

RESISTO:

D4.1 _ACTIVE AND PASSIVE SENSOR DEFINITION



RESISTO

D4.1 – ACTIVE AND PASSIVE SENSOR DEFINITION

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_D4.1_190403_01	Version:	1.0
Deliverable:	D4.1	Date:	03/04/2019
		Status:	APPROVED

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

Approval Status	
Prepared by:	Rodoula MAKRI (ICCS)
Approved by: (WP Leader)	Giuseppe CELOZZI (TEI)
Approved by: (Coordinator)	Federico FROSALI (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, Panagiotis Fragkos, Eyangelos Groumpas.	ICCS	Senior Researchers, Electrical Engineers, Telecommunication Experts
Giuseppe Celozzi, Cosimo Zotti, Giuseppe Amato	TEI	Telecommunications Experts, Senior Researchers
Annarita Di Lallo, Alberto Neri	LDO	Senior Researchers, Defence and Security Specialists
Michael Skitsas, Nikolaos Koutras	ADI	Senior Researchers, Electrical Engineers, Defence and Security Specialists
Moisés Valeo, Jose Sanchez, Javier Valera	INT	Senior Researchers, Electrical Engineers, Defence and Security Specialists
Risto Laanoja, Tuuli Lohmus, Henry Roigas	GT	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	15.11.2018		All	Table of contents and draft sections
0.2	22.12.2018		All	Additions and partners contributions
0.9	15.01.2019		All	Final release for review
V1.0	03.04.2019	All	All	Final release

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 delle Officine Galileo 1 – Campi Bisenzio (FI) – 50013 – Italy

Tel.: +39 055 5369640, Fax: +39 055 5369640

E-Mail: frederico.frosali@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

This report summarizes the up to this time point results of Task 4.1.

The aim of the task is 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).

Thus, as a primary target, Task 4.1 aims to define the active and passive sensors that are going to be used in the framework of the three macro-scenarios during the pilot cases.

Deliverable D4.1 and its follow-up D4.2 address the following objectives:

- to define, enable and implement a complete set of sensors and cyber tools necessary to detect cyber/physical attacks.
- to extract potential intrusion events and process them into alert functionalities for constant alarm monitoring

in order to contribute to their convergence into a complex event recognition system and to identify effective mechanisms to reduce threat propagation within the complete TLC infrastructure chain.

CONTENTS

ABBREVIATIONS	11
1. INTRODUCTION – PURPOSE OF THE DOCUMENT.....	14
2. CURRENT SITUATION IN TELECOM INFRASTRUCTURES	15
2.1. Introduction and connection to threats and risks in telecom CIs.....	15
2.2. Physical security aspects and challenges	16
2.3. Current protection of telecom equipment in physical locations.....	17
2.4. Mechanisms and sensors for physical security – state of the art	19
2.4.1. Access control and personal identification	19
2.4.2. Perimeter defence	21
2.4.3. Central Security Management System	24
2.4.4. Commercial vendors for CIs protection and physical security.....	25
2.5. Discussion and added value of the RESISTO project	26
3. SENSOR DATA PROTECTION.....	30
3.1. Current telecom Standards concerning threat alarms handling.....	30
3.1.1. Definitions and workflows of current telecom fault / alarm management	31
3.1.2. Alarms, events and probable causes in telecom standards	34
3.2. Sensor Authentication	37
3.2.1. Generic Bootstrapping Architecture (GBA).....	39
3.2.2. The embedded SIM solution.....	40
4. ACTIVE AND PASSIVE SENSORS FOR DIRECT DETECTION OF PHYSICAL THREATS	42
4.1. Sensors for Audio and Video analytics and monitoring tools	42
4.1.1. Audio sensors – description and functionalities.....	42
4.1.2. Video sensors – description and functionalities.....	44
4.2. UAV platform – based sensors	45
4.2.1. Architecture and Functionalities of the Mini-UAV platform	46
4.3. Passive radar – the AULOS® sensor	48
4.3.1. Working principle	48
4.3.2. Illuminators of opportunity.....	51
4.3.3. Architecture and Functionalities of the passive radar.....	52
4.3.4. Potential Physical Threats to be detected	55
4.4. Active and passive sensors for airborne threats (i.e. UAVs)	57
4.4.1. Working principle	57
4.4.2. Active Sensors – Radars	58
4.4.3. Passive Acoustic Sensors	61
4.4.4. Architecture and Functionalities of the radar and acoustic system	62

4.4.5.	Potential Physical Threats to be detected	65
5.	NETWORKS AS SENSING SYSTEMS AGAINST PHYSICAL THREATS	67
5.1.	Signal Monitoring WSNs as Sensing systems	67
5.1.1.	Architecture and Functionalities.....	67
5.1.2.	Potential Physical Threats to be detected	68
5.2.	Femtocells-based Sensing systems	68
5.2.1.	Architecture and Functionalities.....	68
5.2.2.	Potential Physical Threats to be detected	69
5.3.	KSI Blockchain overview and use in telecom network monitoring	69
5.3.1.	KSI Infrastructure	71
5.3.2.	KSI Integration	72
5.3.3.	KSI Integration Patterns.....	72
6.	SUMMARY AND CONCLUSIONS.....	74
7.	REFERENCES.....	75

LIST OF FIGURES

Figure 1 - Telecom pillar in antenna parks	17
Figure 2 - Camera-based surveillance systems	22
Figure 3 a) Underground cable system of protection of perimeter from MicroTrac-II - b) Intrusion detection system (Israel)	23
Figure 4 - Perimeter defence by BG-Optics	23
Figure 5 - Central security management system (boards and control room)	24
Figure 6 - Conceptual operation of security management systems	25
Figure 7 - Fencing in remote CIs (from Intrepid Security Supplier of Security and Loss)	27
Figure 8 – System Context	34
Figure 9 - UAV fleet provided by ADITESS	46
Figure 10 - The Mini-UAV (CGS) environment.....	47
Figure 11 - The Mini-UAV platform architecture	47
Figure 12 - PCL working principle	48
Figure 13 - Comparison of monostatic and bistatic RCS.	49
Figure 14 - PCL basic geometry and processing scheme.....	50
Figure 15 - Accuracy and detection range of some sources of opportunity.	51
Figure 16 - AULOS® functional block diagram.	52
Figure 17 - Deployable AULOS® at Farnborough International Airshow in July 2012.	53
Figure 18 - FM and DVB-T circular arrays.....	54
Figure 19 - AULOS® transport configuration with cover.	54
Figure 20 - Air traffic near Fiumicino international airport.	55
Figure 21 - Results from SeaBilla experiments for DVB-T based AULOS®.	55
Figure 22 - Early radar prototype with directive antennas.....	59
Figure 23 – Current ICCS radar prototype	60
Figure 24 - Early acoustic arrays prototype.....	61
Figure 25 – Current ICCS acoustic arrays prototype	61
Figure 26 - Acoustic sensors data processing.....	62
Figure 27 - Operation environment of combined radar and acoustic sensors	63
Figure 28 - Radar Response: a) Noise floor, b) Small Cessna type aircraft (150m distance)	64
Figure 29 - Acoustic response: a) Movements in various heights and distances, b) UAV approaching for landing	64
Figure 30 - Drone's movement: a) Rpm measurement, b) drone in hover, c) drone in movement.....	65
Figure 31 - The commercial drone used for the tests.....	65
Figure 32 - The general architecture of a femtocell inside a cellular network.	69
Figure 33 KSI Blockchain append-only record	70
Figure 34 The layers of KSI Infrastructure.....	71
Figure 35 KSI Core and top-level Aggregators	72
Figure 36 Example provenance graph is formed by the lifecycle of a document.....	73

ABBREVIATIONS

2G, 3G, 4G	Second, third and fourth generation of mobile phone systems
3GPP	3rd Generation Partnership Project
5G	5th generation mobile wireless standards
ADAC	Automatically Detected and Automatically Cleared
ADMC	Automatically Detected and Manually Cleared
API	Application Programming Interface
APN	Access Point Name
ASAP	Alarm Severity Assignment Profile
ASIC	Application Specific Integrated Circuit
B2B	Back-to-Back gateway
CCA	Critical Communication Application
CCS	Critical Communications System
CO	Conditional-Optional
DDoS	Distributed Denial of Service
DMO	Direct Mode Operations
DN	Domain Name
EC-GSM-IoT	extended coverage GSM IoT
ETSI	European Telecommunications Standard Institute
EM	Element Manager
EU	European Union
eUICC	embedded Universal Integrated Circuit Card
FM	Fault Management
FS	Function Set
GGSN	Gateway GPRS Support Node
GSM	Global System for Mobile communications
GSSI	Group Short Subscriber Identity
HW	HardWare

IETF	Internet Engineering Task Force
IIC	Industrial Internet Consortium
IIoT	Industrial Internet of Things
IOC	Information Object Class
IoT	Internet of Things
IPsec	Internet Protocol Security
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)
LTE-M	simplified term for LTE-MTC LPWA (Long Term Evolution Machine Type Communication Low Power Wide Area)
M	Mandatory
MNO	Mobile Network Operator
MO	MO Managed Object
MOC	Managed Object Class
MOI	Managed Object Instance
NB-IoT	Narrowband IoT
NE	NE Network Element
NM	Network Manager
PC	Personal Computer
O	Optional
OS	Operations System
PPDR	Public Protection and Disaster Relief
PTT	Push To Talk
QoS	Quality of Service
SIM	Subscriber Identity Module
SW	SoftWare

TCCE	TETRA and Critical Communications Evolution
TEE	Trusted execution environment
TEA2	TETRA Encryption Algorithm #2
TETRA	TErrestrial Trunked RAdio
TG	Talk Group
TLS	Transport Layer Security
TMO	Trunked Mode Operations
UE	User Equipment
UICC	Universal Integrated Circuit Card
VPN	Virtual Private Network
WP	Work Package

1. INTRODUCTION – PURPOSE OF THE DOCUMENT

The present Deliverable D4.1 is the first report of WP4 “Tools and techniques for Monitoring and Detection of cyber-physical threats”. This WP deals with the implementation of a variety of hardware and software tools and technologies for detection and monitoring of anomalous conditions, intrusions and threats. Deliverable D4.1 and its follow-up D4.2 address the following objectives of the WP4 ones:

- To define, enable and implement a complete set of sensors and cyber tools necessary to detect cyber/physical attacks.
- To extract potential intrusion events and process them into alert functionalities for constant alarm monitoring

In order to contribute to their convergence into a complex event recognition system and to identify effective mechanisms to reduce threat propagation within the complete TLC infrastructure chain.

This report summarizes the up to this time point results of Task 4.1. The aim of the task is 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). Thus, as a primary target, Task 4.1 aims to define the active and passive sensors that are going to be used in the framework of the three macro-scenarios during the pilot cases.

The RESISTO project, apart from the overall platform for a holistic security response to various kinds of threats, provides also 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.

As it will be shown in a later section of the present report, these sensors and tools to be provided show different level of maturity; from ready-made systems to advanced lab or pre-industrial prototypes or even integrated sensor networks and relevant firmware. These sensors address mainly physical threats along with combined cyber-physical threats up to the level where a physical intrusion or malfunction may create dangerous and problematic situations in physical and cyber security.

The structure of the present Deliverable D4.1 is as follows:

In the first section, an overview of the current security and protection mechanisms will be given along with the basic tools and sensor-based systems that are being employed in existing telecom critical infrastructures as the current relevant state of the art. The second chapter deals with current standards and recommendations affecting the data obtained by the sensors along with current and future relevant trends in light of the 5G and IoT world that emerges. Then, in the following sections the description of the sensors and tools offered by RESISTO is being made. In chapter 3, active and passive sensors offered by RESISTO partners for direct detection of intrusions into the physical security of the telecom infrastructures are described (namely audio and visual analytics methods, radars and acoustic sensors). Finally, in Chapter 4 the concept of using modern wireless sensor networks themselves as sensing modes against various threats is being presented through specific cases.

The aim is, from the one hand, to present a complete and overall picture of the current situation in the majority of the telecom CIs and from the other hand, to adequately explain and highlight the added value that will be provided by the RESISTO project against these kind of threats. 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.

2. CURRENT SITUATION IN TELECOM INFRASTRUCTURES

2.1. Introduction and connection to threats and risks in telecom CIs

The RESISTO project foresees prevention, detection, response and mitigation functionalities against all kinds of threats and risks in telecom CIs. Within WP2 a discussion concerning the classification of threats is being held, providing an overview of the relevant knowledge. The various threat standards and models (NIST, ISO, STRIDE tec.) foresee various classes of threats depending on the point of view and the hierarchy of security principles. However, the most general classification concerning the affected system types in telecom critical infrastructures includes the following:

- physical threats that affect physical systems, buildings and infrastructure and
- cyber-threats that exploit vulnerabilities in computer systems and cause possible harm in the digital realm,
- cyber-physical threats that exploit vulnerabilities and can cause possible harm in systems controlled and monitored by computer-based algorithms i.e. human-driven intrusions in the physical domain that can also cause security issues in the cyberspace.

Physical threats include intrusion and malicious attacks affecting also the vicinity of the critical telecom infrastructure, (i.e. deliberate unauthorised access for causing damages or terrorism actions), airborne and land threats (explosions, bombing by aircrafts or land vehicles, hostile drones and UAVs bearing weaponry), deliberate jamming and causing of damages along with natural hazards (weather, earthquakes, fire etc.). Non-deliberate threats such as system or power failures by accidental reasons are also classified within the physical threats due to their similar impact to the telecom system and its components.

Cyber threats affect the whole telecom operation as a software system and service and basically involve intrusions, cybercrime and deliberate malware in the telecom operator's firmware causing a broad impact to the telecom services and customers' personal data. Combined cyber-physical threats on the other hand include disruptions to information systems, which directly affect physical infrastructure services or intrusions to the physical domain that can cause possible harm in systems controlled and monitored by computer-based algorithms.

The present Deliverable deals with the active and passive sensors, provided by the RESISTO project, that address detection of threats and attacks mainly in the physical domain as well as the combined cyber physical threats that affect the telecom operator's system following an intrusion, problem or damage in the telecom facilities. Means and ways to detect these kinds of intrusions are examined not only for direct detection of threats (cameras, radars and acoustic sensors) but also through actuators and wireless sensor networks that can be considered as cells of the wider telecom network. And this is also a very important aspect when considering the large impact that wireless networks have on interconnected critical infrastructures, especially in light of the emerging 5G and Internet of Things (IoT) world that is approaching fast. The aim of all kinds of sensors is to provide alerts and intrusion events to the RESISTO platform contributing to the overall protection concept of the project as well as to the risk and resilience assessment of the overall telecom infrastructure (dealt in WP3) through the long term control loop.

However, telecom critical infrastructures already employ security systems especially at their main buildings and headquarters, as all critical facilities do. Thus, the aim of the RESISTO project is to act complementary to the existing systems and to provide more advanced and sophisticated security

features tailored to the modern needs for increased security which are more demanding than the conventional approaches of the past decades.

In the present section, an overview of the current security and protection mechanisms will be given along with the basic tools and sensor-based systems that are being employed in existing telecom critical infrastructures as the current relevant state of the art. The aim is, from the one hand, to present a complete and overall picture of the current situation in the majority of the telecom CIs and from the other hand, to adequately explain and highlight the advancements that will be provided by the RESISTO project against these kind of threats.

2.2. Physical security aspects and challenges

The most common impression when discussing about physical security in critical infrastructures in general terms, is that of dealing mainly with the protection of building sites. In this context, physical security refers to the protection of building sites and internal equipment from theft, vandalism, natural disasters (i.e. floods, earthquakes), manmade catastrophes, and accidental damage (e.g., from electrical surges, extreme temperatures, heavy rains, and lightning) or unintentionally destructive acts. It requires solid building construction, suitable emergency preparedness, reliable power supplies, adequate climate control, and appropriate protection from intruders. Thus, it requires that building site(s) be safeguarded in a way that minimizes the risk of resource theft and destruction. To accomplish this, decision-makers must be concerned about building construction, room assignments, emergency procedures, regulations governing equipment placement and use, power supplies, product handling, and relationships with outside contractors and agencies¹.

However, physical security is often a second thought when it comes to information security. Since physical security has technical and administrative elements, it is often overlooked because most organizations focus on “technology-oriented security countermeasures”² to prevent hacking attacks³. Hacking into network systems is not the only way that sensitive information can be stolen or used against an organization. Physical security must be implemented correctly to prevent attackers from gaining physical access and cause physical damages and consequently endanger information systems. In this context, cyber threats, apart from relative direct actions, can be also seen as a result of physical security breaches (cyber-physical threats). To this end, the physical element of security is often overlooked; the damage of hardware or vandalism could occur while working with administrative and technical controls as well. Organizations often focus on technical and administrative controls and as a result, security breaches may not be discovered right away⁴.

Physical security is often thought as only controlling personnel access to facilities; however, its relation to achieving data center availability goals is more than crucial. Security professionals with physical security in mind are more concerned about the physical entrance of a building or

¹ <https://nces.ed.gov/pubs98/safetech/chapter5.asp> IES/NCES, National Center for Education Statistics, US Department of Education

² Harris, S. (2013) “Physical and Environmental Security” In CISSP Exam Guide (6th ed., pp. 427-502). USA McGraw-Hill

³ David Hutter (2016) “Physical Security and Why It Is Important” GIAC (GSEC) Gold Certification, SANS Institute InfoSec Reading Room, Copyright SANS Institute, Author Retains Full Rights, <https://resources.infosecinstitute.com/importance-physical-security-workplace/>, <https://www.sans.org/reading-room/.../physical/physical-security-important-37120>

⁴ Oriyano, S. (2014), “Physical Security” In Cehv8: Certified Ethical Hacker Version 8 Study Guide (pp. 393-409). Indianapolis, IN USA: Wiley

environment and what damages a potential intruder may cause. As new technologies such as biometric identification and remote management of security data become more widely available, traditional card-and guard security is being supplanted by security systems that can provide positive identification and tracking of human activity in and around the data center. Before investing in equipment, the CI organizations must carefully evaluate their specific security needs and determine the most appropriate and cost-effective security measures for their facility⁵.

The challenges of implementing physical security are much more problematic now than in previous decades. Laptops, tablets and smartphones all have the ability to store sensitive data that can be lost or stolen. Organizations are obliged to safeguard personnel, information, equipment, IT infrastructure, data, equipment, people, facilities, systems, and company assets (and all information and software contained therein).

2.3. Current protection of telecom equipment in physical locations

It is clear that the physical security aspects described above affect all types of Critical Infrastructures, including the Telecom ones. However, it should be noted that for the Telecom CIs the issues of both physical and cyber threats are of major importance since they affect greatly one another. Nevertheless, although cyber threats are given the major attention which it is reasonable since data security is a primary factor, the physical security ones are not regarded evenly.

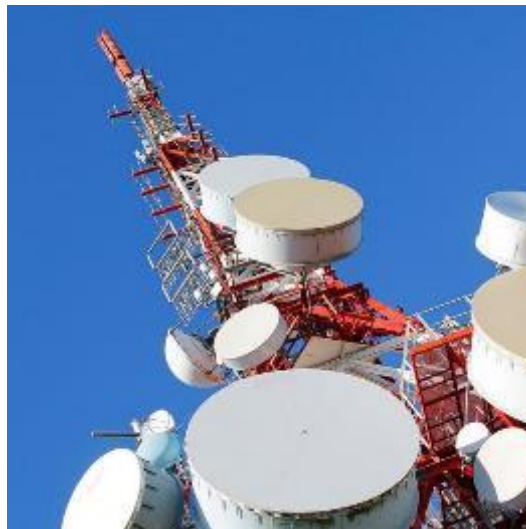


Figure 1 - Telecom pillar in antenna parks⁶

Telecom equipment is typically located in sites owned by the telecom Operators. Telecom sites are usually part of an established and enforced physical security perimeter. The main purpose of such a perimeter is to prevent unauthorized access to physical sites and therefore damage to the telecom site facilities.

⁵ Suzanne Niles (2015), "Physical Security in Mission Critical Facilities", White Paper 82, revision 2, APC White Papers, part of the Schneider Electric white paper library produced by Schneider Electric's Data Center - Science Center, <https://it-resource.schneider-electric.com/.../wp-82-physical-security-in-mission-critica...>

⁶ <https://www.cpni.gov.uk/critical-national-infrastructure-0>

A physical perimeter shall include all areas that telecom facilities are located and depending on the security requirements of the assets and the results of a risk assessment the strength of each of the perimeters should be defined. External doors and windows should be suitably protected against unauthorized access with physical barriers and should, if possible, be alarmed and monitored; in particular special care should be taken in case of unoccupied areas. This is true for most of the equipment which are in physically protected areas. The type of physical protection that is available in each site can vary from perimeter security, like a fence or a wall.

In controlled and restricted areas or rooms, access is made through door with access control, via a badge, or by a physical key. Depending on the size of the site, the facilities could be monitored by CCTV. Alternative power sources are used that can be activated in case of power shortage to guarantee the equipment functioning for some time while the primary power source is being restored. At the same time there are some interdependences since all the above facilities will make use of the telecom infrastructure to deliver data or notifications to the security management system, which will therefore not be noticed if the telecom infrastructure is not working properly.

Security equipment deployed on site can have different levels of integration with the telecommunication system; many of them rely on the possibility to use the site LAN. For instance: surveillance cameras, access control panels, door locks, and fire detectors are connected to the local network via ethernet or via Wi-Fi. This, however, makes them open for any attack to the telecom infrastructure and availability. It is therefore necessary that sensors like e.g. surveillance cameras, should guarantee the possibility to operate also when the network connection is down; for example local buffering or storage of the video recordings are needed to be made.

In some cases, an auxiliary board can be deployed in the same shelf/cabinet used for the telecom equipment included in the site hardware infrastructure and via direct connection to deliver specific alarms to the Operation System (OSS) monitoring the telecom equipment. Typically, the auxiliary boards can detect simple on/off situations like a door being opened or the fire alarm detector, interrupting a simple circuit. This on/off behaviour can be associated in the OSS software to indicate a specific alarm situation.

In almost all cases there is protection against natural hazards through sensors inherent to the facility from its construction (i.e. protection against lightning through the power unit or fire and smoke alarms). However, due to its nature the protection against this kind of hazards is often associated or combined with the civilian protection and civil security procedures and mechanisms on state or municipality level.

Usually, the most sophisticated physical security mechanisms are implemented for the security of the central telecommunication buildings and headquarters. These mechanisms include entrance and access control, surveillance through camera networks, cards and biometrics identification and perimeter defence in the most advanced implementations, as it will be seen in a later paragraph. In the majority of the cases, the physical security is being outsourced through SLAs to respective specialised security companies either for implementing the respective protection mechanisms or for administrating the security management or both. The above are usually implemented in an integrated unified security system, with security control rooms for monitoring and response, addressing physical security mainly at the central telecommunication buildings and headquarters where large number of the telecom organization's personnel is employed and is present on day-to-day basis.

However, it should be noted that this is rather not the case in all the telecom infrastructures and assets that a telecom provider/ISP/organization possesses. Telecom pillars, cabins, antenna parks or even fibre optics terminals in remote and rural areas are not given equal treatment as in large central telecom buildings; the situation is even more critical in mountainous villages and / or remote small

islands, where in certain cases the only security mechanism applied is locking the doors or employing security guards.

Nevertheless, the above hierarchy is considered reasonable since at the main buildings or large headquarters, the majority of the organization's personnel is working while the Network Operation Centers (NOC) and the main backhaul fiber optics terminals exist and need security protection. On the other hand, cost is one of the most important parameters, since the investment in advanced security mechanisms for the many remote assets could turn to be high enough, limiting the cost-effectiveness, not considering the needed resources in time and effort for the relevant implementations. Thus, it is most common for major telecom organizations to invest in disaster or redundancy centers along with fail-over techniques for the main telecommunication services.

2.4. Mechanisms and sensors for physical security – state of the art

The main physical security solutions, mechanisms and sensors used in protecting telecommunication assets are given in the following, indicating simultaneously the current commercial state of the art in such critical infrastructures. As denoted earlier, usually the most sophisticated physical security mechanisms are implemented for the security of the central telecommunication buildings and headquarters. In the majority of the cases integrated unified security systems are implemented addressing mostly visual inspection and access control, following a predefined security plan.

The first steps in a security plan is to identify the areas, rooms and entry points that need different rules of access. Thus, different levels of security are employed depending on potentially stringent access methods to achieve added protection. By this way, an inner area is protected both by its own access methods and by those of the areas that enclose it. In addition, any breach of an outer area can be met with another access challenge at a perimeter further in. This can be employed in areas that might have concentric boundaries (i.e. site perimeter, building perimeter, computer area and computer rooms along with equipment racks) or with side-by-side boundaries (i.e. visitor areas, offices, utility rooms)⁷. Thus, the strategies used to protect the organization's assets need to have a layered approach. It is harder for an attacker to reach their objective when multiple layers have to be bypassed to access a resource.

Various access levels and fragmentation / separation of the main building in zones are then employed, depending on the foreseen physical threats and the type of area to be protected so that to prevent unauthorized people to enter or access the site and use equipment.

The main physical security mechanisms along with related sensors or components used per case are described in the following:

2.4.1. Access control and personal identification

Access control takes place at main entrances (input / output) especially for personnel and vehicles. For the organization's personnel and visitors, various methods may be of use involving personal identities, entrance cards and in most sophisticated cases biometrics and related measures.

Concerning entrance cards again a large variety exists on the market including: Personal cards with data and photo, limited validity cards for visitors / suppliers, smart cards with onboard processor,

⁷ Suzanne Niles (2015), "Physical Security in Mission Critical Facilities", White Paper 82, revision 2, APC White Papers, part of the Schneider Electric white paper library produced by Schneider Electric's Data Center - Science Center, <https://it-resource.schneider-electric.com/.../wp-82-physical-security-in-mission-critica...>

magnetic stripe cards (with a simple magnetic strip of identifying data) or magnetic spot cards (barium ferrite card), Weigand cards, bar-code cards and infrared shadow ones. The types of interaction with the relevant card readers may be of swipe, insert, flat contact, and even with no contact as in proximity cards or proximity tokens (i.e. the Mobil Speedpass®). Apart from their ability to be reprogrammed, the above types of cards present resistance to counterfeiting and also provide ability to allow access only in permitted areas (floors) per employer. The programming process may be separate for visitors and vendors while an escort mode may be also used in these particular cases in conjunction with anti-passback mode.

Keypads and coded locks are also in wide use as a method of access control. They are reliable and very user-friendly, but their security is limited by the sharable and guessable nature of passwords as personal access codes (PAC) or personal identification numbers (PIN) are implied.

The most sophisticated tools used are the biometrics sensors, which are used mostly for verification of the identity rather identification of a person. Biometric scanning techniques and relevant sensors have been developed for a number of human features: Fingerprint scanners (shape of fingers and thickness of hand), Iris (pattern of colours), Face (relative position of eyes, nose and mouth or even biometrics models), Retina (pattern of blood vessels), handwriting (dynamics of the pen as it moves) and Voice (with voice recognition systems).

Biometric devices are generally very reliable. The main sources of unreliability for biometrics is the possibility that a legitimate user may fail to be recognized ("false rejection") and the erroneous recognition, either by confusing one user with another, or by accepting an imposter as a legitimate user ("false acceptance"). Nowadays, many commercial vendors offer a wide range of biometric devices which can be used either independently as stand-alone method or in combination to existing security measures like smart cards, and thus it is highly likely to become the best practice for access control. The main considerations when choosing a biometric technique are the equipment cost, the failure rates and the user acceptance, especially in cases where specific specifications should be regarded (i.e. distance from the sensors, light etc).

Access control in internal areas (rooms i.e. data Center, NOC, E/M power supplies): In these cases the usual measures taken include the following: Controlled access (in entries / exits) is applied in critical areas and simultaneous monitoring by CCTV (E / M, Data Center, NOC, etc.) takes place. Additionally on the roof surveillance and protection is being held through Access Control and CCTV. Usually, guests must be accompanied while in certain cases entrance is allowed only to predefined program-based areas. Almost in all cases CCTV and Access Control systems are interconnected.

Vehicles' plate recognition system: in Parking areas and at all entrances, gardens, or HW facilities that vehicles may access, the checking of incoming / outgoing vehicles is being held by reading of the vehicles' plates with high definition cameras and PTZ surveillance cameras with large zoom while eliminating 'blind spots'. Bulletproof checkpoints at the entrances may be present as well, while recording of the surrounding area and parking management systems can also be applied, accompanied by the use of license plates databases of employees and access control procedures for transporter / carriers. This is also enabled by intercommunication of the entrance checkpoints with the control room while silent panic buttons in all positions are also available.

In **High Security Areas** (i.e. NOC, H-Sat etc.) the same Access Control mechanisms as in critical areas are usually applied, such as: check of incoming / outgoing people, visual surveillance and recording of activities, tamper alarms, cameras at entrances, floors, roof, or E / M spaces etc. Depending on the desired security level, special measures that can be taken include detection of explosives, chemicals, or even of weapons and metal objects carried by visitors.

Furthermore, **Explosives Detectors** can also be used in parallel to access control in high security areas or at the entrances: three different detection systems (i.e. gates) for explosives and hidden

objects (metal objects, weapons etc.) and metal detection units, capable of detecting any explosive material within hand-luggage's or carried by visitors, highlighting also the material with colour. Sophisticated and advanced detectors can be employed guaranteeing minimum detection time while interconnected with the automated control system of the operator: thus, remote control and silent alarm capabilities are in order along with performance reporting for staff security.

2.4.2. Perimeter defence

In most demanding situations, more sophisticated mechanisms such as perimeter defence ones are also applied. These include both internal cases (main building or headquarters) and external cases (outer area perimeter) and incorporate a variety of sensors and combined detection and protection systems.

Building perimeter: This refers mostly to the internal cases and especially the perimeter defence for major buildings of the infrastructure and headquarters. The building perimeter usually includes a combination of the following measures: Access Control on inputs / outputs of the building and of sensitive critical areas, Surveillance and tracing of interior violations, Motion detectors and magnetic contacts, Webcams around the building, Tamper alarm even glass breaking (window) detection along with protection of critical electrical equipment (usually located at the basements).

Outer perimeter: On the other hand the outer perimeter defence refers to external cases incorporating the whole infrastructure area by employing: full monitoring and tracking of the point of violation, visual surveillance of the perimeter, enhance lighting in dark areas and hidden (i.e. infra-red) illumination, cameras covering the entire perimeter, sirens alert along with Electronic Fencing Systems.

The sensing systems that are usually employed in this kind of more sophisticated detection and protection mechanisms against physical threats include the following:

- **Access control systems:** with biometrics or card readers as already described in the previous section.
- **Camera-based surveillance systems:** These include the following sensors:
 - IP cameras of high definition for outdoor use. These are capable for day / night operation and covering wide zones (i.e. 10m) along the perimeter, providing also motion detection. This camera system enables parallel monitoring (either in control rooms or checkpoints) with automatic recordings and alarm dedicated monitors.
 - Optical Surveillance with High-Analysis Cameras. Mega Pixel cameras are deployed around the building providing supervision of all surroundings or protection of the E/M infrastructures and the courtyard. Usually the ability to analyse individual images from a single camera is offered, resulting up to 10 times (and more) larger coverage than a simple camera, with multiple digital extended zoom.
 - Panoramic Surveillance of the environment. PTZ cameras are installed on the roof, with dual camera control (at the control room and the entrance checkpoints). The functionalities involved can provide the ability to override the control of the camera from the control room, along with an interface of PTZ cameras with the perimeter tampering system. Usual camera features include: High Resolution of 520 TVL, high sensitivity less than 1 lux and powerful zoom (i.e. x35 or more).



Figure 2 - Camera-based surveillance systems⁸

The optical surveillance of the building entrances usually incorporates:

- Surveillance cameras at all major inputs / outputs
- High-resolution cameras around the building and at all auxiliary entrances and emergency exits
- CCTV and Access Control system interconnection

while, the perimeter lighting can be also enabled through: installation of IR / invisible lighting elements, CCTV surveillance (i.e. Dome, MegaPixel, etc.) and collaboration of cameras with electronic fencing system. The camera-based surveillance systems can also accommodate vehicle license plate recognition at all entrances as described previously. Furthermore, these systems are often combined with silent panic buttons in all positions contributing to the intercommunication of the entrance checkpoints with the control room.

- **Intrusion detection systems:** apart from the camera surveillance systems, intrusion detection sensors provide an all-around glazing at the ground and lowest floors. The relevant functionalities

⁸ <https://videokray.ru/p147746941-ohrana-perimetra.html>

include the surveillance of openings (doors, windows, etc.) and sliding doors while the relevant sensors include magnetic contacts, motion detectors and crystal breaking detectors among others.

- **Electronic fencing systems:** these are more sophisticated and thus more expensive solutions which incorporate invisible underground sensing cables (buried cables). These kind of fencing systems create an invisible detection field as shown in the figures below which is not affected by vegetation and the natural environment. The detection range can vary with usual widths of around 3m and with accuracy of less than 1m. Graphic on-line representation can be visible to the central management while there is the possibility of partial or total activation of the fence or interfacing with CCTV.

INTREPID MicroTrack II
 ПОДЗЕМНАЯ КАБЕЛЬНАЯ СИСТЕМА ОХРАНЫ ПЕРИМЕТРА

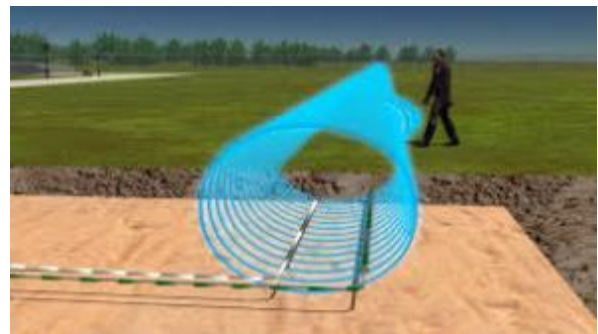


Figure 3 a) Underground cable system of protection of perimeter from MicroTrac-II⁹ - b) Intrusion detection system (Israel)¹⁰

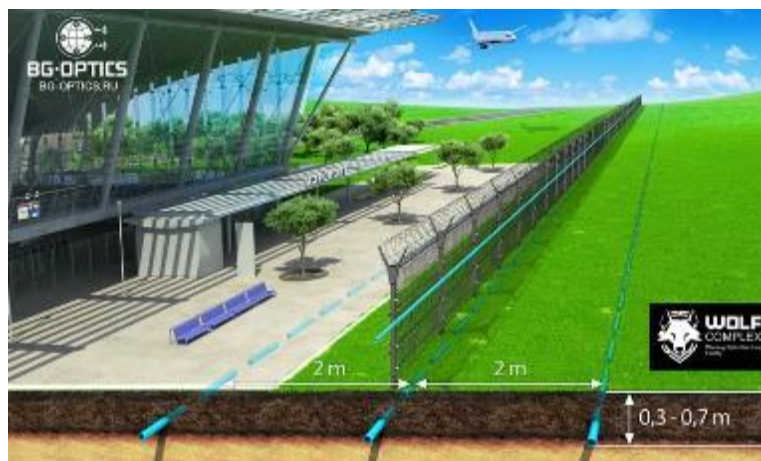


Figure 4 - Perimeter defence by BG-Optics¹¹

⁹ <https://kz.all.biz/en/underground-cable-system-of-protection-of-g1334520>

¹⁰ <https://i-hls.com/archives/13894>

¹¹ <http://www.bg-optics.com/volk.html>

- **Associated operation procedures:** The above sensing and detection systems against intrusion and malicious actions are usually combined with associated operation procedures of the telecom infrastructure's security staff. Thus, Security Guards patrols take place through specific route and time planning based on patrol scenarios while they are crosschecked with CCTV and intrusion detection systems. Furthermore, Evacuation Plans are being practiced by the operator's staff through building predefined evacuation processed and plans involving specific measures i.e. automated output counting units and similar.

2.4.3. Central Security Management System

Generally, the above detection and sensing systems are administrated as standalone or within a general framework of a security management system. In many cases the overall security management systems are outsourced through SLAs to specific companies and relevant organizations specialized in security and safety with simultaneous transfer of the relevant Administrative rights. In this sense, separate Security Divisions are assigned within each operator's organization involving an overall System Central Control within a Security Control Room with racks for equipment, console with screens, control panel, keyboard and PTZ controls along with the ability to override functions at the entrance checkpoints (i.e. bar control, PTZ cameras etc.).



Figure 5 - Central security management system (boards and control room)

The security management systems are often designed to be compatible with International Security Standards and to comply with the principles and procedures of large state / commercial organizations. Their main functionalities are to facilitate the integration with IT applications, to provide encryption and high compression of network data and data integrity, to obtain high performance on WAN installations, to administrate visitor management programs, to maintain internal black lists and external blacklists by government agencies, to conduct internal audits of users and operators and to result in direct and complex reports. However, it should be noted that the security management systems usually conduct the orchestration of the various sensors and surveillance mechanisms, indicating the faults and providing physical alarms while the handling and tackling of the faults and alarms is being managed instead by the fault or alarm management of the telecom operator as it will be seen in the next Chapter.

The system architecture usually involves: TCP / IP technology and communication through TCP / IP LAN network with the management centre, expansion capability through WAN TCP / IP and IP ready equipment, high response speeds, remote management / monitoring through client – server and autonomous operation in case of loss of communication with the server. Additional features include: dual connection for each local distributor with the central units and central units in Hot-Standby arrangements, dedicated UPS for the security management system and double routes or additional wiring or dual flow for each local distributor from the central distribution board, along with back-up power from UPS to the main switchboard.

A most common, and almost obligatory, facility is the maintenance of redundancy networks and / or disaster centres along with backup with dual central server and simultaneous operation in order to tackle security issues not only associated with physical intrusion events but also loss of communication due to overload or natural disasters such as floods, lighting and earthquakes.

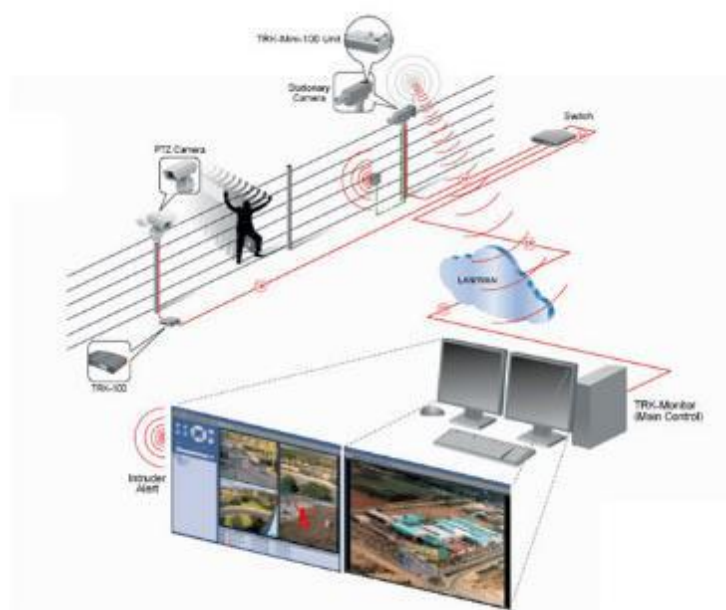


Figure 6 - Conceptual operation of security management systems¹²

2.4.4. Commercial vendors for CIs protection and physical security

A lot of vendors are active in the global market for physical security mechanisms and features for the protection of critical infrastructures in general.

The subjects of related activities present a large variety such as: access flooring, cabling / wiring, backup power networks, UPS and energy management systems, fire protection and fume detection systems, motion detection along with Data Centers / Data Center Facility Management among others.

As seen from the Critical Facilities Summit 2018 (Conference and Exhibition)^{13,14} held in Nashville, USA on 14-16 October 2018, the best of the mission critical community was brought together along

¹² <http://www.promptautomation.com/perimeter-security.html>

¹³ <https://www.linkedin.com/showcase/critical-facilities-summit-2018/>

¹⁴ <https://www.criticalfacilitiessummit.com/exhibits/SearchResults.aspx?id=0>

with all senior level professionals responsible for the design, construction, management and operations of all mission critical facilities. Among the relevant vendors the following can be highlighted:

- Siemens: on Building automation, HVAC controls and components for critical facilities.
- TYCO: offering solutions for Fire & Security
- Ident Solutions: Creator/provider of FEDCHECK, a software platform providing instant, secure visitor screening utilizing NCIC (FBI database) information.
- JLJ General Contracting: Critical Infrastructure remodel specialist.
- Nlyte Software: as the leading data center infrastructure management (DCIM) solution provider.
- ORR Protection Systems Inc.: for fire protection systems and related services for mission-critical businesses.
- PlantLog: offering complete analytics and reporting suite and O&M logging software used for operator rounds and shift communication logs.
- PatchSee; for Patch Cables
- Panduit Certified DataCenter: for Cabling
- Raritan Americas, Inc.: for power management, DCIM software, and KVM for data centers.
- Schneider Electric: which is global specialist in energy management and automation.
- Sealco: providing data center solutions including cleaning, containment and products.
- Service Logic, LLC: for Commercial / Mission Critical / Industrial HVAC and Energy Efficiency Services.
- Stream Critical Environments Services: providing complete operations and facility services for mission-critical environments.
- TimeMaster: for electronic locks, access control, door hardware and more.
- Upsite Technologies (Grommets & Blanking Panels)
- APC: offering UPS, Cooling, Racks & DC Equipment
- LAMPERTZ: for Safe DC Solutions

While the list can be enriched with Austin Hughes Solutions Inc., CPG, Fireline Corporation, Kidde Fire Systems, IronBox, ONICON / Air Monitor Corporation, Sunbird Software, Tripp Lite among others.

2.5. Discussion and added value of the RESISTO project

From the description of the current situation in telecom infrastructures presented in the previous sections the following results can be derived.

The various current solutions, either employed separately or in combination or even under an overall framework, apart from their detection features, present specific advantages: Due to their commercial manner as commercial off-the-self holistic products, regular upgrades can be offered by the respective vendors, while compatibility with proven third-party applications can be guaranteed along with international certifications. Especially the access control solutions can show unlimited scalability

for checkpoints and system users and can utilize fully customizable user interfaces in order to facilitate integration with the individual and general security systems.

However, it should be emphasized the fact, that the use of all the above security mechanisms depends on their relevant cost which is being regarded as an important factor. To this respect, the combination of all the above solutions along with an overall security management system are usually being employed for very critical infrastructures as the main buildings involving NOCs or fibre optics terminals and the large headquarters buildings. There, security management systems are often employed where access control mechanisms (smart cards, biometrics etc.) are mainly used. Due to cost limitations, most sophisticated features such as buried cables or electronic fences are used in headquarters or main buildings rather than in remote facilities since they are more expensive. Of course, all buildings are protected against fire and smoke since these are inherent to the building constructions.

As it has been argued previously, such sophisticated methods are hardly found in other decentralized telecom infrastructures: such as in antenna parks or in telecom infrastructures in remote islands or mountainous regions more expensive or more sophisticated security measures are rarely observed. There, security guards may be employed, while ordinary wire fencing is the main protection measure.



Figure 7 - Fencing in remote CIs (from Intrepid Security Supplier of Security and Loss)¹⁵

It should be emphasized that despite the control and intervention by the current Security management systems to the telecom operations, the main functionality pursued, apart detection, is deterrence. To this respect, the principles governing the basic elements and procedures of the usual physical security plans are the following: detection, deterrence, response and recovery / re-evaluation. However, the procedures used mainly address a rather limited implementation than a holistic tackling of the relevant principles addressed. Due to this, the following can be mentioned:

In current telecom infrastructures' security systems, detection is seen as a physical detection of an intruder, either human or vehicle attempting to illegally access the telecom premises and facilities. To this end, the architecture of the security systems and the relevant equipment are mainly focus to address the personnel identification and access control. Thus, the overall security measures that can be employed as described previously are mainly meant for deterrence purposes. The deterrence

¹⁵ <http://yousense.info/696e747265706964/intrepid-security-supplier-of-security-and-loss.html>

principle is conducted thought the organization's policy, operating procedures and control. In the same manner, the response principle is mostly addressed through the same procedures and actions by the guard staff. Recovery and re-evaluation mainly affect the operational procedures of the security staff.

As an example, limitations and weaknesses can be noticed in the majority of the existing access control systems: in certain cases, reluctance in employing the newest commercial models, possibly due to cost reasons, current systems may result in being unable to manage access permissions or to manage visitors and issue anonymous cards and especially to integrate and manage ambient information. Furthermore, since the currently employed systems are not part or whole of a commercial solution, best practices for physical security systems are difficult to be not followed resulting in limited controller capabilities and limited protection of entry / exit points (i.e. only to main entrances of the main building) or even limited scalability systems maintaining only a minimum coverage of the surrounding environments. Moreover, newest trends in physical security such as pattern recognition and machine learning techniques are rarely employed to classify persons, vehicles and other objects that are moved within the controlled area of the infrastructure and to extract profiles, relevant semantic information and useful data to event processing and correlation platforms for further analysis. Current processes often require large effort of the operator and the security personnel when monitoring a huge number of sensors on a day-to-day basis. Another important issue that needs to be taken into account is that the current security systems focus on tackling the physical threats. Furthermore, in a similar way the impact that a physical threat has on cyber aspects (cyber-physical threat) seems to be dealt separately. Thus, back-up infrastructure, network and equipment are mainly employed in order to deal with relevant risk and to provide adequate protection and response of the telecom networks. To this respect, disaster centres or failover capabilities on backup systems are involved along with mechanisms to facilitate the capability of the management from a central station to relevant checkpoints all over the country.

In this sense and based on all the above, it is seen that a holistic security system such as that proposed by the RESISTO is not clearly evident yet in telecom infrastructures. RESISTO foresees complete confrontation of the overall aspect, addressing both cyber and physical threats and their combinations on the impact they have on the telecom infrastructures procedures and tackling mechanisms. Through RESISTO the whole circle from prevention, detection, protection, response and mitigation is being addressed with a unified security platform addressing both cyber and physical threats and providing adequate prevention and mitigation through a full cycle of risk and resilience quantities.

However, as it has already been discussed, and due to the increase in terrorism actions nowadays, the threats in modern telecom infrastructures involve quite more complex aspects than the ordinary physical security systems can handle. Furthermore, all kind of issues endangering telecom facilities, including airborne threats are on the table for that matter and need to be confronted. As malicious acts and related threats turn to be more advanced and sophisticated nowadays it seems that current approaches should be enhanced with more flexible platforms that could integrate more advanced mechanisms along with an increased degree of resilience, as that offered by the RESISTO approach. To this respect, the RESISTO solution provides novel measures and techniques both for physical and cyber threats.

However, it should be emphasized the fact that the RESISTO solution does not substitutes the current existing physical security measures; instead, RESISTO focuses on being complementary to the existing security management systems implemented in the telecom infrastructures and integrating their procedures and aspects up to the level that this is being feasible due to the operators' policies and the procedures involved. The aim of RESISTO, concerning security is twofold; to prove the concept that new sensors for the detection of modern threats can be successfully integrated to an

overall platform and also to adequately present the complementary manner of the RESISTO solution to the current operational procedures and security systems mechanisms existing in telecom infrastructures. Thus, to show, that it is feasible to use the proposed solutions also for critical telecom infrastructures and the above concept includes the proposed, by RESISTO, sensors as well.

In this context and since the present deliverable D4.1 deals with the sensors that are introduced by RESISTO project to enhance detection, protection and security against modern physical and cyber-physical threats, the description of these sensors and mechanisms will be given in the following chapters of this report. The way that these sensors 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 will be the subject of the next version of this report which constitutes the Deliverable D4.2.

3. SENSOR DATA PROTECTION

As it has been noted already and will be seen in the following Chapters, the sensors that are going to be provided within the framework of RESISTO project are either passive and active sensors that perform direct detection or telecom networks that can act as sensing and detecting systems by themselves through actuators and techniques like blockchain. By this way, aspects of both physical and combined cyber-physical threats are addressed.

Since all detecting and sensing devices provide alarms and events to the security or operation management, specific issues concerning their data protection and authentication need to be considered. To this respect, the relevant aspects are described herein, before proceeding to the description of each sensor that will be made in the next sections of the present Deliverable.

The presentation will start with an overview of current standards and recommendations concerning data and alarm handling addressing physical and cyber-physical threats. In the following current and future trends concerning sensor authentication and relevant data protection will be provided, also in light of the emerging 5G networks and Internet of Things (IoT) with the use of wireless sensor networks (WSN).

3.1. Current telecom Standards concerning threat alarms handling

As we have discussed previously, the purpose of the sensors that are currently used in telecom critical infrastructures are to provide alarms and related intrusion events to the overall management of the facilities in case of a problem arisen. Depending on the nature of the problem these alarms are treated by the telecom operator's management according to specific procedures which have already been defined by Telecommunication Standards and relevant telecom International bodies as alarm management recommendations. The main related general Standards and Recommendations are:

- the "ITU-T M.3703 SERIES M: Telecommunication Management, including TMN and network maintenance: Common management services – Alarm management – Protocol neutral requirements and analysis"¹⁶ along with its related recommendations of the same series
- the "ETSI Technical Specification 3GPP-5G TS 32.111-2 V15.0.0 (2018-06) concerning Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Telecommunication management; Fault Management; Part 2: Alarm Integration Reference Point (IRP): Information Service (IS) (3GPP TS 32.111-2 version 15.0.0 Release 15)"¹⁷ and
- the "ITU -T CCITT Recommendation X.733 concerning Data Communication Networks – Information Technology – Open Systems Interconnection – Systems Management: Alarm reporting Function"¹⁸.

The above Standards and Recommendations provide basically the requirements and analysis for one of the common management services as the alarm management is. The functional requirements for the alarm management interface include the management functions for alarm forwarding and filtering, clearing of alarms, storage and retrieval of alarms in/from the agent, configuration of alarms, alarm

¹⁶ <https://www.itu.int/rec/T-REC-M.3703/en>

¹⁷ https://www.etsi.org/deliver/etsi_ts/132100_132199/13211102/15.00.00_60/ts_13211102v150000p.pdf

¹⁸ <https://www.itu.int/rec/T-REC-X.733/en>

acknowledgement and alarm notification failure. The above reports provide a detailed information model supporting the above functions across the management interface.

It has to be noted, however, that the above standards and recommendations are telecom ones and as such they do not specifically foresee clear recommendations related to risks, alarms and events caused by direct physical or cyber-physical threats. Instead, any kind of problem or malfunction in the overall telecom network and facilities (either physical or cyber or combined) is being defined as a “fault” and as such is being treated within the relevant telecom standards. In this respect, for example, errors in the overall system are being considered as faults; the same stands for problems and malfunctions that are caused by physical or other threats. According to ITU-T X.733 the following definitions are set.

- **error:** A deviation of a system from normal operation.
- **fault:** The physical or algorithmic cause of a malfunction. Faults manifest themselves as errors.
- **alarm:** A notification, of the form defined by this function, of a specific event. An alarm may or may not represent an error.
- **alarm report:** A specific type of event report used to convey alarm information.

Thus, all kinds of faults may need repairing actions and in any case have to be tackled by the fault management or alarm management system of the telecom network. And that is important, also in the RESISTO case, especially considering the interconnection of the telecom CIs with other Critical infrastructures (as in WPs 5 and 8) such as the Power Energy Critical Infrastructures where any kind of malfunction (i.e. short circuits or loss of power) are again being characterised and confronted as faults, including the effect of natural disasters (i.e. lighting) and physical threats to the power network.

To this end, in the following, a brief assessment of the relevant telecom standards and recommendations is being provided focusing on the issues that are associated with physical (and/or cyber/physical) threats, in order to present a complete overview on what is currently being used in confronting the related risks and subsequent alarms and events. This overview, will start with the basic definitions and workflows recommended to be employed by the current fault or alarm management systems within the telecom operators, providing in the end the selected alarms qualifications specifying probable causes of faults that are connected to physical and combined cyber – physical threats.

3.1.1. Definitions and workflows of current telecom fault / alarm management

A network is typically composed of a number of network elements (NE) of various models and different vendors that implement the network communication requirements.

Failures in a NE causes, most of the time, a reduction of the function or quality partial or in some cases complete unavailability of the NE. It is therefore necessary to detect, isolate failures to reduce the propagation of the fault to other NEs, use diagnostic and test routines to determinate the fault cause and use the appropriate maintenance procedures to remove the cause of the fault.

Fault management (FM) has the purpose of detecting failures as promptly as possible and to limit their effects on the network quality of service (QoS). The solution can be achieved by repairing/eliminating the cause of the failure, reconfiguring existing equipment or bringing other equipment into operation. Threshold mechanisms on counters can identify trends leading to a progressive degradation of service; monitoring error rates can detect such trends providing early warnings.

An Alarm is a notification that indicates a fault condition. If an incident causes the generation of several notifications providing correlation among them is utterly important and helpful in the alarm handling. In the *ITU-T M.3703 SERIES M: Common management services – Alarm management – Protocol neutral requirements and analysis* the following useful definitions can be derived:

active alarm: An alarm that has not been cleared and which is active until the fault that caused the alarm is corrected and a "clear alarm" is generated.

alarm notification: Notification used to inform the recipient about the occurrence of an alarm.

clear alarm: Notification used to inform the recipient about the cessation of an alarm and thus the underlying fault condition.

The faults that may occur in the network can be grouped into one of the following categories:

- Hardware failures
- Software problems
- Functional faults
- Loss of some or all of the NE's capability due to overload
- Communication failures between two NEs, or NE and Operation System (OS), or OS and OS.

For each detected fault, an agent will generate appropriate alarms and each alarm should be uniquely identified. The alarm can generally include the following information, where applicable:

- the managed entity;
- the device/resource/file/functionality/smallest replaceable unit as follows:
 - for hardware faults, the smallest replaceable unit that is faulty;
 - for software faults, the affected software component, e.g., corrupted file(s) or databases or software code;
 - for functional faults, the affected functionality;
 - for faults caused by overload, information on the reason for the overload;
 - for all the above faults, wherever applicable, an indication of the physical and logical resources that are affected by the fault and a description of the loss of capability of the affected resource;
- the fault type (communication, environmental, equipment, processing error, QoS, security types, etc.);
- the severity of the fault (indeterminate, warning, minor, major, critical);
- the probable cause of the fault;
- the specific problem;
- the time at which the fault was detected;
- the nature of the fault; any other information that helps understanding the cause and the location of the abnormal situation (system/implementation specific).

The overall network health requires continuous monitoring of the faults in the network and proper notification to network management applications. Some faults can influence the operational state of

the logical and/or physical resource(s) triggering a change of state; thus, detection of state changes is as important as the notification of the alarms themselves for a proper network handling.

System operators will use the active alarm list as well as the historical alarm and state changes together with test procedures for complete analysis. This is being done using an operations system on the network management layer which in turn will collect faults from the Element Managers (EM) which are connected to the NEs of an i.e. 3GPP system or similarly on any other telecommunication system.

The following phases are important for fault handling, fault detection and recovery.

Fault detection - Detection of a fault is demanded to the network entities involved and is their responsibility to report a fault immediately and generate an alarm. Autonomous self-check circuits/procedures observation of measurements, counters and thresholds are the tools to implement detection. The threshold measurements may be predefined or based on performance measurement administered by the Element Manager [as in b-ITU-T M.3704].

It is requested, for instance, that a hardware fault, affecting a physical resource but also degrading the logical resource(s) that this hardware supports, should generate one single alarm for the faulty resource (i.e., the resource which needs to be confronted) and a number of events related to state management for all the physical/logical resources affected by the fault, including the faulty one itself. In case a network entity is not able to recognize that a single fault manifests itself in different ways, the single fault is detected as multiple faults and originates multiple alarms. It is however necessary, that once the fault is tackled, the network entity should be able to clear all the related alarms.

When a fault involves and affects the connection media between NE and OS each affected NE/OS shall detect the fault and generate a communication alarm toward the managing OS, which in turn shall perform the correlation. All faults should have well-defined conditions for fault occurrence and fault clearing conditions. However, there are exceptions to this rule; for instance, ADMC faults cannot be cleared by the network entity itself, as no clearing condition exists. Another example would be when the network entity has to restart a software process due to some inconsistencies, and normal operation can be resumed afterwards. For faults which do not result in standing conditions there is no need for any action, since the fault condition lasted for a short period of time only and then disappeared (e.g. crossing of some observed threshold by the NE in an interval that is not observed in the next interval). However, events must still be generated by the faulty network entities in any case.

Fault recovery - After a fault has been detected, the faulty units/components shall be identified; this can be a software component that needs to be corrected and replaced or a HW component that needs to be physically replaced. Once a fault has been detected, the NE may be able to autonomously take recovery actions. The Element Manager shall be able to put back in service a faulty unit(s) that has (have) been replaced or repaired with the minimal possible disturbance to the communication service. NE may be able to perform recovery actions if requested by the operator; if for instance he has deduced a faulty condition by analysing and correlating alarm reports or performing proactive maintenance. The recovery actions depend on the existence of redundant resources provided in the NE in order to achieve fault tolerance and to improve system availability. When no redundancy is in place, recovery shall be performed by means of isolation and removal faulty resource, removal of dependent resources and functions and notifying all actions to the OS. Repair actions proposed from x.733 are used to specify one or more solutions when the cause is known; for instance retry, or replace of media or to be switched in standby equipment.

The ITU-T M.3703 SERIES M defines the interfaces to communicate alarm information of the involved managed objects to network management systems layer. In our case the same or a proper filtered subset of this information will be sent to the RESISTO platform for the same purpose. As an example, extracted from 3GPP TS 32.111-2 V15.0.0 (2018-06), the itf-N management interface is defined between the Element Management (EM) layer and network management (NM) layer according to the

ITU-T M.3703 SERIES M: Telecommunication Management network (an overview of which can be found in *ITU-T M.3000 SERIES M: TMN and Network Maintenance - Overview of TMN Recommendations*). The general workflow of the system context for an Integration Reference Point (IRP) as found in 3GPP TS 32.150 is shown in the diagram below.

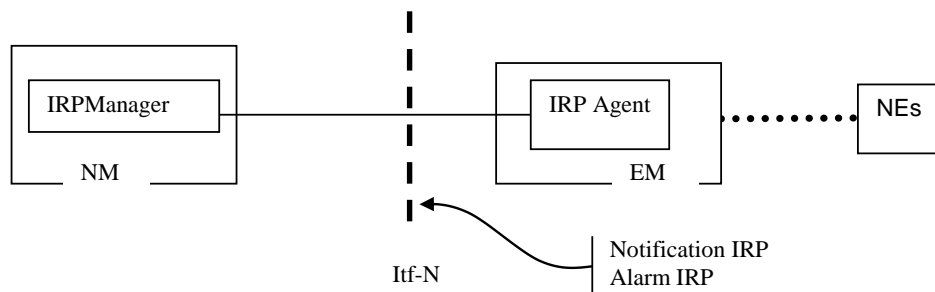


Figure 8 – System Context

The following events shall be collected:

- events and failures occurring in the subordinate entities;
- events and failures of the connections towards the subordinate entities and also of the connections within the 3GPP system;
- the network configuration (alarms and related state changes coming from network resources, although this is not part of the Fault Management).

This means that notifications generated by the Fault Management are sent to the Network Management layer as alarm reports or state change event reports.

A notification will contain a number of fields with relevant information to the fault to reason process in particular the object class and instance, that identifies the system's part affected by the fault, the Alarm/Event type and the Probable Cause. Once the reason of the fault is analysed, the proper actions that need to be taken in order to put the system back to normal operation are identified.

3.1.2. Alarms, events and probable causes in telecom standards

Alarm type or Event types

In particular the following event types are of specific interest when a security breach is detected:

Integrity violation: An indication that information may have been illegally modified, inserted or deleted.

Physical violation: An indication that a physical resource has been violated in a way that suggests a security attack.

Security service or mechanism violation: An indication that a security attack has been detected by a security service or mechanism.

It can also be argued that the above event types can actually be considered as a possible side effect of a cyber-attack. Furthermore, some type of attacks might be detected considering the impacts on the QOS of the telecommunication system, as in the following:

Operational violation: An indication that the provision of the requested service was not possible due to the unavailability, malfunction or incorrect invocation of the service.

The following entities are defined (according to [ITU-T X.733]):

Quality of service: An alarm of this type is associated with degradation in the quality of a service.

Communications: An alarm of this type is associated with the procedure and/or process required conveying information from one point to another.

Processing error: An alarm of this type is associated with a software or processing fault.

Time domain violation: An indication that an event has occurred at an unexpected or prohibited time.

The following types can also be an indication of a possible physical attack (according to [ITU-T X.733]):

Environmental: An alarm of this type is associated with a condition related to an enclosure in which the equipment resides.

Equipment: An alarm of this type is associated with an equipment fault.

In 3GPP TS 32.111-2 V15.0.0 (2018-06) and ITU-T X.733, "alarmInformationList", depending on the "alarmType" parameter, means "Integrity Violation", "Operational Violation", "Physical Violation", "Security Service or Mechanism Violation" or "Time Domain Violation" indicating a security alarm.

Furthermore, the following parameters apply only in case of a security alarm: "ServiceUser" which identifies the service-user whose request for service provided by the "serviceProvider" led to the generation of the security alarm. "ServiceProvider" which identifies the service provider whose service is requested by the "ServiceUser" and the service request provokes the generation of the security alarm while the "SecurityAlarmDetector" carries the identity of the detector of the security alarm. Furthermore, the parameter "Quality of Alarms" can be useful when automatic-correlation engines are used to evaluate the quality of the information reported by the alarm.

Although, alarm response is still not an automated process involving deterministic decisions this is of fundamental importance to enable automatic elaboration of information. The key to secure the quality of the information presented to the operator is to present alarm notifications of high operational relevance, in a timely fashion. If e.g. secondary logs, status or performance data are provided, it must be possible to easily separate those from the alarms.

Probable Causes: ITU-T X.733 defines further qualification of the alarm specifying a probable cause, following a classification of the majority of probable causes described in this Standard that could indicate a physical-attack or cyber-attack. Indicative examples of this manner are given in the following table:

Probable Causes	
SW or HW module has been tampered causing intentionally failures in the overall system	
<i>application subsystem failure:</i>	A failure in an application subsystem has occurred (an application subsystem may include software to support the Session, Presentation or Application layers);

<i>file error:</i>	The format of a file (or set of files) is incorrect and thus cannot be used reliably in processing;
<i>configuration or customization error:</i>	A system or device generation or customization parameter has been specified incorrectly, or is inconsistent with the actual configuration;
<i>corrupt data:</i>	An error has caused data to be incorrect and thus unreliable;
<i>processor problem:</i>	An internal machine error has occurred on a Central Processing Unit;
<i>software error:</i>	A software error has occurred for which no more specific Probable cause can be identified;
<i>software program abnormally terminated:</i>	A software program has abnormally terminated due to some unrecoverable error condition;
<i>software program error:</i>	An error has occurred within a software program that has caused incorrect results;
<i>version mismatch:</i>	There is a conflict in the functionality of versions of two or more communicating entities which may affect any processing involving those entities.
Congestion or overload of the system or network caused by a DOS attack	
<i>bandwidth reduced:</i>	The available transmission bandwidth has decreased;
<i>call establishment error:</i>	An error occurred while attempting to establish a connection;
<i>communications protocol error:</i>	A communication protocol has been violated;
<i>communications subsystem failure:</i>	A failure in a subsystem that supports communications over telecommunications links, these may be implemented via leased telephone lines, by X.25 networks, token-ring LAN, or otherwise;
<i>I/O device error:</i>	An error has occurred on the I/O device;
<i>congestion:</i>	A system or network component has reached its capacity or is approaching it;
<i>CPU cycles limit exceeded:</i>	A Central Processing Unit has issued an unacceptable number of instructions to accomplish a task;
<i>degraded signal:</i>	The quality or reliability of transmitted data has decreased;
<i>local node transmission error:</i>	An error occurred on a communications channel between the local node and an adjacent node;
<i>loss of frame:</i>	An inability to locate the information that delimits the bit grouping within a continuous stream of bits;
<i>loss of signal:</i>	An error condition in which no data is present on a communications circuit or channel;
<i>out of memory:</i>	There is no program-addressable storage available;
<i>output device error:</i>	An error has occurred on the output device;
<i>performance degraded:</i>	Service agreements or service limits are outside of acceptable limits;
<i>resource at or nearing capacity:</i>	The usage of a resource is at or nearing the maximum allowable capacity;
<i>response time excessive:</i>	The elapsed time between the end of an inquiry and beginning of the answer to that inquiry is outside of acceptable limits;

<i>retransmission rate excessive:</i>	The number of repeat transmissions is outside of acceptable limits;
<i>storage capacity problem:</i>	A storage device has very little or no space available to store additional data;
Physical intrusion or natural disaster	
<i>enclosure door open;</i>	
<i>excessive vibration:</i>	Vibratory or seismic limits have been exceeded;
<i>fire detected;</i>	
<i>flood detected;</i>	
<i>heating/ventilation/cooling system problem;</i>	
<i>humidity unacceptable:</i>	The humidity is not within acceptable limits;
<i>leak detected:</i>	A leakage of (non-toxic) fluid or gas has been detected;
<i>material supply exhausted:</i>	A supply of needed material has been exhausted;
<i>power problem:</i>	There is a problem with the power supply for one or more resources;
<i>pressure unacceptable:</i>	A fluid or gas pressure is not within acceptable limits;
<i>pump failure:</i>	Failure of mechanism that transports a fluid by inducing pressure differentials within the fluid;
<i>temperature unacceptable:</i>	A temperature is not within acceptable limits;
<i>toxic leak detected:</i>	A leakage of toxic fluid or gas has been detected.

Table 1 – Indicative example on Probable Causes

3.2. Sensor Authentication

In autonomous cyber-physical systems, integrity and availability become more important than confidentiality. Losing control of locks, vehicles, or medical equipment is far worse than having someone eavesdrop on them. Therefore, properties like message freshness, proximity, and channel binding also become essential, sometimes in unexpected ways. For example, proximity-based security systems used in smart car keys, access cards, and contactless payment systems verify freshness, but they don't verify proximity, so two attackers can relatively easily relay the signal from a device in a victim's pocket, gaining access to the resource.

IOT Applications typically are a combination of micro services that are used to create a service. These applications can be statically located or dynamically migrated to the environment that is optimal for their realization. The security of the applications will be the result of the application code itself and the platform it is using. In cases where applications can migrate, it is important that migration between platforms happens securely¹⁹. In cloud systems, applications can be securely placed on trustworthy platforms by using attested information that comes from roots of trust in the cloud infrastructure.

After devices or applications have used identities to establish contact, the exchange of data is secured by different kinds of security protocols. The Internet Engineering Task Force (IETF) has

¹⁹ Persson et. al., Calvin – Merging Cloud and IoT, <http://www.sciencedirect.com/science/article/pii/S1877050915008595>

driven the standardization of several new lightweight profiles of existing security protocols. One example is an authorization framework based on OAuth suitable for resource access in constrained environments²⁰. By reusing existing solutions where possible, innovation is accelerated and integration with existing systems is made easier.

To protect information in the presence of intermediaries, traditional secure protocols such as IPsec and TLS are not sufficient, as they support only trust models with fully trusted endpoints. As a rule of thumb, authorization to access information should be given on a need-to-know and need-to-change basis. To accomplish this goal, end-to-end security is needed at the application layer. Object security (the use of information containers providing confidentiality, integrity, and origin authentication) is the preferred solution to protect message exchanges, since it enables end-to-end security independently of intermediaries and lower layers in the protocol stack.

Currently, many IoT data integrity and authentication solutions rely on extending proprietary implementations from traditional machine-to-machine (M2M) systems. Other solutions borrow traditional web mechanisms like certificates that require additional infrastructure to be fully effective. On the other side Telecommunications industry is already successfully managing authentication on a large scale therefore solution based on telecom authentication are to be preferred in our opinion.

The purpose of connectivity is to facilitate the secure interaction of applications on the device and in the serving network nodes. This requires two crucial functions: identification based on credentials and secure data transport. IoT connectivity must be able to handle billions of devices and will be realized through heterogeneous access technologies. Many devices will be deployed in capillary networks and connected to cellular networks via gateways. Enablers in the cellular network can then provide device management, secure bootstrapping, or assertions such as verifying device location or trustworthiness of platforms. Evolved 3GPP technologies such as LTE-M, NB-IoT and EC-GSM-IoT are superior solutions designed to meet IoT requirements²¹. They provide global connectivity and offer unrivaled robustness compared with unlicensed spectrum. The use of encryption on the radio interface makes traffic analysis significantly harder.

Based on pre-provisioned device credentials, access technologies need to provide automatic and secure remote provisioning of connectivity credentials. 3GPP credentials have traditionally been provisioned on physical UICC cards, requiring dedicated readers and local manual provisioning. An embedded UICC (eUICC) enables remote provisioning and management of credentials. By generating credentials on the device, the risk of breaches is reduced²². The next logical and necessary step is to use the trusted execution environment that is already integrated in the baseband or application processor. This evolution offers reduced hardware cost and power consumption, improved speed, and flexibility to use new types of credentials.

The IoT, including interworking with existing identities and credentials in various industries, is one of the main 5G focus areas²³. Industry customers want a single service layer agreement with a single connectivity aggregator providing reasonable and predictable fees. For some use cases, it might be a security benefit only to allow connection from a single base station or access point, while other use cases such as transportation require global roaming. As the IoT consists of so many different

²⁰ IETF, Authentication and Authorization for Constrained Environments (ACE), available at <https://tools.ietf.org/html/draft-ietf-ace-oauth-authz>

²¹ Ericsson, Cellular Networks for Massive IoT, January 2016, available at: [White paper IoT.pdf](#)

²² GSMA, IoT Security Guidelines, available at: <http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/>

²³ Ericsson, 5G Security – Scenarios and Solutions, June 2015, available at: [White paper 5g security.pdf](#)

ecosystems, flexibility is a must. There must be a possibility to bootstrap connectivity credentials from device credentials, or application credentials from connectivity credentials.

As a general consideration on the credentials protection, we can say that to avoid spreading of attacks, like in the case of other systems, also IOT devices credentials should be unique, shall not remain unchanged to factory defaults when are deployed in field. Device user and password shall be resettable, and eventually forcibly reset when deployed or accessed by the user. Passwords should also be such that brute force or guess methods shall not succeed.

The same applies to debug modes and backdoor left by programmers. Two-factor authentication (2FA), based on password plus a random codes generation it is another strong feature to implement. A better approach to the problem is to adopt a future proof IAM solution. When a new service or a fleet of connected IoT devices (such as smart meters) is deployed ensuring security is tight from the very beginning is important. Success lies in creating future-proof, secure IAM solutions that, in turn, become business solutions. Digital identity, IAM, cloud security management need to be integrated to implement the correct digital identity management solution that can prevent security breaches.

The technologies to implement automated and secure authentication and authorization solution comprise the following: PKI, GBA, Blockchain, OAuth, OpenId Connect and LoRa.

There is need for resilient, advanced IAM spans across IoT devices for internet banking to smart metering-based services. Some may need more security than others: internet banking, for example, will need the highest security multi-factor authentication (MFA), consent and authorization. With many IoT devices' service life spanning decades, having the right mix of algorithms and key sizes for the authentication, authorization and encryption protocols is a must. Mobility is the key to new services. This means digital identity solutions across mobile, federated or IAM cloud-based platforms are crucial. Identity exposure and unexpected digital threats can protect users from unauthorized access. Identity validation, consent, attribute sharing, and trust management are key.

3.2.1. Generic Bootstrapping Architecture (GBA)

This technology supports device authentication and communication security at the transport layer in advanced cellular networks around the world. GBA leverages SIMs to create strong session keys between devices and data analysis systems. It enables operators to create symmetric encryption security, with the added value of having mutually authenticated both the device and its enterprise server. This technology can now be extended to provide equally strong authentication and data integrity for the IoT. It is based on an existing, globally scalable infrastructure and can be built into every device.

For IoT applications, existing cellular networks offer distinct advantages over alternative wide area network (WAN) technologies, such as unlicensed low power wide area (LPWA). The global reach, QoS, ecosystem, TCO, scalability, diversity and security of cellular networks are all vital factors that can support the fast uptake and success of IoT.

To minimize resource (bandwidth) consumption as well as consume less energy IoT systems can be accessed via Gateways. Another way to reduce power consumption is to spend most of the time in sleeping mode and wakeup only when really needed and rely on proxies to cache requests and responses. Moreover, gateways are needed to bridge different transmission technologies and offload processing. Mesh topologies even require every node to be able to be an intermediary.

While proxies and gateways are necessary in many IoT deployments, they open pathways for attacks. Even when security protocols like IPsec and TLS are used, there is commonly a breach in security when an intermediary can read, change, or inject information without being detected. A trust model involving a multitude of trusted intermediaries breaks down as soon as the security of one of these

intermediaries is compromised. Application layer security is needed to address such challenges. Another challenge related to this situation is working out how to maintain trust in data that is processed on its way from sensor to consumer.

Devices - hardware roots of trust

As many IoT devices are placed in exposed environments, these devices should have the means to automatically protect their functioning and the data they contain. Sensitive data in non-secure storage needs to be encrypted and integrity protected to obtain a secure storage function. Devices must cryptographically verify firmware and software packages at boot or update and should maintain the ability to receive remote firmware updates even in case of malware infection. Devices should have enough storage to carry out automatic rollback in the event of an update failure, but malicious rollback to older versions of the firmware or software with critical vulnerabilities must be prevented.

These security features must be kept isolated from the applications on the devices. Hardware based isolation can be used for these security features and is needed to protect applications from other applications and potentially compromised operating systems. This type of functionality constitutes a root of trust – traditionally provided by dedicated hardware, but now achievable with trusted execution environments (TEEs) isolated from the rich execution environment (REE) in common processors, including low-cost embedded processors. For deployments where cost is important, the use of TEE is preferred. Strong device security is necessary to protect sensitive data and prevent IoT devices from being used as stepping stones for attacks.

Modern cryptographic algorithms are significantly faster than legacy algorithms; even asymmetric cryptography runs well on everything except processors in the most constrained ultra-low-cost segment. Furthermore, the energy cost of symmetric cryptography is negligible compared with that of wireless communication. Lightweight cryptography is needed for some environments, but not for the IoT in general. Strongest encryption based on IPsec and/or TLS/SSL possible should be preferred as communication between devices can be hacked, a device may be able to use strong encryption on available computing resources and the protocol used. Where encryption cannot be used messages can be signed and only the digital signatures verified. A future challenge is that the current asymmetric algorithms need to be replaced with post quantum resistant variants, where keys and signatures are expected to be much larger. For IoT devices in exposed environments, protection against side-channel attacks is essential to prevent leakage of keying material through timing information, power consumption, electromagnetic waves, or sound.

3.2.2. The embedded SIM solution

The GSMA's Embedded SIM Specification provides standard mechanism for the remote provisioning and management of machine to machine (M2M) connections. Provisioning initial operator subscription, and the subsequent change of subscription from one operator to another. GSMA Embedded SIM is a vital enabler for Machine to Machine (M2M) connections including the simple and seamless mobile connection of all types of connected machines.

SIM cards can support additional security features to support authentication in IOT services. Machine-to-machine Device access for Provisioning a Subscription requires a mechanism for remote access if the necessary credentials to gain mobile network access. The MNO will have to be able to respond to requests to change Subscription (contract) from one MNO A to a different MNO B, without having physical access to the Embedded UICC in the Device in question. The GSMA standard²⁴ describes

²⁴ GSMA, "Embedded SIM Remote Provisioning Architecture", December 2013: <https://www.gsma.com/iot/wp-content/uploads/2014/01/1.-GSMA-Embedded-SIM-Remote-Provisioning-Architecture-Version-1.1.pdf>

the architecture which enables remote Provisioning and Subscription management, while maintaining the same level of security of current HW based SIM. Including the safe keeping of keys for cryptographic functions for MNO Network Access and IMSI or other Customer identities.

4. ACTIVE AND PASSIVE SENSORS FOR DIRECT DETECTION OF PHYSICAL THREATS

In the previous Chapter an overview of the current situation of security and protection sensors and mechanisms against physical threats in critical telecom infrastructures was presented. As it was discussed, the increased security requirements nowadays imply the employment of new approaches and solutions such as the RESISTO one. In this context, in the following Sections the presentation of the sensors and mechanisms to be integrated in the RESISTO platform will be given for the detection of physical threats in telecom CIs. The presentation will begin in this Chapter with the description of the functionalities of the active and passive sensors that are going to be implemented for direct detection of physical threats (i.e. physical intrusion, airborne threats etc.) while in the next Chapter the functionalities of the telecom networks themselves as sensor mechanisms will be provided.

4.1. Sensors for Audio and Video analytics and monitoring tools

Audio and Video analytics sensors will constitute an audio/video-based surveillance system provided by ADITESS. This system along with the Audio Analytics Component (AAC) and Video Analytics Component (VAC) will be integrated in the RESISTO platform providing physical security solutions.

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 and for the early identification of illicit activity. Pattern recognition and machine learning techniques are used to extract acoustic events (i.e. gunshot, screaming, glass breaking) or to classify persons, vehicles and other objects that are moved within the controlled area of the infrastructure.

Upon an event detection by analytics algorithms, a video clip is generated and delivered to the security operator. Security operator is notified with an alert about the suspicious activity and with important information about the event (location, etc.). This intelligent process reduces the effort of the operator by monitoring in a 24/7 base a huge number of sensors. Additionally, the early detection of events (real-time) and the ability to extract semantic information (i.e. type of event, illegal access in restricted area, and location of the event) can provide useful data to event processing and correlation platforms for further analysis.

In RESISTO, beyond the acoustic event detection, audio analytics will be enhanced with techniques capable for localization of the source of the detected event. This feature, will be used as an input to the video sources (CCTV) cameras in order to adjust the position to the source of the acoustic event. The added value of this integration (between audio and visual sensors) is the ability to provide to the security operator a real-time picture of the field where the event occurred. Furthermore, cross-correlations of audio and video analysis results will be developed in order to provide more accurate and precise alerts.

4.1.1. Audio sensors – description and functionalities

A microphone is a transducer that converts sound into an electrical signal. Different types of microphones are in use, which employ different methods to convert the air pressure variations of a sound wave to an electrical signal. Microphones are used in many applications such as telephones, sound recording, two-way radios, audio-based surveillance systems, etc. In this project, we will use two types of microphones, the omni-microphone and the array microphone. The first one will be used to provide solutions for acoustic event detections and the second type to provide capabilities to localize the source of the event.

Omni Microphone: This sensor is a highly-sensitive, omnidirectional, 3-pole microphone. Through a USB sound card, a connection of the microphone to an embedded PC (e.g. Raspberry 3) is being made where the first level of detection algorithms will be placed and executed. The output of this audio system will be the detected and classified events.

Specifications:

- Directivity: Omni-directional (360°)
- Sensitivity: -23dB (1kHz at 1Pa)
- Signal to Noise Ratio: 58dB+
- Frequency Response: 50 ~ 18,000Hz
- Plug: 3.5mm 3-pole gold-plated
- Size: 28.0mm x 9.0mm (without cable)
- Cable Length: Approx. 1.3M(4.3ft)
- Weight: Approx. 26g
- Power supply: Plug-in power, no batteries required
- Operating Temperature: -5°C ~ 45°C



Indicative Model: EDUTIGE Lavalier Microphone ETM-006.

Array Microphone: A microphone array is any number of microphones operating in tandem. The main purpose of this sensor is to apply the event detection algorithms with the feature to locate the source of the sound. Similar with the other audio sensors, the array microphone will be attached to the embedded PC. Additionally, further to the event detection this audio system will provide information about the direction of the source of the detection. Using this sensor, intelligent algorithms will be applied in order to detect anomalous audio events and to localize (estimate) the position of the acoustic source, in such way that the PTZ video sensor will be steered.

Specifications:

- Microphone Operation Mode: stereo (uni-directional x 2)
- Sensitivity: -44 dBV/Pascal
- Impedance: 200 Ohm
- Frequency Response: 50 Hz
- Max Sound Pressure: 115 dB
- Audio Input Details: Uni-directional - 50 - 8000 Hz



Indicative Model: Andrea 2S Superbeam Array Microphone

4.1.2. Video sensors – description and functionalities

A camera is an optical instrument for capturing still images or for recording moving images, which are stored in a physical medium such as in a digital system. Closed-circuit television (CCTV), also known as video surveillance, is a set of cameras that are used for surveillance and transmit real-time images to the central control. In the RESISTO project, we will integrate a smart surveillance system that constitutes form video sensors (cameras), embedded or other computational units and video analytics algorithms. Video segments of interest, will be generated (upon the detection of alert) and stored for further use and notification of security personnel. For the project's needs, we will use two type of CCTV cameras, the fixed camera and a PTZ camera. The second one support Pan, Tilt and Zoom operations.

Outdoor IP-based CCTV Camera: The IP CCTV Camera will be connected to the system in order to provide seamless image of the area of interest.

Specifications:

- Frame Rate: 25FPS (VGA), 23FPS (720P)
- Network: Ethernet, Wireless
- Diagonal Angle of View: 76°
- Horizontal View Angle: 69°
- Lens Type: f:2.8mm, F:2.6
- Infrared Mode: Automatic or manual
- Firewall: Supports IP Filtering
- Motion Detection: Supported



Indicative Sensor: Foscam FI9803P

Outdoor IP-based CCTV PTZ Camera: The IP CCTV Camera will be connected to the system in order to provide seamless image of the area of interest. Additional to the previous sensor, this sensor provides the feature of PTZ (Pan/Tilt/Zoom). Based on this, the video sensor can receive a trigger from a different sensor in order to move the camera to a desired location.

Specifications:

- Frame Rate: 30FPS
- Network: Ethernet, Wireless
- Diagonal Angle of View: Max 75°
- Horizontal View Angle: 30~70° (Pan/Tilt angle:H355°,V=78°)
- Lens Type: f:2.8mm~12mm, F:1.6
- Infrared Mode: Automatic or manual
- IR Range: 20m (65.6 feet)
- Firewall: Supports IP Filtering



- Motion Detection: Supported

4.2. UAV platform – based sensors

ADITESS has developed during research and design phases a variety of UAV systems, a new concept in UAV market: designed from existing cots platforms or from ADITESS design, in order to minimize the development cost. As it was derived from general aviation standards, it is optimized for reduced cost of operations. The Mini-UAV systems could also prepare for navigation in controlled civilian airspace and for compliance to certification requirements that will become applicable to all UAS addressing homeland security applications and flight operations in European sky. The platforms are based on existing cots and they are enhanced with various payload such as cameras (i.e. Daylight, IR), GPS modules, CBRN sensors as well as other software modules in order to fulfil every client's requirements individually.

In RESISTO project, the purpose of UAVs platforms is twofold:

- (a) to enhance the video surveillance system with aerial image and
- (b) to evaluate the anti-drone techniques that will be developed and integrated in RESISTO.

For the first objective, ADITESS UAV fleet is equipped with electro-optic sensors that contain thermal camera as well as day camera. For the second objective, ADITESS will cooperate with ICCS who provides the anti-drone techniques so that all types of sensors provided by both partners to be work together for the use cases.

In particular, ADITESS UAVs' fleet is using and developing three types of UAV platforms: Multirotor type, Helicopter type and Fixed-Wind type, as these are shown in the following figure.



Figure 9 - UAV fleet provided by ADITESS

The main UAV on board sensor (camera) is being described in the following:

UAV Onboard IP Camera – CM100: A lightweight miniature camera (multi-sensor) designed for integration on Mini-UAV Platforms. The Electro-optical and LWIR lenses provide excellent performance at day and night.

Specifications:

- Position Accuracy: 0.022° or 380μrad
- Elevation: ±115°
- Azimuth: 360° Continuous
- Slew Rate: 105°/s or 1.83rad/s
- Power: 12W
- Voltage: 9 - 36v
- Electronics: High Speed 32bit
- Communication Link: Ethernet / RS232
- Analogue Output: Composite
- Digital Output: .h264 up to 10Mbps
- Snapshots: 1280x720 (Stored on Board)



Indicative Sensor: UAV Vision CM100.

4.2.1. Architecture and Functionalities of the Mini-UAV platform

Apart from the platform and sensors, a Mini-UAV system is constituted from the Ground Control Station (GCS), the communication equipment (Air to Ground and Ground to Infrastructure using LTE/4G or physical network if applicable). To facilitate the operation of UAV systems within an infrastructure, ADITESS developed the Task-Based Guidance (TBG) component. TBG is an intelligence web-based component for the coordination of UAV teams, platforms and sensor configuration.

In particular, TBG can be considered as a decision support system for the selection of the appropriate Mini-UAV platform (platform, payload, communication) and ground control station (GCS) based on several criteria including the mission analysis (path, time, covered distance, range), GCS locations, risk metrics and specifications of the equipment.

The result of the TBG component on a mission request is the generation of the mission plan, as shown in the following figure:

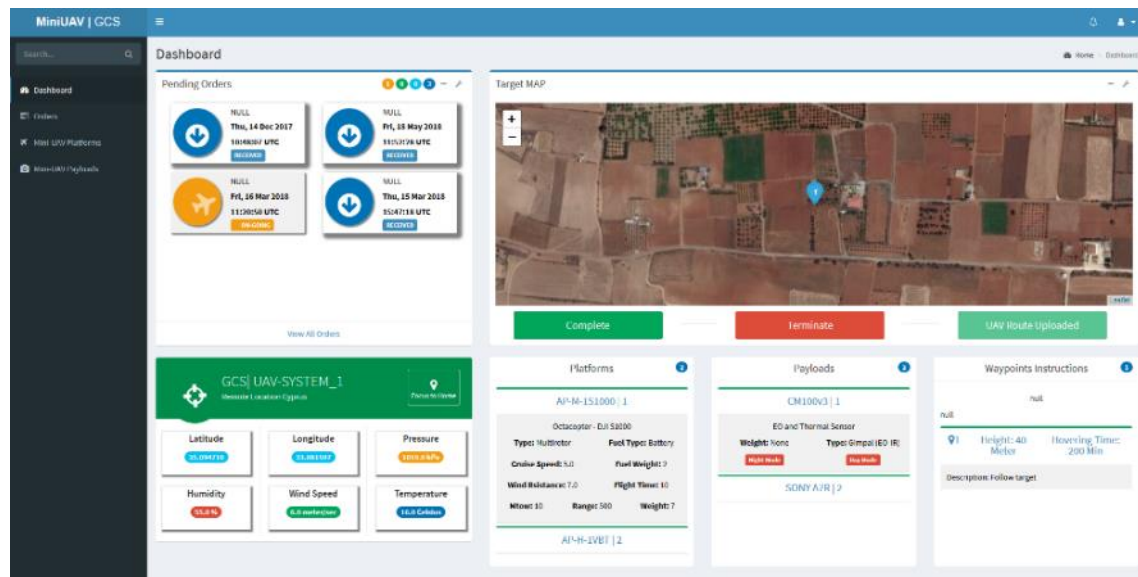


Figure 10 - The Mini-UAV (CGS) environment

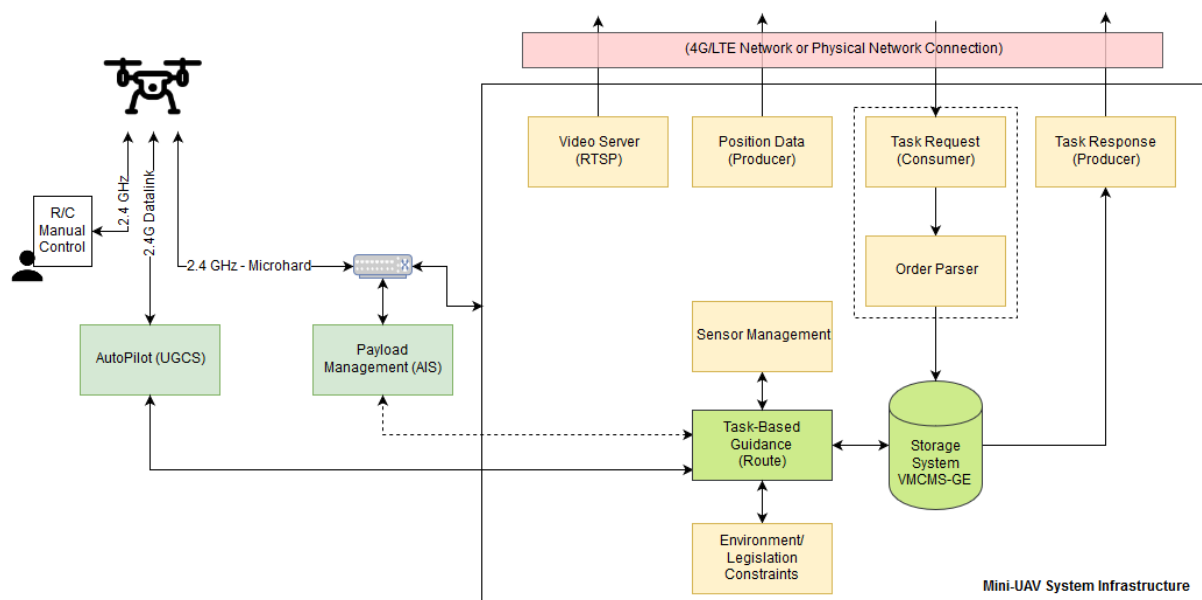


Figure 11 - The Mini-UAV platform architecture

The above figure provides the architecture of the Mini-UAV system including the Mini-UAV platform (integrated with sensor), communication equipment and the software modules/components to enable the interaction with RESISTO platform.

4.3. Passive radar – the AULOS® sensor

As discussed in the previous Chapter, malicious actions in recent decades employ more advanced tools and techniques than the conventional ways (i.e. intrusion, bombing on the ground etc.) used in the past. Current physical threats against critical infrastructures also employ airborne and ground means even from larger distances, aiming to increase their impact and damaging effectiveness on their targets, especially when these are of critical importance or even landmarks on the area. Large telecom buildings, infrastructures and main headquarters could be such targets when considering their impact in cascading effects in the vicinity and their interconnections to other CIs.

Therefore, surveillance systems for longer ranges, involving the vicinity areas of telecom CIs are required with the primary aim to increase the probability of detection of low flying aircrafts and helicopters. Related countermeasures for these kind of threats are close to the limits of employing military actions, however the time needed for the relevant reaction and response may not prevent the impact to the telecom CIs in time. To this respect, employment by the telecom operators themselves of longer range surveillance solutions such as the low cost passive radars that are presented herein.

4.3.1. Working principle

The passive sensor developed by Leonardo (LDO), named AULOS® after the ancient Greek wind instrument, can detect and track targets through the processing of Frequency Modulation (FM), commercial radio and Digital Video Broadcasting–Terrestrial (DVB-T) signals, respectively around 100 MHz and 640 MHz. Passive radars, usually referred to as passive covert radars (PCR) or passive coherent location (PCL), they use no dedicated transmitter equipment; instead they exploit existing transmissions in their environment and attempt to locate targets using echoes from these “transmitters of opportunity”. The PCL working principle is schematically depicted in Figure 12.

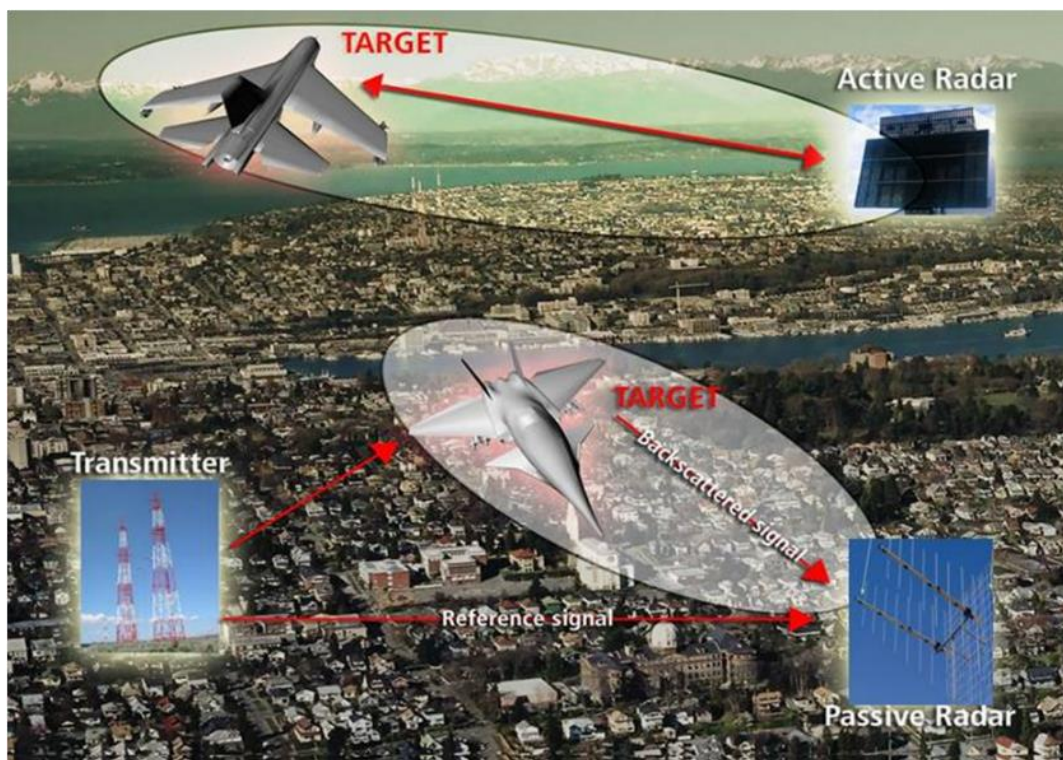


Figure 12 - PCL working principle

By avoiding the need for a dedicated transmitter equipment, PCL results in a number of advantages that can be fruitfully exploited in the considered application. Among these advantages, passive radars are compatible with the environment - they do not generate additional electromagnetic pollution and yield a limited impact on the landscape - and can operate in close proximity to residential areas and, more specifically, in an urban environment. These characteristics are well in line with modern green-view of technology.

In addition, PCL systems face the erosion of the electromagnetic spectrum due to the widespread of telecommunications equipment and carry out effectively the surveillance function for homeland defence and security. Moreover, thanks to their covert operation, PCL systems are invisible to ELINT (Electronic Intelligence) devices so that they yield a low vulnerability to deliberate interference.

A further advantage is the possibility of inclusion in an integrated surveillance network, compensating the dependence of the passive radar coverage on the number of opportunity emitters and their power level. Finally, passive radar systems benefit from bistatic geometry (i.e., receiver and transmitter are located apart) because bistatic geometry enhances target Radar Cross Section (RCS), as shown in Figure 13.

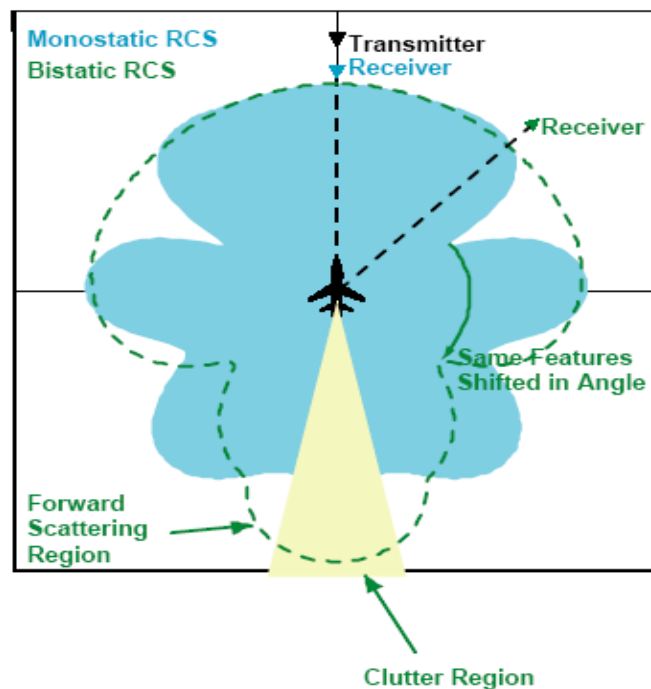


Figure 13 - Comparison of monostatic and bistatic RCS.

The typical basic PCL geometry and processing scheme is depicted in Figure 14.

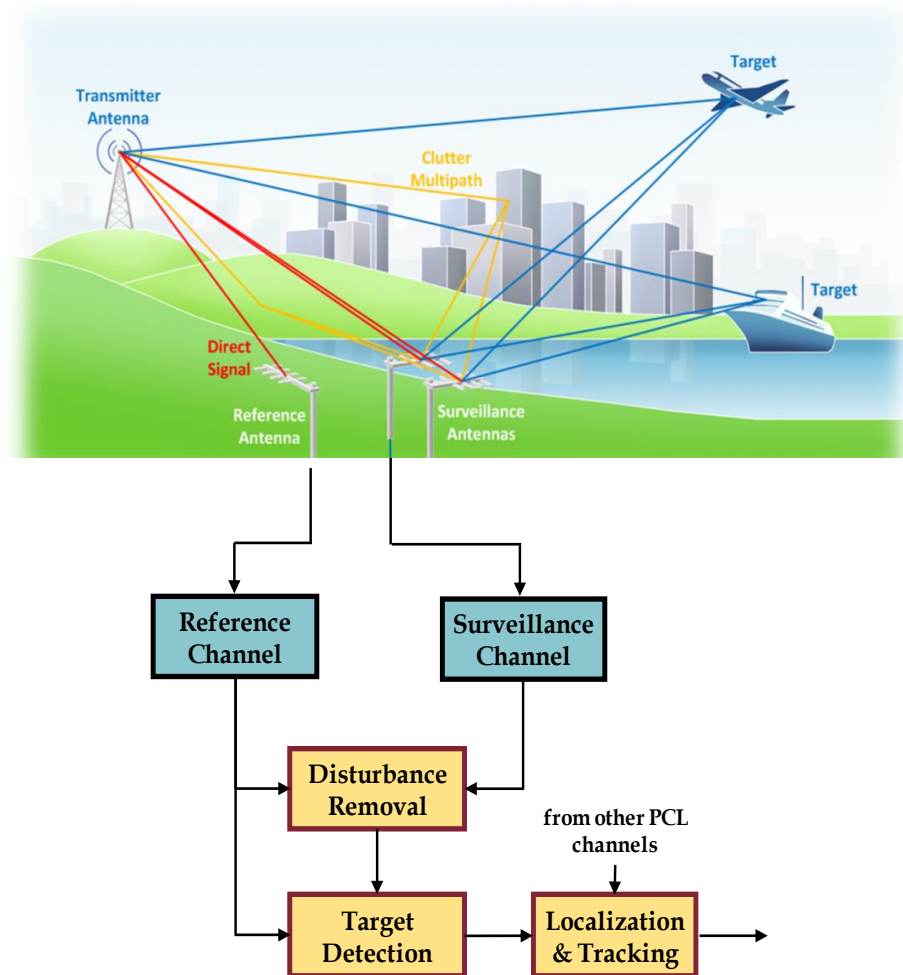


Figure 14 - PCL basic geometry and processing scheme.

The low power signal reflected from the target is collected by the main PCL receiver (typically known as the surveillance channel) using a directive antenna steered toward the direction to be surveyed. Since the transmitted signal is not known at the receiver, an auxiliary PCL receiver (typically known as the reference channel) is usually connected to an additional directive antenna steered toward the transmitter of opportunity.

The signal collected at the reference channel is first used to remove undesired contributions that have been received, along with the moving target echo, on the surveillance channel (basically the direct signal and strong clutter/multipath echoes). After the cancellation stage, the detection process is based on the evaluation of the bistatic two-dimensional (range-velocity) cross-correlation function between the surveillance and the reference signal over appropriate integration times (i.e. coherent processing intervals). A Constant False Alarm Rate (CFAR) threshold can be then applied on the obtained map to automatically detect the potential targets according to a specific CFAR detection scheme. Finally the echoes received at multiple surveillance antennas and/or at different PCL receivers might be exploited for effective Target Direction of Arrival (TDoA) estimation, and subsequent localization and tracking stages in Cartesian coordinates.

4.3.2. Illuminators of opportunity

Radar sensors obviously aim to provide a long detection range, a large volumetric coverage (in elevation) and excellent range (related to the instantaneous bandwidth of the signal) and angle resolution. The sources that have been considered and compared as possible illuminators of opportunity for AULOS® are:

- FM (Frequency Modulation) emitters (around 100 MHz);
- DVB-T (Digital Video Broadcast - Terrestrial) emitters (around 640 MHz);
- DAB (Digital Audio Broadcasting) emitters (around 210 MHz).

Figure 15 shows a simplified volumetric cover that can be obtained using DVB-T, DAB and FM signals as sources of opportunity for passive sensors. Table 2 synthesises qualitatively the expected performance of passive sensors operating in the three bands.

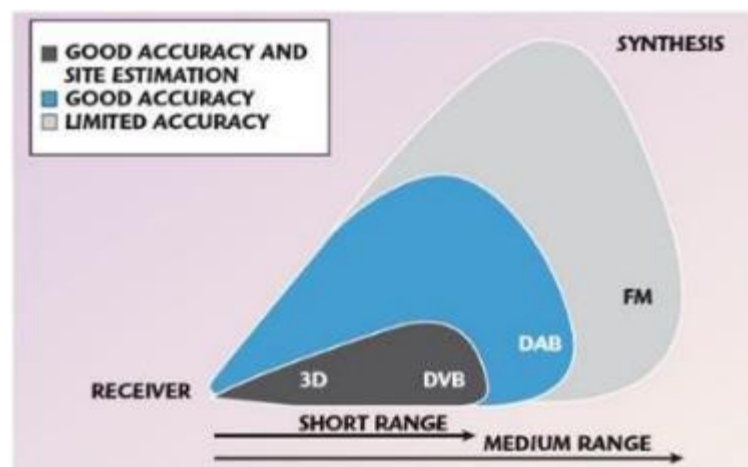


Figure 15 - Accuracy and detection range of some sources of opportunity²⁵.

Illuminators of opportunity	Range	Elevation coverage	Range resolution	Angular resolution	Doppler resolution	Ambiguity function
FM	++	++	-	-	++	-
DVB-T	-	-	++	++	+	++
DAB	+	+	++	+	-	++

Table 2 - Expected performance using FM, DVB-T and DAB illuminators of opportunity.

The analysis of Figure 15 and Table 2 explains Leonardo's choice to design a dual-band PCL based on FM and DVB-T signals:

²⁵ Adapted from: D. Poullin et al: "3D Location of opportunistic targets using DVB-SFN network: experimental results".

- it provides the best performance in terms of range and accuracy;
- FM PCL can detect farther targets and designate them to DVB-T PCL;
- DVB-T PCL has a better track accuracy and allows target state estimation refinement;
- frequency and geometry diversity play an important role against target fading;
- the dual-band operation enhances the immunity to ECM (Electronic Counter Measures).

4.3.3. Architecture and Functionalities of the passive radar

AULOS® consists of four distinct subsystems:

- the Passive Radar sensor, that collects, receives and processes target reflections, to detect them and extract their position and velocity;
- the Local Track Processor, that receives Passive Radar plots, forming primary tracks;
- a Local Monitoring and Control Station, that provides for plot and track visualization and storage and for the monitoring and control of the system;
- communications interface equipment.

AULOS® functional block diagram and the messages the above four subsystems exchange are reported in Figure 16.

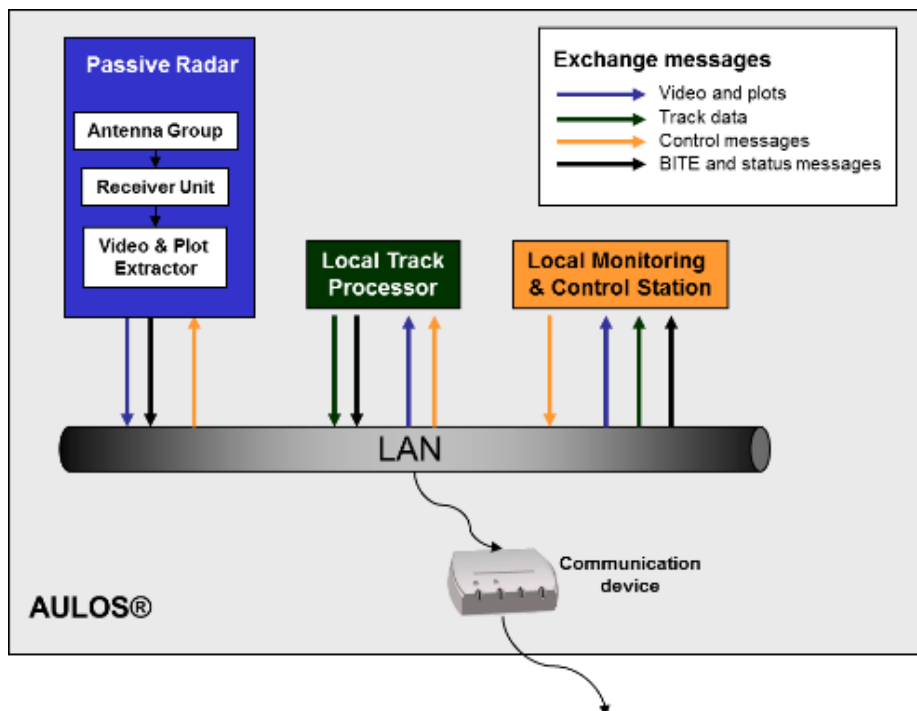


Figure 16 - AULOS® functional block diagram.

As for the Passive Radar component, it is made of the following subsystems:

- the Antenna Group, which includes two 8-element circular antennas, the supporting mast, the analogue Front End Receivers (FER);
- the Receiver Unit;
- the Video & Plot Extractor.

Design and realization activities carried out in the previous years have brought into being the deployable AULOS® shown in Figure 17. In this version, the Antenna Group is equipped with a telescopic pole to move and deploy the antenna array, while a motor home hosts the Receiver Unit, the Visualization Console and the power supply.



Figure 17 - Deployable AULOS® at Farnborough International Airshow in July 2012.

Figure 18 illustrates how the Antenna Group hosts both the FM and DVB-T circular arrays. The pole is a pneumatic telescopic mast composed of 9 sections with a base diameter of 250mm and a top diameter of 115mm. The mast with the antennas mounted on top guarantees radar performance with:

- winds up to 18 m/s (60 km/h) without the use of guy ropes;
- winds up to 30 m/s (108 km/h) with gusts up to 40 m/s (158 km/h), in accordance with IEC 60721 3-4 class IE42, with the use of three orders of guy ropes.

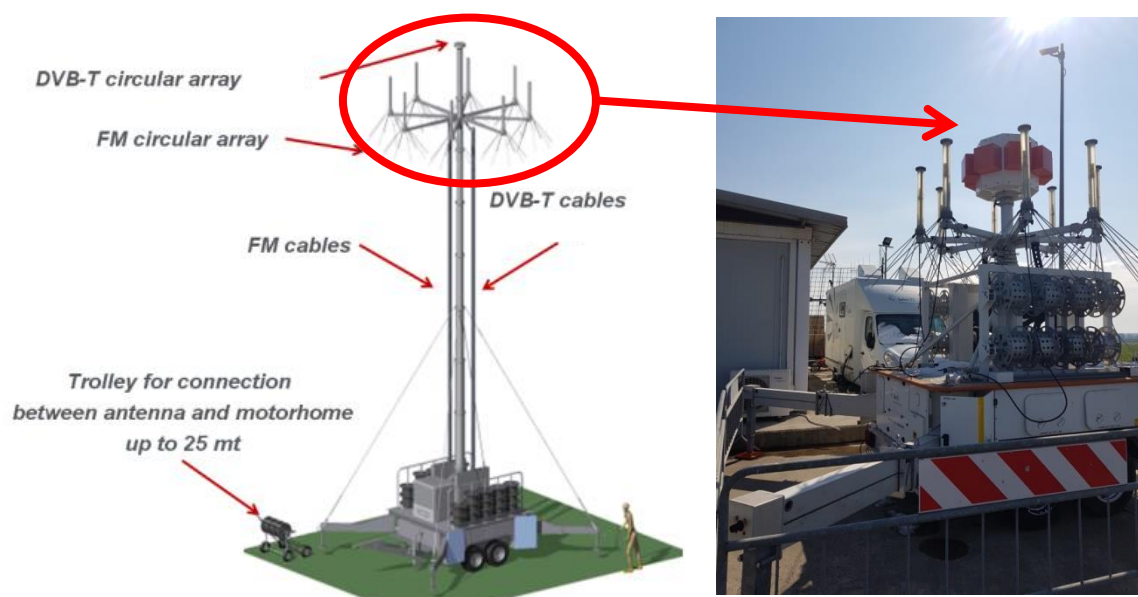


Figure 18 - FM and DVB-T circular arrays.

The transport solution for the deployable AULOS® system is shown in Figure 19.



Figure 19 - AULOS® transport configuration with cover.

A large database of recordings is available after a number of years of live data capture. For example, the AULOS® performance has been characterized in dense civil air traffic areas. The following Figure 20 compares ADS-B (Automatic Dependent Surveillance – Broadcast) and PCL tracks near Fiumicino International Airport, located on the left hand side of the red line (the right end coincides with Leonardo premises in Rome Tiburtina).



Figure 20 - Air traffic near Fiumicino international airport.

Figure 21 shows some experimental results obtained in the framework of the FP7 “SeaBilla” project: the DVB-T based AULOS® detected sea targets well beyond the standard radar horizon (LoS, Line of Sight), suggesting that the expectations on PCL potentialities might be increased to include long range maritime target detection and localization capabilities.

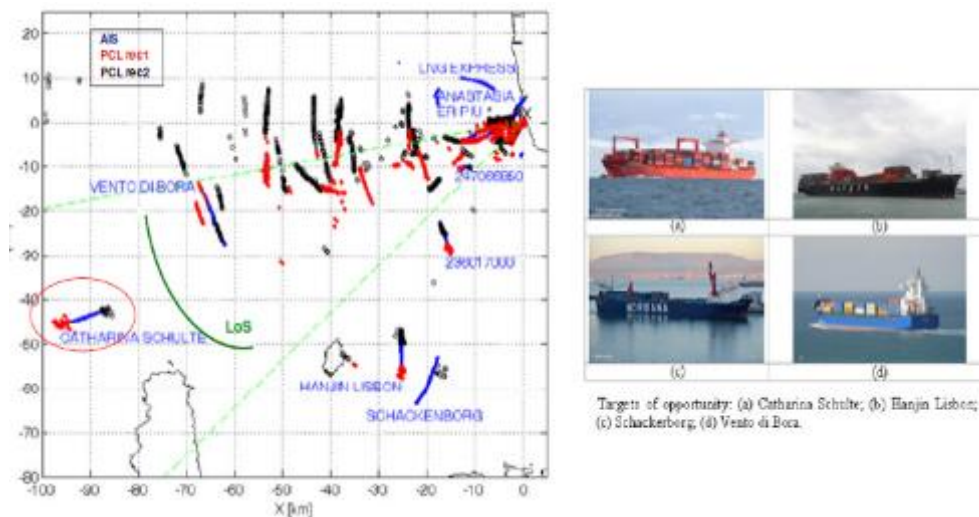


Figure 21 - Results from SeaBilla experiments for DVB-T based AULOS®.

4.3.4. Potential Physical Threats to be detected

Passive radar technology may be conceived as a complementary gap filler to improve the situational picture in currently critical infrastructure protection’s surveillance systems with the primary aim to increase the probability of detection of low flying aircraft and helicopters. With specific reference to AULOS® passive radar family, the following considerations apply:

- In the FM (Frequency Modulation) band version, AULOS® passive radar detects and tracks targets by processing reflections from non-cooperative commercial radio emitters in the FM

band (88÷108 MHz). FM illuminators provide large elevation coverage, but are affected by poor range resolution. In this portion of the electromagnetic spectrum, the waveform of opportunity (wavelength is about 3 metres) inherently increases target Radar Cross Section (RCS) and also interacts with an aircraft to create resonance, independently of fuselage shape.

- The DVB-T (Digital Video Broadcast – Terrestrial) based AULOS® exploits DVB-T emitters (450÷810 MHz), which instead guarantee good accuracy for target detection and tracking within a reduced elevation coverage. RCS enhancement is mainly due to bistatic geometry.

The main characteristics of FM and DVB-T signals are summarized in Table 3.

Characteristic	FM	DVB-T
Frequency range	88-108 MHz	450-900 MHz
Transmitter power	> 50 dBW	40-50 dBW
Type of modulation	Analogue frequency modulation	Digital (COFDM)
Channel bandwidth	Bandwidth varying with information content (maximum 200 kHz)	Constant bandwidth 7.6 MHz
Elevation coverage	Medium	Low
RCS enhancement	Significant	Poor

Table 3 - FM and DVB-T signals main features.

From the analysis of the previous table, pros and cons of each illuminator of opportunity are easily figured out.

- FM illumination provides extended range detection at medium elevation, thanks to high transmitter power and target RCS enhancement. The long integration time that can be implemented without huge computational load (the channel bandwidth is only 200 kHz) provides also optimum Doppler resolution. On the other hand, FM illumination is affected by coarse and variable range resolution.
- DVB-T illumination achieves constant and good range resolution (40 m) with low elevation coverage.

The combined use of FM and DVB-T bands may permit AULOS® passive radar to cope well with the detection and tracking of low flying aircraft: FM AULOS® may take advantage of RCS enhancement to early detect these targets and designate them to the DVB-T AULOS® for accurate tracking. From the design and implementation viewpoint, FM and DVB-T signals not only ask for different antennas and receivers (the carrier frequency is different!), but also require to cope with completely different issues:

- on the FM side, reference beam-forming, check of ambiguity function quality, surveillance beam forming, adaptive clutter and direct interference suppression, advanced Cartesian tracking;
- on the DVB-T side, reference signal reconstruction using diversity of antenna elements, bit-error correction, ambiguity function sidelobes control, high computational load.

With specific reference to detection and tracking of low flying aircraft, main issues are related to radar horizon limitations. Passive radar technology might be affected by radar shadow as well, but AULOS® is a deployable ground system that may be located at suitable height, even in locations not so close to the area of interest, thanks to the detection enhancement that has been presented and justified above (bistatic geometry, short wavelength). In addition, due to the low carrier frequency of the exploited transmissions, the radio wave is expected to travel beyond the normal line of sight thanks to the combination of different propagation mechanisms. This is especially true over sea paths where super-refractive conditions are prevalent.

As regards technology exploitation, the unique advantage of passive radars of not requiring any permission for frequency use enables end users to supply themselves with low cost, eco-compatible and exclusive radar stations, which can focus on specific objectives, breaking the interagency dependence that often disrupts normal operations.

4.4. Active and passive sensors for airborne threats (i.e. UAVs)

Additional active and passive sensors that are going to be used in the framework of RESISTO project focus specifically in detecting airborne threats as UAVs and drones, flying at rather short ranges from the targeted CI. The rapidly proliferating use of unmanned devices, in many aspects of commercial and everyday life, has brought about new and emerging challenges. In many cases, such as regulating air traffic and security, early detection of such objects is more than crucial. Furthermore, UAVs can be maliciously used as potential types of human-driven physical threats against civil critical Infrastructures.

Herein, the term “active” is used to describe the use of RF waves, typically originating from radar systems. An existing implementation of a Continuous Wave Doppler (CW Doppler) Radar is used providing useful results for determining many of the detection parameters (frequency used, target's RCS, signal processing etc.) by taking into account data derived from outdoor measurements of UAV and drone platforms (such as the commercial off-The-Shelf (cots) DJI Phantom 3 Advanced Drone²⁶). “Passive” methods denote the reception of signals emitted by such platforms. Those signals may be in the microwave/RF (e.g. remote controls) or the sound/acoustic (e.g. propulsion) frequency region; hence, the focus is on exploiting the acoustic imprint of UAVs as captured by microphone systems.

The specific airborne threat detection system is a set of tools designed and developed to detect the presence of small UAVs and drones as airborne threats and to provide alarm signals. The system consists of active and passive sensors namely radar and acoustic sensors respectively. The above system's components can be either used separately or in combination. In the following, each sensor will be described and then the description of the combined system architecture will be provided.

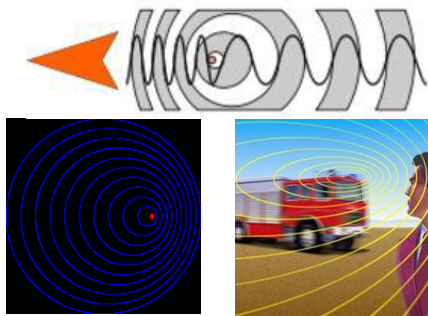
4.4.1. Working principle

The main scientific principle behind both types of sensors is the well-known Doppler Effect. According to that, a change in frequency (or wavelength) of a wave occurs between the signal transmitted by a source and that received by an observer when the wave source is moving relative to the observer²⁷. Therefore, the Doppler shift is the apparent change in frequency (and thus, in wavelength) due to the

²⁶ Al. Kyritsis, R. Makri, M. Gargalakos and N. Uzunoglu, “Active and Passive Methods for the Detection of Drones and Small Airborne Objects”, 4th International Conference on “Operational Planning, Technological Innovations and Mathematical Applications OPTIMA 2017” (25-26 May 2017, Hellenic Military Academy, Athens, Greece), pp. 190-191

²⁷ https://en.wikipedia.org/wiki/Doppler_effect, https://en.wikipedia.org/wiki/Doppler_radar

relative motion of two objects; When the two objects are approaching each other, the Doppler shift causes a shortening of wavelength (increase in frequency) and when the two objects are receding from each other, the Doppler shift causes a lengthening of wavelength (decrease in frequency)²⁸. The same principle stands for both electromagnetic and sound signals, as shown in the figures below and the general relevant equation, where: f_d is the Doppler frequency shift, f_o the transmitted frequency, v is the target's velocity and c the speed of light.



$$f_d = \frac{2v}{c} f_o$$

4.4.2. Active Sensors – Radars

The radar sensor to be used in the RESISTO project is of a Doppler type. A Doppler radar uses the Doppler Effect to derive velocity data about moving objects at a distance. For a Doppler radar to measure speed, an accurate measurement of the original transmitted frequency and the reflected return frequency (echo) is required (assuming the general case of monostatic radar). The difference in the two frequencies is the Doppler frequency shift, and is a direct indication of the object's speed, giving direct and accurate measurements of the radial component of a target's velocity relative to the radar. By this way the Doppler radar can provide the measured speed, which is relative to the range r of the target (radial distance) along with the target's angle of arrival. The Doppler CW radar is able to detect and track fast moving targets providing good visibility in harsh conditions (dusk, rain or snow). In contrast to optical or infrared systems, Doppler radars detect more accurately small sized objects in the (optimal) 3 GHz - 30 GHz frequency band with adequate sensing ranges.

ICCS exploited and tested its existing Doppler CW radar lab prototypes at microwave frequencies (X-band / 10-12GHz, K-band / around 24GHz, 2.5GHz and 875MHz) with the one in 24GHz band yielding optimal results. As shown in the figures below, various lab prototypes of the 24GHz Doppler radar have been developed with directive antennas providing adequate results for forward and backward motion.

²⁸ <http://www.rfcafe.com/references/electrical/doppler.htm>

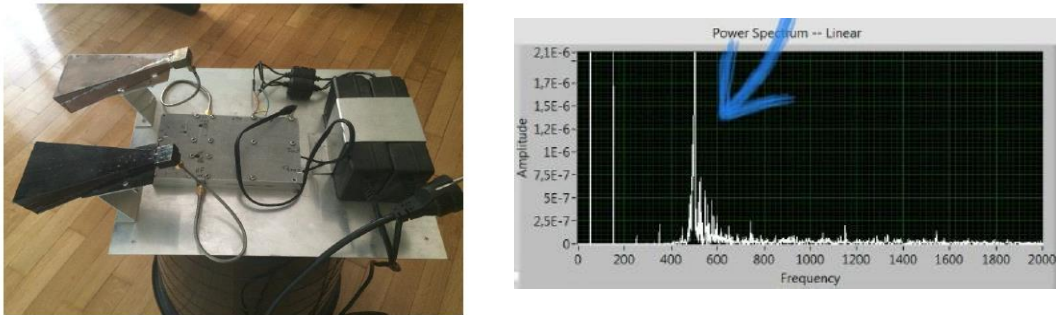


Figure 22 - Early radar prototype with directive antennas

The specific Doppler radar is a continuous wave monostatic one, where both the transmitting and receiving antenna are close together, practically at the same point. The general principle of operation is as follows: a 24GHz continuous signal is emitted from the transmitting antenna illuminating the target. Part of the energy of the wave is scattered from the target surface and returns to the receiving antenna. If the target moves towards to the beam, due to the Doppler Effect the frequency received (echo) will be shifted. The transmitting signal is generated by a VCO and following frequency multiplication and amplification stages. The receiving Doppler shifted echo signal, after LNA amplification, is then down-converted (I and Q signals) to provide the desired frequency shift (500 – 600 Hz).

The current 24 GHz Doppler CW radar prototype is shown in the figures below where 25 dB antennas have been adjusted along with a mechanical construction to provide 360 degrees scanning, emulating the omnidirectional operation.



Figure 23 – Current ICCS radar prototype

However, it should be noted that radar's detection capability depends on the target's RCS (Radar Cross Section) and its ability to distinguish between small objects and clutter that the sensor will also pick up especially for objects with low RCS as the drones are. Generally, the RCS (radar cross section: the effective aperture of the target) reflects the degree that the target can be detected and depends on a variety of parameters such as: the relative position of the target in respect to the radar, the frequency of operation along with the relative incident and scattering angles and most importantly the target characteristics, namely the aperture / profile, its material and dimensions relatively to the wavelength.

Different complex targets are expected to present a wide range of different RCS profiles with values fluctuating up to two orders of magnitude depending on the orientation²⁹. Low RCS makes the detection within cluttered environments very demanding with trade-offs between false alarm rates and detection probabilities³⁰. Indicatively, it should be noted that although a large cargo airplane has a RCS of 100, a fighter aircraft shows RCS of 4, while a stealth has RCS 0.1 and a bird of 0.01.

To this respect, low RCS of airborne objects, such as UAVs and drones, is tackled with advanced signal processing and the combined use of other sensors such as the acoustic ones, as seen below.

²⁹ M. Ritchie, F. Fioranelli, et al "Micro-Drone RCS Analysis", pp. 452-456, 2015 IEEE Radar Conference, Johannesburg, October 2015

³⁰ Bar-Shalom, Y., et al, "Tracking in a Cluttered Environment with Probabilistic Data Association", Automatica, 11: pp. 451-460, 1975

4.4.3. Passive Acoustic Sensors

The acoustic sensors used in the present system are a set of high sensitivity dynamic microphones forming an array. Acoustic sensors have many advantages that include non-line-of-sight, omnidirectionality, passiveness, low-cost and low-power, playing a potential key role in situational awareness; since they do not depend on the target's size, but rather on its acoustic signature i.e. sound of the engine. Acoustic microphone arrays are used as a second sensor modality to detect broadband acoustic emissions from approaching targets. Various lab prototypes have been developed and tested; either forming linear arrays or diagonal (cross format) which yield to be the most optimal ones. In the following figures the early linear prototypes are shown:



Figure 24 - Early acoustic arrays prototype

While in the following photos the current prototypes of acoustic diagonal microphone arrays (4 microphones arranged in a cross format) as tested within the anechoic chamber of ICCS:



Figure 25 – Current ICCS acoustic arrays prototype

By exploiting the target's strong emitted sound harmonics, moving targets can be detected and tracked regardless of their size by acoustic sensors. This is being held through tracking of the strong sound harmonic lines they emit mainly in the 20 Hz–2 kHz range³¹. Having captured the sound signal

³¹ T. Pham & L. Sim, "Acoustic detection and tracking of small, low-flying threat aircraft," 23rd Army Science Conf., Orlando, FL, 2002

of the target, two methods can be used either independently or combined. The first method is the time-domain waveform cross correlation of the captured waveform with a previously recorded sound waveform of the target, where the flight details (height, distance from the microphone) of the UAV are known in advance. In this sense, a sound signal of the UAV or drone under test, captured through i.e. Audacity software in a controlled environment, can be used as reference, for cross-correlation with the experiments to follow. The second technique is to perform Harmonic Line Association in the frequency domain and extract the necessary results from the harmonics of the fundamental frequency as seen in the relevant spectrograms. Indicative figures of the use of each method are given in the figures below:

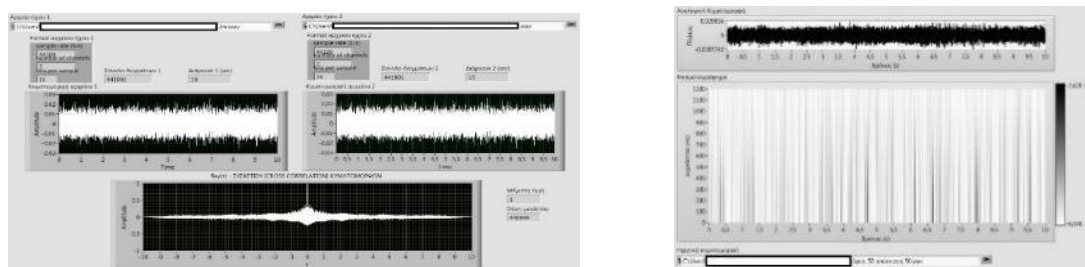


Figure 26 - Acoustic sensors data processing

Nevertheless, acoustic sensing depends on the environmental conditions and related sources of acoustic attenuation (e.g., temperature, wind speed and direction). New technology trends show that detecting low RCS moving targets can be made feasible by implementing mixed techniques³²; these emerge as a promising solution while they can be also combined with visual methods (i.e. cameras). These aspects are going to be employed within the framework of the RESISTO project.

4.4.4. Architecture and Functionalities of the radar and acoustic system

The radar and acoustic sensors can be used either separately or in combination. The whole setup is being accomplished through a multiplexing console physically connected to the sensors and Arduino software to an embedded PC (e.g. Raspberry 3) that perform the mechanical control and the data capturing. The sensing-data and signal processing is performed through a windows-based computer (laptop or desktop). Target detection visualization is enabled through specific application already developed in LabView software which controls the whole setup.

The 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/asn time and respective spectrograms, alarm indications when a received signal peak lies above a predefined threshold (when a target is detected) or sensitivity levels, inclusion of recording of specific sessions for post-processing of data, simultaneous visualisation of all waveforms from all the 4 microphones and the radar, data storage with fast data recording and association with data by other software tools such as Audacity software.

The main control and operation environment through LabView application is shown in the following figures:

³² W. Shi, G. Arabadjis, B. Bishop, P. Hill, R. Plasse and J. Yoder, "Detecting, Tracking, and Identifying Airborne Threats with Netted Sensor Fence", The MITRE Corporation Bedford, Massachusetts, U.S.A, 2011, Chapter in Book: "Sensor Fusion - Foundation and Applications", Dr. Ciza Thomas (Ed.), ISBN: 978-953-307-446-7, InTech, Available from: <http://www.intechopen.com/books/>

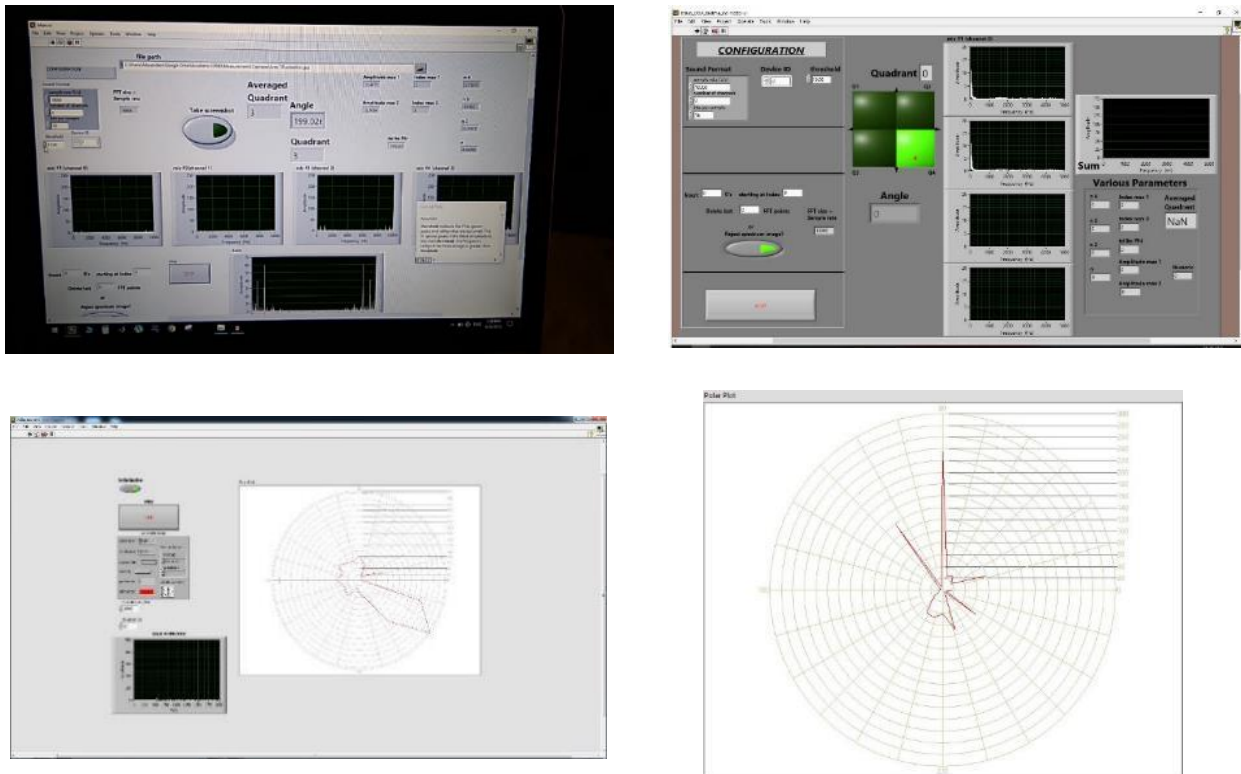


Figure 27 - Operation environment of combined radar and acoustic sensors

Additional functionalities of the specific LabView application include the direction of arrival of the target either in polar coordinates and/or in quadrants, through special control of the radar sensor and relevant Labview code, as this is shown in the above figures.

Advanced signal processing and machine intelligence / machine learning techniques 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. Neural network techniques are expected to increase the ability of distinguishing low RCS targets and to advance the overall performance.

Concerning the integration of the above 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 PSIM Security and Resilience platform. The overall detection system is a standalone one and thus a relevant interface will be defined. Consequently, and since the aim of the airborne threats detection system is to extract and provide potential intrusion events corresponding to the presence of potential moving airborne threats (UAVs and drones), a threat event with relevant attributes will be provided.

The whole current setup has already been tested with various types of small aircrafts and UAVs. Drones have also been tested in laboratory environment. Indicative results are shown in the following:

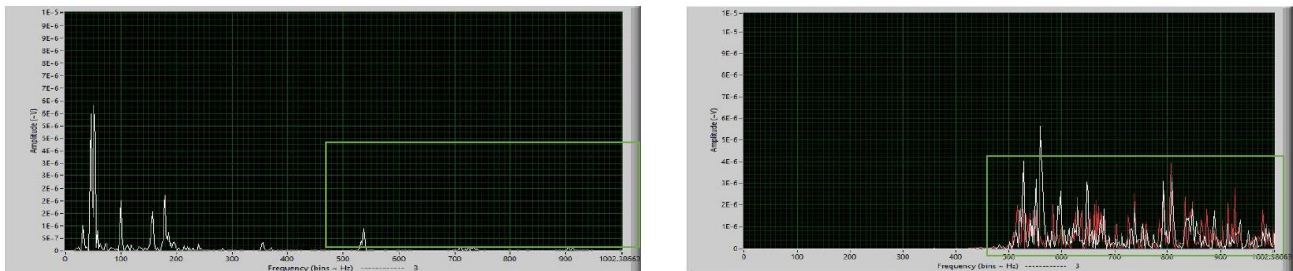


Figure 28 - Radar Response: a) Noise floor, b) Small Cessna type aircraft (150m distance)

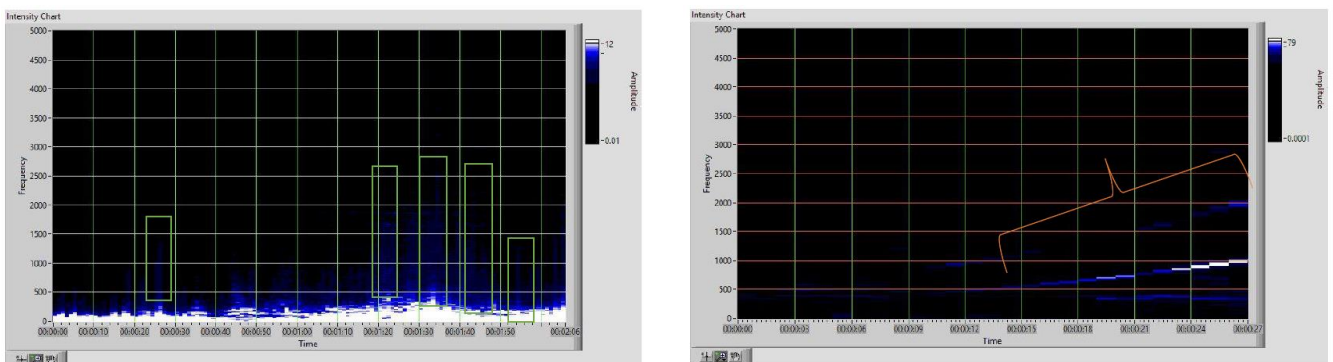


Figure 29 - Acoustic response: a) Movements in various heights and distances, b) UAV approaching for landing

From the above figures it is clear that the discrimination of targets is achieved; especially in the last figure when the UAV is approaching for landing an increase in frequency is noticed due to Doppler.

Early prototypes of the system have already been tested in lab environments for drones' detection where the following interesting conclusion has to be noted. 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 representation is not so clear; the derived conclusion is that the radar mainly detects the fast movement of the propellers (as in figures below):



Figure 30 - Drone's movement: a) Rpm measurement, b) drone in hover, c) drone in movement

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.

The above tests have been made with a commercial DJI Phantom 3 Advanced Drone shown in the following figure:



Figure 31 - 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.

4.4.5. *Potential Physical Threats to be detected*

In light of the emerging use of unmanned devices, UAVs or drones are nowadays more and more considered as potential human-driven physical threats. Anomalies and airborne threats to specific telecom CIs (i.e., remote antenna parks and/or telecom pillars on high rooftops) are mainly monitored through visual methods (i.e. cameras); the threat has to be in rather close proximity to be detected which leaves less time for reaction.

Counter-UAV and counter-drone technology has already seen extensive use in certain applications. On the battlefield, relevant systems have so far most commonly been used for base protection,

complementing existing weapons such as counter-mortar systems and surveillance platforms. There is also growing interest in portable and mobile systems that could be used to protect ground units and convoys. In civilian environments, counter-UAV technology has so far primarily been used for airspace protection at airports, security during large events such as party conventions and sports games, VIP protection, and counter-smuggling operations at prisons. Future common applications could include airspace defence around sensitive facilities, port security, maritime security, and personal use over private property. More than 200 discrete relevant products exist in the market, aiming either detection or interdiction, from more than 150 manufacturers. Main challenges include: Detection Effectiveness, False Negatives and False Positives, Distinguishing Legitimate and Illegitimate Drone Use, Interdiction Hazards (like falling down or kinetic problems), Legal framework and Lack of Standards³³.

In terms of the detection and tracking, as described above, the radar sensors detect the presence of small unmanned aircraft by their radar signature (often employing algorithms to distinguish between other small, low-flying objects) while the acoustic ones detect drones by recognizing the unique sounds produced by their motors. Current commercial systems mostly rely on a library of sounds produced by known drones, which are then matched to sounds detected in the operating environment. However, in the framework of RESISTO, the acoustic signature detection independently of the known library is pursued. Using suitable broadband signal processing techniques, observable characteristics of the acoustic signals are extracted, associated with such small flying objects. Verifying the notion that small airborne objects can be detected early enough via sensor systems is the main focus of the relevant system described above. Furthermore, the emission of high-frequency waves (active methods) may be complemented by receiving the acoustic output (passive) of such systems to accomplish detection.

Combinations of the two methods are beginning to emerge as integrated solutions for monitoring the airspace over critical infrastructures and especially telecom ones; aligning the results and theoretical basis with modern system implementations, progressing by this way the relevant state of the art for a low cost, low power combination. These combinations with other methods may include as well: electro-optical (EO) systems which detect UAV and drones based on their visual signature and infrared (IR) ones based on their heat signature. Radio-frequency techniques may be also used which identify the presence of UAVs and drones by scanning for the frequencies of operation along with geo-references.

In the framework of RESISTO, this technical assessment through the relevant use cases and scenarios will be held with commercial drone platforms as the above described DJI Phantom 3 Advanced Drone) along with the UAV platforms of ADI (ADITESS). To comply with newest technology trends, implementation of mixed techniques will be pursued; potentially in conjunction with visual methods (i.e. optical or thermal cameras), depending on the ADI platforms payloads and depending on the final use cases to be implemented in telecom CIs. Furthermore, ICCS's radar and acoustic sensors system can be used complementary to the passive radar provide by Leonardo.

Nevertheless, the RESISTO platform will integrate 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 failproof. Therefore, the combination of active and passive sensors may provide additionally situational awareness and perimeter defence against low-flying threat aircrafts for telecom CIs when employed within an overall holistic platform as the RESISTO one.

³³ Arthur Holland Michel, "Counter Drone systems", Center for the Study of the Drone at Bard College, Edited by Dan Gettinger, February 20, 2018, <http://dronecenter.bard.edu/counter-drone-systems/>.

5. NETWORKS AS SENSING SYSTEMS AGAINST PHYSICAL THREATS

In light of the emerging 5G telecom infrastructures, Internet of Things (IoT) networks are expected to be expanded in the near future and to dominate in everyday life with the use of wireless networks and wireless sensor networks (WSN) distributed in large areas and infrastructures.

Thus, it is of great importance that these telecom sensing facilities are capable of adequately tackling physical and combined cyber-physical threats. While sensing networks are in order with advanced features, it is reasonable that these networks obtain additional security functionalities as well, in order to be capable of detecting and responding to risks and physical threats, being either human driven or as consequences of natural disasters. By this way, the emerging sensor networks of the IoT world will act by themselves as detecting systems; this notion presupposes certain added features both in the hardware and software / firmware of these wireless sensor networks or wireless networks in general as current and future parts of telecom critical infrastructures.

The above concept will be evaluated within the RESISTO project in the respective use cases and validation scenarios mainly in the framework of WP9's macro-scenario. In the following, the description of such representative concepts is presented, provided by partners Integrasys (INT) and Guardtime (GT): signal monitoring WSNs and femtocells-based sensing systems as networks that simultaneously act as detecting systems of physical or combined threats. These functionalities can be made feasible through the implementation of emerging methods and functionalities such as blockchain to guarantee sensor data protection and integrity. The exploitation of the blockchain technique in the framework of RESISTO for detection and sensing purposes will be described as well to provide a complete overview of the whole concept.

5.1. Signal Monitoring WSNs as Sensing systems

In the physical premises of a telecom operator / infrastructure owner it is essential to make sure that only authorized personnel gain access to the premises. In order to achieve this, a system based on Bluetooth and 802.11 physical addresses whitelists (or simply based on any wireless device detection, for more restrictive premises) will be implemented.

The non-authorized users will be detected by using a Signal Presence Detection System based on a Signal Monitoring WSN which will allow both detecting non-whitelisted (or simply any wireless device, for more restrictive premises) and also capturing signal measurements from these devices.

These users could also be localized with a rough position estimation through a network made up of several of these signal monitoring sensors and a central processing node, inside or outside the premises, which would compute the positioning based on the signal power received from the sensors.

The Signal Monitoring Sensors will have the following basic components:

- 802.11 transceiver in monitor mode, monitoring the 2.4 and 5 GHz ISM band
- Bluetooth (BR/EDR/LE) transceiver monitoring the Bluetooth 2.4 GHz ISM band
- Microcontroller/Mini-pc

5.1.1. Architecture and Functionalities

The data (addresses and measurements) would be sent from the monitoring sensors to an access point or gateway inside the premises which manages the list of non-authorized users and calculates their coarse location based on received measurements such as RSSI. In order to make the sensors

trustable, the firmware of all of the monitoring sensors and the access point/gateway will be signed by the firmware developer and every other party in software supply chain by using KSI Signature (anchored in Guardtime's KSI Blockchain); supported by a server inside the premises. The integrity of the firmware in any sensor/gateway/access point will be checked against the pre-set signature. It is possible to conduct audits of operating environment integrity, using both automatic checks and by exporting tamper evident forensic data for third party inspection.

The network would also include a central processing node which communicates with all of the signal monitoring sensors.

5.1.2. *Potential Physical Threats to be detected*

This is a list of some of the potential threats that could be detected:

- Breaking and entering into the telecom critical Infrastructure premises carrying a Bluetooth or WiFi electronic device which is turned on.
- Guests who are granted physical access into the premises without bringing any connected devices but they manage to turn on a hidden Bluetooth or WiFi electronic device, possibly gaining non-authorized privileges to critical equipment inside the premises with malicious intentions.

5.2. Femtocells-based Sensing systems

The main objective of this system is to provide protection mechanisms from femtocell stations that may be maliciously used to compromise Radio Access Networks. In order to achieve this, the firmware of the femtocell will be signed by the firmware developer and every other party in software supply chain by using KSI Signature (anchored in Guardtime's KSI Blockchain); supported by a server inside the premises. The workflow of operation is again similar to the previous WSN sensing systems. Again, the integrity of the firmware in any sensor/gateway/access point will be checked against the signature. It is possible to conduct audits of operating environment integrity, using both automatic checks and by exporting tamper evident forensic data for third party inspection.

Also the femtocells will be kept track of by using a GNSS sensor added to the station. To make sure the GNSS Lat-Lon coordinates will be trustable, the observables received from the GNSS satellites will be sent to a gateway/access point with the signed firmware which will run the positioning algorithms to create a trusted femtocell location.

The Femtocell sensing system will have the following basic components:

- Very-small-sized cell station (a Home eNodeB, HeNB in LTE 4G terminology) with signed firmware which guarantees integrity
- GNSS sensor inside or near the station solution with RINEX observables generation.



5.2.1. *Architecture and Functionalities*

Femtocells are placed inside homes or offices to improve cellular operator's coverage. The diagram below explains the general architecture of a femtocell inside a cellular network.

The cell phones are connect to the femtocell (depicted in purple colour) which is a smaller-sized version of the regular macro/micro cell (black triangle in the picture) which are commonly deployed by

operators. The femtocell connects to a router, which has Internet access, used as a backhaul to the core network.

The femtocells should be constantly located to avoid potential threats, explained in the following paragraph. In order to achieve this, the femtocell has to include a GNSS sensor inside the device or attached to it, which will generate positioning observables. To avoid observables tampering, these positioning observables or readings would be sent to a gateway/access point with signed firmware which will generate the trusted coordinates.

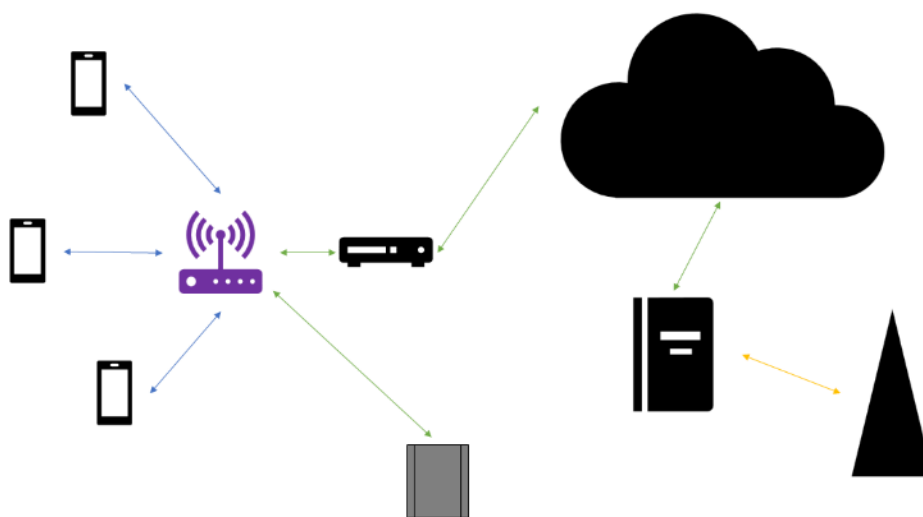


Figure 32 - The general architecture of a femtocell inside a cellular network.

5.2.2. Potential Physical Threats to be detected

The original purpose of a femtocell is to provide extended coverage or capacity to residential or professional customers. However if femtocells are used properly in the concept described above, they can detect the following threat: a customer changing the original location of the femtocell without notifying the operator. The positioning coordinates of the femtocell have to be provided to the cellular operator when the device is installed and usually a change of the location would be received as an alert in the operator's system, but some customers may alter/tamper with the positioning location values without the operator noticing.

5.3. KSI Blockchain overview and use in telecom network monitoring

Since the above network sensing systems are based to Blockchain method, a brief description of this technique is presented in the following in order to provide a complete overview of the whole concept.

KSI Blockchain is a method and a globally distributed network infrastructure for the issuance and verification of KSI signatures. Unlike traditional digital signature approaches, e.g. Public Key Infrastructure (PKI), that depend on asymmetric key cryptography, KSI uses only hash-function cryptography, allowing verification to rely only on the security of hash-functions and the availability of a public ledger commonly referred to as a blockchain.

A blockchain is a distributed public record of events; an append-only record of events where each new event is cryptographically linked to the previous as shown at the diagram below. New entries are created using a distributed consensus protocol.

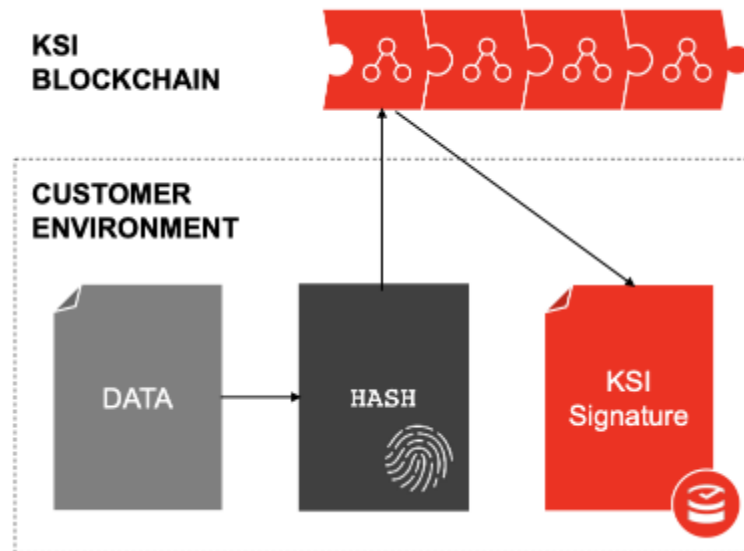


Figure 33 KSI Blockchain append-only record

A user interacts with the KSI Blockchain system by submitting a hash-value of the data to be signed into the KSI infrastructure and is then returned a signature which provides cryptographic proof of the time of signature, integrity of the signed data, as well as attribution of origin (i.e. which entity generated the signature).

The benefits of the KSI Blockchain include:

- **Massive Scale.** The KSI signatures can be generated at exabyte-scale. Even if an exabyte (1,000 petabytes) of data is generated around the planet every second, every data record (a trillion records assuming 1MB average size) can be signed using KSI with negligible computational, storage and network overhead.
- **Portability.** The properties of the signed data can be verified even after that data has crossed geographic or organizational boundaries and service providers.
- **Data Privacy.** KSI does not ingest any customer data; data never leaves the customer premises. Instead, the system is based on one-way cryptographic hash functions that result in hash values uniquely representing the data, but are irreversible such that one cannot start with the hash value and reconstruct the data; data privacy is guaranteed at all times.
- **Independent Verification.** The properties of the signed data can be verified without reliance or need for a trusted authority.

The benefits of KSI Blockchain in communication network monitoring:

- **Improved cybersecurity:** Registering assets in the KSI Blockchain fixes their state in time – whether it is an item in the population registry or an event in a law enforcement system. This guarantees integrity; a blockchain backed asset is immutable (without having to put the asset

itself to the blockchain). Furthermore, the technical capabilities of the KSI Blockchain allow to constantly monitor the state of assets by re-verification at scale. This provides true situational awareness across threat monitoring network.

- **Insider Threat Mitigation / Fraud Detection:** Constant monitoring and instant alerting of all data, systems and processes prevents malicious activities and manipulations even by authorized insiders. KSI Signature cannot be backdated or forged by anyone – making it impossible to cover up tracks of manipulations (e.g. by deleting or altering audit logs). KSI-backed systems are resilient to tampering; making manipulation and fraud evident or preventing it in the first place.

5.3.1. KSI Infrastructure

KSI Infrastructure is layered and hierarchical. KSI Blockchain is created and maintained by the KSI Core cluster; requests are accepted, and responses are distributed using a hierarchy of Aggregator nodes. The blockchain is distributed using a hierarchy of Extender nodes.

Lowest layer, customer-facing Aggregator and Extender are packaged into so-called Gateway server.

The core and aggregation, extender networks are operated as a permissioned blockchain, by Guardtime. Branches of aggregation and distribution hierarchies can be operated by third parties. Gateway is usually hosted at the end-user premises. Within the RESISTO project, Guardtime operates all KSI Infrastructure components, providing access to pre-configured endpoints.

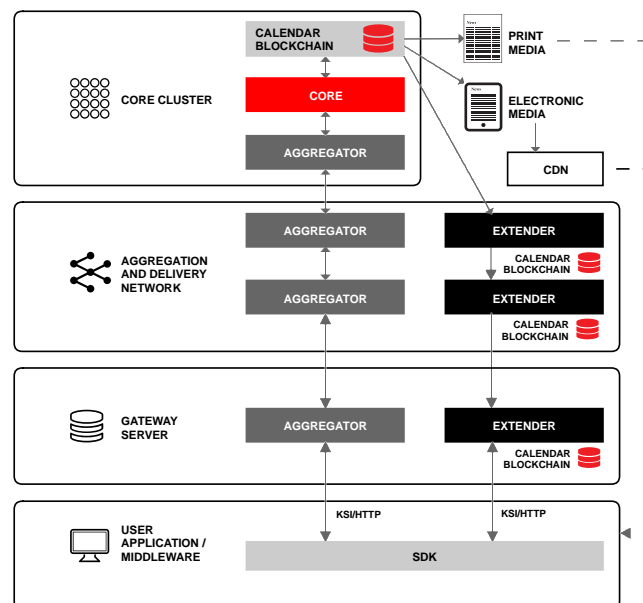


Figure 34 The layers of KSI Infrastructure

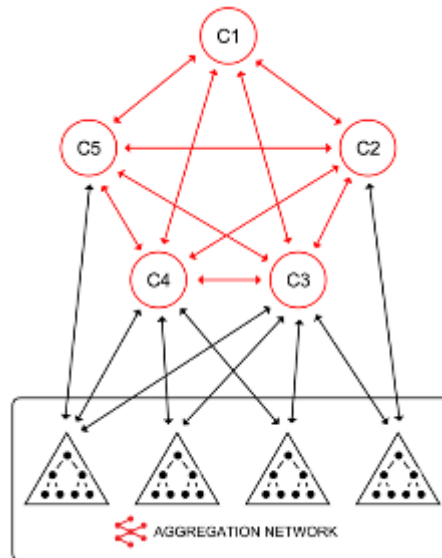


Figure 35 KSI Core and top-level Aggregators

5.3.2. KSI Integration

KSI signatures are server-based, meaning that signing data requires online access to the KSI service. The verification of the signatures can be done both offline and online. There are two major options for generic integration with KSI:

- KSI Software Development Kit (SDK)
- Catena middleware

The KSI SDK provides the lowest level of integration. It enables "full access" to the KSI functions (signing, extending, verifying) and lets the integrator to fine-tune everything that is possible. As a consequence, it leaves many common challenges (such as signature storage and extension) to the integrator to solve.

Catena is a middleware that is meant to address the common integration challenges (such as asynchronous signing, signature persistence and automatic extension). It provides the integrators also with additional higher-level functionality; annotate signatures, link signing events (data provenance) in order to reduce the effort for building the entire solution. Inside, Catena uses the same SDK for performing the low-level KSI operations.

5.3.3. KSI Integration Patterns

KSI Signature (literally, anchoring data in blockchain) proves data immutability, i.e., that data existed at its registration time, with included attributes, and it haven't changed since.

- **Executable Integrity:** KSI provides an authentication mechanism against external hacking and insider tampering of the Machine images prior to deployment.
- **Event Integrity:** KSI establishes accountability for events, enabling parties to prove that the logs have not been compromised by external hacking or insider tampering.

- **Storage Integrity:** KSI provides for independent authentication of every object in persistent storage, enabling regulatory compliance for data integrity, on commodity hardware, in the Cloud.

Secure Provenance provides cryptographic proof of the chronology of the ownership, custody and modifications to electronic data.

Provenance may turn out to be critical in approval processes, in supply chain, or in any other business process or transaction where the lineage of the set of events has a significant role in the integrity and trustworthiness of the information. Provenance is applicable in any situation where an immutable chain of signing events needs to be formed so that no event in the chain can be injected, removed or modified.

Provenance is not limited to a single organization and can be used across multiple organizations or trust domains.

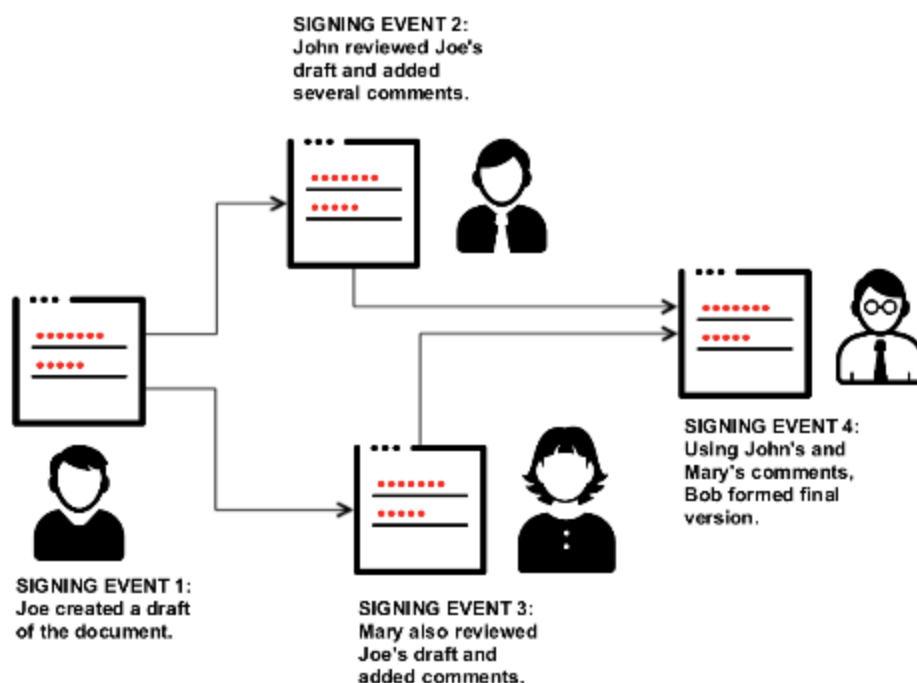


Figure 36 Example provenance graph is formed by the lifecycle of a document

6. SUMMARY AND CONCLUSIONS

The present Deliverable D4.1 reports the status the description of the sensors and mechanisms that are provided by the RESISTO project to enhance detection, protection and security of the telecom critical infrastructures against intrusions and modern physical and/or combined cyber/physical threats.

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 concept of employing wireless networks as sensing networks by themselves, using firmware methods such as blockchain, is also presented. 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.

This report represents the first Deliverable of Task 4.1 and deals only with the description of the relevant sensors. The way that these sensors 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 will be the subject of the next follow-up version of this report which constitutes the Deliverable D4.2 in order this Task to be finalised.

7. REFERENCES

Apart from the references already denoted within the txt, the following ones were also considered:

INDEX	REFERENCE
1	RESISTO – Grant Agreement. Project Starting Date: May, 1 st 2018
2	ouini M and Rabai L B A 2016 Threats Classification Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security (Advances in Information Security, Privacy, and Ethics) ed M Gupta et al (IGI Global) pp 368–92
3	International Telecommunication Union, Geneva, Switzerland 2004 ITU-T Recommendation E.408 (05/2004): Telecommunication Networks Security Requirements.
4	International Telecommunication Union, Geneva, Switzerland ITU-T Recommendation X.800 (04/2008): Security Architecture for Open Systems Interconnection for CCITT Applications
5	CVE: Common Vulnerabilities and Exposures https://cve.mitre.org/
6	2014 DDoS Quick Guide https://www.us-cert.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf (accessed 10/2018)