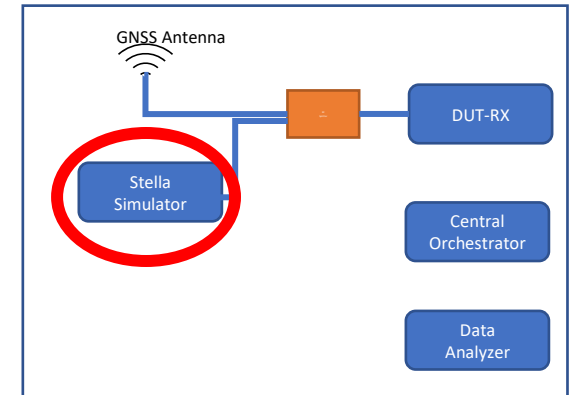
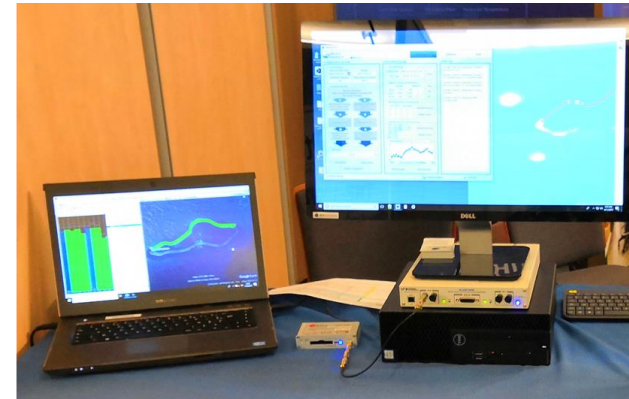
- Ergonomic GUI / Monitoring Widgets /API

GNSS Signal Generation:

- Multi Antenna, Multi Trajectories

Interference generation:

- Various ITF models available: DME/TACAN, VOR, WGN, JTIDS, NLFM, RADAR, etc...

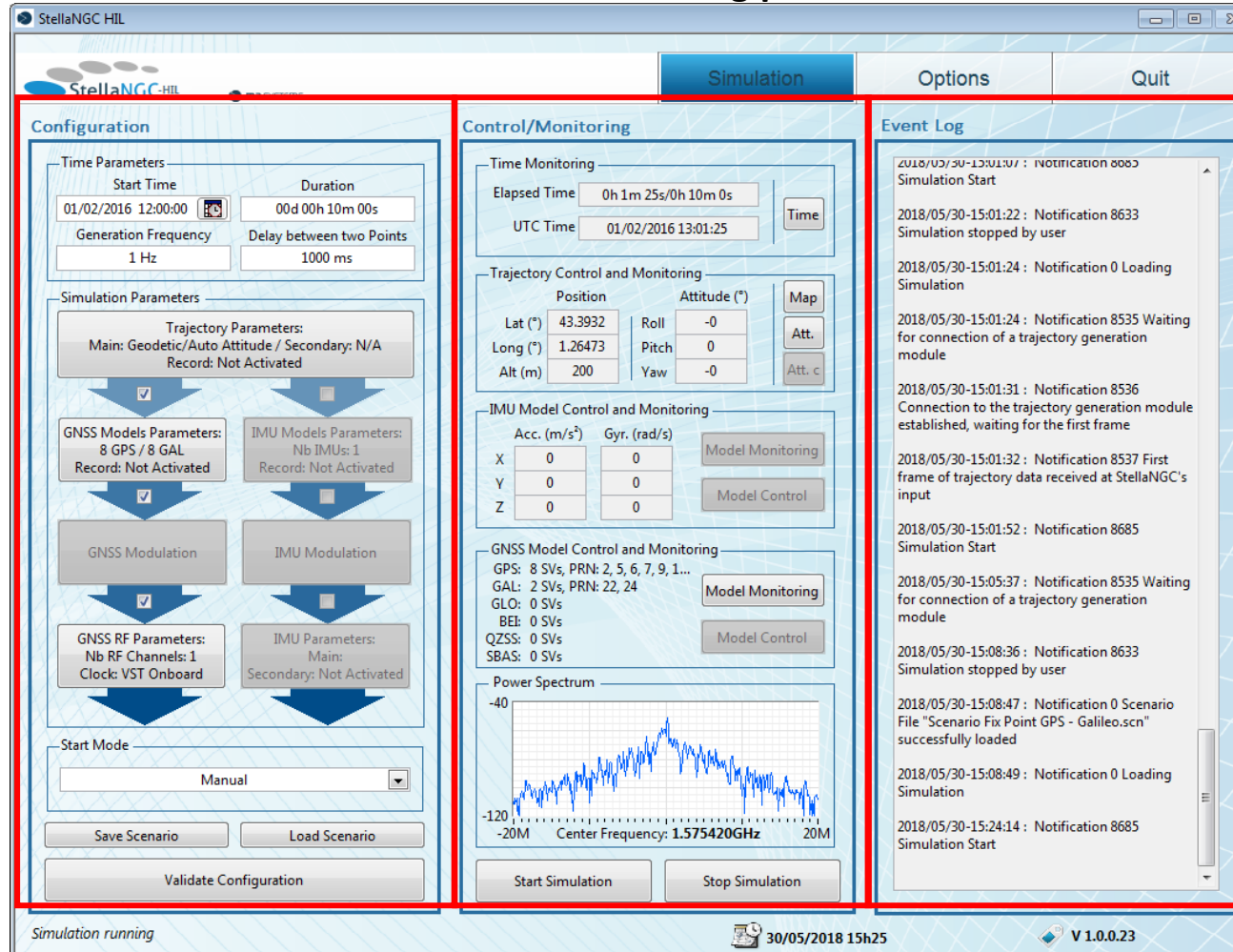


GNSS Attack Generator- STELLA SIMULATOR

► GUI

Control/monitoring panel

Configuration panel

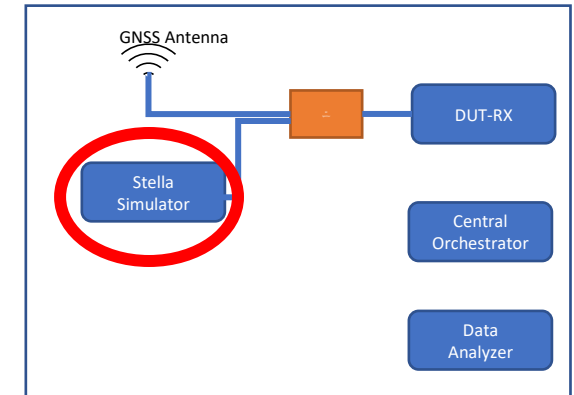


The screenshot displays the StellaNGC HIL GUI with three main panels:

- Configuration Panel:**
 - Time Parameters:** Start Time (01/02/2016 12:00:00), Duration (00d 00h 10m 00s), Generation Frequency (1 Hz), Delay between two Points (1000 ms).
 - Simulation Parameters:**
 - Trajectory Parameters:** Main: Geodetic/Auto Attitude / Secondary: N/A, Record: Not Activated.
 - GNSS Models Parameters:** 8 GPS / 8 GAL, Record: Not Activated.
 - IMU Models Parameters:** Nb IMUs: 1, Record: Not Activated.
 - GNSS Modulation:** (checked)
 - IMU Modulation:** (unchecked)
 - GNSS RF Parameters:** Nb RF Channels: 1, Clock: VST Onboard.
 - IMU Parameters:** Main: (checked), Secondary: Not Activated.
 - Start Mode:** Manual.
 - Buttons:** Save Scenario, Load Scenario, Validate Configuration.
- Control/Monitoring Panel:**
 - Time Monitoring:** Elapsed Time (0h 1m 25s/0h 10m 00s), UTC Time (01/02/2016 13:01:25).
 - Trajectory Control and Monitoring:** Position (Lat: 43.3932, Long: 1.26473, Alt: 200), Attitude (Roll: -0, Pitch: 0, Yaw: -0). Buttons: Map, Att., Att. c.
 - IMU Model Control and Monitoring:** Acc. (m/s²), Gyr. (rad/s). Buttons: Model Monitoring, Model Control.
 - GNSS Model Control and Monitoring:** GPS: 8 SVs, PRN: 2, 5, 6, 7, 9, 1...; GAL: 2 SVs, PRN: 22, 24; GLO: 0 SVs; BEI: 0 SVs; QZSS: 0 SVs; SBAS: 0 SVs. Buttons: Model Monitoring, Model Control.
 - Power Spectrum:** Graph showing frequency from -20M to 20M Hz, centered at 1.575420GHz.
 - Buttons:** Start Simulation, Stop Simulation.
- Event Log Panel:**
 - 2018/05/30-15:01:07 : Notification 8863 Simulation Start
 - 2018/05/30-15:01:22 : Notification 8633 Simulation stopped by user
 - 2018/05/30-15:01:24 : Notification 0 Loading Simulation
 - 2018/05/30-15:01:24 : Notification 8535 Waiting for connection of a trajectory generation module
 - 2018/05/30-15:01:31 : Notification 8536 Connection to the trajectory generation module established, waiting for the first frame
 - 2018/05/30-15:01:32 : Notification 8537 First frame of trajectory data received at StellaNGC's input
 - 2018/05/30-15:01:52 : Notification 8685 Simulation Start
 - 2018/05/30-15:05:37 : Notification 8535 Waiting for connection of a trajectory generation module
 - 2018/05/30-15:08:36 : Notification 8633 Simulation stopped by user
 - 2018/05/30-15:08:47 : Notification 0 Scenario File "Scenario Fix Point GPS - Galileo.scn" successfully loaded
 - 2018/05/30-15:08:49 : Notification 0 Loading Simulation
 - 2018/05/30-15:24:14 : Notification 8685 Simulation Start

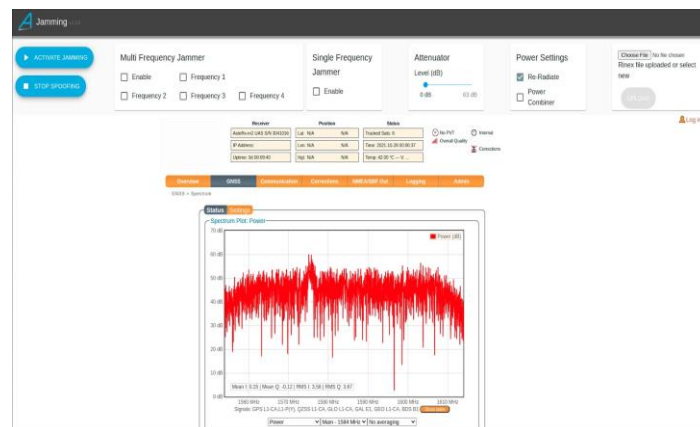
Simulation running 30/05/2018 15h25 V 1.0.0.23

Event log



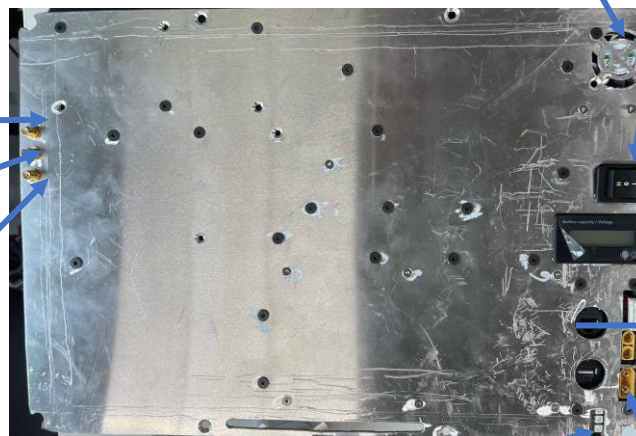
COTS-GNSS Attacker

- COTS Jammer and COTS Spoofer
- Multi frequency and multi constellation
- Combines signals for cable configuration
- Integrated Spectrum Analyzer
- Portable & Battery powered



TCP-IP over ethernet

GPS-IN
GPS-OUT
ANT-OUT



COOLING
POWER
SELECTOR

STATUS-LED

EXTERNAL
POWER

BATTERY
CHARGER



IT Attack Generator

Some UAVs use standard Wi-Fi links for **Command and Control** communication or to control their **payloads**.

This attacker exploits their known vulnerabilities over Wi-Fi.

Attacks are configurable and they cover at least:

- Wi-Fi traffic capture
- Wi-Fi DeAuth
- Evil Twin
- Brute Force attacks



ITAG Details

- ITAG can be deployed as VM or Physical PC with connected WiFi network interfaces.
- It's based on a Kali Linux image, extended with auxiliary components like developed Attack Generator server and discovery/attack tools
- Discovery/Attack toolchain designed in a "Plugin" way, which allow extending the list of attacks without braking changes on integration or reporting sides
- ITAG integration and control done by Central Orchestrator Ansible capabilities which provides automated scheduled behavior
- Manual interactions also possible to be performed on ITAG through the CO CITEF user interface.

Data Analyser

- Analyses raw data for each complete or failed test
- Evaluates data according preconfigured KPIs
- Generates reports in HTML and PDF formats

Final report

[CyTEF] TP-CC-001/002

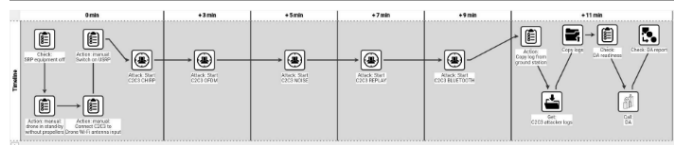
Date

07 April 2022 15:31 UTC

Description

CyTEF TP-CC-001/002 test for SAT

Test plan sequence



Test sequence list

- Check: SRP equipment off was executed with delay: 0 min
- Action: manual: Switch on USRP was executed with delay: 0 min
- Action: manual: Connect C2C3 to Drone Wi-Fi antenna input was executed with delay: 0 min
- Action: manual: drone in stand-by without propellers was executed with delay: 0 min
- Attack: Start C2C3 CHIRP was executed with delay: 0 min, with parameters: run_target=C2C3_Attacker duration=30 target=c2c3 command=startAttack lowfreq=5170 highfreq=5250 sweeptime=2 txpower=30 attacktype=1 attackparam=1

Type

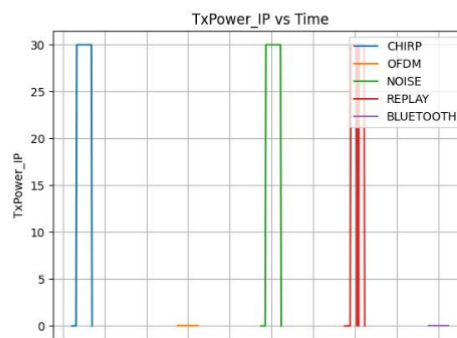
C2C3

Parameters

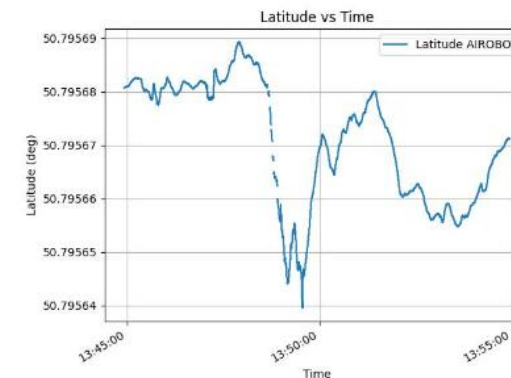
C2C3_BLUETOOTH : run_target=C2C3_Attacker duration=30 target=c2c3 command=startAttack lowfreq=-1 highfreq=-1 sweeptime=2 txpower=30 attacktype=4 attackparam=0.5 C2C3_REPLAY : run_target=C2C3_Attacker duration=30 target=c2c3 command=startAttack lowfreq=5170 highfreq=5250 sweeptime=2 txpower=30 attacktype=4 attackparam=0.5 C2C3_NOISE : run_target=C2C3_Attacker duration=30 target=c2c3 command=startAttack lowfreq=5170 highfreq=5250 sweeptime=2 txpower=30 attacktype=3 attackparam=0.5 C2C3_OFDM : run_target=C2C3_Attacker duration=30 target=c2c3 command=startAttack lowfreq=5170 highfreq=5250 sweeptime=2 txpower=30 attacktype=2 attackparam=0.2 C2C3_CHIRP : run_target=C2C3_Attacker duration=30 target=c2c3 command=startAttack lowfreq=5170 highfreq=5250 sweeptime=2 txpower=30 attacktype=1 attackparam=1

Results

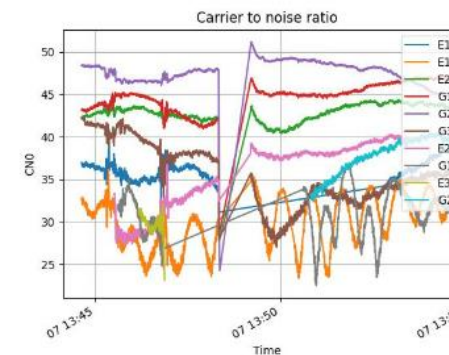
TXPOWER



Latitude vs time AIROBOT



GNSS : Carrier to Noise Ratio



Attacks on the drone

COTS_JAMMING attack

Start Time

Proof of Concept

- The design was validated with the implementation of a proof of concept
- All components in the overall design were implemented and demonstrated
- CO deployed in ESEC/Redu, Attack Generators in DronePort
- Three different types of drones.
- Cable configuration in GNSS and C2/C3 attacks.
- Air attacks against Wi-Fi link.
- DJI mini link tested in an anechoic chamber.

Locations



DronePort



RMA chamber



Redu (IT Infrastructure)

Systems Under Test



Airobot Custom

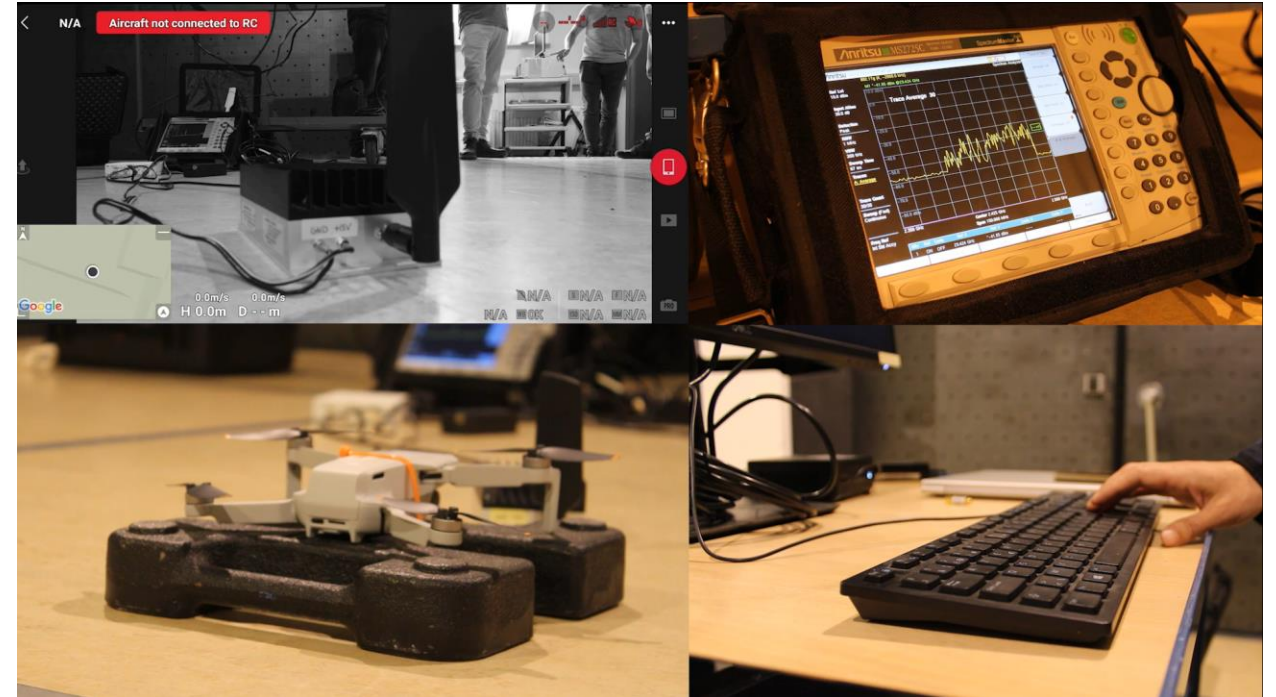


DJI Drones



Boreal

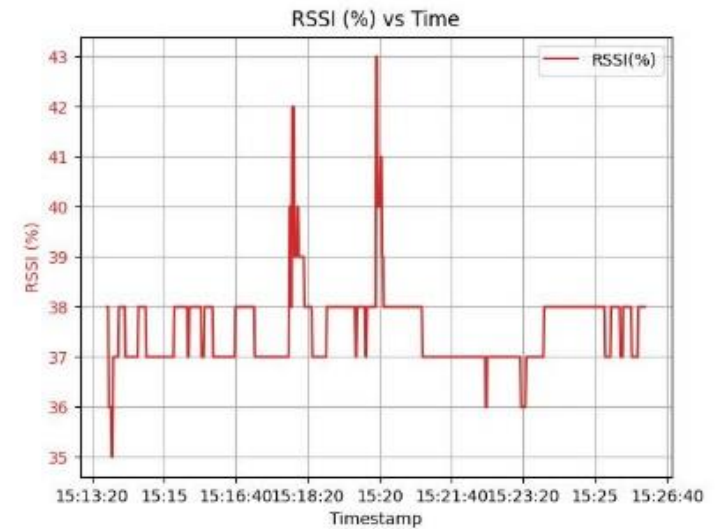
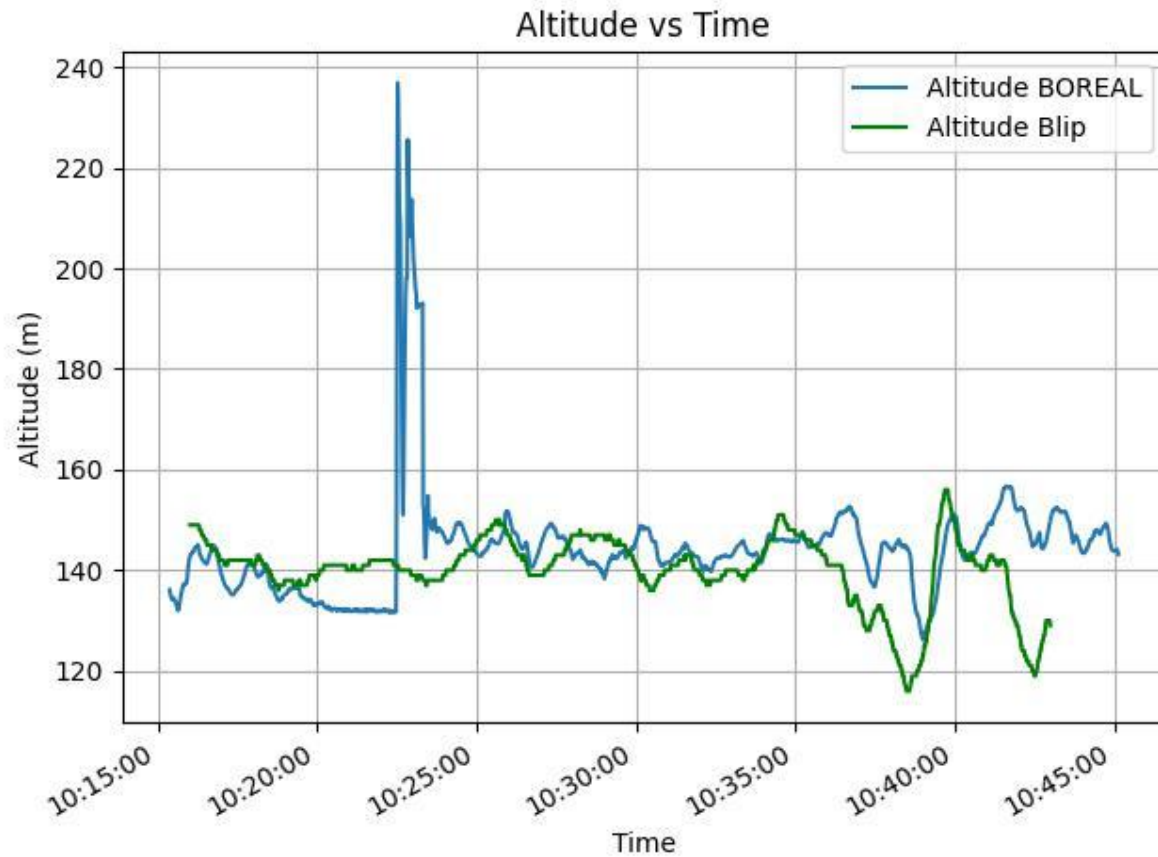
Proof of Concept (Videos)



Results

- Successful proof of concept executed on the 13/04/2022 in DronePort.
- 15 different test scenarios executed. 6 of them during the demo.
- Generated Reports are kept in the Central Orchestrator.
- All three reference drones were affected by the attackers
 - Different GNSS receivers and communication links have different levels of resilience
 - Dedicated drone communication protocols are more resilient to accidental and intentional interferences versus general purpose Wi-Fi
 - Interesting metrics are: required time and power until successful attack

Some examples of reports



Legal framework for Jamming in Belgium

- The general rule is that jamming is forbidden.
- Controlled in Belgium by BIPT/IBPT
- The use of Jammers is restricted to the following cases:
 - Fixed Places: Prisons, military terrains, etc.
 - Ad-hoc places: Limited in time, and location.
 - For testing and formation purposes: Limited in time and scope.
- Request to BIPT/IBPT is needed in advance
- Problem: Request from drone manufacturers to use jammers for testing their own drones
 - Use of agreed premises such as the future CyTEF

Business Model

- Certification of commercial/recreational drones according to standards
- Reference test facility for Defense drones and scenarios
- Leasing of equipment
- Support R&D activities for UAV and C-UAV

Proposed steps after project closure

- Reaching levels required as an approved evaluation facility
- Enhanced test methodology and normative survey
- Use of the facilities for a reference drone certification
- Multi-capability: several SUT in parallel
- General-purpose unmanned scenarios

Thank you for your attention!

Questions?

