

RESISTO: D4.2_ACTIVE AND PASSIVE SENSORS DEPLOYMENT PLAN



RESISTO

D4.2 – ACTIVE AND PASSIVE SENSORS DEPLOYMENT PLAN

Document Manager:	Rodoula Makri	ICCS	Editor
--------------------------	---------------	------	--------

Project Title:	RESilience enhancement and risk control platform for communication infraSTructure Operators
Project Acronym:	RESISTO
Contract Number:	786409
Project Coordinator:	LEONARDO
WP Leader:	TEI

Document ID N°:	RESISTO_D4.2_200515_01	Version:	1.0
Deliverable:	D4.2	Date:	15/05/2020
		Status:	APPROVED

Document classification	Public
--------------------------------	---------------

Approval Status	
Prepared by:	Rodoula MAKRI (ICCS)
Approved by: (WP Leader)	Giuseppe CELOZZI (TEI)
Approved by: (Coordinator)	Bruno SACCOMANNO (LDO)
Advisory Board Validation (Advisory Board Coordinator)	NA
Security Approval (Security Advisory Board Leader)	NA

CONTRIBUTING PARTNERS

Name	Company / Organization	Role / Title
Rodoula Makri, Panos Karaivazoglou, Apostolos Papafragkakis, Athanasios Panagopoulos, Nikolaos Lyras, Anargyros Roumeliotis, Takis Kelefas	ICCS	Senior Researchers, Electrical Engineers, Telecommunication Experts
Giuseppe Celozzi, Cosimo Zotti, Giuseppe Amato	TEI	Telecommunications Experts, Senior Researchers
Michael Skitsas, Nikolaos Koutras	ADI	Senior Researchers, Electrical Engineers, Defence and Security Specialists
Javier Valera, Jose Sanchez, Moisés Valeo	INT	Senior Researchers, Electrical Engineers, Defence and Security Specialists

DISTRIBUTION LIST

Name	Company / Organization	Role / Title
PMT	RESISTO CONSORTIUM	NA
Markus MULLER	EC DG REA	EC Programme Officer
General Public	NA	NA

REVISION TABLE

Version	Date	Modified Pages	Modified Sections	Comments
0.1	15.05.2019		All	Table of contents and draft sections
0.2	22.08.2019		All	Additions and partners contributions
0.3	15.10.2019		All	Request to D2.8 involved telecom operators to decide upon their final Use Cases, in order D4.2 to be finalized
1.0	15.05.2020		All	Final version

COPYRIGHT STATEMENT



© 2018-2021 This document and its content are the property of the RESISTO Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the RESISTO Consortium or the Partners detriment and are not to be disclosed externally without prior written consent from the RESISTO Partners. Each RESISTO Partner may use this document in conformity with the RESISTO Consortium Grant Agreement provisions.

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Program, under the Grant Agreement No 786409.

The views and opinions in this document are solely those of the authors and contributors, not those of the European Commission.

PROJECT CONTACT



LEONARDO
Via Puccini 2 – Genova – 16154 – Italy
Tel.: +39 348 6505565
E-Mail: bruno.saccomanno@leonardocompany.com

RESISTO PROJECT – PUBLISHABLE EXTENDED ABSTRACT

Communications play a fundamental role in the economic and social well-being of the citizens and on operations of most of the CIs. Thus they are a primary target for criminals having a multiplier effect on the power of attacks and providing enormous resonance and gains. Also extreme weather events and natural disasters represents a challenge due to their increase in frequency and intensity requiring smarter resilience of the Communication CIs, which are extremely vulnerable due to the ever-increasing complexity of the architecture also in light of the evolution towards 5G, the extensive use of programmable platforms and exponential growth of connected devices. The fact that most enterprises still manage physical and cyber security independently represents a further challenge. RESISTO platform is an innovative solution for Communication CIs holistic situation awareness and enhanced resilience (aligned with ECSO objectives). Based on an Integrated Risk and Resilience analysis management and improvement process availing all resilience cycle phases (prepare, prevent, detect, absorb, etc.) and technical resilience capabilities (sense, model, infer, act, adopt), RESISTO implements an innovative Decision Support System to protect communication infrastructures from combined cyber-physical threats exploiting the Software Defined Security model on a suite of state of the art cyber/physical security components (Blockchain, Machine Learning, IoT security, Airborne threat detection, holistic audio-video analytics) and services (Responsible Disclosure Framework) for detection and reaction in presence of attacks or natural disasters. Through RESISTO Communications Operators, will be able to implement a set of mitigation actions and countermeasures that significantly reduce the impact of negative events in terms of performance losses, social consequences, and cascading effects in particular by bouncing efficiently back to original and forward to operational states of operation.

EXECUTIVE SUMMARY

The present Deliverable D4.2 reports and describes the final list of the sensing systems and mechanisms that are provided by the RESISTO project to enhance the detection of intrusions and modern physical and/or combined cyber/physical threats. In this context the D4.2 is being considered as the follow up of the pervious Deliverable D4.1; in D4.2, all the upgrades and developments that took place in the meantime are also presented.

Furthermore, within D4.2 the way that these detection systems will be utilized, combined and orchestrated together to accommodate the RESISTO solution within the framework of the pilot use cases and relevant scenarios at the telecom pilot sites is given. All the relevant deployment details per sensing system are given, and also in respect to the corresponding Use Cases, already described in D2.8, where the specific sensing systems will be used and deployed during the pilot implementation in the framework of WP7, WP8 and WP9.

CONTENTS

ABBREVIATIONS	11
1. INTRODUCTION: OVERVIEW OF PHYSICAL THREATS DETECTORS - CONNECTION WITH THE USE CASES	13
1.1. Important clarifications for the D4.2 sensors – differences in relation to D4.1	14
1.2. Mapping of the threat detectors in respect to the RESISTO Use Cases	15
1.3. Relevant User requirements mapping	17
2. DIRECT DETECTION: AUDIO AND VIDEO ANALYTICS SYSTEM.....	19
2.1. Short description of the sensing system	20
2.1.1. Detection objectives of the sensing system – what is meant to be measured	22
2.2. General deployment requirements	22
2.3. Specific deployment of the sensing system in Use case 1: sub-scenario 2	22
2.3.1. Setup of the sensing system.....	22
2.3.2. Deployment phases of the sensing system	23
2.3.2.1. Lab tests of the sensing system	23
2.3.2.2. Preliminary short experiments with the sensing system	23
2.3.2.3. Foreseen final deployment	23
3. DIRECT DETECTION: UAV PLATFORM-BASED SURVEILLANCE SYSTEM.....	24
3.1. Short description of the sensing system	24
3.1.1. Detection objectives of the sensing system – what is meant to be measured	25
3.2. General deployment requirements	25
3.3. Specific deployment of the sensing system in Use case 2: sub-scenario 1 & 2	25
3.3.1. Setup of the sensing system.....	26
3.3.2. Deployment phases of the sensing system	26
3.3.2.1. Lab tests of the sensing system	26
3.3.2.2. Preliminary short experiments with the sensing system	26
3.3.2.3. Foreseen final deployment	26
4. DIRECT DETECTION: AIRBORNE THREATS DETECTION SYSTEM.....	27
4.1. Short description of the sensing system	27
4.1.1. Detection objectives of the sensing system – what is meant to be measured	34
4.2. General deployment requirements	35
4.3. Specific deployment of the sensing system in Use case 1: sub-case 1 and Use case 2: sub-case 1	35
4.3.1. Setup of the sensing system.....	37
4.3.2. Deployment phases of the sensing system	38
4.3.2.1. Lab tests of the sensing system	39
4.3.2.2. Preliminary short experiments with the sensing system	41

4.3.2.3.	Foreseen final deployment	43
5.	NETWORKS AS SENSING SYSTEMS: RADIOFILTER	44
5.1.	Short description of the sensing system	44
5.1.1.	Detection objectives of the sensing system – what is meant to be measured	46
5.2.	General deployment requirements	49
5.3.	Deployment of the sensing system in a Generic Use case	49
5.3.1.	Setup of the sensing system in the framework of a Generic Use Case	50
5.3.2.	Deployment phases of the sensing system	54
5.3.2.1.	Lab tests and short experiments of the sensing system.....	54
5.3.2.2.	Foreseen final deployment	58
5.3.2.3.	Sensitivity of the monitoring system sensors.....	58
6.	NETWORKS AS SENSING SYSTEMS: RANMONITOR	59
6.1.	Short description of the sensing system	59
6.1.1.	Detection objectives of the sensing system – what is meant to be measured	60
6.2.	General deployment requirements	62
6.3.	Deployment of the sensing system in a Generic Use case	62
6.3.1.	Setup of the sensing system in the framework of a Generic Use Case	63
6.3.2.	Deployment phases of the sensing system	64
6.3.2.1.	Lab tests and short experiments of the sensing system.....	64
6.3.2.2.	Foreseen final deployment	67
7.	OTHER SENSOR DEPLOYMENT – NATURAL EVENTS SENSING PLATFORMS	68
7.1.	Use Case 2 - Sub Case 2 – Natural Disasters affect telecom assets: network loss and telecommunication congestion	68
8.	SUMMARY AND CONCLUSIONS.....	69
9.	REFERENCES.....	70

List of Figures

Figure 1 – Intelligence Audio/Video Surveillance System	19
Figure 2 – Sensor Data Flow.....	20
Figure 3 – Audio Analytics Component	21
Figure 4 – Video Analytics Component	21
Figure 5 – Mini-UAV platforms for surveillance	24
Figure 6 – ICCS airborne threats detection system (active sensor - radar component)	28
Figure 7 – ICCS airborne threats detection system (passive sensors - acoustic components).....	28
Figure 8 – Airborne threats detection system: architectural concept	29
Figure 9 – main control and operation environment	31
Figure 10 – Various snapshots of actual operation – UAV detection.....	33
Figure 11 – visualization plots and tools of the airborne threats detection system's application.....	34
Figure 12 - The commercial drone used for the tests.....	39
Figure 13 – Operation plots from lab tests	40
Figure 14 – Rooftop tests with drone	40
Figure 15 – The radar detection polar plots from short experiments	41
Figure 16 – Acoustic signatures of the airborne platforms and direction of arrival quadrants	42
Figure 17 – RADIOFILTER Overall Architecture.....	45
Figure 18 – Critical Infrastructure diagram in a generic Use Case.....	50
Figure 19 – Planned RADIOFILTER deployment in a generic Use Case	51
Figure 20 – Setup phase at RADIOFILTER deployment in a generic Use Case	52
Figure 21 – Training phase at RADIOFILTER deployment in a generic Use Case	53
Figure 22 – RADIOFILTER threats detection at the critical infrastructure in a generic Use Case	54
Figure 23 – RADIOFILTER Web User Interface running in the test campaign without any events detected	55
Figure 24 – RADIOFILTER Secured Radio Sensor.....	55
Figure 25 – RADIOFILTER Web User Interface upon Unauthorized Device Event Detection	56
Figure 26 – RADIOFILTER Web User Interface upon Unauthorized AP Event Detection	57
Figure 27 – RADIOFILTER Web User Interface upon Unauthorized Connection Event Detection	57
Figure 28 – RANMONITOR Overall Architecture.....	59
Figure 29 – RANMONITOR deployment in a generic Use Case	63
Figure 30 – RANMONITOR threats and attacks detection in a generic Use Case.....	64
Figure 31 – RANMONITOR Web User Interface running in the test campaign. The Cell Map is shown.	65
Figure 32 – RANMONITOR Web User Interface running in the test campaign. The Detected Cells and Band Visualization are shown	65
Figure 33 – Radio-Cyber RAN Sensor	66
Figure 34 – RANMONITOR Web User Interface upon Unauthorized Cell Event Detection.....	67

ABBREVIATIONS

2G, 3G, 4G	Second, third and fourth generation of mobile phone systems
API	Application Programming Interface
APN	Access Point Name
ASIC	Application Specific Integrated Circuit
B2B	Back-to-Back gateway
CCA	Critical Communication Application
CCS	Critical Communications System
DMO	Direct Mode Operations
ETSI	European Telecommunications Standard Institute
EU	European Union
GGSN	Gateway GPRS Support Node
GSM	Global System for Mobile communications
GSSI	Group Short Subscriber Identity
HW	HardWare
ISI	Inter System Interface
ISSI	Individual Short Subscriber Identity
ISITEP	Inter System Interfaces for TETRA-TETRAPOL Networks
ITSI	Individual TETRA subscriber Identity
LTE	Long Term Evolution (= 4G)
MNO	Mobile Network Operator
PC	Personal Computer
PPDR	Public Protection and Disaster Relief
PTT	Push To Talk
QoS	Quality of Service
SW	SoftWare
TCCE	TETRA and Critical Communications Evolution
TEA2	TETRA Encryption Algorithm #2

TETRA	TErrestrial Trunked RAdio
TG	Talk Group
TMO	Trunked Mode Operations
UE	User Equipment
VPN	Virtual Private Network
WP	Work Package

1. INTRODUCTION: OVERVIEW OF PHYSICAL THREATS DETECTORS - CONNECTION WITH THE USE CASES

The present Deliverable D4.2 “Active and passive sensors deployment plan”, is considered as the follow up of the previous Deliverable D4.1 “Active and passive sensors definition” within WP4 “Tools and techniques for Monitoring and Detection of cyber-physical threats”.

It is reminded that WP4 deals with the implementation of a variety of hardware and software tools and technologies for detection and monitoring of anomalous conditions, intrusions and threats. Both Deliverables are the outcome of Task 4.1 which aims to monitor and detect intrusions anomalies in the vicinity of telecom CIs (i.e. buildings, remote antenna parks, “grey zones”, telecom pillars on high rooftops), either ground-based or airborne (small UAVs or drones).

The previous D4.1 dealt with the selection and description of the active and passive sensors that were going to be used in the framework of the three macro-scenarios during the pilot cases (in WP7, WP8 and WP9 respectively). It is reminded that, apart from the overall platform for a holistic security response to various kinds of threats, the RESISTO project also provides a variety of sensors and detection tools. These constitute applications of emerging technologies in order to address intrusion events in the telecom infrastructures and to provide the relevant alerts to the overall RESISTO platform.

Thus, the previous Deliverable D4.1 gathered and described all the relevant systems, available in principle from certain RESISTO partners, to formulate a “pool of sensing systems” that could potentially be exploited during the RESISTO pilot implementation. These tools present different level of maturity (from lab prototypes to pre-industrial prototypes or even integrated sensor networks and relevant firmware) and mainly address physical threats and “combined” cyber-physical threats (where a physical intrusion event may enable dangerous situations and threats in the cyber domain).

Based on the above pool of sensing platforms and tools for physical threats, the present Deliverable D4.2 proceeds certain steps forward. ***The Deliverable D4.2 exploits the description and definition of the various (more than 10) RESISTO Use Cases and relevant scenarios that took place within Deliverable D2.8 and thus D4.2 describes the plan and the way of how the various RESISTO sensing platforms can be deployed in order to serve the relevant scenarios and to facilitate the appropriate conductance of the Use Cases piloting implementation within WP7, WP8 and WP9.***

Thus, in respect to D4.1, the D4.2 provides an updated pool of sensing tools and relevant platforms, describing the relevant upgrades, adjustments and developments that took place in the meantime by the respective partners. Furthermore, it describes in technical terms the various planned steps for the deployment of each of these sensing platforms within the content and storytelling of the relevant Use Cases and piloting scenarios where these tools will be employed. ***Thus, the connection and respective deployment within the relevant Use Cases, described in detail within D2.8, is the driving force behind the content of the present Deliverable D4.2.***

As it is evident from both the previous D4.1 and the present report D4.2, RESISTO offers certain sophisticated and modern sensing tools and platforms, including both active and passive sensors along with advanced software implementation tools behind. ***Thus, D4.2 upgrades the definitions set within D4.1 as follows: from the active and passive sensors referred in D4.1 we are now moving to Direct Detection sensing systems in D4.2. Furthermore, the networks as sensing systems in D4.2 have been further upgraded and adjusted in respect to D4.1*** providing a more comprehensive and holistic process for the relevant implantation as it will be seen in the relevant Chapters.

Based on the above and before proceeding to the specific technical content of the D4.2, certain clarifications and definitions should be made first especially to denote the differences between this Deliverable D4.2 and the previous D4.1. These clarifications are given in the following:

1.1. Important clarifications for the D4.2 sensors – differences in relation to D4.1

In order to better understand the content of the D4.2 Chapters and since D4.2 is the follow-up of D4.1, the following clarifications in respect to the terms and definitions appearing in the previous D4.1, the following clarifications should be made:

First of all, we keep the main discrimination between “Direct Detection sensors and tools” and “Networks as sensing systems” which was first introduced within D4.1. Thus the main sensing mechanisms remain the same with the D4.1. However, it has to be noted that D4.1 was mostly focusing in describing the sensors themselves instead of their functionalities as integrated tools. Instead D4.2, based on the adjustments and optimizations that took place in the meantime forwards the description to overall systems, most of them incorporating both active and passive sensors. Thus, ***in D4.2 we are moving from sensors to whole detection systems.***

This in certain cases incorporates the ***merging of functionalities*** (such as the inclusion of the KSI blockchain to the “networks as sensing systems” tools) and in other cases the ***change of titles of the sensing tools themselves***, due to the integration and optimization actions that took place in between. In the following table the relevant upgrade and change of titles for the respective tools between the D4.2 and the previous D4.1 is indicated in order to highlight the upgrade and optimization developments of the respective tools that took place in the meantime:

Title of the RESISTO sensing tools (matching)		Implemented by the partner:
D4.2 – present report – New Titles	D4.1 – Previous Titles	
Direct detection of physical threats		
Audio and Video analytics System	Sensors for Audio and Video analytics and monitoring tools	ADITESS
UAV platform-based Surveillance System	UAV platform – based sensors	ADITESS
Airborne Threats detection system	Active and passive sensors for airborne threats	ICCS
Networks as sensing systems		
RADIOFILTER	Signal Monitoring WSNs as Sensing systems (including block chain functionalities)	INTEGRASYS
RANMONITOR	Femtocells-based Sensing systems (including block chain functionalities)	INTEGRASYS
Other sensor deployment – natural events sensing platforms		TEI (newly introduced)

Table 1 - Final selection and incorporation of sensing platforms within D4.2

From the above table it is evident the change of names of the respective sensors due to their integration and upgrade in overall systems in the meantime from the submission of D4.1 until the present submission of D4.2. Also, a new platform for incorporating natural events sensing platforms has been introduced within D4.2.

Based on the above D4.2 represents the final selection, deployment and implementation of the sensing systems and tools that will be used within the RESISTO pilot phases.

1.2. Mapping of the threat detectors in respect to the RESISTO Use Cases

As it is already stated, the deployment of the sensing mechanisms described in the present Deliverable D4.2 is strongly connected to the relevant Use Cases and sub-scenarios, already described within D2.8, that the detections systems will be employed. In order to clear out this connection the certain classification is being given in the following Table:

D4.2 sensing systems	Implemented by the partner:	Respective Use Cases (and responsible telecom operator)
Direct detection of physical threats		
Audio and Video analytics System	ADITESS	Use Case 1 – subcase 2 (hosted by OTE)
UAV platform-based Surveillance System	ADITESS	Use Case 2 – subcases 1 & 2 (hosted by OTE)
Airborne Threats detection system	ICCS	Use Case 1 – subcase 1, Use Case 2 – subcase 1 (Both hosted by OTE)
Networks as sensing systems		
RADIOFILTER	INTEGRASYS	It will be implemented in various Use Cases, most indicatively: Use Case 5 – subcase 1 & 2 (hosted by TIM)
RANMONITOR	INTEGRASYS	It will be implemented in various Use Cases, most indicatively: Use Case 4 – (hosted by BTC) Use Case 7 – (hosted by RTV)
Other sensor deployment – natural events sensing platforms	TEI (newly introduced)	Use Case 2 – subcases 2 (hosted by OTE)

Table 2 - Mapping of the threat detectors in respect to the RESISTO Use Cases

From the above Table it is seen that the Direct Detection systems are mainly involved in the WP7 Use cases hosted by OTE. These refer either directly to physical threats or to the so called “combined” cyber-physical threats (where a physical intrusion may enable attacks in the cyber domain). And this is reasonable since the specific sensing tools are meant mainly for physical threats and thus can be employed in the **Use Case 1 “Core Network Failure caused by Physical & Cyber Attacks to Telecommunication sites”** and **Use Case 2 “terrorist Attack and Natural Hazards causing network failure and telecommunication congestion”** and their related sub-scenarios. Especially in the Use Case 2 which foresees natural hazards (i.e. severe storms or earthquakes) the natural events sensing platforms can also serve in the relevant sub-scenario.

Concerning the 2 systems (RADIOFILTER and RANMONITOR) representing “networks as sensing systems”, these are meant to be implemented in a variety of scenarios mainly for the WP8 and WP9 Use Cases, which are more focused on the network (interconnection and future networks) domain. Thus, these “networks as sensing systems” tools can accommodate the **Use Case 5 “Protection of Cloud Storage Services” sub-case 1 on Healthcare and sub-case 2 on smart manufacturing** hosted by TIM. Furthermore, they can be employed in the **Use Case 4: “Disruption of major sporting event by combined physical & cyber-attack by a terrorist organization”** hosted by BTC and **Use Case 7: “Maritime Safety and Emergency Case”** hosted by RTV.

The above are the most representative Use Cases where the RADIOFILTER and RANMONITOR tools can be applied. The relevant deployment procedure for these tools is described in detail within this report (at the related Chapters), however, the exact location and implementation will be decided on site upon the definition of the pilot area by the hosts / telecom operators which will take place within the evolution of the relevant WP8 and WP9. Nevertheless, quite many discussions have been taken place among the relevant partners and the deployment aspects have already been defined as it will be seen in the relevant Chapters.

RESISTO added value

As a final result it can be noted that both the Use Cases defined in D2.8 and the final list of the sensing systems to be deployed as they are described within this Deliverable D4.2, successfully present the RESISTO added value in enhancing the prevention, detection, response and mitigation processes in critical telecom Infrastructures. New more sophisticated detection techniques are introduced both for direct detection mechanisms and for employing wireless networks as sensing systems in order to successfully tackle the emerging, more sophisticated attacking methods.

For example, in light of the emerging use of unmanned devices, UAVs or drones are nowadays more and more considered as potential human-driven physical threats. Thus, counter-UAV and counter-drone technology has already seen extensive use in certain applications. The same can be noted for audio and visual analytics as well as the use of wireless networks as intrusion sensors. The exploitation of modern machine learning and artificial intelligence technologies further advances the relevant attempts. Moreover, there is also growing interest in portable and mobile systems that could be used to protect ground units of critical infrastructures. All these contribute to the state-of-the-art and innovative detection solutions that are offered and will be implemented by the RESISTO project.

To comply with newest technology trends, the RESISTO platform integrates a variety of different sensor types against physical threats in order to provide a more robust detection capability and to overcome the inherent limitations of each technology. The use of multiple detection elements is intended to increase the probability of a successful detection, given that no individual detection method is entirely fail proof. Therefore, additional situational awareness will be achieved against modern, sophisticated threats and ways of attacks through the specific detection methods employed within the overall holistic RESISTO platform. And these methods will be tested and deployed

throughout the RESISTO Use Cases to showcase the relevant RESISTO added value in comparison to existing security systems.

1.3. Relevant User requirements mapping

The D4.2 sensing systems deployment is in compliance with the RESISTO user requirements as these were set within D2.1. The most general user requirements addressed are the following:

Requirement Identity Code	Requirement Description	Requirement Verifiability
RES_FUN_0006	RESISTO shall provide physical intrusion detection based on a variety of sensors, such as audio/video/radar and other passive and active sensors.	D
RES_FUN_0010	The RESISTO system should be able to detect Cyber/Physical threats, e.g. related to the cloud infrastructure.	D
RES_FUN_0020	Physical threats detection of the RESISTO platform should include data collected from sensors protecting access to systems.	D
RES_FUN_0030	The RESISTO system shall be able to receive, collect and process alert events relevant to physical detection.	D
RES_FUN_0130	The RESISTO platform should include a tool to detect radio interference, such as from Wi-Fi or cellular networks whose coverage spans the telecom facility or radio jammers.	D and/or A
RES_FUN_0200	The RESISTO system should detect different kinds of attacks: cyber and physical ones.	D
RES_FUN_0850	The <i>Smart Spectrum Surveillance (SSS) tool</i> should periodically or on operator demand generate a report with a summary of the events that the SSS is able to detect (non-registered radio devices presence for the Access Control module and non-registered/missing cells or interferences in the Cell Monitor module).	D
RES_FUN_0960	The <i>Airborne Threats Detector</i> should have reports available in the Cockpit.	D
RES_SEC_0030	RESISTO should detect attempted intrusions by unauthorized persons and applications.	D
RES_FUN_0110	The RESISTO system should be able to help avoiding telecom facility equipment and/or private information theft by collecting data from specific sensors and providing mitigation measures.	D

Based on all the above, in the following sections the description of the final list of the RESISTO detection and sensing systems is being made. Both direct detection of intrusions into the physical security of the telecom infrastructures are described (namely audio and visual analytics, surveillance platforms and airborne threats detection system), as well as the “networks as sensing systems” using modern wireless sensor networks as sensing nodes against various threats are being presented through specific cases. Each system is being described in a separate Chapter.

The aim is to present the final list of the sensing systems that will be used for the detection of physical and cyber-physical threats within the framework of the RESISTO Use Cases, providing more advanced and sophisticated security features tailored to the modern needs for increased security and protection.

2. DIRECT DETECTION: AUDIO AND VIDEO ANALYTICS SYSTEM

Video and Audio sensors are widely used in surveillance operations and protection of critical infrastructures. Intelligence algorithms are applied in audio and video streams for the real-time detection of events for the early identification of illicit activity.

The Audio Analytics Component (AAC) within RESISTO, allows the acoustic event detection to fill the gap when other analytics are not in the position to provide results in dark environments, incidents residing outside the field of view or the inability to detect events due to overcrowded areas. Based on ongoing research, during the RESISTO project, ADITESS developed an intelligent audio analytics module which allows the detection of abnormal behavior regardless of the field of view; based on well-established methods and tools from the fields of audio coding, machine learning and speech recognition and allowing for efficient operation on low cost power limited devices (or embedded systems) for the detection of gunshots and other acoustic related events within the environment.

The Video Analytic Component (VAC) is part of the overall ADITESS Surveillance System used within RESISTO. The VAC provides the necessary visual analytic functionalities for automatic or semi-automatic surveillance. The VAC processes the visual content coming from multiple sensors (i.e., day cameras, thermal sensors, SWIR sensors, Electro Optical Sensors). The goal of the processing of the visual content is mainly to detect people, objects, and/or events related to physical protection and perimeter security. In addition, the VAC will be capable of processing real-time content as well as pre-recorded videos.

The deployment of such systems during the RESISTO implementation will be done on dedicated for surveillance hardware resources (servers, GPUs, etc.) and additional software to be integrated for the establishment of an intelligence alerting mechanism targeting the physical security of Telecom Infrastructure.

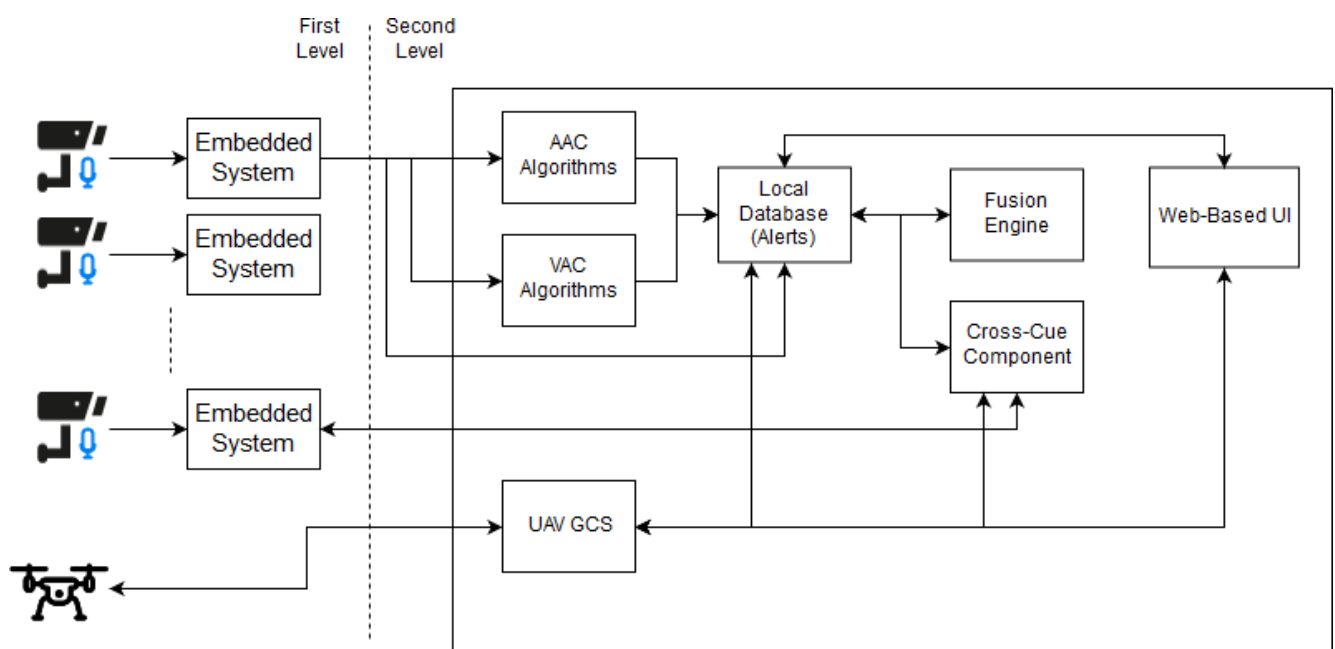


Figure 1 – Intelligence Audio/Video Surveillance System

2.1. Short description of the sensing system

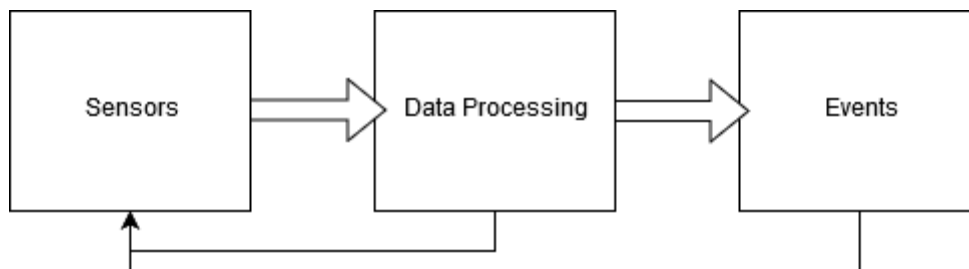


Figure 2 – Sensor Data Flow

The data processing modules (AAC, VAC) are receiving data from the sensing devices while the processing output is delivered to the event management system for knowledge extraction, correlation and visualization.

The sensing devices are divided in two main categories:

- Audio Sensors - Microphones
- Video Sensors – Cameras

which were described in detail in the previous Deliverable D4.1; for the sake of a complete presentation and adequate connection with the D4.1, a brief description of the sensing devices is given below:

Audio Sensors

Two types of microphones are included in the proposed surveillance system. The first type is the Omni Microphone what will be used to provide solutions for acoustic event detections. The second type of microphone is an array microphone able to provide capabilities to localize the source of the event.

Indicative Models:

- EDUTIGE Lavalier Microphone ETM-006
- Andrea 2S Superbeam Array Microphone

More details and specifications for the audio sensors have been provided in deliverable D4.1.

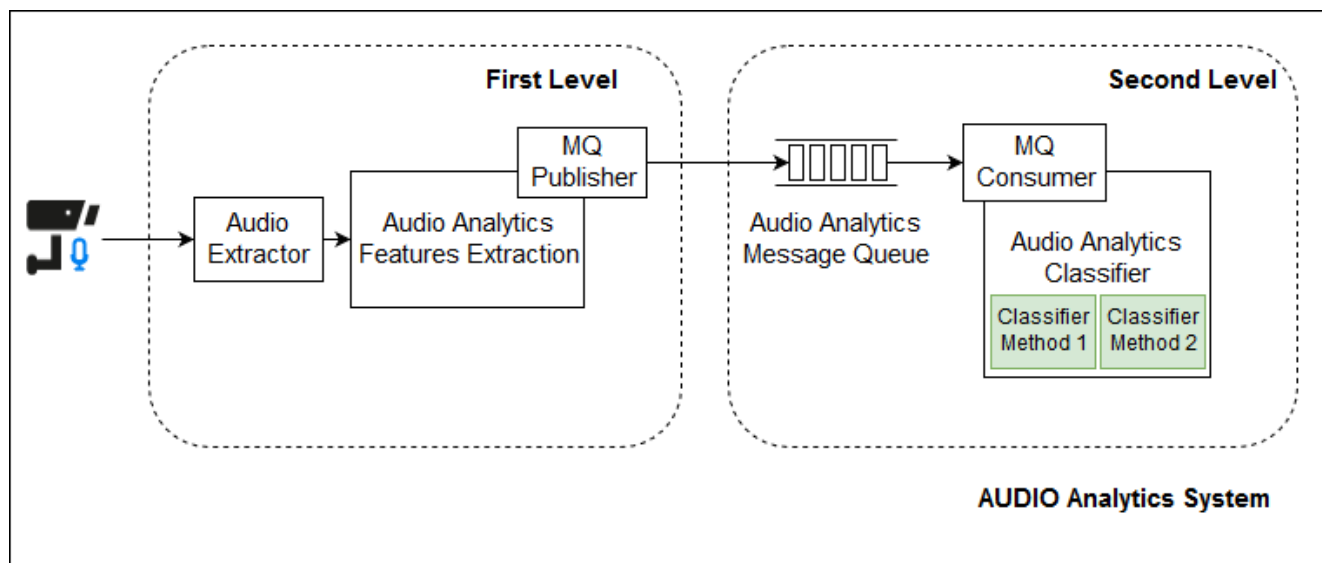


Figure 3 – Audio Analytics Component

Video Sensors

Regarding the visual sensing, the surveillance system will use two type of CCTV cameras, the fixed camera and a PTZ camera. The second one supports Pan, Tilt and Zoom operations.

Indicative Models:

- CCTV Camera - Foscam FI9803P
- CCTV PTZ Camera -

More details and specifications for the audio sensors have been provided in deliverable D4.1.

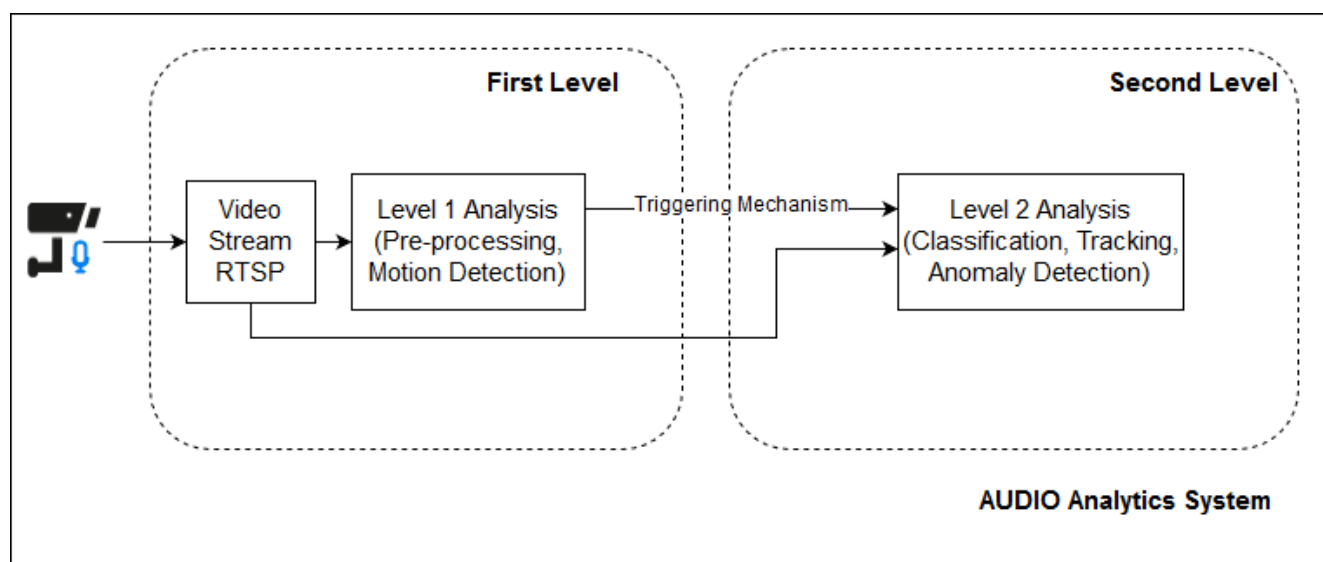


Figure 4 – Video Analytics Component

2.1.1. Detection objectives of the sensing system – what is meant to be measured

To enable the physical security of the telecom infrastructure, a surveillance system by ADITESS will be deployed. The main objective of this system is the early detection of abnormal and illicit activity related to the protected areas. As we already mentioned, two main components, the AAC and the VAC will be utilized for this purpose.

The AAC is applied on the audio digital streams for the detection of acoustic events. Based on classification algorithms, the extracted features of the audio signal are classified in order to detect gunshots, screaming, glass breaking and other events related to illicit activities. Similar to AAC, the VAC component aims to the real-time processing of video streams for the detection and classification of objects. The main functionality of VAC covers the camera motion detection, person detection, vehicle detection while further processing on top of detected objects can be applied for the identification of abnormal activities. Such activities include, the illicit appearance of public in restricted areas, virtual fence, group of people, etc.

2.2. General deployment requirements

The AAC and VAC system will be deployed on dedicated servers with specialized processing capabilities. The AAC will be deployed in a distributed manner where the feature extractor will be executed on embedded systems attached to the microphones (e.g. Raspberry PI 3) and the classifiers can be deployed on workstations with more computational resources (e. g Intel NUC). The VAC component will be deployed on a dedicated bare metal machine with GPU processing capacity. The integration of the AAC, VAC with the message bus, local databases and other supporting components (e.g. fusion engine) will be hosted on virtual machines on a dedicated server.

The sensor placement will be based on a site survey and after a risk analysis of vulnerabilities and potential physical security threads. The CCTV system will cover the area of interest while a small percentage of overlap will be foreseen. On the other hand, microphones will be placed near cameras considering the omni-coverage as well as the directional coverage. Finally, UAV systems with cameras related payload can be deployed to cover areas dynamically and after an order or command from the RESISTO platform. The integration of UAV video streams with the video analytics sub-system will be done either using direct digital links or through LTE networks using a VPN connection.

2.3. Specific deployment of the sensing system in Use case 1: sub-scenario 2

The 2nd sub-scenario of Use Case 1 utilizes the deployment of a Smart Surveillance system for the perimeter protection of a telecom facility (i.e. OTE building). For the needs of this scenario visual and audio sensors will be deployed. The algorithm to be used will be trained for the detection of abnormal behavior including the intrusion of an illicit person to the protected area.

2.3.1. Setup of the sensing system

Two different setups of sensors will take place in this scenario. The first one is about the development and configuration of the smart surveillance system and will take place on ADITESS premises while the second will take place on OTE premises. During the first case, CCTV and microphones will be deployed in a controlled environment for testing of detection of intruders in a restricted area. During the pilot phase, the same sensors will be deployed on OTE premises and a configuration of parameters such as location will take place. The smart surveillance system will remain available during the whole duration of the pilot.

The processing of images and audio streams will be done by computational resources dedicated to this purpose. The integration with the RESISTO platform will be done through the KAFKA broker where the exchange message will form an event in a JSON format.

The video streams as well as the alerts as a result of the detectors will be visualized through the RESISTO HMI Platform.

2.3.2. Deployment phases of the sensing system

As we already mentioned, the deployment of surveillance systems will be done initially on ADITESS premises and then to the pilot site, OTE Premises, as follows:

2.3.2.1. Lab tests of the sensing system

The initial deployment and configuration of the video and audio sensing system will take place on ADITESS premises. In particular the following will take place: During these tests, the detectors as stand-alone components will be tested followed by the surveillance integrated system. The development and configuration of the event message will be evaluated and prepared as the output of the system. Furthermore, the audio and video system will be integrated by the fusion component for the common identification and correlation of targets.

2.3.2.2. Preliminary short experiments with the sensing system

The second phase of the work on surveillance systems, foreseen through the project implementation, aims on the integration of the system with the RESISTO platform. A series of integration tests will be performed using a VPN account and through the connection with RESISTO KAFKA broker. At this phase, the deployment of sensors on a dedicated building owned by ADITESS will take place where the processing of video and audio streams will be done at ADITESS premises. The final stage of this phase will be the execution of scenarios similar to the use case with personnel of ADITESS in order to evaluate the performance of the surveillance system as a perimeter protection and intrusion detection system.

2.3.2.3. Foreseen final deployment

The last phase will be the deployment of the smart surveillance system at OTE premises and the visualization of streams, alerts through the RESISTO HMI Platform. Final development and configuration of detection parameters as well as the calibration of sensors will take place before the execution of the pilot.

3. DIRECT DETECTION: UAV PLATFORM-BASED SURVEILLANCE SYSTEM

Aerial Imagery and Aerial Surveillance are important aspects for a surveillance system. The surveillance application is already enhanced with these features. For the needs of the RESISTO project, Mini-UAV Systems have been integrated in the physical security and the relevant usage is two-fold: (a) to provide aerial image using state-of-the art Gimbal (Camera stabilization system) and surveillance cameras, and (b), to provide useful metadata including telemetry data and target data. The usage of such systems enables the remote operation and the ability to provide real-time images from sites that are located outside the main infrastructure of the telecom operator. For example, a Mini-UAV system can be ordered to navigate in a non-populated infrastructure (e.g. Antenna station) to assess remotely a situation. This will be the main objective with the usage of remote imagery from UAV systems.

3.1. Short description of the sensing system

In the RESISTO project, three types of Mini-UAV platforms are available to execute surveillance operations: a Multirotor type, a Helicopter type and Fixed-Wind type. All the platforms have been prepared to carry a surveillance camera combining thermal and daylight sensors. The Mini-UAV system that will be used in the surveillance operations consists from the Mini-UAV platform, the payload and the Ground Control Station (GCS).



Figure 5 – Mini-UAV platforms for surveillance

The GCS is responsible for managing the pre-flight and in-flight operation of the UAV and its payload. Upon a UAV order request, the GCS handles the incoming order for the preparation and execution of the flight plan. The navigation of the UAV can be done autonomous or with the manual control of the operator.

Three communication links will be established to support the integration of the UAV systems with the RESISTO platform:

- Air to Ground (Payload): Through this digital data link the UAV image will be transmitted to the GCS.
- Air to Ground (Navigation): The navigation data and telemetry readings will be available through a digital data link. This is similar technology with the payload link, however, we will use an isolated system for the avionics to ensure and fulfil the safety requirements.
- Ground to Ground: Through this link, which can be a local network or a VPN connection using LTE, the video stream and UAV metadata will be available to the RESISTO Platform.

3.1.1. Detection objectives of the sensing system – what is meant to be measured

As we already mentioned, the usage of Mini-UAV systems as direct detection sensors will aim to provide remote images (video streams) from sites that are not covered from the CCTV systems and in general the fixed surveillance infrastructure. Once the video stream reaches the ground processing elements and particularly the video analytics (VAC), the detection of objects and abnormal behavior can be also applied similar with the perimeter protection. Additionally, the tracking capabilities of the surveillance UAV payload as a stand-alone feature or through the VAC functionalities can also be applied.

3.2. General deployment requirements

The operation of the UAV system is restricted to some external conditions mainly related to weather. Apart from the flight-ability of UAVs, the connectivity with the telecom infrastructure and integration with the smart surveillance system should be maintained. For the scope of the RESISTO project, two alternatives can be applied. In the case where a LAN either through wired or wireless links is available the GCS can directly connect to the infrastructure. On the other hand, the connection of GCS with telecom infrastructure through available broadband networks and the usage of VPN connections can also be established. It is worth mentioning that Digital Data Links (wireless) can also assist the connectivity and can be combined with the two connection approaches.

3.3. Specific deployment of the sensing system in Use case 2: sub-scenario 1 & 2

During a terrorists attack with a hostile UAV against an antenna pillar (sub-scenario 1) or during a natural disaster where the communication in the nearby areas network is affected (sub-scenario 2), a friendly UAV will be utilized to perform an inspection operation. The UAV will be equipped with a surveillance camera. The UAV experts will be responsible for the entire operation while communication engineers and software developers will assist the integration and transmission of real-time data.

3.3.1. Setup of the sensing system

The UAV system will be deployed in a location near the remote telecom facility that could be affected by a natural disaster or by potential malicious actions (i.e. a nearby monitoring point or a main sub-station within the telecom operator's network throughout the country). The deployment process will include the deployment of Ground Control Station (GCS), the preparation of a UAV fleet and the establishment of connection between the GCS and RESISTO infrastructure. In particular for the RESISTO pilot implementation, the deployment will be done in a controlled by ADITESS airfield while the communication will be assisted by VPN and LTE networks. The availability of the UAV platforms will cover the duration of the pilot.

The main objective of this setup is to integrate the UAV Video stream with the VAC and all the functionalities will be applied. Additionally, the UAV telemetry data such as the position, the covered path, orientation will be available for visualization purposes.

3.3.2. Deployment phases of the sensing system

Similar with the Audio and Video analytics system, the deployment of UAV for the pilot will be executed in three phases, as follows:

3.3.2.1. Lab tests of the sensing system

Communication links, quality of images and the establishment of broadband networks followed by the integration with the surveillance system will be done through lab tests without flights. Follow a checklist approach, the process of integration will be executed while configuration and fine tuning of the parameters will be feasible.

3.3.2.2. Preliminary short experiments with the sensing system

A UAV flight campaign targeting the verification of the lab work will be done in this phase of the pilot exercise. As we mentioned, the flights will be executed in a dedicated airfield and the back-end infrastructure will be hosted at ADITESS premises. The UAV performance indicators including range and bandwidth will be evaluated and adapted for the needs of the pilot.

3.3.2.3. Foreseen final deployment

The latest stage of this use case is the deployment of the UAV system for the final pilot. Due to flight restrictions and law requirements, the UAV flights will be performed in Cyprus (same airfield of test flights) while the data will be adapted and translated to fulfil the location requirements of the pilot. The image from the site will be transferred to OTE premises for further processing and visualization.

4. DIRECT DETECTION: AIRBORNE THREATS DETECTION SYSTEM

In the previous Chapter the role of drones and UAVs in modern surveillance systems has been highlighted since they can carry monitoring and inspection payload providing a flexible, efficient and cost-effective relevant solution. This is acknowledged by RESISTO as the relevant surveillance UAV platforms are exploited within the implementation Use Case scenarios. However, apart from that role, small aircrafts, drones or UAV platforms can also be hostile when used for terrorist attacks and malicious actions. Current attack trends are more sophisticated nowadays, as seen from recent conflicts worldwide where airborne threats like UAVs or small aircrafts are used as unmanned attackers with payload meant for surgical bombing or limited but accurate attacks. This creates a precedent on that current and future terrorists may attack with drones / UAVs, or drone swarms carrying explosives. Apart from that, drones and UAVs can also be used for malicious actions without necessarily causing major damages; i.e. breaching a perimeter and enabling other kinds of threats such as cyber ones or enabling other kinds of attacks. All the above trends concerning airborne threats were addressed within the Deliverable D2.8 and especially the Use Cases 1 and 2 (to be piloted by OTE, ICCS and ADITESS).

In order to address these modern kinds of airborne threats, the RESISTO project incorporates an airborne threats detection system for the early detection of airborne objects (such as small aircrafts, UAV platforms or larger drones etc.) approaching or breaching the potentially existing protection measures of a telecommunication infrastructure. This airborne threats detection system is offered by ICCS involving specific active and passive sensors like electromagnetic radars and acoustic sensors (dynamic microphones) in combination. This detection system can operate both in a stand-alone mode and in combination with the audio / visual analytics systems presented in the previous chapter.

4.1. Short description of the sensing system

Active and passive sensor units

The working principles and the technical details for the radar and the acoustic sensors of the overall airborne threats detection systems have already been described within the Deliverable D4.1. The whole system is a laboratory prototype developed by ICCS. A short description of the relevant sensors and the overall functionalities with the latest updates are given briefly in the following.

The “active” part of the sensors consists of a Continuous Wave Doppler (CW Doppler) monostatic Radar where both the transmitting and receiving antenna are close together, practically at the same point. This Doppler CW radar prototype operates at 24GHz and 25 dB antennas have been adjusted along with a mechanical construction to provide 360 degrees scanning, emulating the omnidirectional operation.

The general principle of operation is as follows: the continuous electromagnetic signal is emitted from the radar’s transmitting antenna illuminating the airborne threat object (target). Part of the energy of the wave is scattered from the target surface and returns to the radar’s receiving antenna. If the target moves towards to the beam, due to the Doppler Effect the frequency received (echo) will be shifted and thus can be exploited and processed providing the target’s movement characteristics.

In order to adequately accomplish the relevant operation, advanced signal processing is being used to distinguish airborne objects with low RCS (radar cross section of the target) while the unit can operate either as stand-alone sensor or in combination with the acoustic sensors or other sensor configurations as well. This electromagnetic radar sensor is shown in the figures below.



Figure 6 – ICCS airborne threats detection system (active sensor - radar component)

As far as the passive sensors are concerned, these refer to acoustic (sound sensors) which consist of a set of high sensitivity dynamic microphones forming an array. Acoustic microphone arrays are used as a second sensor modality to detect broadband acoustic emissions from approaching targets. The microphones can form various configurations; either forming linear arrays or diagonal (cross format) which yield to be the most optimal ones. In the following figures the acoustic diagonal microphone arrays (4 microphones in a cross format) are seen within the anechoic chamber of ICCS:

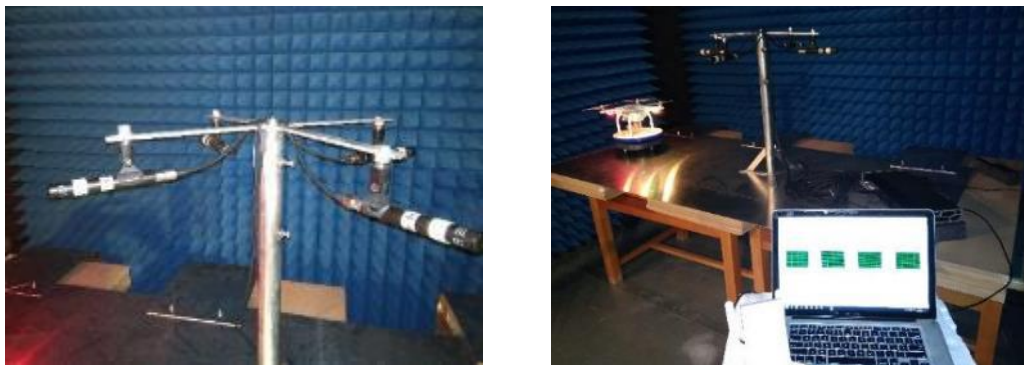


Figure 7 – ICCS airborne threats detection system (passive sensors - acoustic components)

These acoustic sensors mainly track the strong sound harmonic lines that small aircrafts and UAVs emit mainly in the 20 Hz–2 kHz range (sound of their propulsion). For the sound processing, again advanced signal processing algorithms and mainly two methods are being used; a) time-domain waveform cross-correlation of the captured waveform with a previously recorded sound waveform of the target (i.e. UAV or drone under test) used as reference and b) Harmonic Line Association in the frequency domain and extract the necessary results from the harmonics of the fundamental frequency as seen in spectrograms. The two methods are usually being conducted in combination. In the same way as the radar sensors, the acoustic sensors unit can operate either as stand-alone sensor or in combination with the radar sensors or other sensor configurations i.e. vibration sensors as well.

Airborne threats detection system: architecture and functionalities

As it has already been stated both the radar and acoustic sensors of the airborne threats detection systems can be used either as stand-alone or in combination with each other or with other sensors. However, as it has already been shown in the literature (as this was described within the previous D4.1 Deliverable), detecting moving targets of even lower RCS can be made feasible by implementing mixed techniques; thus by implementing the above sensors in combined configurations together and along with other sensors or visual methods (i.e. cameras). Based on the above, the airborne threats detection system that is going to be deployed within the framework of the RESISTO project will implement combined configurations as these also currently emerge as promising related technology trends.

Based on the above, the most general configuration for the above architectural concept is given in the following schematic diagram which also presents the connections among the various sensing units:

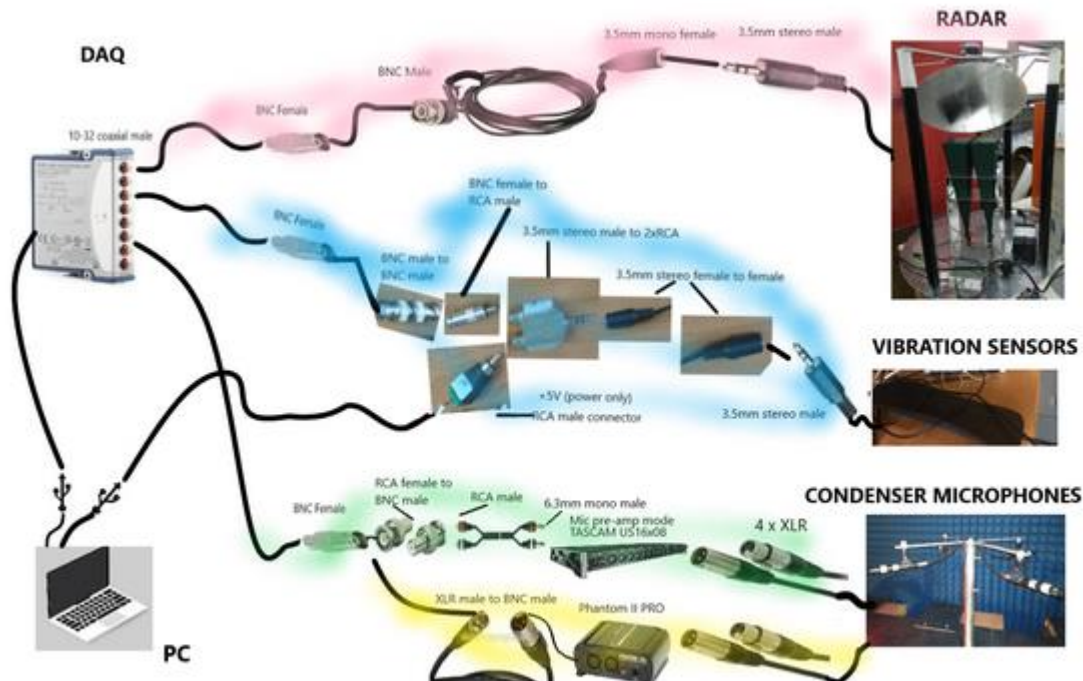


Figure 8 – Airborne threats detection system: architectural concept

From the above schematic, it is seen that 4 (four) main connection paths have to be used in order to provide a combined configuration of the various sensing units with the DAQ (Digital Acquisition) card and the control & processing unit (computing device i.e. laptop, PC etc.). A relevant brief description of these four connection paths is given in the following.

The Digital Acquisition card (DAQ) NI 9231 of National Instruments is an 8-channel analog input module with a 51.2 kS/s update rate, 24-bit resolution, and ± 5 V input range. Channels on the NI 9231 allow for high dynamic range measurements necessary to fully utilize modern measurement

microphones, accelerometers and other types of sensors. In addition, the module includes built-in anti-aliasing filters that automatically adjust to the desired sampling rate, removing the need for external sensor power and reducing the complexity of the data acquisition system. Thus, the specific card is capable of the simultaneous data acquisition of up to 8 different signals (8 channels i.e. 8 sensors) with virtually flawless synchronization among them which enables the combination of different sensing systems.

The sensing-data and advanced signal processing is performed through a windows-based computer (desktop PC or laptop which is better for outdoors deployment as in the RESISTO pilots). The detection visualization is enabled through specific application already developed in LabView software which controls the whole setup and provides the necessary visual environment as it will be seen later on.

The upper (pink) connection path denotes the configuration with the radar sensor through simple BNC and 3.5mm cables for the radar I and Q Doppler channels. The middle (light blue) connection path connects through relevant cable assemblies the vibration sensors with the DAQ card. The vibration sensors are basically very sensitive acoustic sensors combined with accelerometers in order to detect vibrations of a surface that may be caused in the vicinity by an intruder, and this is a showcase of how different kinds of sensors can also be combined with the respective configuration. The lower two connecting paths (light green and yellow ones) denotes the configuration for the adjustment of the acoustic microphone sensors to the DAQ card. Basically the two paths show alternative ways, depending on how much background noise exists in the surrounding environment and thus received by the microphones; to this end, for obtaining less noisy solutions, the yellow connecting path is preferred.

The main and most general control and operation environment through LabView application as updated in respect to the one presented within D4.1 is shown in the following figure, where through the polar diagram the movement of the airborne threat (target) can be shown. However, other visualization options and windows are also available through the LabView application. The whole environment acts as a virtual console for the control and operation of the radar system and this environment is being connected through the appropriate HMI interface with the RESISTO platform:

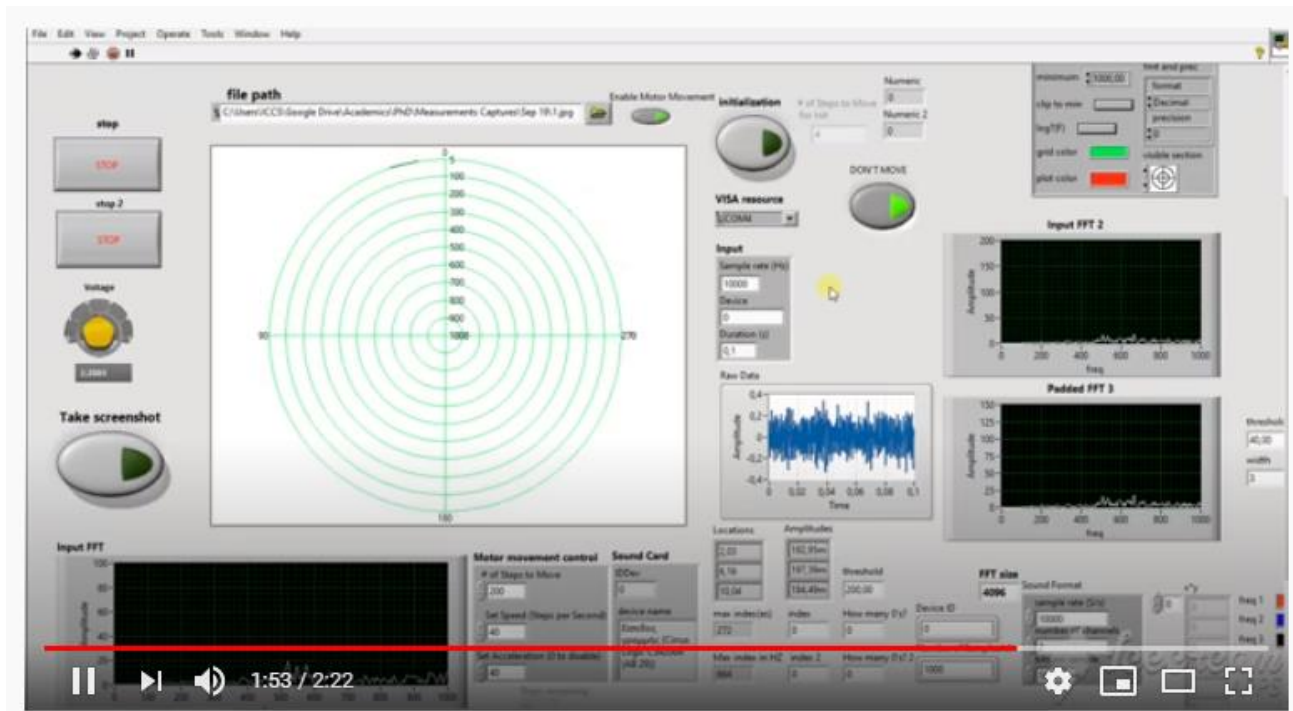
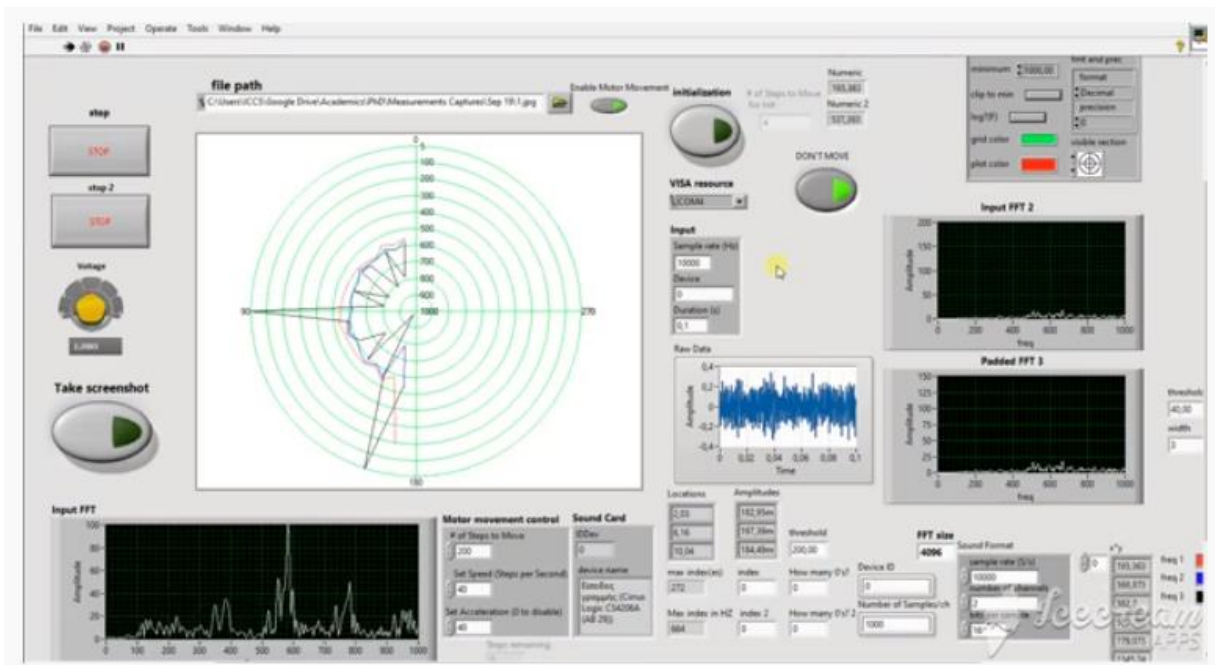
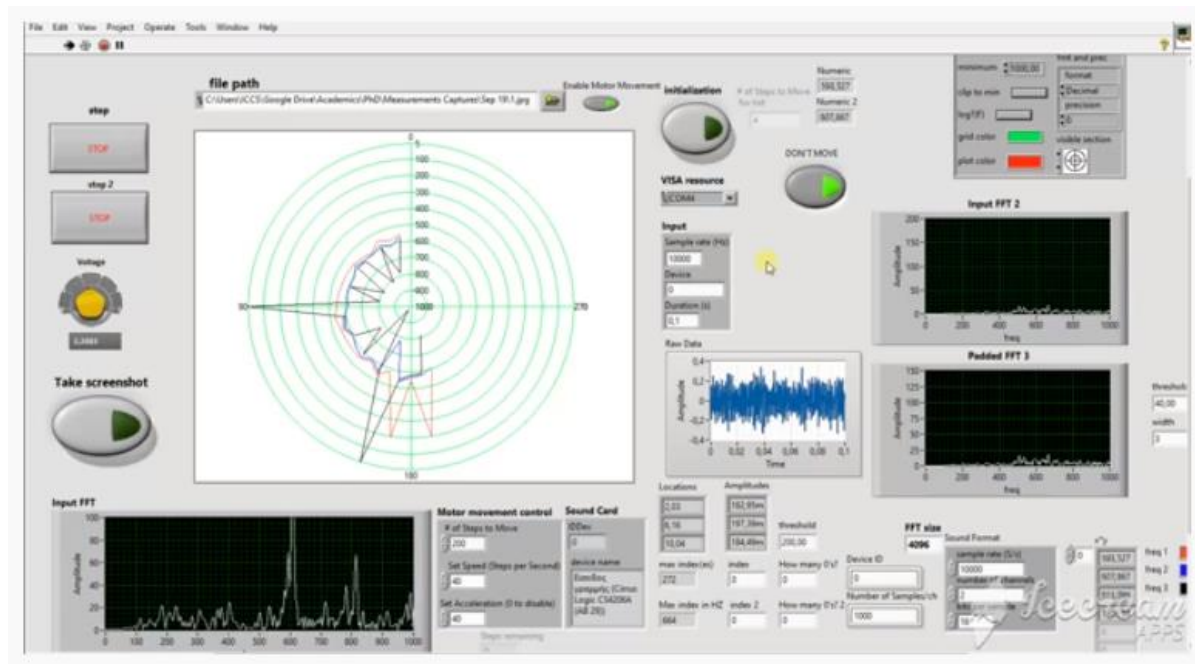


Figure 9 – main control and operation environment

The whole system and Labview application can provide the following functionalities: view and processing of both radar and acoustic waveforms, performance of FFT and visualization of power spectrum versus frequency, of amplitude versus frequency or/and time and respective spectrograms, alarm indications or sensitivity levels, inclusion of recording of specific sessions for post-processing of data and association with data by other software tools (i.e. Audacity software etc.).

The whole setup has already and is regularly been tested in laboratory environment and on the field with various types of small aircrafts and UAVs, as it will be detailed in a next paragraph. In the following figures, the system's application is shown for various approaches of such airborne platforms, while updating and debugging continuously takes place.



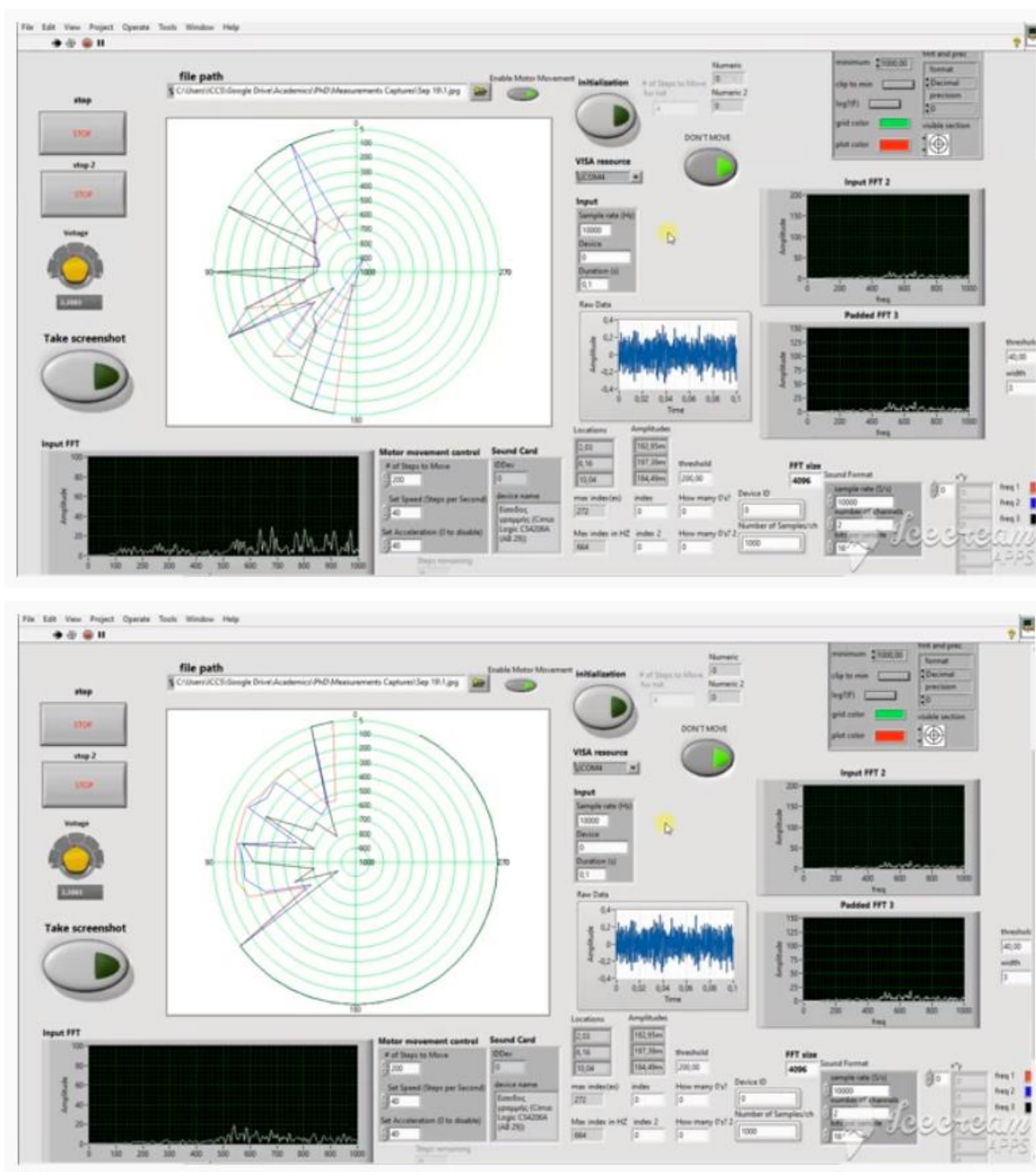


Figure 10 – Various snapshots of actual operation – UAV detection

From the figures above it is shown that when the UAV is approaching an increase in frequency shift is noticed due to Doppler; thus for larger frequency shifts (and for a specific amplitude threshold) the target's path moves to inner circles at the polar coordinates diagram of the Labview application. The system can detect the drone's movement when the drone is approaching or moves away from the radar. However, when the drone is at hover mode the radar mainly detects the fast movement of the propellers.

In the above snapshots, a small commercial off-the-Shelf DJI Phantom 3 Advanced Drone was used which was flying around 70-100 m above the testing place (range, with a height of around 100 m) where the airborne threats detection system was placed. Considering that this small drone is not visible to the human eye in such distances due to its small size (as well as its 4 helices cannot be heard as well), it is seen from the system's application window that the drone's presence and movement is well captured by the system with adequately enough received signal above the noise in a constant manner.

4.1.1. Detection objectives of the sensing system – what is meant to be measured

The main detection objective of the airborne threats detection system is to detect the presence of an airborne object (small aircraft, UAV platforms etc.) in the vicinity of a critical infrastructure. Advanced signal processing and machine intelligence / machine learning techniques in combination with neural networks are applied to the radar and acoustic data, both in the time-domain and the frequency-domain to achieve detection and to estimate the target's angle of arrival and range/velocity. The target's direction (angle) of arrival is shown within the specific LabView application and visualization tool in polar coordinates (while other options i.e. in quadrants are also available, as already described previously), as this is shown in the figures below.

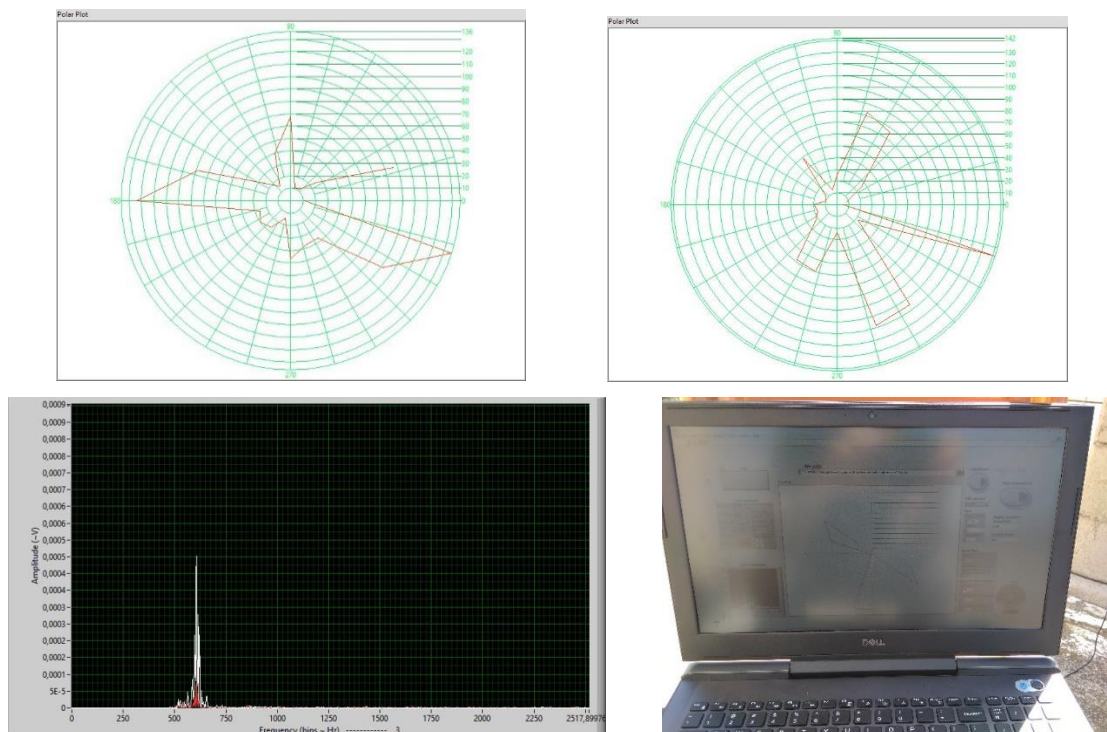


Figure 11 – visualization plots and tools of the airborne threats detection system's application

At the upper snapshots the radar reflected signals at $\sim 350^\circ$ where small aircrafts were flying at more than 400m (left) and 800m (right) ranges are shown; collateral reflections from moving objects (cars) on the runway are also detected. The Doppler shift is shown at the lower image.

Other detection parameters can be extracted indirectly through the signal processing (i.e. frequency shift, the range – distance, the target's RCS etc.) by taking into account the data derived from the outdoor measurements of UAV and drone platforms. Furthermore, the acoustic imprint of UAVs is

captured by microphone systems, exploiting the target's strong emitted sound harmonics (e.g. propulsion) representing the sound/acoustic frequency region; since they do not depend on the target's size, but rather on its acoustic signature i.e. sound of the engine and thus can detect broadband acoustic emissions from approaching targets.

Based on the above, in both Use Cases that the airborne threat detection system will be deployed, as it will be seen in later paragraphs, the main detection objective is to detect early enough as it is described above, the presence of an airborne object which would potentially be an external physical threat and provide the relevant potential intrusion events to the RESISTO platform.

4.2. General deployment requirements

The radar sensor, being an electromagnetic one, needs the target to be in line-of-sight so that to reflect the emitted signal from the radar; for that reason a specific mechanical construction to provide 360 degrees scanning, emulating the omnidirectional operation has been made. On the other hand, the acoustic sensors present omni-directionality and non-line-of-sight need and thus moving targets and their range can be detected regardless of their size by the acoustic sensors, despite that their sensing depends on the environmental conditions and related sources of acoustic attenuation (e.g., temperature, wind speed and direction). Thus, the combined use with other sensing devices is recommended making the acoustic sensors complementary sensing devices to the radar detection.

Other power or mechanical requirements have been already been tackled within the construction and there is no need for special arrangements by the RESISTO system. A power source (either plug or battery) is needed while the data connection can be made either through wired or wireless (WiFi) means and then the integration with the RSISTO system can be accomplished in the same way as the Audio & Video Analytics system presented in the previous Chapters. Concerning the integration of the airborne threats detection system within the overall RESISTO architecture, it should be noted that the sensing tools may act as plug-in modules providing alerts to the LDO's Security and Resilience platform. The overall detection system can also operate as a standalone one and thus a relevant interface is defined in the framework of the WP6 Deliverables through a specific HMI. Consequently, and since the aim of the airborne threats detection system is to extract and provide potential intrusion events corresponding to the detection of moving airborne objects, a threat event with relevant attributes will be provided.

In the framework of the relevant Use Cases that the ICCS airborne threats detection system is part of the whole deployment setup, the system operates together with both of the ADITESS systems (the Audio & Video Analytics system and the friendly UAV platforms) presented in the previous Chapters.

4.3. Specific deployment of the sensing system in Use case 1: sub-case 1 and Use case 2: sub-case 1

The ICCS airborne threats detection system is going to be deployed in the framework of 2 Use Cases, both lead by OTE as the telecom operator of the communication critical infrastructure. Both Use Cases will be piloted in the framework of WP7 concerning the protection of the existing telecom CIs. A brief description of the role of the ICCS airborne threats detection system in these Use Cases is given below.

Use Case 1 – Core network failure caused by physical & cyber-attacks to telecom sites

Sub-Case 1 (cyber-physical attack caused by a UAV)

In general, the main purpose of Use Case 1 is to present showcases of cyber-physical threats and how RESISTO can enhance the detection and especially the correlation between both events (cyber and physical ones); it is considered that a physical attack enables or triggers a threat in the cyber domain and thus the added value of the RESISTO solution is justified.

In the first subcase, the attackers use a UAV to overcome the physical protection and execute the cyber-attack. The RESISTO system, deploying its sensors (i.e. radar for airborne threat detection), detects the UAV and identifies a potential security threat in the cyber domain, activating the provider's cyber detectors, which detect and neutralize the threat. More specifically:

- A UAV is supposed to overcome the physical security (i.e. secure fence protected by OTE's security system) and gain access to a network switch located inside a protected building. The UAV flies over the fence and approaches the building ignoring the physical security of the location, i.e. secure fence and building.
- As it approaches the building, it is detected by the ICCS airborne threat detector (radar) of RESISTO, which issues an airborne threat detection event.
- The drone connects wirelessly to the wireless network from the exterior of the building, gaining access to a network switch and initiating i.e. a DoS attack, which targets the switch.
- Having detected the potential airborne threat, the RESISTO system identifies the cyber assets in the location as "compromised" and initiates different cyber detectors of the provider's network in order them to detect potential threats in the cyber domain.
- Subsequently, the DoS attack is detected and a cyber-attack event is issued by RESISTO. Finally, RESISTO suggests a prevention / mitigation action, i.e. deactivation of the switch and redirection of normal traffic.

It is seen that although separate physical and cyber security mechanisms may be in place, the correlation between the events identified by RESISTO (the physical and the cyber ones) facilitates the efficient detection of the attack and enables its mitigation in its entirety.

Use Case 2 – Terrorist attack and natural hazards causing network failure and telecommunication congestion

Sub-Case 1 (Terrorist Attack in telecom asset cause severe network failure)

In general, the main purpose of Use Case 2 is to show how RESISTO reacts when a physical attack (sub-scenario 1) or a natural disaster (sub-scenario 2) affects severely the telecom provider's network.

In the first sub Use Case (sub-scenario 1), a third party uses a drone (UAV) to attack a telecom provider's facility. In this case the use of modern, sophisticated means for physical attack are examined, without necessarily causing devastating effects; instead, can cause severe damages in the telecom provider's network. Without the RESISTO system, the telecom provider may become aware of the situation when a series of events have happened, leaving very short response time or when a network or service failure is unavoidable, at least for a short time. Since there is no other information available, all the potential causes must be thoroughly investigated in order to identify the real one and suggest a suitable mitigation action, resulting in increased costs in both time and resources. Even if more information was available, a mechanism to correlate all this different types of information in order to efficiently identify and mitigate the threats, would still be necessary.

The various steps of the whole attack-mitigation cycle are the following:

- A hostile UAV is approaching a telecom asset, namely one or more antenna pillars with various types of antennas (base station, links etc.) that are part of the backhaul network. The antenna pillars are supposed to be part of an antenna park located in a remote area.
- The hostile UAV is detected by the airborne threat detector, already installed in the park, which triggers an airborne threat detection event that is sent to the RESISTO correlator.
- The UAV attack renders the telecom asset (antenna pillar) inoperable (i.e. destroyed by bomb). Subsequently the telecom provider's network experiences severe network loss in an extended level. It is considered that mobile communications and generally all the services are down at least in a wide area surrounding the antenna pillar / park.
- Thus, several network and service failure events are fed into the RESISTO system (from the telecom operator's network management system – NMS).
- Correlating the airborne threat detection and the congestion events, the RESISTO system responds, by issuing a damage inspection command to the RESISTO UAV platform-based sensor. Thus, the RESISTO “friendly” UAV takes-off and initiates a damage inspection procedure using on-board cameras in the vicinity of the airborne threat detection event's location.
- The attack and the “destruction” of the telecom asset (antenna pillar) is identified and confirmed. A corresponding event is fed into the RESISTO system. Then RESISTO responds by selecting and suggesting a suitable mitigation action, for example rerouting of the specific backhaul path, activating auxiliary antennas in the vicinity for redirecting mobile services, repairing of the antenna pillar.

The RESISTO system offers both the increased information by integrating a diversity of sensors/detectors and the correlation mechanism to efficiently detect and mitigate such threats.

Role of the airborne threat detection system in the above Use Cases

Despite the fact that each Use Case presents different scope and addresses different aspects in terms of nowadays threats and security in existing telecom infrastructures, from the above description it is seen that in both sub-scenarios the following common characteristics are in order:

- the physical threat is an airborne one, represented by a hostile small aircraft or a UAV platform, without causing devastating effects. The aim is either to enable cyber threats based on the physical intrusion (Use Case 1 - subcase 1) or to cause moderate physical damages locally with, however, severe impact on the telecom's network (Use Case 2 – sub-scenario 1)
- in both showcases the ICCS airborne threats detection system detects the drone and sends an airborne threat detection event to the RESISTO platform correlator

In general, the ICCS airborne threats detection system is also operating in an environment where other additional RESISTO sensing platforms are functioning, such as the “friendly” UAV platform which can be connected to the audio / visual analytics systems, both offered by ADITESS.

4.3.1. *Setup of the sensing system*

Based on the above description, the deployment of both the two showcases presupposes the following:

- The airborne threats detection system is offered by ICCS

- Both the “hostile” and “friendly” UAV platform are offered by ADITESS, which also offers the audio & visual analytics system for deploying both the scenarios of both Use Cases if needed.
- The location of the telecom facility will be offered by OTE along with the testbed emulating the telecom network which also provides the connection to the RESISTO platform.

As it is noted the same deployment setup will be made for the two showcases, since as far as the airborne threats detection system is concerned, no deviations between the two cases is observed. In principle, the UAV system will be deployed within the telecom facility / building in Use Case 1 or in a location near the remote area that could be affected by potential malicious actions in Use Case 2 (i.e. a nearby monitoring point or a main sub-station within the telecom operator’s network throughout the country). In both showcases the exact location will be indicated by OTE and basically a telecom building facility along with an antenna tower (pillar) in the vicinity could be the main requirements.

For the UAV platforms the deployment process will include the deployment of Ground Control Station (GCS), the preparation of a UAV fleet and the establishment of connection between the GCS and RESISTO infrastructure, as these were described in the previous Chapters. It has to be noted though that the UAV flights should be made in open spaces, away from urban environments, since specific regulations for their flights exist. However, in particular where for the RESISTO pilot a remote telecom area near the main headquarters with the above characteristics is difficult to be located or authorised by the telecom operator, the flight deployment will be done in a controlled by ADITESS airfield.

As a consequence, the deployment setup of the ICCS airborne threats detection system follows the deployment of the UAV platforms, since the detection system should detect the (“hostile”) airborne object; in any case the flight will be real and consequently the airborne detection, either this will be done in a real telecom location or in a controlled airfield. In the latter case the communication of both systems with the OTE testbed and RESISTO platform will be assisted by VPN and LTE networks, emulating the whole setup. The availability of the UAV platforms and the ICCS airborne threats detection systems will cover the whole duration of the Use Cases 1 and 2 pilots as these will be determined in WP7.

Specifically for the deployment setup of the ICCS airborne threats detection system no particular prerequisites exist, apart of course from the power supply, since all components are portable and can be deployed and connected in the required locations in a short time, as this will be shown in the next paragraphs from the preliminary experiments conducted already.

Thus, the main objective of this deployment setup is to “integrate”, in the sense of operating together, the airborne threats detection system with the UAV platforms (either “hostile” or “friendly”) and with the video surveillance stream and check the proper operation of all the functionalities foreseen to be applied. Additionally, the airborne threats detection system’s detection and measurement data (range / distance of the target, angle of arrival etc.) will be cross-checked with the UAVs telemetry data (such as the position, the covered path, orientation) to verify the detection and to serve for debugging purposes and all data will be available for visualization.

4.3.2. Deployment phases of the sensing system

In a similar way with the previous sensing systems (audio & visual analytics and UAV based surveillance system deployed by ADITESS) the deployment of the ICCS airborne threats detection system for the RESISTO pilot is also executed in three main phases and in a step by step approach. In this framework, the deployment of the airborne threats detection system, being in any case a laboratory prototype, is being done initially at the ICCS premises for the lab testing and the first experiments before proceeding to the final deployment to the selected pilot site at OTE premises. The

tests and experiments, both those conducted so far and those foreseen for the next period are described in the following.

4.3.2.1. Lab tests of the sensing system

The initial deployment and configuration of the airborne threats detection system is taking place at the ICCS lab facilities. During these tests, the detectors / sensors are tested as stand-alone components in order to test, calibrate and adjust the relevant software environment while controlling the system through the LabView application. The above tests have been made with a commercial DJI Phantom 3 Advanced Drone shown in the following figure, as described in the previous relevant Deliverable D4.1:



Figure 12 - The commercial drone used for the tests

The drone's main characteristics are: weight 1300 gr, maximum dimension 350mm (without the propellers), maximum speed 16 m/s (58Km/h), flight time (battery autonomy) 23 minutes, maximum height 120m, GPS/GLONASS, remote control up to 3.5Km at 2400 MHz. The rotation speed of each wing may vary from 1500 rpm (in hover mode) up to 3500 rpm (in acceleration mode). A rotation speed of 1500 rpm corresponds to 25 turns per second, thus to a fundamental frequency of 25 Hz; since each propeller has 2 wings, frequencies x 50 Hz are expected.

Communication between the components, quality of images and detection aspects along with the integration of the various sensing components to a more compact configuration and especially the debugging and fine tuning of the intelligent algorithms behind, the detection parameters and the application for the whole visualization took place at this stage. Early prototypes of the system have already been tested in lab environments for drones' detection. The whole development involves the system components testing with the drone in hover mode inside the ICCS lab premises but also small range flights at the ICCS building rooftops as shown in the following figures. More specifically:

Test inside the ICCS lab premises involved test inside the lab rooms and inside the ICCS anechoic chamber as well, so that to avoid any other kind of interference (i.e. background noise electromagnetic or even acoustic). There the drone was basically in hover mode or in strictly controlled slight flying movements with low rpms for safety and precaution purposes (since the drone was inside a closed area / compartment). Various settings and configurations for various rotation speeds and acceleration factors were tested as this is shown in the following indicative snapshots taken from a submenu of the LabView general control application; alarm peaks are detected as in the left figure while the right one represents the detection response for higher rotation speeds in acceleration mode.

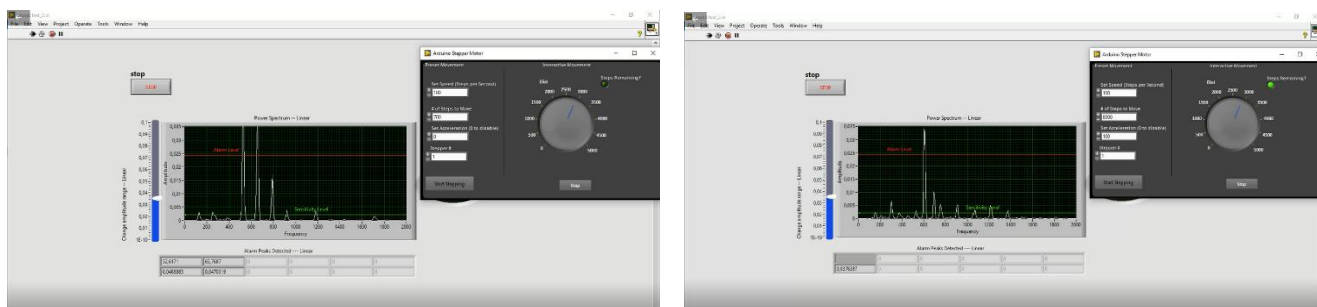


Figure 13 – Operation plots from lab tests

Apart from the above indoor tests, small range flights at the ICCS building rooftops took place in order to test the basic system functionalities, to perform the relevant debugging and to upgrade the application visualization environment and parameters. The drone was flying at a very short range of 70-100m with cautious movement control due to the urban environment, while the detection system was placed on the rooftop as shown in the following figure:



Figure 14 – Rooftop tests with drone

4.3.2.2. Preliminary short experiments with the sensing system

Apart from the lab testing, preliminary experiments of the ICCS airborne threats detection system have already been conducted in nearby airfields that are located in Athens, Greece (where the ICCS premises are). This was exploited by ICCS in order to obtain more measurement data from real flight cases and thus optimize and train the inherent algorithms. The placement of the airborne threats detection system and its components was made at the rooftop so that a good field view towards the airfield was accomplished and thus a line-of-sight without any obstacles could be achieved.

Concerning the electromagnetic RF radar component, strong reflected (echoes) signals were detected from all the airborne platforms flying even from ranges of more than 600m with adequate margins, as seen in the following figures, while various sensitivity thresholds (through Fourier transformation and other techniques) were tested.

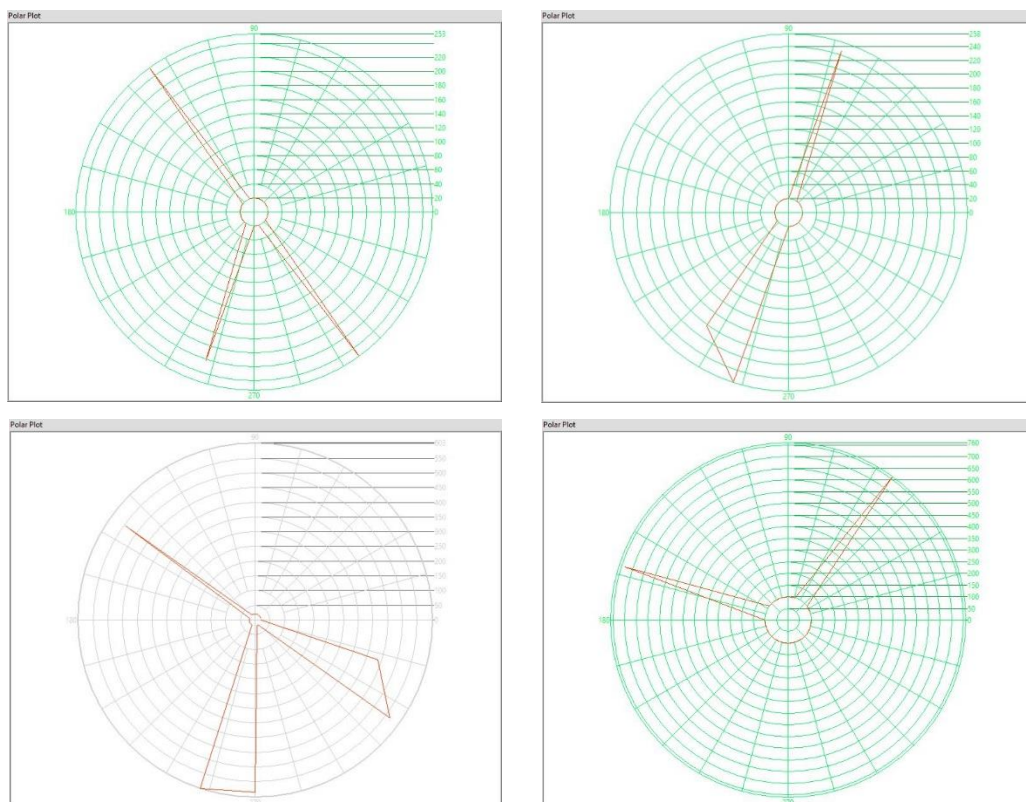


Figure 15 – The radar detection polar plots from short experiments

Concerning the acoustic sensors, quite many acoustic signatures were gathered from all the different airborne objects available (i.e. small aircrafts, UAV platforms such as octocopters, etc.), used to optimize and train the machine learning algorithms behind. The tracking of the direction of arrival (DoA) based on the strongest sound of the airborne platform was adequately performed and stability on the relevant quadrant indicating this DoA was also noticed, as seen in the following snapshots of the application visualization menus.

Another issue to be mentioned is that no aspects related to degradations in performance were noticed due to environmental conditions (i.e. heat and humidity) even after many hours of the system operating under the sun.

The main aim of these independent short experiments is to test, calibrate and optimize the detection aspects and related parameters (i.e. angle of arrival, range etc.); it is clear that the more tests are made, more measurement data are used to train and calibrate the whole system and thus to improve the accuracy in the detection mechanisms. These independent experiments were and are currently being conducted by ICCS, exploiting every relevant opportunity and represent the first stage of such work, targeting the improved performance of the whole setup.

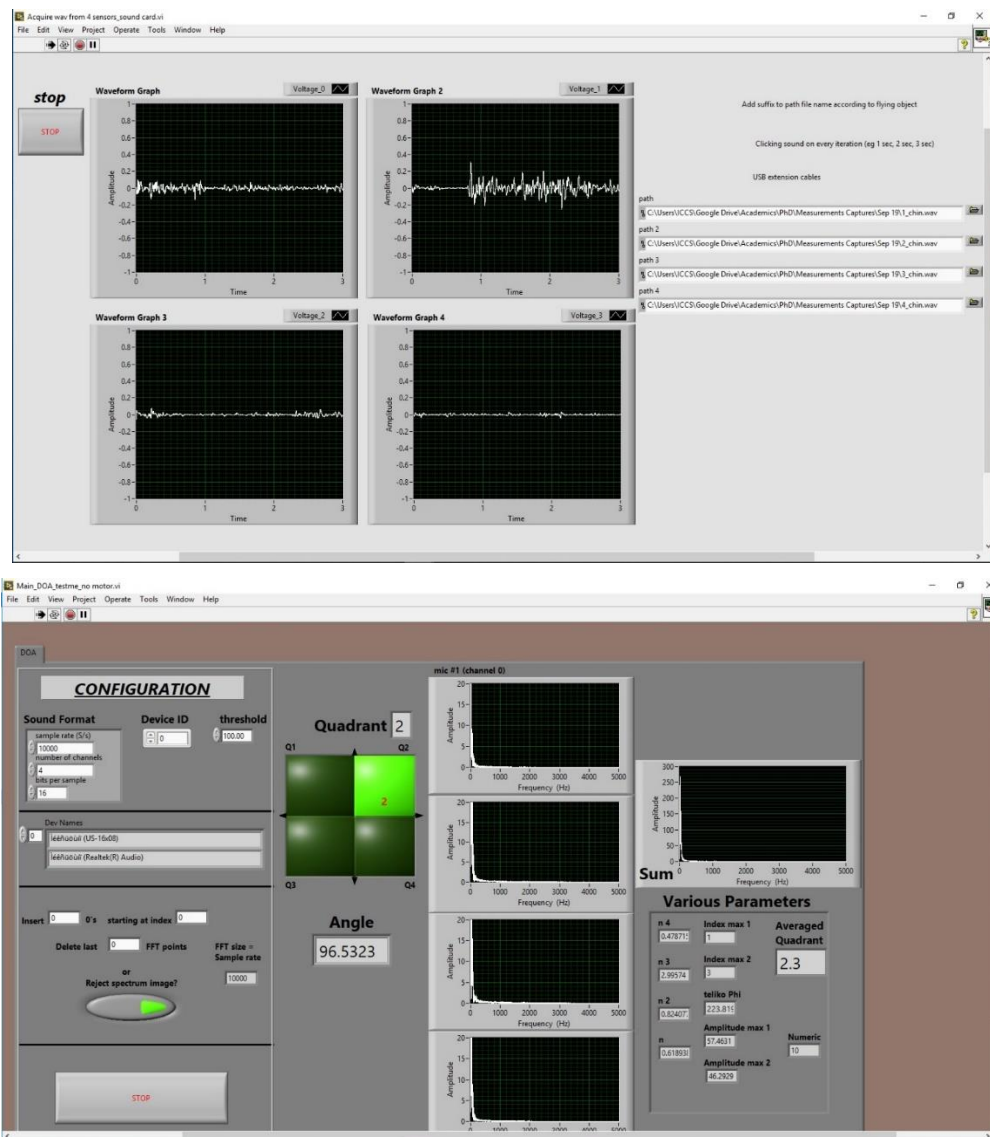


Figure 16 – Acoustic signatures of the airborne platforms and direction of arrival quadrants

The second stage of this work, foreseen through the project implementation and to be conducted in the immediate next period, focuses on the integration of the airborne threats detection system with the RESISTO platform. A series of integration tests will be performed using a VPN account and through

the connection with RESISTO broker. **At this stage, the deployment of the system will take place in a dedicated airfield that is hosted at ADITESS premises in Cyprus specifically for the RESISTO test purposes (as described already in the previous Chapters).**

The system's performance indicators and detection aspects will be evaluated and adapted for the needs of the specific Use Cases so that the appropriate preparations to be made prior to the final project piloting deployment. The development and configuration of the intrusion event messages will be prepared as the output of the system and the interface with the RESISTO platform. Furthermore simultaneous experiments with the ADITESS surveillance systems (audio & video analytics and UAV "friendly" platforms) will be conducted so that to test the common identification and correlation of targets, along with the execution of scenarios similar to the corresponding Use Cases.

It is seen that the whole deployment in this phase of the work corresponds to all the preparation and integration actions before the final deployment phase that follows in the next paragraph.

4.3.2.3. *Foreseen final deployment*

The last phase will be the deployment of the ICCS airborne threats detection system at OTE premises and the issue of potential intrusion events and alerts through the RESISTO HMI Platform. The final development and configuration of the detection parameters as well as the calibration of sensors will take place before the execution of the pilot implementation according to the relevant Use Cases.

Depending on the site area selected by OTE for the execution of both Use Cases 1 and 2, the ICCS airborne threats detection system will follow the UAV flight campaign arrangements that will be done by ADITESS since these existing UAV platforms will be used to emulate the "hostile" airborne threats and thus the "targets" of the ICCS detection system. Concerning the deployment of the UAV system for the final pilot, in case that this cannot be held in an urban environment due to flight restrictions and law requirements (if related test sites are selected by OTE), the UAV flights will be performed in Cyprus (at the same airfield of test flights) while the data will be adapted and translated to fulfil the location requirements of the pilot. The detection data from the site will be transferred to the test beds at OTE premises for further processing, visualization and interface with the RESISTO platform.

5. NETWORKS AS SENSING SYSTEMS: RADIOFILTER

As already denoted in the Introduction Section, the present RADIOFILTER tool is the upgraded tool concerning the implementation of Signal Monitoring WSNs as Sensing systems (including Guardtime's KSI blockchain functionalities) which were described within the previous D4.1 Deliverable. As already stated the follow up of the relevant sensors described in D4.1 is the RADIOFILTER integrated sensing tool given herein.

RADIOFILTER it is a tool developed by INTEGRASYS which offers detection, location and reporting of WLAN based threats and attacks to Critical Infrastructures (CI) protected assets.

The main WLAN based threats that RADIOFILTER is able to monitor are the following:

- Malicious 802.11 WLAN active scanner
- 802.11 WLAN Denial of Service (DoS)
- Rogue 802.11 WLAN Access Point (AP)
- Unauthorized 802.11 WLAN AP inside the CI
- Rogue 802.11 WLAN device
- Unauthorized 802.11 WLAN device attempting to connect to an AP
- Unauthorized 802.11 WLAN client device
- Unauthorized 802.11 WLAN connection (involving an authorized device)
- Unauthorized 802.11 WLAN device location
- Unauthorized 802.11 WLAN unconnected device inside the CI (unauthorized access)

5.1. Short description of the sensing system

RADIOFILTER tool is based on a network of N distributed passive **Secured Cyber Sensors**, deployed at an infrastructure, which continuously scan the data-link traffic and relay this information to a central processing node (**Central Node**). This setup enables the system to monitor the data-link (layer 2) traffic parameters in 802.11 WLAN networks in order to detect, locate and report 802.11 WLAN based threat events to the **RESISTO platform** Short Term Control Loop as Kafka publish messages. The events and useful related information can be visualized also through an external **RADIOFILTER Web User Interface** for standalone use.

The integrity of the cyber sensors' firmware is taken care of by a **Firmware Update Server** which connects to an external **Guardtime KSI Server** for generating KSI signatures of the sensor firmware. Every time there is a new firmware version available, the update server signs a hash of the new firmware with its PKI private key and generates an anonymous KSI signature used as a cryptographic timestamp which provides temporal reference for PKI certificate chain verification. These firmware security anchors (including the current installed firmware KSI signature) are retrieved by the sensor to check that the new firmware version has not been maliciously tampered with.

Below, the architecture is depicted. The blocks in grey correspond to the parts of the RADIOFILTER architecture itself, whereas the blocks in other colours the systems to which it connects

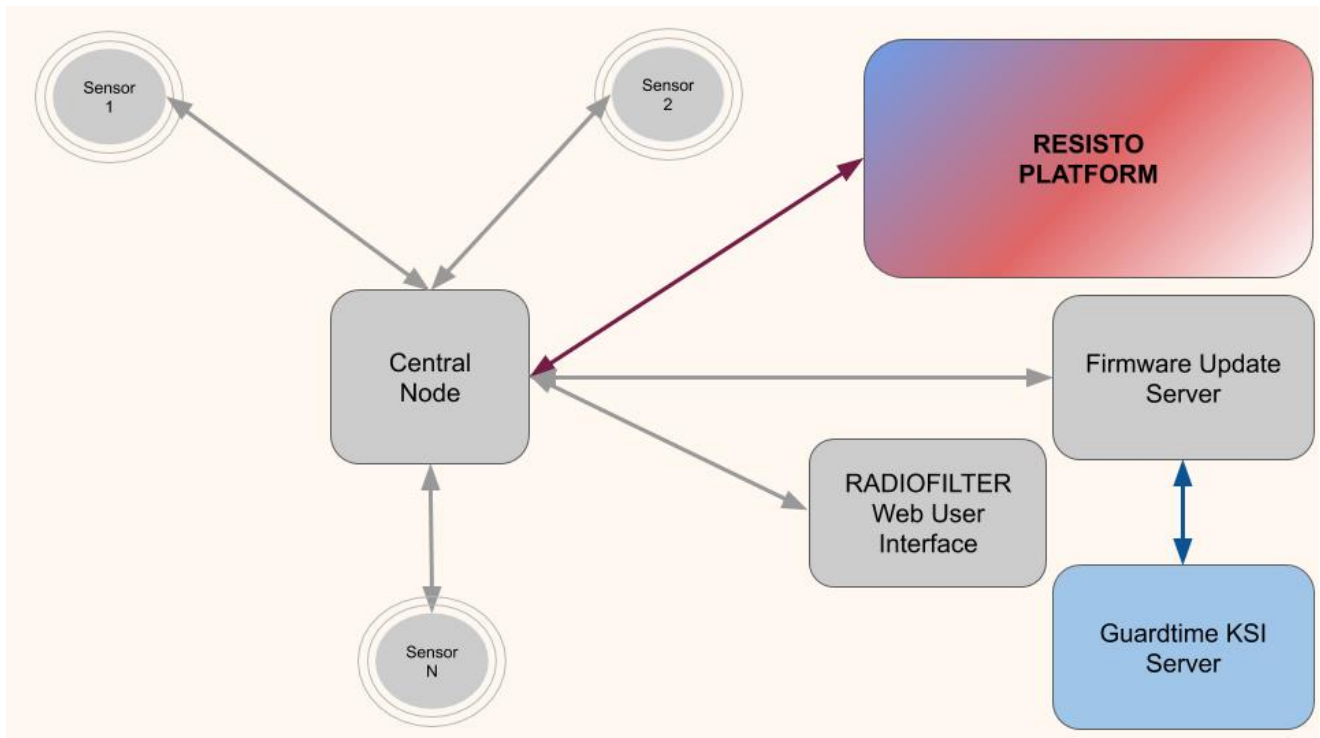


Figure 17 – RADIOFILTER Overall Architecture

Below, a short description of each of these components is provided:

- **Secured Cyber Sensors:** Each monitoring cyber sensor is powered by a small single-board computer. The model that has been chosen is a Raspberry Pi 3B+. This version has the following specifications:
 - 1.4GHz 64-bit quad-core ARM Cortex-A53 CPU
 - 1GB LPDDR2 SDRAM
 - Connectivity: Dual-band 802.11ac wireless LAN (2.4GHz and 5GHz), Bluetooth 4.2 Low Energy and 300Mbps Ethernet (The on-board Ethernet or 802.11ac chips are used for the communications link to the aggregation server).

The sensor is able to monitor the following WLAN technologies IEEE 802 b/g/n/ac, (2.4GHz and 5GHz bands). The monitoring function is performed by a Linksys WUSB6300 adapter connected to the board. The adapter antenna gains are the following:

- Antenna 1: 2.4GHz: 2.31 dBi, 5GHz: 3.84 dBi
- Antenna 2: 2.4GHz: 1.72 dBi, 5GHz: 4.29 dBi

The sensor also includes a secure element (Zymkey 4i module) used to encrypt and store critical data such as root certificates and firmware security anchors.

- **Central Node:** This is the main node in the system and perform several functions:
 - Aggregation module: An aggregation server which collects data captured by the cyber sensors from all the access points, devices and connections in the infrastructure. This data is stored and fed into the processing module.

- Location module: Estimates a specific access point or device location using a fingerprinting method based on machine learning techniques.
 - Processing module: Processes the information from the aggregation and location modules and generate events.
 - Kafka producer: Source of WLAN based threat events data to the RESISTO platform Kafka consumer.
 - Web Server: Server for the RADIOFILTER Web User Interface.
 - Whitelist database: Stores the different infrastructure whitelists used for event detection.
 - Sensor Remote Management: Deals with the configuration of sensor parameters and acts as a gateway with the Firmware Update Server for firmware updates
- **RADIOFILTER Web User Interface**: Web Application that can be accessed on-premises or remotely to visually monitor the events and useful related information. It includes features such as Building Map, Dashboard and Events log
 - **Firmware Update Server**: Manages the sensor firmware updates by using the following modules:
 - Software Updater
 - Build system
 - Signing System (PKI and KSI)
 - Management Server

5.1.1. Detection objectives of the sensing system – what is meant to be measured

In this section a table is shown with the parameters that are measured by RADIOFILTER sensors. A description is given for each of them as well as an indication of whether they are Access Point related, Device related or both. Finally, the last two columns indicate which threats or attacks these parameters help to detect and which are the value or range of values that trigger a detection event.

Parameter	Description / Range to be Measured	AP Related	Dev Related	Threat/Attacks where it helps detection	Anomaly value
SSID	32-byte long name of the AP WLAN network. If all bytes are set to zero, then it is a hidden SSID	Yes	-	Rogue WLAN AP 802.11	Repeated value
BSSID	MAC-Address of the AP or device. 6-byte identifier with the following format: 01:23:45:67:89:AB	Yes	Yes	Rogue WLAN AP 802.11 Rogue WLAN device 802.11	Repeated value

				Unauthorized 802.11 WLAN unconnected devices inside the CI Unauthorized 802.11 WLAN device attempting to connect to an AP Unauthorized 802.11 WLAN AP client Unauthorized 802.11 WLAN device location	Value not whitelisted/allowed
RSSI	Received Signal Strength Indicator in dBm. Typically ranging from -30 to -90 dBm. Where -30 dBm means an excellent level and -90 dBm a very poor level.	Yes	Yes	Rogue 802.11 WLAN AP 802.11 WLAN Denial of Service (DoS) Malicious 802.11 WLAN Active Scanner	Abnormally high value
Channel Number	Center Frequencies in the following ranges: 2412-2471MHz, 5180-5240MHz	Yes	-	Rogue 802.11 WLAN AP	Different value for the same BSSID
				Malicious 802.11 WLAN Active Scanner	Changing values
Channel Bandwidth	Signal occupied channel width: 20, 40 or 80 MHz	Yes	-	Rogue 802.11 WLAN AP	Different value for the same BSSID
				Malicious 802.11 WLAN Active Scanner	Changing values
Encryption Type	Security protocols to secure the wireless network: None (Open), WEP, WPA and WPA2	Yes	-	Rogue 802.11 WLAN AP	Different value for the same BSSID Value different from WPA2
Location	A room level identifier such as: "Room A", "Room B"	Yes	Yes	Unauthorized 802.11 WLAN device location	Unauthorized value
				Rogue 802.11 WLAN AP	Changing values

				Rogue WLAN AP 802.11	Different value for the same <u>BSSID</u>
				Rogue WLAN Device 802.11	
Technology	IEEE 802.11 version. The following can be detected: b/g/n/ac	Yes	-	Rogue WLAN AP 802.11	Different value for the same BSSID
Number of Clients	Number of devices connected to a specific AP	Yes	-	Rogue WLAN AP 802.11	Different value for the same BSSID
				802.11 WLAN Denial of Service (DoS) Malicious WLAN Active Scanner 802.11	Zero or small value
Number of Packets	Number of monitored packets by the cyber sensors	Yes	Yes	802.11 WLAN Denial of Service (DoS) Malicious WLAN Active Scanner 802.11	Abnormally high value in a short period of time
Connection type (Client specific)	Indicates whether traffic from a client goes through the AP (centralized) or not (ad-hoc)	-	Yes	Unauthorized 802.11 WLAN connections	Unauthorized value
Traffic scope	Indicates whether traffic from a client is kept local or reaches external networks (e.g. Internet)	-	Yes	Unauthorized 802.11 WLAN connections	Unauthorized value
Packet type (Monitoring Traffic Activity)	Indicated the type of detected packet type. Some common types include: Beacon, Probe Request and Response, Deauthentication...	-	Yes	Rogue WLAN AP 802.11	Abnormally high number of Beacon type
				802.11 WLAN Denial of Service (DoS)	Abnormally high number of Deauthentication type
				Malicious WLAN Active Scanner 802.11	Abnormally high number of Probe Request type

5.2. General deployment requirements

The infrastructure to be protected must fulfil the following general requirements in order for RADIOFILTER to be properly deployed:

1. The infrastructure must have a 802.11 WLAN network with one or more access points
2. The WLAN technology of the network must be 802.11b, 802.11g, 802.11n or 802.11ac
3. The infrastructure must have connection to external Networks
4. N+1 power plugs for the Central Node and the sensors, where N is the number of sensors to be deployed. If the sensors are going to run on batteries, then a minimum of 1 power plug is needed for the Central Node.

Likewise, the infrastructure owner must provide the following input data:

1. List of threats and attacks to be detected
2. The following whitelists:
 - a. Access Point Whitelist: BSSID of the APs allowed inside the infrastructure
 - b. Device Whitelist: BSSID of the Devices allowed inside the infrastructure
 - c. Client Whitelist: BSSID of the Devices allowed to connect to the WLAN
 - d. Client Connections Whitelist: Type of connections (centralized, ad-hoc, local and internet) allowed for each WLAN client
 - e. Client Locations Whitelist: Locations (e.g.: "Room A", "Room B"...) allowed for each WLAN client
3. Digital map of each floor (including power plugs) of the infrastructure to be protected
4. Infrastructure Network map, including all the devices and their connections

Finally, the deployment of the tool has to follow a set of guidelines:

1. At least one sensor must be deployed per room.
2. The sensors must be placed at a sufficient height above ground level.
3. Enough coverage must be guaranteed from each sensor to the Central Node in case wireless links are used. Otherwise Ethernet cables will be used.

5.3. Deployment of the sensing system in a Generic Use case

As already demoted in the Introduction Sections, the RADIOFILTER is meant to be implemented in a variety of scenarios that can accommodate the **Use Case 5 "Protection of Cloud Storage Services" sub-case 1 on Healthcare and sub-case 2 on smart manufacturing** hosted by TIM. Furthermore, they can be employed in the **Use Case 4: "Disruption of major sporting event by combined physical & cyber-attack by a terrorist organization"** hosted by BTC and **Use Case 7: "Maritime Safety and Emergency Case"** hosted by RTV. The above are the most representative Use Cases where the tool can be applied. The relevant deployment procedure is described in detail herein, however, the exact location and implementation will be decided on site upon the definition of the pilot area by the hosts / telecom operators in the framework of WP8 and WP9. Nevertheless, quite many discussions have been taken place among the relevant partners and the deployment aspects have already been defined as it will be seen in the relevant Chapters. To this respect, the relevant deployment details for the RADIOFILTER are given in the following **for a Generic Use Case**, assuming that this can represent the variety of Use Cases where the tool will be employed.

5.3.1. Setup of the sensing system in the framework of a Generic Use Case

A generic Use Case for the deployment of RADIOFILTER tool is described in this section.

A critical infrastructure operator wants to protect a building with two rooms from confidential information stealing and service disruption risks. The building has an 802.11 WLAN Network and only one AP and reduced set of devices are allowed inside the infrastructure. Besides, the AP only must accept a specific set of client devices and the devices must have location and connectivity restriction.

Below, a diagram of the infrastructure to be protected is shown.

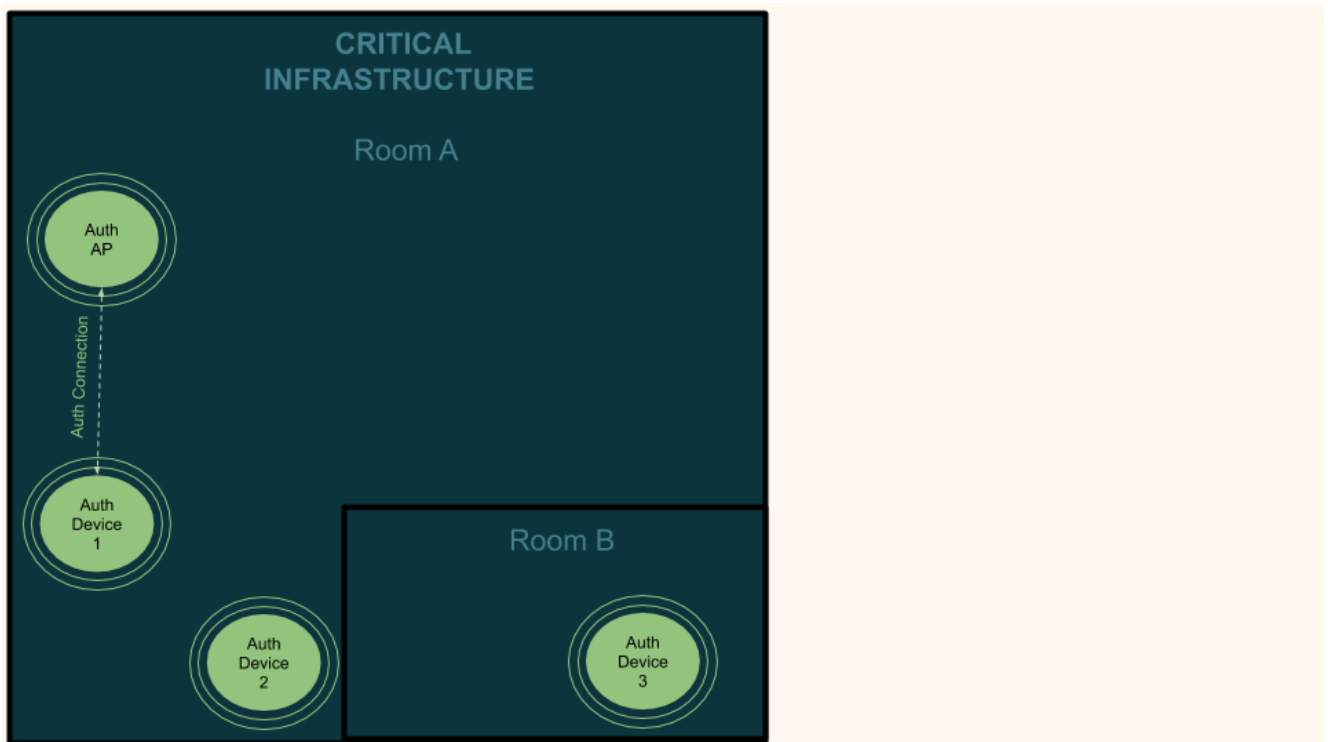


Figure 18 – Critical Infrastructure diagram in a generic Use Case

The deployment of RADIOFILTER at the infrastructure can be divided into three phases that are followed sequentially:

1. **Planning.** Based on the input from the infrastructure owner (Whitelists, Digital Map, Infrastructure Network Map and specific requirements), a survey is made to produce an estimation of the required number and location of sensors as well as the general configuration parameters of the system.

Below, a diagram with an example of an estimation of the location of RADIOFILTER components at the infrastructure is shown.

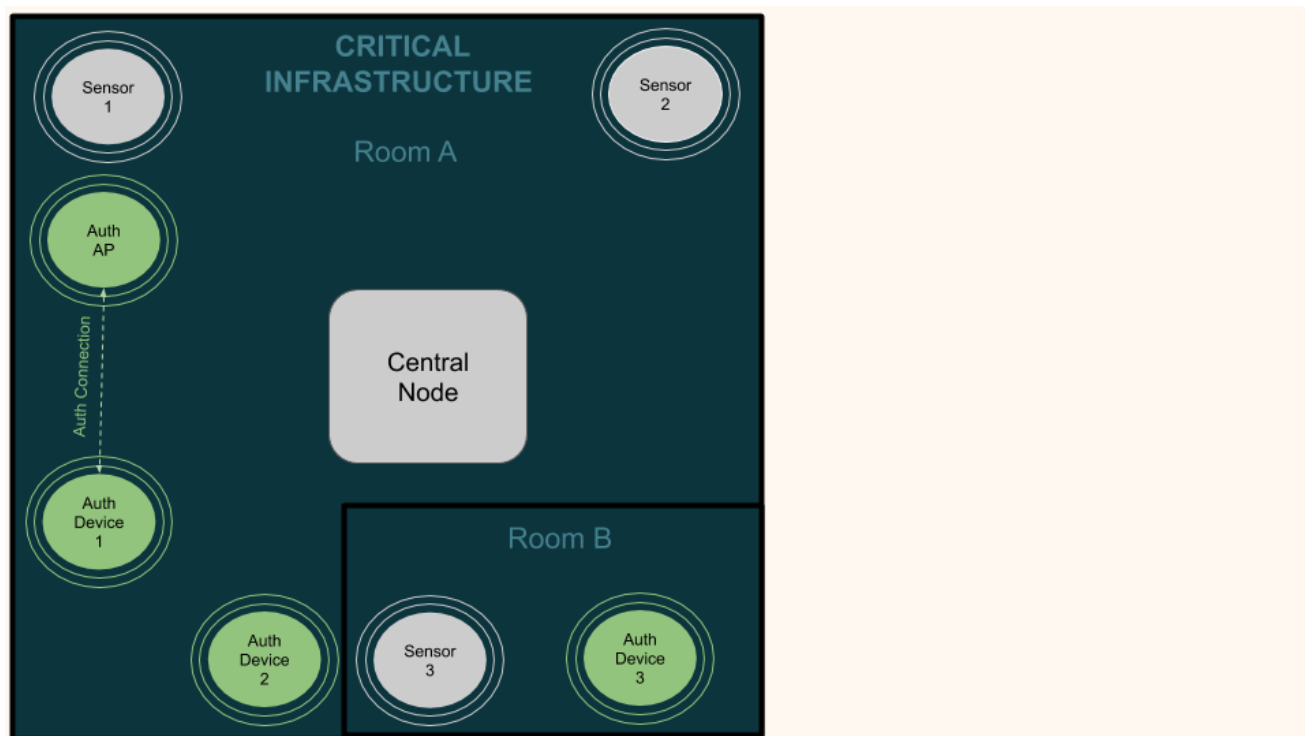


Figure 19 – Planned RADIOFILTER deployment in a generic Use Case

2. **Setup.** All the equipment is carried to the infrastructure and initially set up. Correct operation and connectivity is checked among RADIOFILTER components. Connectivity tests include local level (Sensors \leftrightarrow Central Node) and external (Firmware Update Server \leftrightarrow Central Node, Web User Interface \leftrightarrow Central Node and RESISTO platform \leftrightarrow Central Node), Corrective measures are taken from the initial planning if needed (e.g. poor coverage from one sensor to the Central Node if wireless links are used).

Below, a diagram showing the connectivity between RADIOFILTER components at this phase is shown.

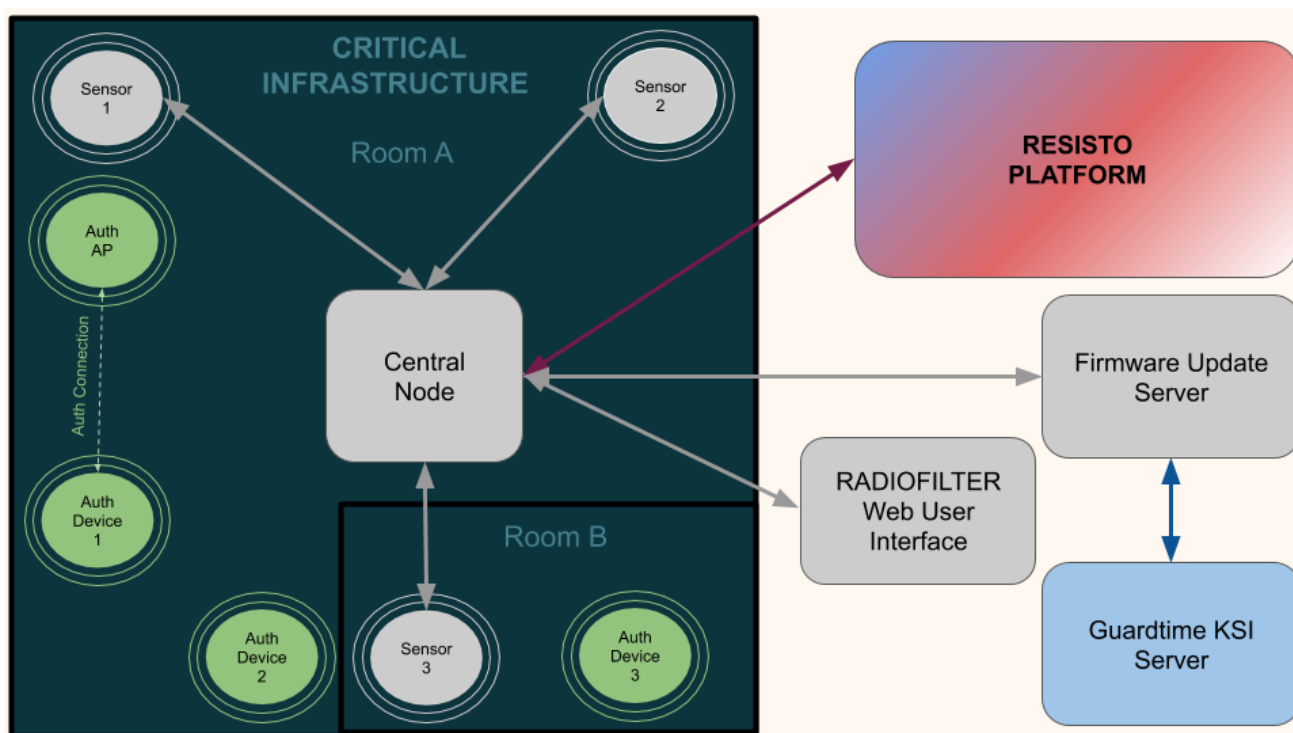


Figure 20 – Setup phase at RADIOFILTER deployment in a generic Use Case

3. Location Training. Once the Initial Setup phase has been completed, the Training phase is started. This phase is needed to enable the location capabilities of the tool. A training device (or set of devices) must be used at least in one location of each room to be protected. Each location will be fingerprinted with the signals levels received by each sensor. This information (training dataset) will be used to train and tune the machine-learning positioning based model will be predict the location of the access points or devices in RADIOFILTER.

Below, a diagram showing the training phase is shown.

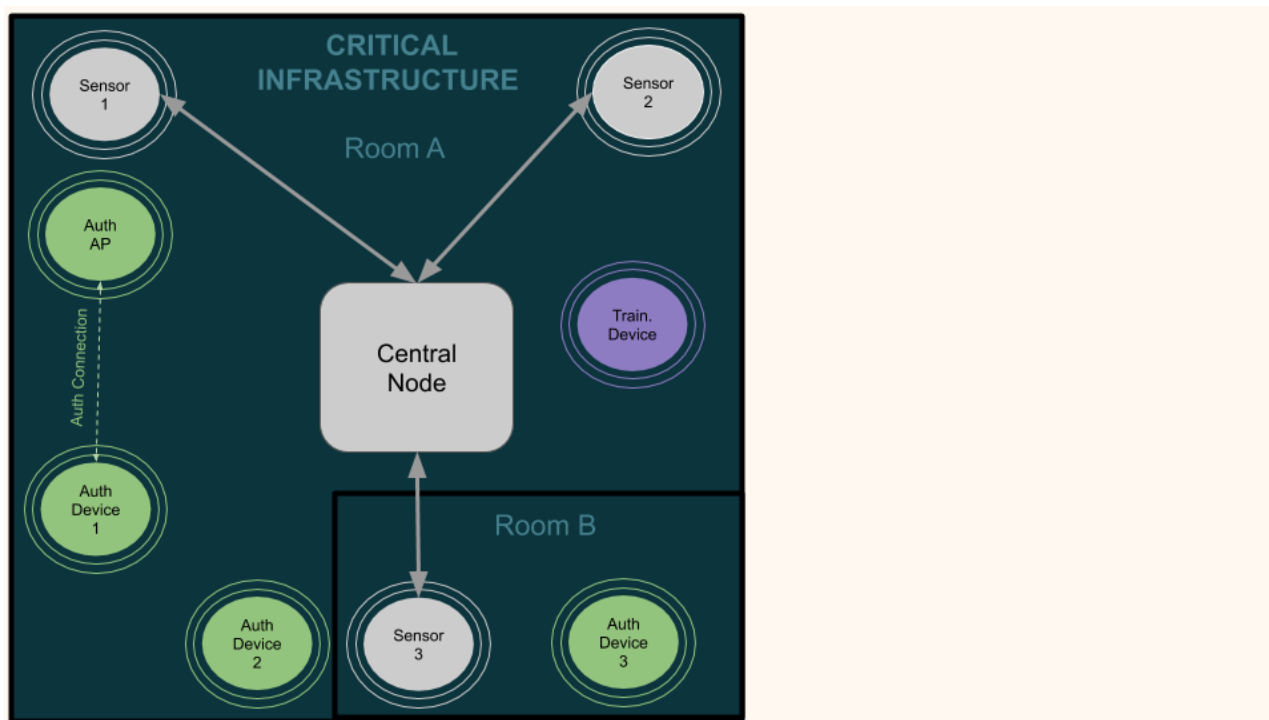


Figure 21 – Training phase at RADIOFILTER deployment in a generic Use Case

Once, the different phases are completed the system is ready to start operating. Upon operation a set of threats events can be detected by the tool at the critical infrastructure. In the diagram below some examples are shown: Rogue 802.11 WLAN Access Point (AP), unauthorized 802.11 WLAN client device, unauthorized 802.11 WLAN device location and unauthorized 802.11 WLAN connection (involving an authorized device).

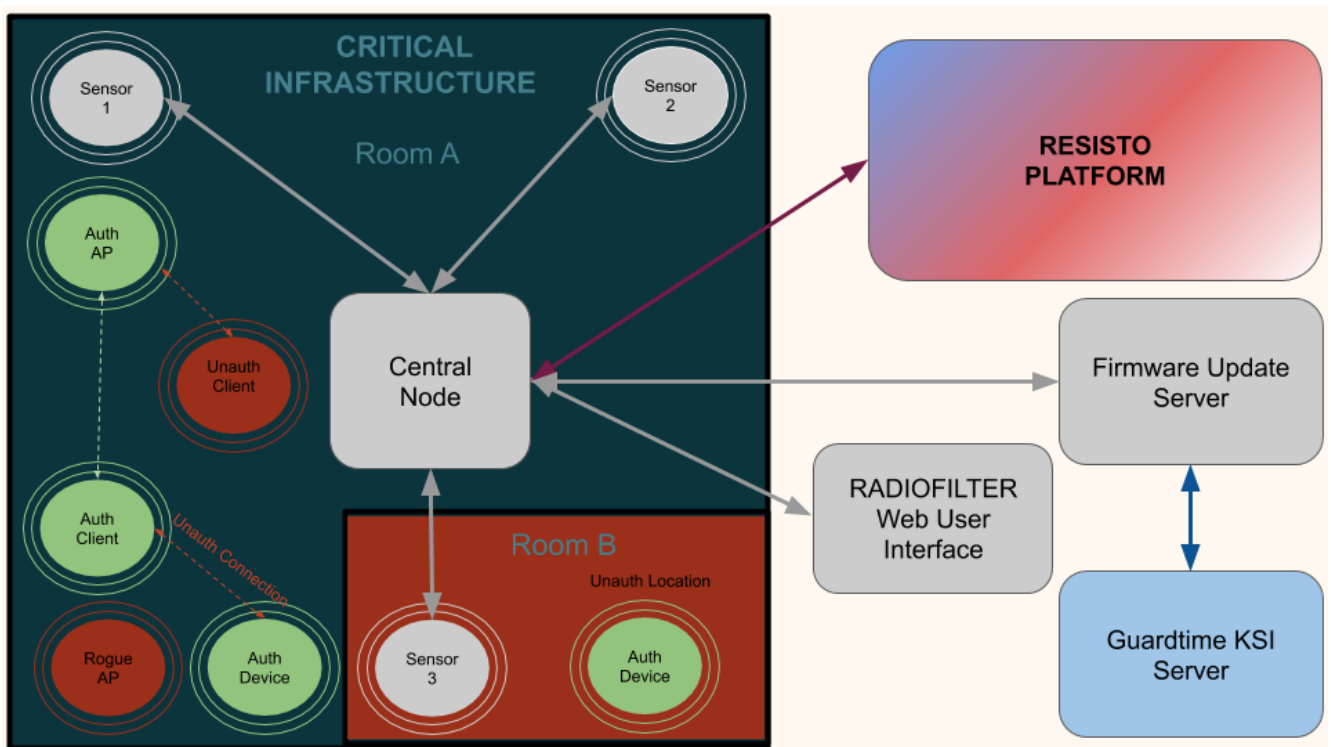


Figure 22 – RADIOFILTER threats detection at the critical infrastructure in a generic Use Case

5.3.2. Deployment phases of the sensing system

5.3.2.1. Lab tests and short experiments of the sensing system

A number of tests have been carried out at Integrasys premises to check the proper operation of RADIOFILTER sensors. The testing premises are made up of two rooms.

The threat events which were tested are the following: Unauthorized Device Event Detection, Unauthorized Access Point Event Detection and Unauthorized Connection Event Detection.

In the figure below, a screenshot of the RADIOFILTER Web User Interface is shown. On the left side, the Building Map is located, whilst on the right side the Dashboard and Events Log can be seen.

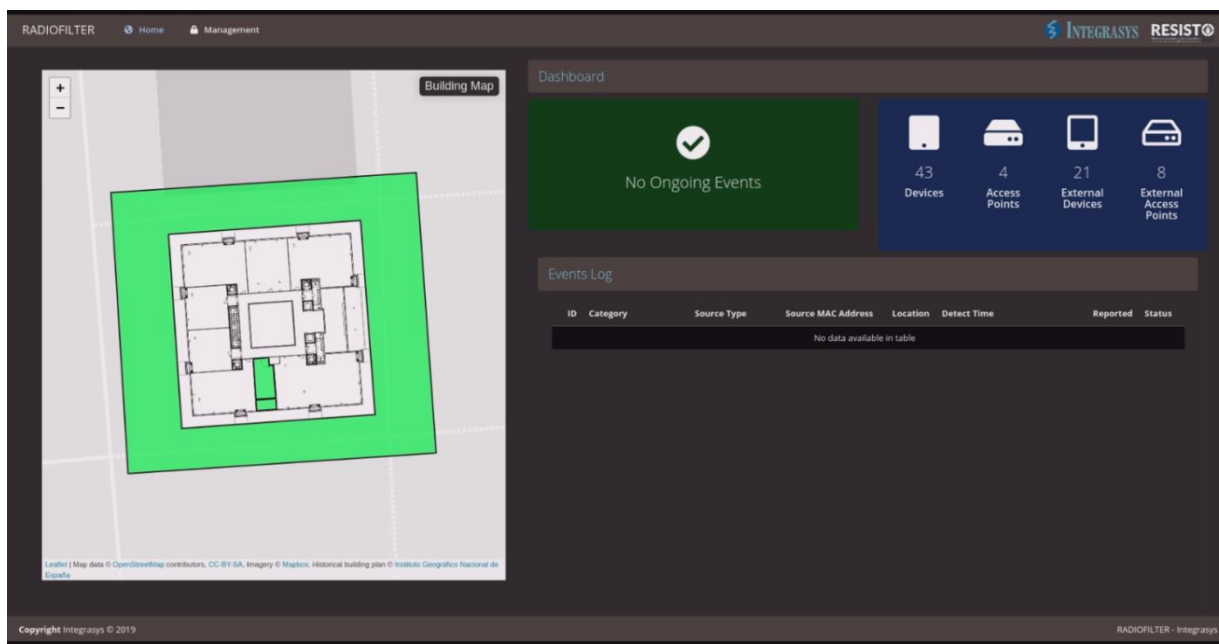


Figure 23 – RADIOFILTER Web User Interface running in the test campaign without any events detected

Below, a picture of one of the radio monitoring sensors used in the test campaign is shown.



Figure 24 – RADIOFILTER Secured Radio Sensor

In order to do the test campaign, the whitelists were generated and stored in the Central Node. Then, the tool was deployed with two sensors at the premises. Wireless connectivity links between the sensors and the Central Node were tested. Also, following the planning and setup phases, a training stage was carried out with a mobile phone as the training device. Then, the tool was ready to test the sensor detection capabilities.

Below, a summary of each test is provided:

- Unauthorized Device Event Detection Test.** A non-whitelisted mobile phone with WLAN connectivity was used to trigger an event in this test. Initially, the WLAN module was switched off and when the module was turned on (touching the WLAN icon in the Shortcut Menu of the phone) the event was detected, as the BSSID (MAC Address) of the device was not in the Device Whitelist. In the figure below, a screenshot of the Web User Interface (left-hand side) and the device screen (right-hand side) is shown. A new event detect message appears at the Dashboard when the device's Wi-Fi is turned on. In the Events Log the event information is displayed and on the map the location of the event (larger room) is shown in flashing red colour.

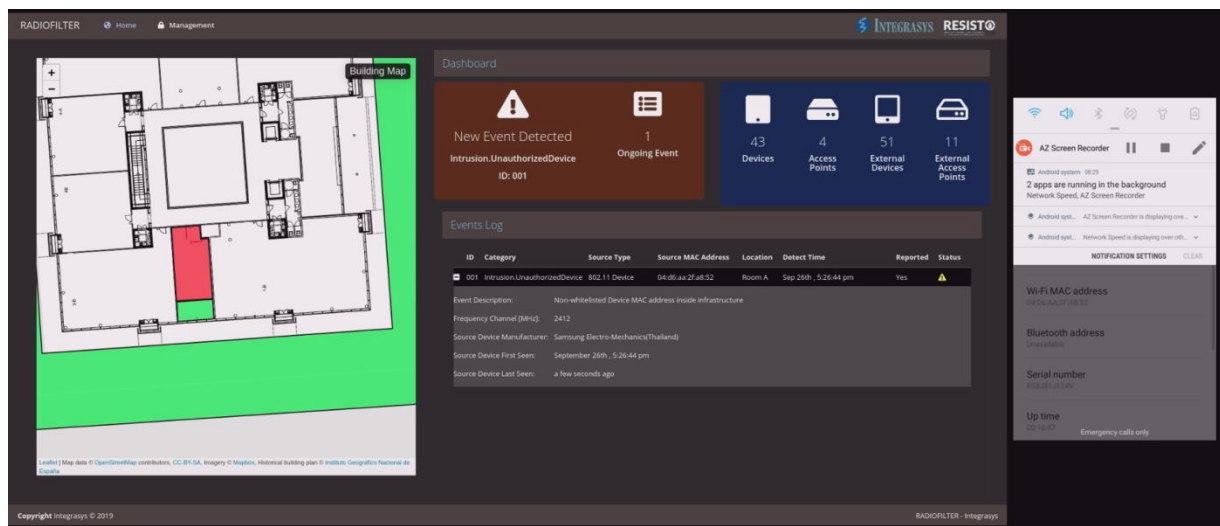


Figure 25 – RADIOFILTER Web User Interface upon Unauthorized Device Event Detection

- Unauthorized Access Point Event Detection Test.** A non-whitelisted WLAN Access Point was used to trigger an event in this test. Initially, the Access Point was switched off and when turned on the event was detected, as the BSSID (MAC Address) of the Access Point was not in the Access Point Whitelist. In the figure below, a screenshot of the Web User Interface (left-hand side) and a picture of the AP (right-hand side) is shown. A new event detect message appears at the Dashboard when the AP is turned on. In the Events Log the event information is displayed and on the map the location of the event (smaller room) is shown in flashing red colour.

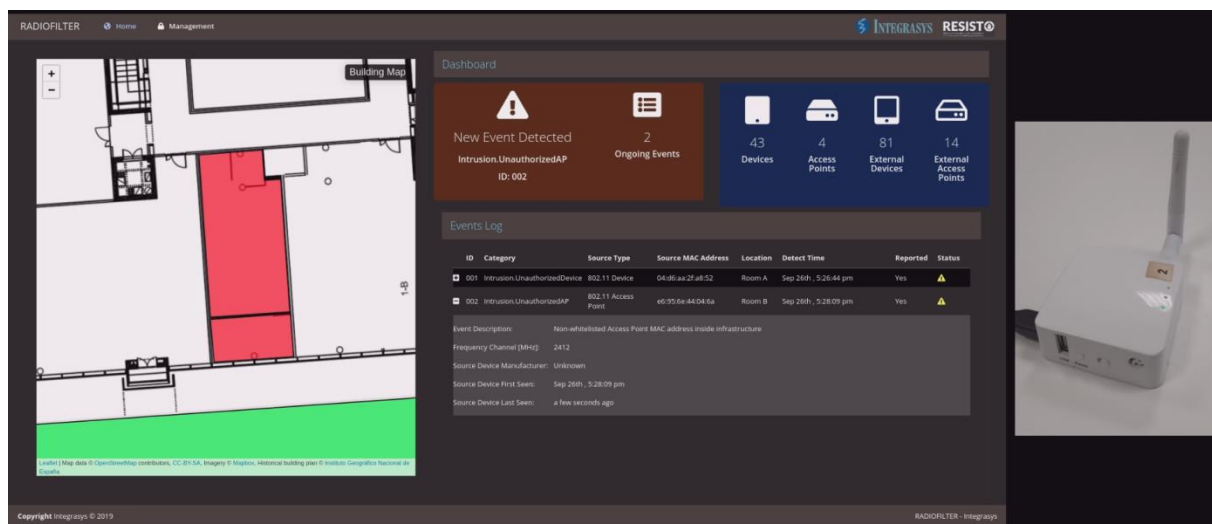


Figure 26 – RADIOFILTER Web User Interface upon Unauthorized AP Event Detection

- **Unauthorized Connection Event Detection Test.** A non-whitelisted WLAN ad-hoc connection between authorized clients was used to trigger an event in this test. Initially, the devices were connected to the AP but not through an ad-hoc connection. A UDP ad-hoc connection was established using the iPerf command-line tool and then the event was detected, as this type of connection was not in the clients Connection Whitelist. In the figure below, a picture of the Web User Interface (left-hand side) and the clients terminal window (right-hand side) is shown. A new event detect message appears at the Dashboard when the connection is established. In the Events Log the event information is displayed and on the map the location of the event (larger room) is shown in flashing red colour.

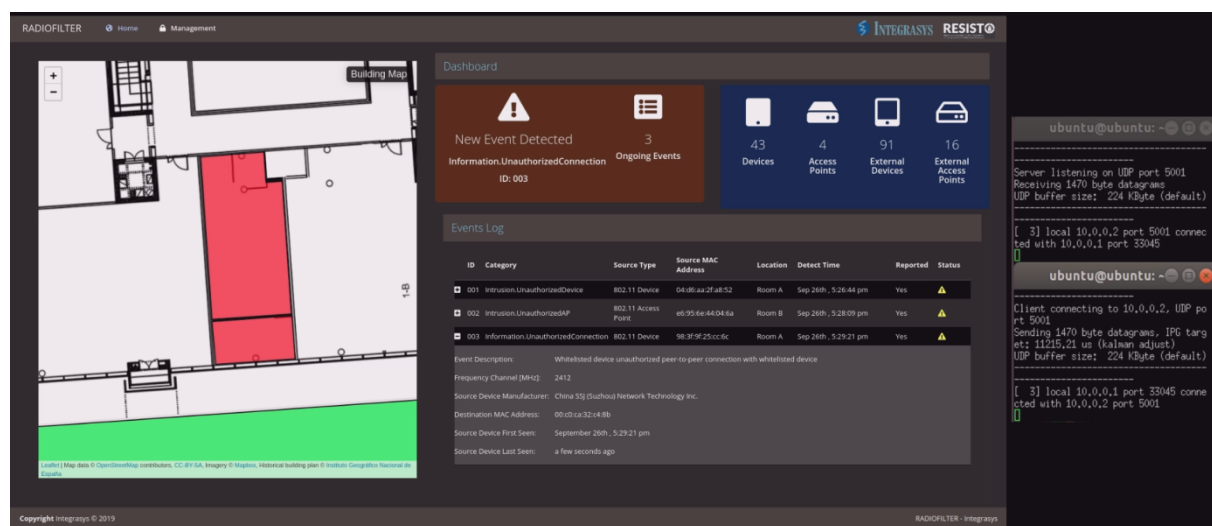


Figure 27 – RADIOFILTER Web User Interface upon Unauthorized Connection Event Detection

5.3.2.2. *Foreseen final deployment*

As already discussed, the exact location and implementation for the final deployment for the various related Use cases will be decided on site upon the definition of the pilot area by the hosts / telecom operators in the framework of the relevant WP8 and WP9. Nevertheless, quite many discussions have been taken place among the relevant partners and the deployment aspects have already been defined as it will be seen in the relevant Chapters.

5.3.2.3. *Sensitivity of the monitoring system sensors*

Sensitivity of the monitoring system sensors indicates the minimum signal strength that the sensors are able to detect and, therefore, will determine to a great extent the number of detected devices. This corresponds to the threat detection function in order to effectively measure the detection capabilities.

This parameter is a number that indicates the capability of the system, the number of devices that the sensor or the sensors which make up the monitoring system is able to analyze. This is useful to evaluate the coverage that could handle the monitoring system. The different values that can be obtained could be for example, a system which is capable of receiving low signal strength, would have a value of 3 (good coverage), a system which is capable of receiving medium signal strength, would have a value of 2 (medium coverage) and a system which is capable of receiving only high signal strength, would have a value of 1 (low coverage).

The measurement method for this detection parameter is rather straightforward. Since, the scenarios and use cases will be evaluated during the pilots the detection capabilities of the overall system under almost real-life conditions, measuring this won't impose any overhead at all. Moreover, even before that, during the testing following the development period, this measurement would be rather easy and will give an indication to the platform what critical infrastructure could be assigned to the monitoring system for the detection of potential threats. Large critical infrastructure could be assigned to system monitoring with high value of this parameter. It would be convenient to decide a standard for the definition of the different values taking account the signal strength of the sensors. This is a single number and it is not time dependent. It can be easily estimated and measured during different phases of the project (see above).

An adequate number of sensors with good signal strength could be included to the monitoring system through the test beds or through the use-case scenarios to improve benefits. Relevant benchmarks can also be sought either in literature or from the telecom operators and end-users. As discussed previously, it is feasible to be and it provides a good indication of the overall detection capabilities of the system. In a commercial version of the system it would probably one of the key marketing points.

6. NETWORKS AS SENSING SYSTEMS: RANMONITOR

As already denoted in the Introduction, the present RANMONITOR tool is the upgraded tool concerning the implementation of Femtocells-based Sensing systems described within the previous D4.1. As already stated the follow up of the relevant sensors described in D4.1 is the RANMONITOR integrated sensing tool given herein. RANMONITOR it is a tool developed by INTEGRASYS which offers detection and reporting of threats and attacks to LTE Radio Access Network (RAN).

The main RAN attacks that RANMONITOR is able to monitor are the following:

- Full-band or partial interference
- Protocol-aware jamming
- Rogue base station
 - IMSI-catcher
 - Poorly configured base stations

6.1. Short description of the sensing system

RANMONITOR tool is based on one or several **Radio-Cyber RAN Sensors**, that can be deployed anywhere, which passively scan the cellular radio spectrum as well as the downlink control channel information and relay this information to a central processing node (**Central Node**). This setup enables the system to monitor the cell parameters and status in LTE RAN networks in order to detect, locate and report to the **RESISTO platform** Short Term Control Loop threat and attack events as Kafka publish messages. The events and useful related information can be visualized also through an external **RANMONITOR Web User Interface** for standalone use. Below, the architecture is depicted. The blocks in grey correspond to the parts of the RANMONITOR architecture itself.

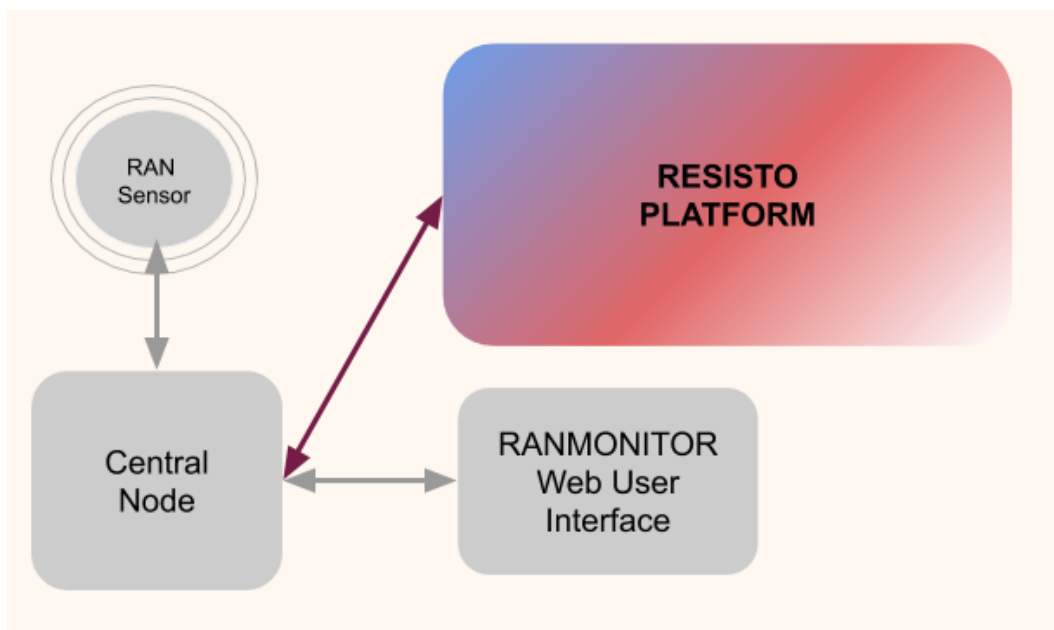


Figure 28 – RANMONITOR Overall Architecture

Below, a short description of each of these components is provided:

- **Radio-Cyber RAN Sensors:** Each monitoring RAN sensor is powered by a standard computer module. A plethora of different models have been tested and can be used. The only requirement is that the module specifications need to be powerful enough to allow for DSP acquisition and processing to be performed without any issues. As a general rule, the unit should have at least USB 3.0 interfaces, SSD disk, high RAM memory and an advanced CPU.

The monitoring functions are performed by a radio cellular modem and by a Software Defined Radio (SDR) Platform able to scan all surrounding channels. The model used for the SDR is the Ettus Research USRP B200 and B210

- **Central Node:** This is the main node in the system and perform several functions:
 - Aggregation module: An aggregation server which collects data captured by the RAN sensors from all surrounding cells. This data is stored and fed into the processing module.
 - Processing module: Processes the information from the aggregation module and generate events.
 - Kafka producer: Source of RAN threat and attacks events data to the RESISTO platform Kafka consumer.
 - Web Server: Server for the RADIOFILTER Web User Interface.
 - RAN Network database: Stores the network cells information
 - Sensor Remote Management: Deals with the configuration of sensor parameters
- **RADIOFILTER Web User Interface:** Web Application that can be accessed on-premises or remotely to visually monitor the events and useful related information. It includes features such as Cells Map, Events log, Detected Cells or Band Visualization

6.1.1. Detection objectives of the sensing system – what is meant to be measured

In this section a table is shown with the parameters that are measured by RANMONITOR sensors. A description is given for each of them. The last two columns indicate which threats or attacks these parameters help to detect and which are the value or range of values that trigger a detection event.

Parameter	Description / Range to be Measured	Threat/Attacks where it helps detection	Anomaly value
MCC	Mobile Country Code. 3-digit code identifying the network's country	Rogue base station	Same value as protected network but with anomaly values in other parameters
MNC	Mobile Network Code. 2-digit code identifying a network within a country	Rogue base station	Same value as protected network but with anomaly values in other parameters
eNB ID	Identifies an LTE eNB within a PLMN	Rogue base station	Value not in RAN Network

	(MCC+MNC). It ranges between 0 and 1048575		database Repeated value
Cell ID (CI)	Identifies a cell/sector within an eNB. It ranges between 0 and 255	Rogue base station	Value not in RAN Network database Repeated value
PCI	Physical Cell ID (PCI) is a physical level cell identifier. It ranges between 0 and 503	Rogue base station	Value not in RAN Network database Repeated value
TAC	LTE Tracking Area Code. It ranges between 0 and 65535	Rogue base station	Value not in RAN Network database Repeated value
EARFCN	E-UTRA Absolute Radio Frequency Channel Number. The carrier frequency is designated by EARFCN, which ranges between 0 and 65535	Rogue base station	Value not in RAN Network database Repeated value
RSRP	Reference Signal Received Power. Power of the LTE Reference Signals spread over the cell channel. It ranges between -140 and -44 dBm	Rogue base station	Excessively high or low value Excessively unstable values
		Full-band or partial interference Protocol-aware jamming	Excessively high or low value compared to expected value
RSRQ	Reference Signal Received Quality. RSRQ is a C/I type of measurement that indicates the quality of the received reference signal. It ranges between -19.5 and -3	Full-band or partial interference Protocol-aware jamming	Low value
Seen Times	Number of times a cell has been seen by the sensor/s	Rogue base station	Low value

Cell throughput	Sum of average throughput of all the users in the cell. Measured in Mbps, Typical values could vary from one cell to another	Rogue base station Full-band or partial interference Protocol-aware jamming	Low value
Window active users	Number of active users in a specific time window	Rogue base station Full-band or partial interference Protocol-aware jamming	Low value

6.2. General deployment requirements

The location where the RANMONITOR RAN sensor and Central Node will be placed must fulfil the following general requirements in order for the tool to be properly deployed:

1. The location must have a relatively high location in order to have good coverage of the area to be monitored
2. The room where it is deployed must have one power plug for the Central Node and one for each RAN sensor

Likewise, the infrastructure owner must provide the following input data:

3. List of threats and attacks to be detected
4. The following RAN network data:
 - a. Network Information: MCC and MNC
 - b. Cell List: Information of each cell (eNBID+CI, PCI, TAC and EARFCN)
 - c. Cell Map: Location of each cell (latitude and longitude coordinates)

6.3. Deployment of the sensing system in a Generic Use case

As already demoted in the Introduction Sections, the RANMONITOR is also meant to be implemented in a variety of scenarios that can accommodate the **Use Case 5 “Protection of Cloud Storage Services” sub-case 1 on Healthcare and sub-case 2 on smart manufacturing** hosted by TIM. Furthermore, they can be employed in the **Use Case 4: “Disruption of major sporting event by combined physical & cyber-attack by a terrorist organization”** hosted by BTC and **Use Case 7: “Maritime Safety and Emergency Case”** hosted by RTV. The above are the most representative Use Cases where the tool can be applied. The relevant deployment procedure is described in detail herein, however, the exact location and implementation will be decided on site upon the definition of the pilot area by the hosts / telecom operators in the framework of WP8 and WP9. Nevertheless, quite many discussions have been taken place among the relevant partners and the deployment aspects have already been defined as it will be seen in the relevant Chapters. To this respect, the relevant deployment details for the RANMONITOR are given in the following **for a Generic Use Case**, assuming that this can represent the variety of Use Cases where the tool will be employed.

6.3.1. Setup of the sensing system in the framework of a Generic Use Case

A generic Use Case for the deployment of RANMONITOR tool is described in this section.

An LTE mobile network operator wants to protect the availability of the service from any degradation in a set of cells located in a specific area. Besides, the operator wants to protect the network users against attacks generated from IMSI-catcher devices.

The deployment of RANMONITOR can be divided into two phases:

1. **Planning.** Based on the input from the mobile operator (Network Information, Cell List, Infrastructure Network Map and specific requirements), a survey is made to produce an estimation of the location of the RAN sensor as well as the general configuration parameters of the system.
2. **Setup.** All the equipment is carried to the building/room where it will be located and is initially set up. Correct operation and connectivity is checked among RANMONITOR components. Connectivity tests include local level (Sensor<->Central Node) and external (Web User Interface<->Central Node and RESISTO platform<->Central Node), Corrective measures are taken from the initial planning if needed (e.g. poor coverage from one sensor to the Central Node if wireless links are used).

Below, a diagram showing the deployed RANMONITOR components, the connection to the RESISTO platform and a protected cellular base station is shown.

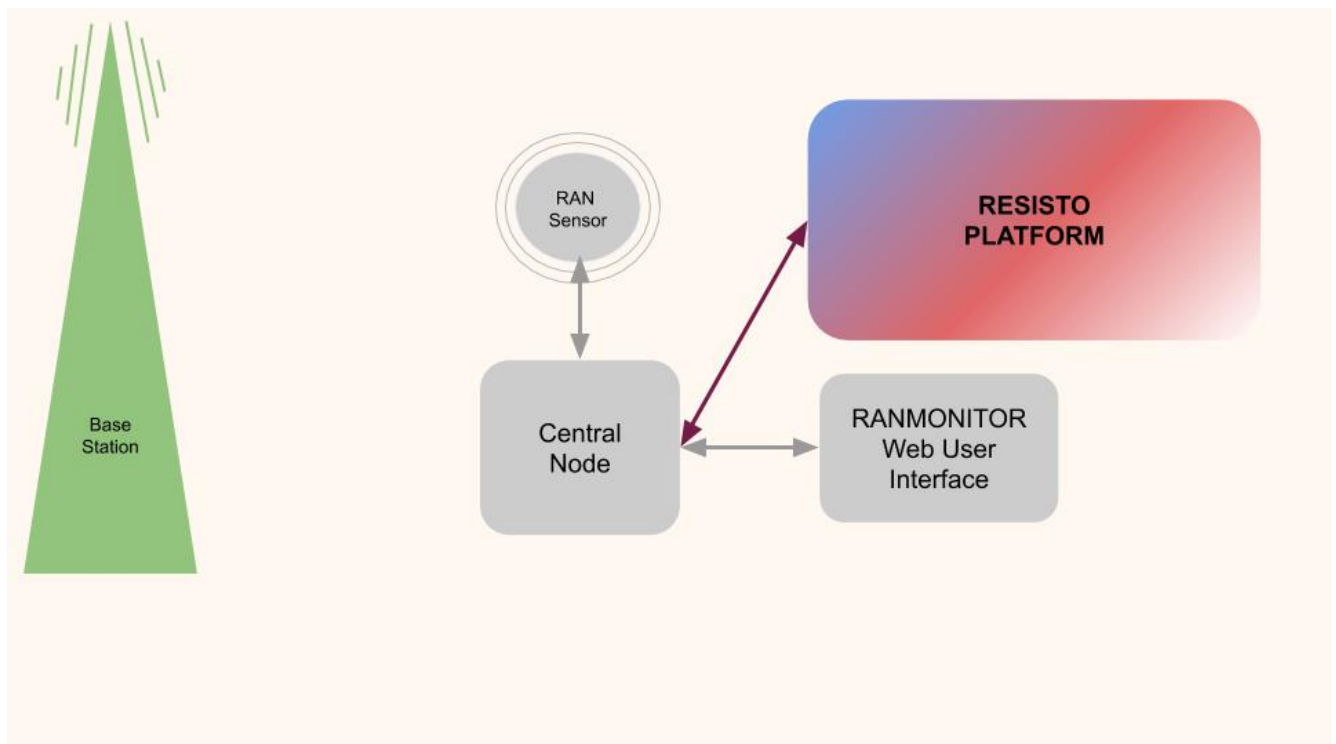


Figure 29 – RANMONITOR deployment in a generic Use Case

Once, the different phases are completed the system is ready to start operating. Upon operation a set of threats and attack events can be detected by the tool. In the diagram below some examples are

shown: Jammer performing a protocol-aware jamming attack, an unintentional interferer causing full-band or partial interference and a rogue base station.

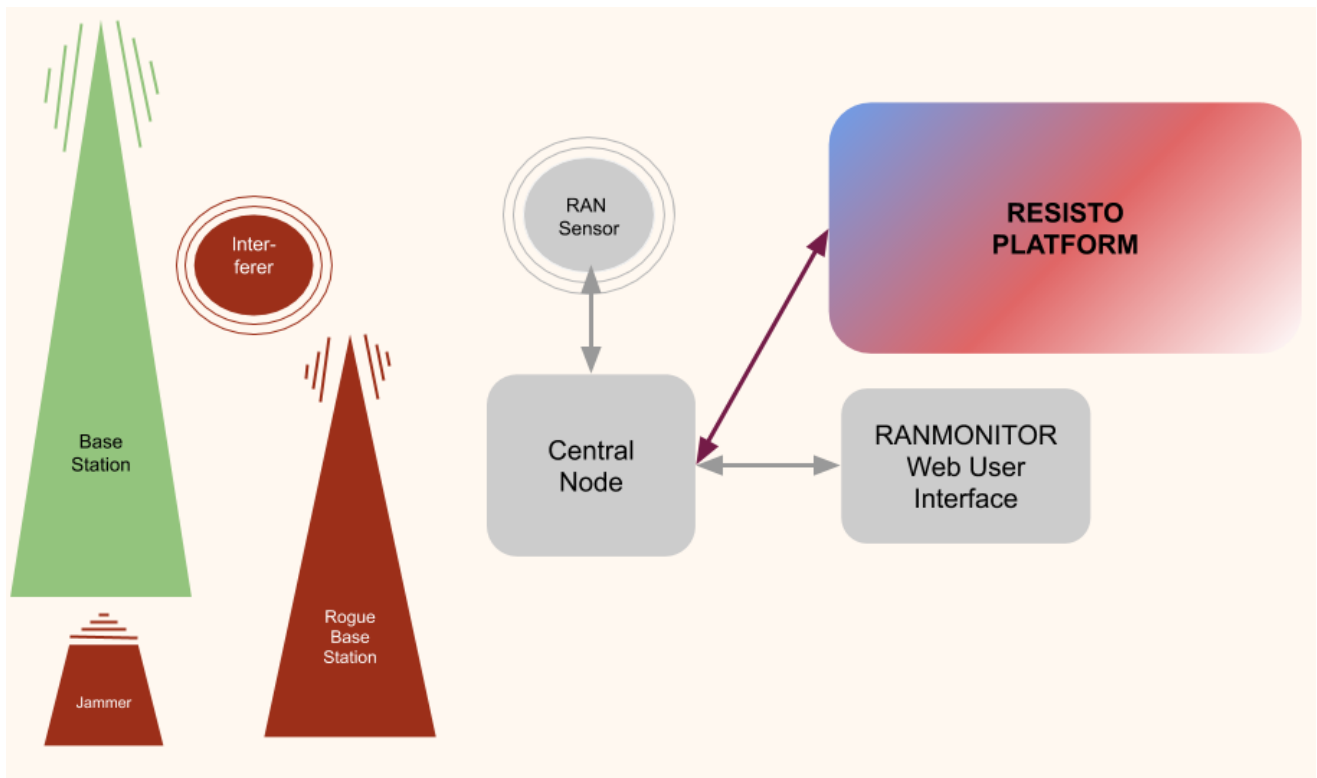


Figure 30 – RANMONITOR threats and attacks detection in a generic Use Case

6.3.2. Deployment phases of the sensing system

6.3.2.1. Lab tests and short experiments of the sensing system

An unauthorized LTE cell (Rogue Base Station) event detection was tested to check the proper operation of RADIOFILTER sensors. The test premises have good coverage near the window, which is the place where the RAN sensor was located.

First, the RAN Network database was initialized with Network Information, Cell List and Cell Map from several mobile operators present in the surrounding area

In the figure below, a screenshot of the RANMONITOR Web User Interface including the Cell Map used in the test is shown.

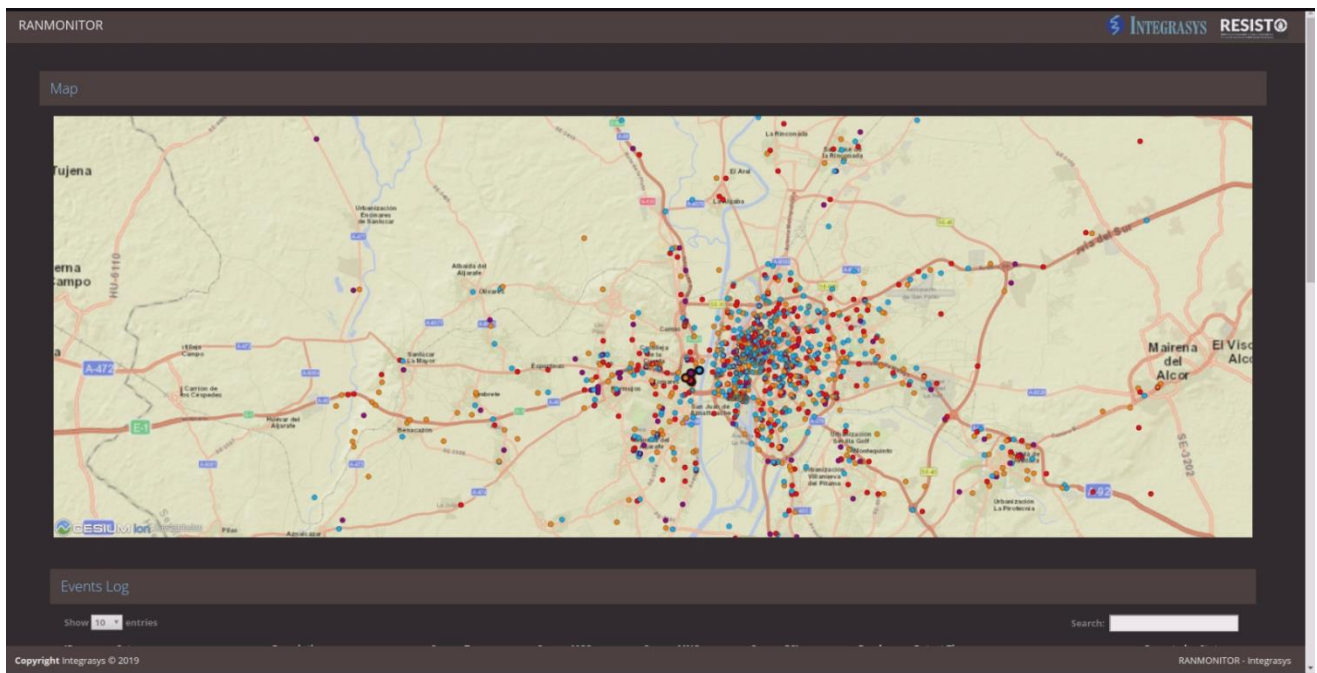


Figure 31 – RANMONITOR Web User Interface running in the test campaign. The Cell Map is shown.

After the planning and setup phases, the tool was ready to test the sensor detection capabilities.

Below, another screenshot of the RANMONITOR Web User Interface is shown including the Detected Cells and Band Visualization at the moment of the test.

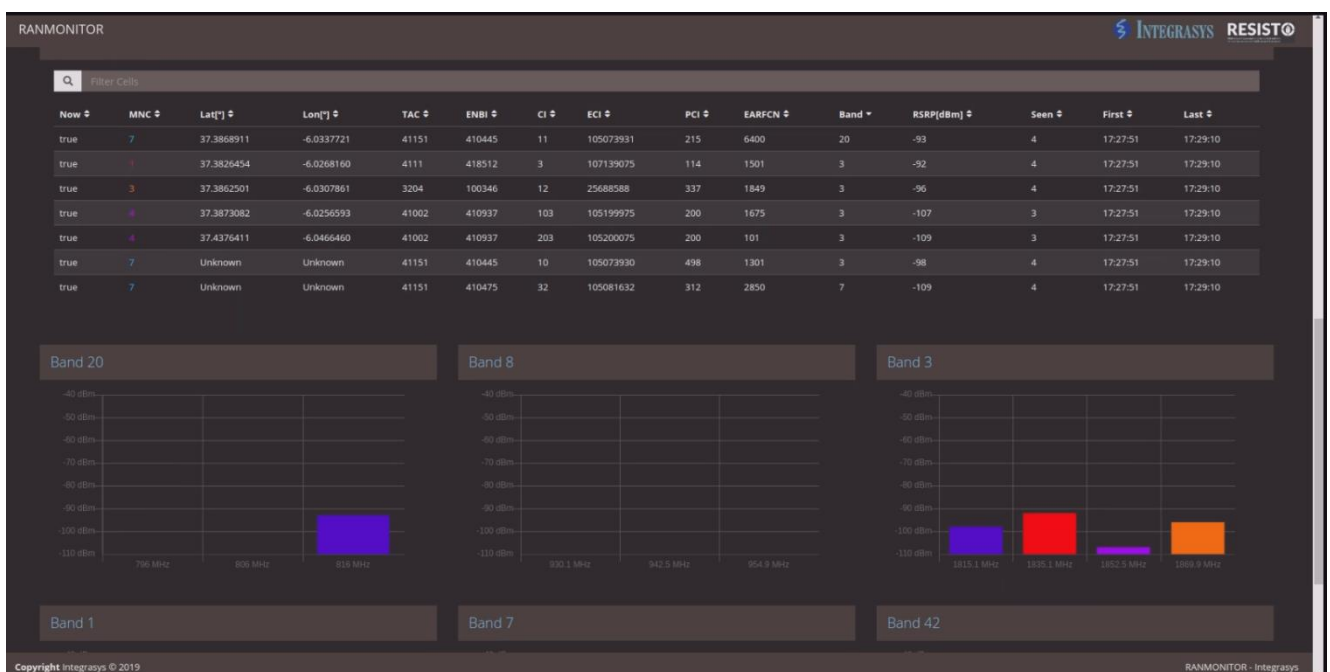


Figure 32 – RANMONITOR Web User Interface running in the test campaign. The Detected Cells and Band Visualization are shown



Figure 33 – Radio-Cyber RAN Sensor

A SDR Rogue Base Station was used to trigger an event in this test. Initially, the Rogue Base Station module was switched off and as soon as it was turned on, it started broadcasting its physical level information parameters which allow extracting the base station identification parameters. At that moment, an Unauthorized Cell event was detected by RANMONITOR tool since this cell was not in the RAN Cell List. In the figure below, a screenshot of the Web User Interface (left-hand side), the SDR Rogue Base Station screen (upper right-hand side) and the modem which is part of the RAN sensor (lower right-hand side) is shown. The new event and its related information appear at the Events Log table and also the rogue cell is added in red colour to the Detected Cells table.

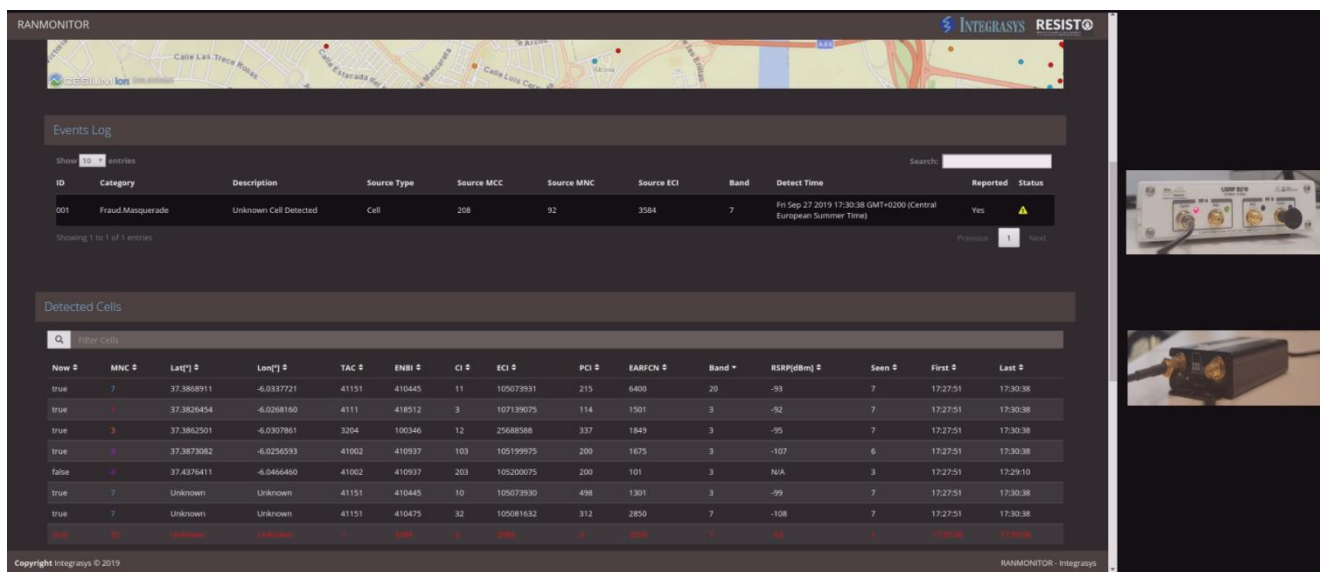


Figure 34 – RANMONITOR Web User Interface upon Unauthorized Cell Event Detection

6.3.2.2. Foreseen final deployment

As already discussed, the exact location and implementation for the final deployment for the various related Use cases will be decided on site upon the definition of the pilot area by the hosts / telecom operators in the framework of the relevant WP8 and WP9. Nevertheless, quite many discussions have been taken place among the relevant partners and the deployment aspects have already been defined as it will be seen in the relevant Chapters.

7. OTHER SENSOR DEPLOYMENT – NATURAL EVENTS SENSING PLATFORMS

Several weather channels, seismic networks are available that can be used to collect events from public or private web API on the internet. The modules will have to be configured with information regarding the geographical coordinates of physical locations that the weather and seismic conditions shall be monitored. Of course the correlation shall take into consideration that a storm or an earthquake can affect a large area, in particular when it comes to adopting redirection of traffic or reallocation of resources. The modules can be active for the entire pilot under study.

The following modules have been implemented to collect data from this sensor networks:

- **OpenWeatherAPI**

OpenWeatherAPI¹ has been used to collect weather information that can be used to correlate specific events on equipment, in particular the ones that are located in the open like cellular antennas.

- **LastQuake Twitter channel**

@LastQuake twitter channel receives tweets regarding earthquakes from all over the world and with proper filtering this can be used as a valuable source of additional information on the seismic events.

- **EARTHQUAKE USGS GOV**

The FDSN Event Web Service Specification, allows to run searches for earthquake information using a variety of parameters this will be used to collect the latest data on earthquake sensors in the areas where the telecom facilities are located.

The use cases in which the natural sensor networks will be involved are:

7.1. Use Case 2 - Sub Case 2 – Natural Disasters affect telecom assets: network loss and telecommunication congestion

In subcase 2 of Use Case 2, a telecommunication congestion due to network loss is caused by a natural disaster that renders a number of assets inoperable.

The various steps of this sub-scenario are described in D2.8 although using the information coming from the sensor networks described above correlation of events can be more precise regarding each site where telecom assets are located, in particular the outdoor ones in case of very severe weather conditions causing twisters and hurricanes, the same is true for earthquakes.

The RESISTO system interfaces with specific natural events sensing platforms such as weather and seismic / earthquake sensing ones. Thus, RESISTO is aware of the natural disaster and simultaneously receives the congestion events from the provider's NMC and monitoring tools and responds by "ordering" a "friendly" UAV to make a damage inspection at the telecom assets in the area that the disaster and congestion occurred.

¹ <https://openweathermap.org/>

8. SUMMARY AND CONCLUSIONS

The present Deliverable D4.2 reports and describes the final list of the sensing systems and mechanisms that are provided by the RESISTO project to enhance the detection of intrusions and modern physical and/or combined cyber/physical threats. In this context the D4.2 is being considered as the follow up of the previous Deliverable D4.1; in D4.2, all the upgrades and developments that took place in the meantime are also presented.

Furthermore, within D4.2 the way that these detection systems will be utilized, combined and orchestrated together to accommodate the RESISTO solution within the framework of the pilot use cases and relevant scenarios at the telecom pilot sites is given. All the relevant deployment details per sensing system are given, and also in respect to the corresponding Use Cases, already described in D2.8, where the specific sensing systems will be used and deployed during the pilot implementation in the framework of WP7, WP8 and WP9.

As it is seen, sensors and tools with various maturity level are offered in order to fill in the gaps in physical security in existing telecom CIs and to provide advanced features in detection and protection processes addressing the modern needs in confronting risks and attacks. The deployment of wireless networks functioning as sensing networks by themselves, is also highlighted.

The foreseen tools involve applications of emerging technologies in order to address intrusion events in the telecom infrastructures and to provide alerts to the RESISTO platform. RESISTO sensors can act complementary to the existing systems and provide more advanced and sophisticated security features tailored to the modern needs for increased security and protection.

9. REFERENCES

[Ref1]	RESISTO – Grant Agreement. Project Starting Date: May, 1 st 2018
[Ref2]	RESISTO Deliverable D2.8: Table-top Read Teaming Results of RESISTO Architecture, Scenarios and Use-Cases
[Ref3]	RESISTO Deliverable D6.1 “SW architecture definition”
[Ref4]	RESISTO Deliverable D4.1 “Active and Passive Sensor Definition”
[Ref5]	RESISTO Deliverable 3.8 “KPIs, quantities and metrics for cyber-physical risk and resilience of telecom CI – final”
[Ref6]	RESISTO Deliverable D6.3 “HMI definition and Platform integration”
[Ref7]	International Telecommunication Union, Geneva, Switzerland 2004 ITU-T Recommendation E.408 (05/2004): Telecommunication Networks Security Requirements.
[Ref8]	International Telecommunication Union, Geneva, Switzerland ITU-T Recommendation X.800 (04/2008): Security Architecture for Open Systems Interconnection for CCITT Applications