

RESISTO

D2.8_TABLE-TOP READ TEAMING RESULTS OF RESISTO ARCHITECTURE, SCENARIOS AND USE CASES



RESISTO

D2.8 – TABLE-TOP READ TEAMING RESULTS OF RESISTO ARCHITECTURE, SCENARIOS AND USE CASES TABULAR REPORT

Document Manager:	Maria BELESITI	OTE	Editor
--------------------------	----------------	-----	--------

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

Document ID N°:	RESISTO_D2.8_200123_01	Version:	1.0
Deliverable:	D2.8	Date:	23/01/2020
		Status:	APPROVED

Document classification	PUBLIC
--------------------------------	---------------

Approval Status	
Prepared by:	Maria BELESITI (OTE)
Approved by: (WP Leader)	Zhan CUI (BTC)
Approved by: (Coordinator)	Bruno SACCOMANNO (LDO)
Security Approval (Security Advisory Board Leader)	Paolo DI MICHELE (LDO)
Advisory Board Validation (Advisory Board Coordinator)	N.A.

CONTRIBUTING PARTNERS

Name	Company / Organization	Role / Title
Maria Belesioti Evangelos Sfakianakis Kostas Chelidonis	OTE	Telecommunication Experts, Project Managers, Network Expert
Ioan Constantin, Horia Gunica, Octavian Echim, Lucian Enescu, Carmen Patrascu	ORO	Cyber Security Expert, IP Network Expert, Information Security Experts, Project Manager
Rodoula Makri, Panos Karaivazoglou, Apostolos Papafargkakis, Athanasios Panagopoulos, Panagiotis Fragkos, Eyangelos Groumpas, Michalis Sofras. Takis Kelefas	ICCS	Senior Researchers, Electrical Engineers, Telecommunication Experts
Michael Skitsas	ADDITESS	Researchers,
Luca Lionetti	TIM	Researchers,
Sylvia Bach	BUW	Researchers,
Zhan Cui, Ian Herwono Selina Wang	BTC	Researchers,
Haab Gael	EMI	Researchers,
Jorge Carapinha , Paula Cravo	ALB	Researchers,
Luis Moreno Fraile	RTV	Researchers,
Marco Carli	RM3	Researchers,
Giuseppe Celozzi, Cosimo Zotti, Giovanna Spadaccio, Gianluca Ferentino	TEI	Senior System manager, senior project manager, senior test manager, senior cybersecurity expert

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	23.10.18	1-16	ALL	Draft ToC
0.2	18.03.19	ALL	ALL	New text
0.3	08.05.19	ALL	ALL	Updated text
0.4	13.06.19	ALL	ALL	New additions
0.5	21.06.19	ALL	ALL	New additions
0.6	05.07.19	ALL	ALL	New additions
0.7	12.07.19	ALL	ALL	Updated text
0.8	26.08.19	ALL	ALL	Updated ToC
0.9	16.09.19	ALL	ALL	New text
0.10	27.09.19	ALL	ALL	New additions
0.11	15.10.19	ALL	ALL	Updated text
0.12	20.11.19	ALL	ALL	Editorial corrections
0.13	07.12.19	ALL	Sections 6, 10, 11, 16, ALL	Integrated RTV contributions, Editorial corrections, Fixed references-References table
1.0	10.12.19	ALL	ALL	Release for SAB Assessment
1.0	23.01.20	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 Puccini 2 – Genova – 16154 – Italy
Tel.: +39 348 6505565
E-Mail: bruno.sacomanno@leonardocompany.com

RESISTO PROJECT – PUBLISHABLE EXTENDED ABSTRACT

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

EXECUTIVE SUMMARY

The present document is a deliverable of the RESISTO project (Grant Agreement No. 786409) funded by the European Commission's Directorate-General for Research and Innovation under its Horizon 2020 Research and innovation programme (H2020).

RESISTO concept is an innovative solution for Communication Critical Infrastructures (CIs) holistic situation awareness and enhanced resilience providing holistic (cyber/physical) situation awareness and enhanced resilience against cyber-physical attacks and disasters. RESISTO will help Communications Infrastructures Operators to take the best countermeasures and reactive actions exploiting the combined use of risk and resilience preparatory analyses, detection and reaction technologies, applications and processes in the physical and cyber domains.

Deliverable 2.8 includes a detailed analysis of the Use Cases, which have been chosen as most relevant and are elaborated so as to show the functionalities of the RESISTO platform. These Use Cases will be piloted in WP7, WP8 and WP9 respectively so as to validate the complete RESISTO concept. Requirements and KPI's, addressed in separate deliverables, are mapped to each use case and an analytic view of all the Test-bed that will be used is given.

CONTENTS

CONTENTS.....	8
List of Figures.....	12
List of Tables	13
ABBREVIATIONS.....	14
1. INTRODUCTION	17
2. Overview of the RESISTO architecture.....	18
2.1. RESISTO overall architecture; brief overview	18
2.1.1. Key Features of the RESISTO System and Architecture functions.....	18
2.1.2. Advances of RESISTO when comparing with other H2020 Projects	20
2.2. High-level Description of RESISTO Main Architectural Entities	21
3. Description of the Use Cases: overview and methodology.....	24
3.1. Main Concepts and Terms.....	24
3.2. Macro-Scenario 1: Protection and resilience of the Current / existing Telecommunication Critical Infrastructures	25
3.3. Macro-Scenario 2: Interdependencies of providers of essential communication services - Interconnected CIs	26
3.4. Macro-Scenario 3: CI evolution towards the future 5G telecom CIs and networks and the emerging IoT world.	27
3.5. Methodology Overview	28
3.5.1. Implementation of the RESISTO Use Cases	30
3.6. Roadmap for the validation process of the Use Cases	31
3.6.1. Key aspects of the validation process of the Use Cases.....	32
3.6.2. RESISTO Long Term Control Loop response through the Use cases	34
3.7. Interconnected CIs validation.....	37
4. Use Case 1: Core Network Failure caused by Physical & Cyber Attacks to Telecommunication sites.....	39
4.1. Introduction and Background	39
4.2. Overall Description of the Use Case 1	39
4.2.1. Sub Use case 1 – Storytelling.....	40
4.2.2. Sub Use case 2 – Storytelling.....	40
4.3. Analysis of the Use Case 1 Sub Use cases	41
4.3.1. Telecom Assets affected.....	42
4.3.2. RESISTO tools involved	43
4.3.3. Impact of threats foreseen in Use Case 1	43
4.3.4. Other consequences - Interconnected Critical infrastructures.....	44
4.3.5. Deployment Topology Example – Test-bed setup.....	44
4.4. Actors and detection tools involved	47
4.5. RESISTO response and Added Value	48
4.5.1. RESISTO Short Term response	48

4.5.2.	RESISTO Long Term response	49
4.5.3.	Innovation addressed.....	49
4.5.4.	Suggested KPIs for Use Case 1 validation	49
5.	Use Case 2: Terrorist Attack and Natural Hazards causing network failure and telecommunication congestion	51
5.1.	Introduction and Background	51
5.2.	Overall description of the Use Case 2 sub Use Cases	51
5.2.1.	Sub Use Case 1 - Storytelling: Terrorist Attack in telecom asset cause severe network failure.....	52
5.2.1.1.	Analysis of the Use Case 2: Sub Use Case 1	52
5.2.1.2.	Telecom assets affected.....	55
5.2.1.3.	RESISTO tools involved	55
5.2.2.	Sub Use Case 2 – Storytelling: Natural Disasters affect telecom assets – network loss and telecommunication congestion	56
5.2.2.1.	Analysis of the Use Case 2: sub Use Case 2	56
5.2.2.2.	Telecom Assets Affected.....	60
5.2.2.3.	RESISTO tools involved	60
5.2.3.	Impact of threats foreseen in Use Case 2	61
5.2.4.	Other consequences - Interconnected Critical infrastructures.....	62
5.2.5.	Deployment topology example.....	62
5.3.	Actors and detection tools involved	62
5.4.	RESISTO response and Added Value	64
5.4.1.	RESISTO Short Term response	64
5.4.2.	RESISTO Long Term response	64
5.4.3.	Innovation addressed.....	64
5.4.4.	Suggested KPIs for Use Case 2	65
6.	Use Case 3: Telecommunication sites.....	66
6.1.	Introduction and Background	66
6.2.	Overall Description of the Use Case	66
6.2.1.	Assets Affected	67
6.2.2.	Impact of the foreseen threats - Interconnected Critical infrastructures	67
6.2.3.	Deployment Topology Example – Test-bed setup	68
6.3.	Actors and detection tools involved	68
6.4.	RESISTO response and Added Value	68
6.4.1.	RESISTO Short Term response	68
6.4.2.	RESISTO Long Term response	68
6.4.3.	Innovation addressed.....	69
6.4.4.	Suggested KPIs for Use Case 3	69
7.	Use Case 4: Disruption of major sporting event by combined physical & cyber-attack by a terrorist organization	70
7.1.	Introduction and Background	70
7.2.	Overall Description of the Use Case	71
7.2.1.	Assets Affected	73
7.2.2.	Impact of threats foreseen in Use Case 4	73

7.2.3.	Deployment Topology Example – Test-bed setup	73
7.3.	Actors involved and detection tools involved	76
7.4.	RESISTO response and Added Value	77
7.4.1.	RESISTO Short Term response	77
7.4.2.	RESISTO Long Term response	78
7.4.3.	Innovation addressed	78
7.4.4.	Suggested KPIs for Use Case 4	79
8.	Use Case 5: Protection of Cloud Storage Services	80
8.1.	Introduction and Background	80
8.2.	Overall Description of the use Case	80
8.2.1.	Sub Use Case 1 – Healthcare	81
8.2.1.1.	Test 1 - Detect tampering on files containing sensitive information after physical access to site	82
8.2.1.2.	Test 2: HW configuration system change	83
8.2.1.3.	Test 3: Disaster response and recovery	84
8.2.1.4.	Test 4: Data exfiltration	84
8.2.2.	Sub Use case 2 – Smart Manufacturing	85
8.2.2.1.	Test 1: Cyber attach to the Manufacturing remote control node	85
8.2.2.2.	Test 2: Cyber attach to the 5G network used to connect the remote robots to the centralized control node	86
8.2.3.	Assets Affected	87
8.2.4.	Impact of the threats foreseen in this Use Case	87
8.2.5.	Deployment Topology Example – Test-bed setup	87
8.3.	Actors and detection tools involved	89
8.4.	RESISTO response and Added Value	91
8.4.1.	RESISTO Short Term and long term response	91
8.4.2.	Innovation addressed	91
8.4.3.	Suggested KPIs for Use Case 5	92
9.	Use Case 6: Cyber and physical protection of network and network elements mechanisms used by critical services that impact users	93
9.1.	Introduction and Background	93
9.2.	Overall description of the Use Cases and test-beds setup	95
9.2.1.	Assets Affected	100
9.2.2.	Impact of the threats foreseen in Use Case 6	100
9.2.3.	Other consequences - Interconnected Critical infrastructures	100
9.3.	Actors involved	100
9.4.	RESISTO response and Added Value	101
9.4.1.	Innovation addressed	101
9.4.2.	Suggested KPIs for Use Case 6	101
10.	Use Case 7: Maritime Safety and Emergency Case	102
10.1.	Introduction and Background	102
10.2.	Overall Description of the use Case	102
10.2.1.	Assets Affected	103
10.2.2.	Deployment Topology Example – Test-bed setup	103

10.2.3.	Impact of the threats foreseen in this Use Case - Interconnected Critical infrastructures	104
10.3.	Actors and detection tools involved	105
10.4.	RESISTO response and Added Value	105
10.4.1.	RESISTO Short Term response	105
10.4.2.	RESISTO Long Term response	105
10.4.3.	Innovation addressed	105
10.4.4.	Suggested KPIs for Use Case 7	106
11.	Use Case 8: PPDR Virtual Operator	107
11.1.	Introduction and Background	107
11.2.	Overall description of the Use Case and Test-beds setup	107
11.2.1.	Assets Affected	112
11.3.	Actors and detection tools involved	113
11.4.	RESISTO response and Added Value	113
11.4.1.	RESISTO Short Term response	114
11.4.2.	RESISTO Long Term response	114
11.4.3.	Innovation addressed	114
11.4.4.	Suggested KPIs for Use Case 8	114
12.	Use Case 9: 5G network response to a security breach	115
12.1.	Introduction and background	115
12.2.	Overall Description of the Use Case	116
12.2.1.	Assets Affected	118
12.2.2.	Deployment Topology Example – Test-bed setup	119
12.3.	Actors and detection tools involved	119
12.4.	RESISTO response and Added Value	121
12.4.1.	Short term control loop	121
12.4.2.	Long term control loop	122
12.4.3.	Innovation addressed	122
12.4.4.	Suggested KPIs for Use Case 9	123
13.	TRACEABILITY MATRICES - KPIs and Requirements Mapping	124
13.1.	KPIs Mapping	124
13.2.	User Requirements addressed by the RESISTO Use cases	125
14.	ETHICAL AND SOCIETAL SCIENCE FEEDBACK ON THE USE CASES	128
15.	CONCLUSION	136
16.	REFERENCES	137

LIST OF FIGURES

Figure 1: RESISTO high level Architecture and key elements	19
Figure 2: RESISTO methodology for use cases description.....	29
Figure 3: Exemplary correlation matrix of system functions and threats. It should be noted, that the entries in the correlation matrix are not normalized but rather refer to a connection strength in arbitrary units	35
Figure 4: Exemplary visualization of a resilience matrix (performance metrics vs threats). The performance functions and threats are taken from actual inputs but the curves are not realistic, i.e. not based on real data or a realistic simulation	36
Figure 5: Attack location in OTE's premises, subcases 1 & 2.....	41
Figure 6: High level OTE Core Lab – Cloud lab topology.....	45
Figure 7: RESISTO slice Core Lab Description	46
Figure 8: Example location of a telecom asset in remote sub-urban areas	54
Figure 9: Traffic at 19/7/2019 during earthquake.....	58
Figure 10: Drop Call & short Calls Rate	58
Figure 11: Support of Unicast and Multicast technologies for TV content delivery (data plane)	71
Figure 12: UK network infrastructure for unicast and multicast services	72
Figure 13: BTC test-bed (initial) architecture for multicast and unicast video delivery	74
Figure 14: TIM Cloud storage critical infrastructure Healthcare Scenario	87
Figure 15: Critical infrastructure Smart Manufacturing Scenario	88
Figure 16: Physical layout of ORO test-bed	95
Figure 17: 5G test-bed- physical layout	96
Figure 18: 5G Network Slicing NGMN.....	96
Figure 19: ORO Use Case - testing diagram	97
Figure 20: Use case 7 Topology	102
Figure 21: Use case 7 Topology of Emergency service provision	104
Figure 22: Use case 7 Topology of Maritime Use Cases	104
Figure 23: Use case 8-Attacks on Services and protocols.....	109
Figure 24: Use case 8 network slicing	110
Figure 25: Use case 8 5G MEC architecture slices	110
Figure 26: Use case 8 proposed architecture	111
Figure 27: Use case 8 MEC Virtualization architecture.....	112
Figure 28: Use case 8 assets affected	113
Figure 29: Threat landscape for 5G network scenarios.....	115
Figure 30: Use case 9 initial state	117
Figure 31: Use case 9 phase 1 (preparation)	117
Figure 32: Use case 9 phase 2 (activation)	118
Figure 33: Use case 9 phase 3 (migration).....	118
Figure 34: Use case 9: 5G use case topology and basic components.....	119
Figure 35: Use case 9: General example of network slicing management functions [15]	120
Figure 36: Use case 9: Overall use case decision making by RESISTO short term loop.....	121

LIST OF TABLES

Table 1 – Storage format of RIs in the Knowledge Base of the RESISTO platform, based on the matrix structure of potential events and performance functions.....	37
Table 2 – Identified actors in the “physical & cyber-attacks in telecom sites” Use Case 1.....	47
Table 3 – Detection Sensors that will be used in Use Case 1.....	48
Table 4 – Suggested KPIs to be measured during the pilot activities of Use Case 1.....	50
Table 5 – Identified actors for Use Case 2.....	63
Table 6 – Detection Sensors that will be used in Use Case 2.....	63
Table 7 – Suggested KPIs to be measured during the pilot activities of Use Case 2.....	65
Table 8 – Suggested KPIs to be measured during the pilot activities of Use Case 3.....	69
Table 9 – Actors of Use Case 4.....	76
Table 10 – Suggested KPIs to be measured during the pilot activities of Use Case 4.....	79
Table 11 – Use Case 5 stakeholders.....	89
Table 12 – Use Case 5 actors.....	90
Table 13 – Suggested KPIs to be measured during the pilot activities of Use Case 5.....	92
Table 14 – Use Case 6: Sub Use Case 1.....	98
Table 15 – Use Case 6: Sub Use Case 2.....	99
Table 16 – Use Case 6 actors involved.....	100
Table 17 – Suggested KPIs to be measured during the pilot activities of Use Case 6.....	101
Table 18 – Suggested KPIs to be measured during the pilot activities of Use Case 7.....	106
Table 19 – Suggested KPIs to be measured during the pilot activities of Use Case 8.....	114
Table 20 – Use Case 9 - Actors Related to 5G.....	119
Table 21 – Suggested KPIs to be measured during the pilot activities of Use Case 9.....	123
Table 22 – KPI’s mapping to RESISTO use cases.....	124
Table 23 – Requirements as described in D2.6 [1].....	127
Table 24 – Use case owners’ input on involved techniques and personnel.....	131
Table 25 – Use case owners’ input on potential societal impact.....	135

ABBREVIATIONS

2G, 3G, 4G	Second, third and fourth generation of mobile phone systems
ACLs	Access Control Lists
API	Application Programming Interface
APN	Access Point Name
ASIC	Application Specific Integrated Circuit
AV	Antivirus detection
B2B	Back-to-Back gateway
BNG	Broadband Network Gateway
CCA	Critical Communication Application
CCS	Critical Communications System
CCTV	Closed Circuit TV
CDN	Content Delivery Network
CI	Critical infrastructure
CPS	Cyber-Physical Systems
CPU	Central Processing Unit
DMO	Direct Mode Operations
ETSI	European Telecommunications Standard Institute
EU	European Union
FW	Firewall
GGSN	Gateway GPRS Support Node
GSM	Global System for Mobile communications
GSSI	Group Short Subscriber Identity
HW	HardWare
HTTP	HyperText Transfer Protocol
ICT	Information and Communication Technology
IDS	Intrusion detection systems
IGMP	Internet Group Management Protocol
IoT	Internet of Things
IPS	Intrusion prevention systems

IPTV	Internet Protocol Television
ISI	Inter System Interface
ISSI	Individual Short Subscriber Identity
ISITEP	Inter System Interfaces for TETRA-TETRAPOL Networks
ITSI	Individual TETRA subscriber Identity
KPIs	Key Performance Indicators
LTCL	Long Term Control Loop
LTE	Long Term Evolution (= 4G)
MNO	Mobile Network Operator
NaaS	Network as a Service
NFV	Network Functions Virtualization
NOC	Network Operations Center
NSSP	Network Slice Subnet Provider
OTT	Over-the-Top
PC	Personal Computer
PPDR	Public Protection and Disaster Relief
PSIM-C	Physical Security Management Center
PTT	Push To Talk
QoS	Quality of Service
RTU	Remote Terminal Unit
SDN	Software Defined Networking
SDS	Software Defined Security
SLA	Service Level Agreement
SOC	Security Operation Center
SP	Service Provider
SW	SoftWare
TCCE	TETRA and Critical Communications Evolution
TEA2	TETRA Encryption Algorithm #2
TETRA	TErrestrial Trunked RAdio
TG	Talk Group
TMO	Trunked Mode Operations

UE	User Equipment
UAV	Unmanned Aerial Vehicle
VM	Virtual machine
VPN	Virtual Private Network
WP	Work Package

1. INTRODUCTION

The present deliverable will serve as a “reference document” for all upcoming work packages of the RESISTO project, covering important issues on use cases and pilots as well as the requirements and KPI’s that will be used. The work involves consideration of the three macro-scenarios as starting point, and identification of actors’ role for validation, through evaluation.

A systematic methodology has been proposed to solicitate, analyse and describe use cases. In conjunction with the identification of the involved actor groups, it ensures all selected use cases are realistic, can be piloted and tested on the RESISTO platform to validate each of three macro-scenarios as they are presented in the RESISTO project.

The use cases are depicted in form of user stories and they all have a standard structure with description of actions that will take place, the actors participating and of course bounding conditions. The details of use cases presented in this document are subject to change. It will evolve during the project duration.

This document describes the activities to support procedures needed for RESISTO platform adapting to the different environments involved in the project and provides a thorough analysis of the candidate use cases. These high-level procedures and the use cases will guide the integration phases within the technical work packages, and therefore, this deliverable will be a common reference point for the RESISTO consortium.

In addition, the deliverable collects all candidate topologies and test-beds that will be used for the implementation and validation of the use cases in the framework of WP7, WP8 and WP9.

This deliverable addresses the following:

- Brief description of the RESISTO architecture that will be activated through the short and long terms responses.
- Description of the Use Cases, extraction and validation methodology and basic principles for the definition and identification of the use cases, as well as overview of the 3 Macro scenarios, as they are presented in the DoW.
- Thorough description of all project’s use cases and scenarios; both those already suggested within the DoW as well as others differentiated to showcase more clearly RESISTO functionalities.
- Traceability matrices of the KPI’s and User Requirements that are addressed by the Use cases, as well as related ethical issues.

2. OVERVIEW OF THE RESISTO ARCHITECTURE

Before proceeding to the description of the RESISTO Use Cases and the methodology of their elicitation and validation, a brief overview of the RESISTO architecture will be provided in this Chapter in an abstract format. This will be used in the following Chapters as a reference in order to better understand the various reaction steps and functionalities that are made by the RESISTO platform and will be described per Use Case; towards the full cycle of the identification, detection and correlation of threats up to response and mitigation measures so that a new cycle of protection and prevention to be initiated.

The RESISTO system architecture is extensively described in detail within Deliverables D2.6 [1] and D2.7 [2]. Thus, herein the most significant architectural aspects that are at the forefront of addressing the identification and response to both physical and cyber threats will be highlighted, to enable the description of each Use Case that will follow in the next Chapters.

2.1. RESISTO overall architecture; brief overview

RESISTO aims to enhance and advance the security and resilience of the critical communications infrastructures, by developing a system of systems, encompassing an eco-system of technology innovations and operational models.

RESISTO takes up this challenge by fostering an integrated risk-resilience analysis and assessment of the communication CIs, detection of threats/attacks even in more sophisticated cases, faster and more cost-effective response, so that all these to result in a better informed and more efficient decision making. The final achievement would be a holistic understanding of the overall situation across the cyber and physical domain of the telecom CIs affected by the various threats, as well as the relevant impact to other interlinked CIs. These allow for better reaction and more efficient selection of countermeasures and mitigation actions.

2.1.1. Key Features of the RESISTO System and Architecture functions

The RESISTO platform is modular and adaptable to interfacing with the existing infrastructures through the following five core functions that represent a full cycle of reaction:

- **Identification** – Define and maintain a knowledge base on physical and cyber security risks to systems, assets, data, and capabilities characterizing the Telecommunication CIs.
- **Protection** – Develop and implement the appropriate safeguards to ensure delivery of CI services. The high degree of redundancy that usually characterizes telecommunication networks will be further emphasized in order to implement solutions with high resilience, with respect to both physical and cyber-attacks. Graceful degradation of performance, when under attack, will take advantage of Communication or Network Functions Virtualization (NFV) and Software Defined Networking paradigms.
- **Detection** – Early and timely discovering the occurrence of physical and cyber security events. This function includes the continuous monitoring of the security status of the CI which operates in a highly dynamic environment with changing threats, vulnerabilities, technologies, business processes and services. KPI monitoring and interdependency models will be further exploited to evaluate impacts, recurrent patterns, and the occurrence of complex events. In order to provide a timely detection of a cyber/physical attack, RESISTO leverages on using innovative technologies, properly integrated with security solutions/components already available in the communication CI.

- **Response** – Orchestrate and implement effective response to a detected security event. RESISTO investigates the joint use of Security Function Virtualization and Software Defined Security. Moreover, identifying the best response requires tools for the automatic impact assessment of the security risks and performance and effectiveness of potential countermeasures.
- **Mitigation** – Develop and implement the appropriate activities to mitigate the impacts of threats and to restore as much as possible capabilities or services that were impaired due to security events.

In the following figure RESISTO's logical architecture is depicted, as described in D2.6 [1] in order to highlight, in terms of block functionalities, the enhancements of the RESISTO approach.

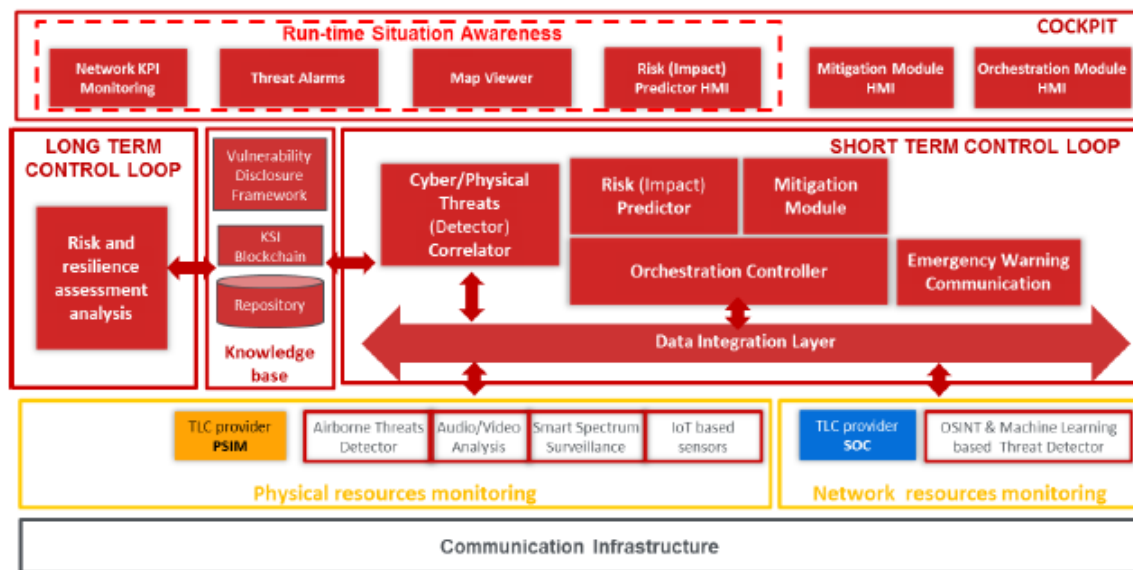


Figure 1: RESISTO high level Architecture and key elements

RESISTO encompasses two different control loops:

- **a Long Term control loop** is in charge of defining configuration of the system according to the security assessment, and updating it on a periodic basis or when particular events takes place (new threats or discovery of previously undetected vulnerabilities). It mainly consists of the “Risk and resilience assessment analysis tool” that identifies the context, analyzes the interdependencies (physical, cyber, logical) and the risks evaluating them semi-quantitatively and quantitatively, and suggests the risks treatment through “Resilience indicators” as summarizing measures of communication CI’ resilience in its operational phase;
- **A Short Term control loop** in charge of promptly reacting to attacks and threats that may impact the operational life of the system. It is the real-time component of the platform that:
 - Monitors the Physical and Cyber security status of the infrastructure, correlating the physical and cyber domain events in order to detect anomalies and provide early warnings on security attacks by detecting threats in advance, supported also by the innovative detection tools brought by the project.

- Performs the “Interdependency analysis”, (Risk Predictor), by simulating the impact with respect to performance degradation of detected anomalies and security attacks on the communication CI and interlinked CIs, based on cascading effects, to verify the resilience of the communication services.
- Based on Risk Indicator target values and multi objective (operational, economic, social) analysis suggests to the operator (Workflow Management) the actions to be enforced (Software Defined Security) to mitigate the risks or to recover from a damaged situation, and orchestrates them.

The long term risk and resilience assessment and improvement process, conducted offline at regular times), determines criticalities and long terms strategies, also based on up to real time assessment quantities and key performance indicators.

The short-term control loop, as a direct (and faster) response, enhances situation awareness, (almost) real-time response and bouncing back up to forward to even better states of systems as preselected by the long-term approach. Also the short term control loop incorporates the advanced modelling and simulation for the generation of resilience quantities and key performance indicators, needed for evaluating assessment in the long term approach.

2.1.2. *Advances of RESISTO when comparing with other H2020 Projects*

The whole concept but also the integration of the above described two control loops are the main advances that RESISTO offers in respect to other relevant EU H2020 projects, i.e. CockpitCI¹, MICIE² and ATENA³. Especially the ATENA³ project is a good reference basis, since certain partners of the present consortium were also involved in that project.

The ATENA³ above project focuses on various CIs and aimed at leveraging the outcomes by exploiting advanced features of ICT and Cyber Security, to be tailored and validated in selected Use Cases, in order to be adopted at operational industrial maturity level. The objectives of the ATENA project were:

- Develop a Unified Modelling Framework and with ad-hoc models to control physical flow efficiency and improve resilience across CIs against threats and related ICT infrastructures when envisaged as complex systems.
- Define dynamic security paradigms for resilience of Cyber-Physical systems since current CIs are increasingly being controlled by ICT networked objects and are becoming Cyber-Physical Systems (CPS) where industrial Ethernet based on IP protocol is widely adopted. Thus, ATENA developed methodologies and technologies for increasing CPS auto-reconfiguring capability when a fault or an attack affects their functionalities.
- Develop new anomaly detection algorithms and risk assessment methodologies within a distributed Cyber-Physical environment addressing a distributed Intrusion Detection System and a vulnerability assessment taking into account the problems related to the interdependent nature of all CIs.
- Develop a suite of integrated ICT networked components for detection and reaction in presence of adverse events in industrial distributed systems.

¹ <https://cockpitci.itrust.lu/home/index.htm>

² <https://www.cis.uniroma1.it/en/node/5603>

³ <https://www.atena-h2020.eu/>

- Validate the ATENA models and tool suite in significant Use Cases that included several cyber-threats, such as:
 1. Electricity domain with CI operators (grid transmission and distribution, customer site – smart home, smart neighbourhood operation and physical protection of the electrical grid and customer site);
 2. Gas domain (distribution and automatic load-shedding management);
 3. Water domain (water distribution and treatment);
 4. ICT domain (premises network, field network, corporate network and inter-domain services).

The results of these Use Cases will be also taken into consideration within RESISTO since they can be exploited for examining interconnected CIs to the telecom ones and their cascading effects.

Moreover, RESISTO builds upon the following ATENA³ functionalities:

- The enforcement of the prevent-detect-react approach by developing real-time reaction strategies to mitigate the consequences of detected treats.
- The introduction of the so-called Software Defined Security, in the field of CIs by supervising their control, operational and corporate networks.
- The introduction of a distributed intrusion and anomaly detection system to cope with the distribution of the functionalities in modern CIs and to detect physical anomalies caused by cyber-attacks

As it will be seen later on, the ATENA Use Cases would provide a good reference basis for the RESISTO interconnected CIs scenarios and assessment validation.

Based on the above, RESISTO provides a more holistic and integrated solution based on Software defined Security but with the inclusion of the two control loops addressing both short term and long term responses and thus the full cycle of tackling threats and vulnerabilities; not only in the cyber domain as ATENA but also in the physical ones as well as in combined cyber-physical threats.

2.2. High-level Description of RESISTO Main Architectural Entities

Based on Figure 1 above, the RESISTO high level architectural key elements are presented briefly below:

Data Integration Layer. SW module, based on an Enterprise Service Bus technology, to facilitate integration of the platform on the existent infrastructure in order to acquire, normalize and store data and information on events. The inputs are represented by data and information of critical event from the PSIM-C and the SOC and external context data (e.g. other CIs resilience status data, data exchange on identified threats with national CERTs) to be correlate; the output are data and information of critical event normalized.

The RESISTO Cockpit: The RESISTO Cockpit acting as the main user-interface provides to the users the following functionalities:

- Real-time situation awareness of potential threats and alarms and related data, along with indicators to assess the resilience of the infrastructure. The link among different threats and alarms is shown as well as the correlation rule. The user can take over the management of an alarms with the support of the “Workflow management” that suggests actions and tasks to accomplish, showing relevant information and progress of the activities;

- The model simulation for interdependency analysis that allows to simulate the impact of the identified threats on the modelled infrastructure and evaluate potential cascading effects;
- Geo-referenced data representation on a map, derived from sensors warning about critical events and data processed from the integrated systems to enhance real-time knowledge of potential critical situation.

Short term control loop: The short term control loop is essentially based on the following components:

- **Risk Predictor:** that evaluates the impacts of exploitations and countermeasures. In particular: (i) it gathers data on anomalies and security attacks from the physical domain (PSIM-C), the cyber domain (SOC), and the Correlator Engine”, (ii) it predicts the effects of countermeasures on the CI, accounting for interdependencies among virtual and physical domains, (iii) it models the interdependencies of CI elements, with the simulation of the short-term effects of failure both in terms of faults propagation and with respect to performance degradation.
- **Resilience Indicators – Real time:** set of indicators to measure in real-time the risk and resilience of the communication infrastructure derived as output of the “Risk and resilience assessment analysis”.
- **Decision Support System – Correlator engine:** this is a rule-based engine customized to detect threats, alarms, critical events defined by the “Risk and resilience assessment analysis” and the “Interdependency analysis” able to detect critical situations to manage. The correlator engine consists of two components:
 - an event stream processing module in order to identify threats and dangerous situations through the analysis of heterogeneous data sources in real-time using several event correlation techniques, such as temporal correlation (based on event time) and logical or causal ones. Events satisfying the correlation criteria are collected in event windows. A pattern-matching algorithm is then applied to determine a specific threat situation.
 - the machine learning algorithms module in order to analyze the behavior of the RESISTO platform and the phenomena affecting the system in order to make decisions accordingly. The results of the application of machine learning algorithms will enhance the way the RESISTO platform detects dangerous situations by means of the correlation and definition of new rules and thresholds which trigger alarms. This module will be also able to build intelligent defense models to prevent damages created by cyber-attacks. In this regard, the use of classification algorithms (e.g. Artificial Neural Networks) for analyzing the network traffic, inspecting the system logs and correlating these data with the monitoring of resource utilization of the systems, can lead to significant improvements in detecting anomalies and attacks occurring over the communications network.

The Correlator is a logically centralized entity. However, it will take advantage of the Network Function Virtualization (NFV) and Software Defined Networking (SDN) of the underlying communication network to enable seamless distribution of detection and analysis functions among several geographical dispersed points of presence (such as data centers), creating the means to implement fog-computing topologies.

Decision Support System – Workflow management: this is a software engine providing configuration and execution of automatic or semiautomatic processes, consisting of sequences of actions and reactions, which can be triggered by the events defined by the Correlation engine. This tool allows presentation of information to the users, activating other modules, suggesting mitigation actions or

counter-attack measures. It is coupled with the reaction/resilience mechanism build around the concept of Software Defined Security (SDS) that performs a dynamic, flexible reconfiguration of security/resilience mechanisms and relocation (virtualization) of security functions, in a way similar to what currently done in SDN. The “Workflow management” receives the output of the “Correlator engine” and can be customized implementing protection actions, tasks and counter-measures.

Decision Support System - Software Defined Security (SDS): A reaction/resilience mechanism based on that integrates mitigation and resiliency functionalities into a unique framework able to dynamically and proactively react to the evolving threats by enforcing the most appropriate security policies in each CI node. Such framework is fed by the DSS, taking the data stored into the Knowledge Base as valuable input parameters. The core SDS components are:

- the Mitigation Module that selects the countermeasures, performing the updating of the security policies, on the basis of a multi objective analysis aimed at: increasing the resilience of infrastructure and services to customers, minimizing the risk of cascading effects, minimizing the impact on system performance.
- the Orchestration Module that manages the cyber physical resources needed to apply the security policies stated by the Mitigation Module. The role of the network security orchestrator is to build complex security functions and services from less complex/primitive security mechanisms/functions. In this process, the orchestrator has to consider service specific requirements, in terms of Authenticity, Integrity, Confidentiality, etc. This is done through the entire lifecycle of a function/service, i.e. deployment, operation, monitoring and termination. In addition, it analyses the network situations in real time, diagnoses and predicts existing or emerging network issues, and determines and coordinates reactive or proactive actions to resolve issues.
- The “Knowledge Base” which is the database (DB) storing set of information about Communication CI configuration, security procedures, protection-reaction/mitigation strategies, recovery procedures. Data stored on the DB are secured and their integrity monitored and enforced.
- The Long term control loop which is in charge of defining configuration of the system according to the security assessment, and updating it on a periodic basis or when particular events takes place (new threats or discovery of previously undetected vulnerabilities) the Long term control loop essentially builds upon the following components:
 - Risk and resilience assessment analysis tool that, based on context holistic modeling, identifies risks, evaluates them in a semi-quantitative and quantitative modes and suggests the risks treatment and mitigation strategy
 - The Long Term Control Loop summarizes measures of the CI resilience in its operational phase, while assesses and classifies the most effective of mitigation measures -

3. DESCRIPTION OF THE USE CASES: OVERVIEW AND METHODOLOGY

In this Section, the steps followed to elaborate the RESISTO Use Cases elicitation will be summarized. The methodological approach starts from the three “Macro-Scenarios”, as these are described in the DoW and goes towards the use cases and the analysis of their scenarios.

Respective KPIs to be measured for evaluating the RESISTO added value in each use case are also provided, based on the pool of KPIs already defined in D3.7 and D3.8 Deliverables. The three Macro-Scenarios along with each respective use case follow and address the User Requirements extracted from D2.1 Deliverable. Traceability matrices of both the KPI’s and the User Requirements mapping per use case are also provided in Chapter 13 to enable reference for the project’s outcomes and the evaluation of the RESISTO added value in each use case.

3.1. Main Concepts and Terms

Before proceeding, certain definitions for the corresponding methodology concepts and terms are provided herein; moreover, the interrelations between such concepts are also given. This “set of concepts and terms” will be used in the part of the use cases’ analysis, in order to define the key technological aspects which are related to the project’s specific objectives. The following terms are taken into account:

- **Macro-Scenarios:** A set of Use cases serving and proving a high-level conceptual goal.
- **Use case:** The Use cases describe application examples of a macro-scenario, highlighting key benefits of the RESISTO context, with a specific concept as a common basis for certain respective scenarios.
- **Scenario:** A particular “instantiation” of a specific Use case, aiming to elaborate upon certain sets of parameters, in order to demonstrate and assess the specific Use Case.
- **End-Users:** They consume services provided by the Service Providers (SPs).
- **Assets:** Facilities, Equipment, infrastructure, network, staff and other properties or assets (whether tangible or intangible) used in the telecommunications business.
- **KPIs:** Key Performance Indicators are used to evaluate factors that are crucial to the success of the system under consideration.
- **Requirements:** These are categorized as “functional” and as “non-functional”. A requirement pertains to the technical aspects that the corresponding system must fulfil.
- **Evaluation:** An attribute usually representing some property subject to change⁴. Examples for potential parameters of a small cell network can be, *for example*: Coverage increase and increase in functionality offered to the user.
- **Actor:** Actors and actors’ interactions are being analyzed explicitly in the subsection below.
- **Impact:** Consequences of attacks or failures to Communications Infrastructure. It can be immediate or cascading.

Three initial macro scenarios have been identified in the DoW as “promising fields” for the applicability of the RESISTO concepts, which can be further used as the basis for the formulation of a number of specific use cases. A description of the three scenarios is given in the following

⁴ Institute of Electrical and Electronic Engineers (IEEE) (2000). IEEE 100: The Authoritative Dictionary of IEEE Terms, 7th edition. IEEE Press, December 2000.

subsections, by highlighting the main challenges, the applications and services in-scope as well as the respective RESISTO components and capabilities.

According to the DoW, specific main Use cases have been suggested for each Macro-Scenario, while certain others refers to more than one Macro-scenario and thus are mentioned as “impacted”, since they are affected by the conductance and the outcomes of the main ones.

3.2. Macro-Scenario 1: Protection and resilience of the Current / existing Telecommunication Critical Infrastructures

Macro-Scenario 1 is meant to be examined in the framework of WP7.

The aim of this macro-scenario is to jointly activate all the necessary assets, infrastructures, people and networks so that to operationally validate the Current telco Infrastructures protection against physical and cyber threats. More specifically it aims:

- To deploy piloting of a large number of Use Cases addressing the detection, prevention, response, mitigation and protection requirements of existing facilities and infrastructures
- To implement an innovative integrated platform and tools for protection actions against real world, known or potentially provisioned, combined physical and cyber threats based on the so-far relevant experience
- To specify the architecture of the various test-beds and to pave the way for federation of facilities and joint actions
- To mobilize assets, key personnel and networks, engaging the end-users to actively organize and execute the pilots
- To encounter technological challenges within existing telecommunication systems and infrastructures
- To plan, facilitate, demonstrate and provide tangible feedback and evaluation in existing premises and infrastructures.

This macro-scenario creates the baseline for federated actions against a miscellany of evolving physical and cyber threats, addressing real operating conditions, affecting the telecom end-users and also situations concerning the impact on the general public. Thus, setting the basis for the logical interconnections of the Scenario pilots to achieve federation aspects. The design of the pilot Use Cases for the 1st Macro-Scenario will take place, tailored to the specific existing, cyber-physical telecom Infrastructures that are involved.

Within the DoW, 5 Main Use Cases, each lead by a respective Operator are attributed to the Macro-Scenario 1:

- Core Network Failure caused by Physical & Cyber Attacks to Telecommunication sites (lead by OTE)
- Telecommunications congestion caused by natural (Earthquake) or man-made (i.e. Multiple Terrorist Attacks) hazards (lead by OTE)
- Protection of ISP Backbone Nodes (lead by TIM)
- Telecommunication sites (lead by RTV)
- Disruption of major sporting event by combined physical & cyber-attack by a terrorist organization (lead by BTC)

Furthermore, the effects that another Use Case would have on existing telecom CIs protection will be also explored herein, indicating the data exchange between the macro scenario 1 and the second Macro-Scenario, as Impacted Use Case:

- Cyber and physical protection of network and network elements mechanisms used by critical services that impact users (lead by ORO in WP8)

3.3. Macro-Scenario 2: Interdependencies of providers of essential communication services - Interconnected CIs

Macro-Scenario 2 is meant to be examined in the framework of WP8.

This second macro-scenario focuses on addressing Interconnected/Interdependent CIs; interdependencies of providers of essential communication services to other interlinked CIs and related cascade effects in the vicinity caused by indicative threat cases in Telecom infrastructures through sufficient responding and innovative protection measures. The main objectives to be addressed are the following:

- To deploy piloting in selected representative Use Cases (3 Main ones and 3 Impacted) mostly addressing the effects that threats against telecom infrastructures would have and the impact on a general protection framework
- To derive lessons learned and best practices of the comparative analyses and end user validation
- To address organizational procedures providing opportunities for inclusion within current corporate facilities
- To demonstrate that a risk / resilience based protection architecture can incorporate tools anticipating cascade effects
- To encounter technological challenges through an innovative integrated platform and tools for identification and protection in a more general approach (i.e. affecting wider area zones and a variety of assets other than telecom)
- To plan, facilitate, demonstrate and provide tangible feedback and evaluation in related cases.

This macro-scenario acts as the liaison between the baseline (formed in the first macro-scenario) and the envisioned future networks and their protection (third macro-scenario) as this can be demonstrated in the context of the main and impacted Use Cases involved. Thus, setting the basis for the functional interconnections of the Scenario pilots through established federation aspects. In this second macro-scenario the following use cases will be described:

- Protection of Cloud Storage Services (lead by TIM)
- Cyber and physical protection of network and network elements mechanisms used by critical services that impact users (lead by ORO)
- Maritime Safety and Emergency Case (lead by RTV)

The effects that other Use Cases have in terms of interdependencies will be also explored, indicating the connections and data exchange between all three macro-scenarios, as Impacted Use Cases:

- Cyber-attacks at the core network (in connection to OTE's Use Case in macro-scenario 1)
- PPDR Virtual Operator (lead by RTV in macro-scenario 3)
- 5G network response to a large scale natural disaster in Lisbon (lead by ALB in macro-scenario 3)

3.4. Macro-Scenario 3: CI evolution towards the future 5G telecom CIs and networks and the emerging IoT world.

Macro-Scenario 3 is meant to be examined in the framework of WP9.

The macro-scenario 3 addresses the Future communication infrastructures that rapidly emerge in technology and market terms. Future networks named as 5G will introduce better capabilities in terms of bandwidth, speed and latency involving new technology advancements such as nanocells, SDN and NFV to allow for these improvements and expanded broadband services realizing IoT. To this respect, resilience and the ability to provide and maintain an acceptable level of service against any faults of this network will be indeed a challenge. Threats for services can range from natural disasters to targeted cyber-physical attacks that is to say a very wide range of topics needs to be tackled and new innovative networks that are not still implemented as commercial services needs to be dealt.

All the above result in a very challenging scenario in terms of bringing new aspects on cyber physical threats; in order to increase the resilience of such a 5G network, risks have to be identified and appropriate resilience metrics have to be defined for the service to be protected covering the whole chain: Distributed backhaul, Cloud Storage and platform system, RF communication head-end along with Applications and data, Services provided and a wide variety of users. To deal with this, this third macro-scenario's particular objectives are:

- To provide in situ demonstrations of RESISTO solution, on 5G envisioned network nodes, promoting applicability
- To facilitate the pilot execution and demonstration of market-related interest and impact pilots so that to make the outcomes and results of WP9 available to various related stakeholders and policy makers for future operations
- To evaluate and validate the RESISTO solution within a pure market-oriented environment
- To contribute by the experimental 5G networks piloting to the future commercialization of RESISTO system

This scenario provides the envisioned future networks and their protection as this can be demonstrated in the context of the experimental networks involved.

The 3 main pilot Cases which will exploit future networks being currently at experimental service such as 5G, LoRA, Sigfox implementing the complete RESISTO platform, will be analyzed in this deliverable. More specifically these use cases are:

- Smart Manufacturing Data Integrity Protection using a block-chain based mechanism (lead by TIM)
- PPDR Virtual Operator (lead by RTV)
- 5G network response to a large scale natural disaster (lead by ALB)

Since IoT networks and WSNs are closely tight to the 5G emerging services, the relevant interdependencies and data exchange between second and third macro-scenario, will be considered through the following Impacted Use Case:

- Maritime Safety and Emergency Case (lead by RTV in macro scenario 2).

3.5. Methodology Overview

From the above it is clear, that even from the DoW a large pool of application Use Cases, addressing the high-level concepts of each Macro-Scenario are already in order.

However, in order to design the final Use Cases that are going to be implemented within the RESISTO validation framework, a specific set of actions and pre-assessment was necessary in order to select those Use cases that would be feasible to be implemented and validated given the ability of the RESISTO various tools and telecommunications test-beds, as these are defined in the relevant RESISTO Deliverables.

This section presents the methodology which has been adopted by RESISTO, in order to perform a multi-dimensional analysis of the proposed use cases, as these are to be selected with the aim of purely serving the defined RESISTO aims. Such kind of analysis will be multi-directional, because it will enable deliverable D2.8 to serve as a reference document for the work, which will be carried out in the work-packages 7, 8 and 9 during the piloting trials.

In this sense, the methodology will allow us to define the technological benefits that will result from the RESISTO outcomes as well as any corresponding evaluation criteria for the level of fulfilling such outcomes and benefits.

As already stated in the previous sub-sections, the project has already defined three important areas (the 2 Macro-Scenarios) where RESISTO has the ambition to go beyond the state of the art, namely:

- The protection and resilience of the Current existing Telecommunication Critical Infrastructures
- Interdependencies of providers of essential communication services to other interlinked /interconnected CIs and related cascade effects in the vicinity
- CI evolution towards the future 5G telecommunication infrastructures and networks and the emerging IoT world.

Based on these, a thorough analysis of each Use Case took place in order the respective scenarios, tests and experiments per Use Case to be finally selected and designed.

The main concept, beneath this process is that: ***the Use Cases that would be finally selected and designed are those that it would be feasible to be operational validated in the end given the available test-beds, facilities, people involved and offered technological tools within the framework of the project.***

To this respect, as it will be seen in the Chapters to follow, there are certain diversions in respect to the Use cases suggested within the DoW; certain Use Cases were slightly changed or differentiated in order to be adjusted in the current trends, needs and facilities. However, the main concept of them and their connection to the Macro-Scenarios high level goals still remain the same, as well as their main objective which is to prove the RESISTO added value in current and future telecom CIs.

Considering the above main drivers, the following methodological steps that lead to the complete description of the use cases, have been conducted. Each step is briefly described herein, since the objective is to provide an overview of the approach followed, having also in mind the relevant operational validation that is going to be held for all the Use cases.

These methodological steps are the following:

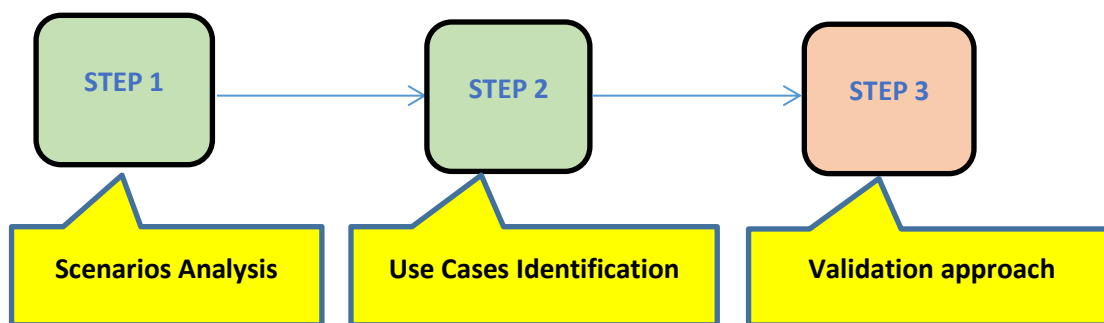


Figure 2: RESISTO methodology for use cases description

- **Step 1: Scenario Analysis:** During this step a thorough analysis of the scenarios, tests and experiments that constitute each Use Case took place taking into consideration the RESISTO platform and its functionalities. Although the description of the Use Cases has been foreseen in the DoW, a more thorough analysis took place in order to form the storytelling of each use case and correlate it to the desired RESISTO operations; the analysis included the foreseen types of threats and attacks, the telecom assets to be affected and the impact that these threats would cause to the telecom CIs or cascade effects in the vicinity or even to people and staff and the provider's operations. This step served as base for the identification of use cases.
- **Step 2: Use cases identification:** Based on the scenarios analysis from the previous step, the identification of the Use cases took place addressing the three pre-defined macro-scenarios; the final selection of the story telling, taking into account the actors participated, the stakeholders for each use case and the RESISTO tools to be involved. The RESISTO response was also identified at this step, including the short term response, potential contribution to the long term response through the risks and resilience objectives involved, and the innovation addressed by each use case. All these constitute the foreseen RESISTO added value in tackling the threat and suggesting mitigation measures. The output of this step is a first, formalized high-level description of the use cases and graphics representation of the test-beds that will be used for the implementation of each use case.
- **Step 3: Validation approach:** Although the first 2 steps have already been completed and are the subject of the present Deliverable, the third step, consisting of the validation of the Use cases will be the subject of the operational validation framework in WP7, 8 and 9. However, as already stated, the validation approach of the Use cases is an important factor of their final selection and design in terms of their feasibility. To this respect, at this point, when designing the Use cases, the following validation parameters were taken under consideration: the availability of the test-beds and their functionalities in emulating threats in the telecom assets and networks, as well the foreseen KPIs to be measured per Use case so that to prove the added value of the RESISTO system but also the feasibility of each conducted scenario. Thus, the validation approach will be further analysed in a following paragraph of this Section.

In the following, a more thorough insight in certain factors that were taken into account or will be exploited through the RESISTO validation framework is being given.

3.5.1. Implementation of the RESISTO Use Cases

It is important to mention that the RESISTO use cases described in this deliverable are not static; instead they will evolve during the project in order to best prove the RESISTO functionalities during the pilot phase of the project. Therefore, some of the attributes from the general description and structure given herein structure may be adjusted and differentiated in later stages through the validation framework iterations.

The main focus of the RESISTO implementation framework is to support the relevant macro-scenarios via elaborating different use cases, in different contexts and applications, while serving a wide diversity of service provision aspect, covering existing needs, filling identified gaps in the telecom's infrastructure's security and providing relevant solutions for the emerging future. These include: changes in network topology; increasing capacity requirements in dense environments, etc. These scenarios will exploit system capabilities and solutions together with network and topology integration.

Hereinafter a set of technical use cases is defined as "linked" to the above described scenarios. It should be noted that every use case touches a specific sector inside the overall RESISTO scope. The combination of all results shall help to define a set of system requirements which, again, shall lead to a project-wide reference framework and architecture. Afterwards, system components can be derived accordingly, accompanied by their functional architectures and interfaces to "better reflect" the technical work-packages effort.

In engineering, use cases constitute an important part of a methodology that helps to design a complex system composed of smaller blocks; in this context, a use case "reflects" such a typical smaller block. Use cases are important so as to extract system requirements and then capture non-conventional requirements, by exploiting corresponding interrelation between the technical use cases thus correlating, *for example*, different attributes and parameters in different use cases.

Even though telecom's transition to all-IP networking has progressed greatly, challenges such as ever-increasing security threats are still ongoing. One of the main issues that telecom operators all around the world are concerned is reliable functioning of critical infrastructures. Critical infrastructures represent "systems and assets, whether physical or virtual, so vital to the telecom operations that the incapacitation or destruction of such systems and assets would have a major impact on the communications".

Reducing current and future risks requires a combination of leading-edge technology accepted sector practices, and timely information sharing throughout and across sectors. In telecom business critical infrastructure environment, for the protection against threats or unexpected events the key is the adoption of a specific security architecture, principles and guidelines for each different type of technology and threat, within these critical infrastructures.

Telecom operators and service providers are in a position to address growing security threats and protect their networks and their customers' data and content. To identify and respond risk operators should understand the likelihood that an event will occur and the resulting impact. Acquiring this information, operators can determine the acceptable level of risk for delivery of services and decide the proper way of handling it (e.g. mitigating the risk, transferring the risk, avoiding or accepting the risk), depending on the potential impact to the delivery of critical services.

3.6. Roadmap for the validation process of the Use Cases

The objective of this process is the validation and evaluation of the results achieved during the pilot implementation of the RESISTO system. The main features of RESISTO platform will be validated per Use Case. For each pilot trial RESISTO functionalities will be verified by the actors involved, with their own assets and data coming from their own system, as described per Use Case in the previous Sections.

As stated in the DoW, the validation procedure allows the definition of an adoption path for the RESISTO platform and services to be used as best practice that would also enable future exploitation. Thus, an extended validation process is foreseen based on the different operational Use Case pilots, described previously, formed in various sets of configurations in terms of context, organization and impact, altogether consisting the RESISTO overall Validation Framework.

As already denoted, the selected Use Cases, spanning from resilience of current and future Communication Infrastructures to cascading effects on interconnected CIs, will reflect real life exercises for the telecom critical infrastructures protection, with realistic cases, not simple guided demos. And that is evident throughout the description of the RESISTO Use Cases that will be held in the sections to follow.

The RESISTO operational validation and evaluation framework, according to the DoW, will be conducted within the framework of 3 WPs:

- WP7 “Operational validation scenario #1: (Improving of resilience of) Current telco Infrastructures”,
- WP8 “Operational validation scenario #2: (Improving of resilience of) interconnected CIs” and
- WP9 “Operational validation scenario#3: (Improving of resilience of) future 5G telco Infrastructures”.

Each one of the above WPs addresses each macro-scenario, in other words a set of Use Cases that formulate a significant overall concept, where RESISTO could prove its added value in enhancing the resilience and response of telecom infrastructures in three application domains: current / existing telecom CIs, the emerging future ones and the interdependencies between those and other CIs in the vicinity.

The assessment and evaluation of each Use Case scenario will be coordinated by a Telecom Operator, namely the one who provides the relevant test-bed; while a set of sensing, detecting and processing tool, modules and interfaces will be used spanning through all technologies, functionalities and modules that are offered by the RESISTO system.

Two Iterations of field runs are foreseen for the validation process:

- Within the first iteration the “Testing of all tools” in terms of technical development and integration will take place along with the first validation feedback. Thus, the tools developed in RESISTO will be verified and their integration will be tested. As such, many aspects, problems and testing bugs are expected to occur needing immediate tackling, especially regarding their integration. To this respect, the focus is rather on the establishment of a solid base of satisfactory overall system’s performance. Simultaneously the first validation feedback would be gathered and assessed to give space for further improvements, paving the way for the second final iteration.
- In the second phase a more “in deep operational validation” will be performed and all the uses cases will run and evaluated in a parallel way allowing for commonly extracted results to be used

as best practices. KPIs and metrics measurements will be finalised to provide the overall assessment of the RESISTO solution in enhancing the telecom CI's resilience and prove the RESISTO added value.

The exact implementation and operational validation details will be defined within the framework of the Deliverables D7.1, D8.1 and D9.1 which deal with the "Macro-Scenario 1 / 2 / 3 Test plan definition". In the framework of these Deliverables the following will be designed and defined:

- The definition and establishment of a baseline methodology to be followed during the whole piloting conductance.
- The implementation schedule, period of operational validation (start and end times, time duration etc.). The plan of the pilot deployment is influenced by the availability of the system components, the appropriate and the test requirements of the end-users.
- The involvement of actors that will take part in the validation and verification process as implementation and validation testers, their qualifications and their training procedure (who will they be i.e. technical staff or telecom providers' employees independent from the project, how will they be trained etc.)
- The methodology that the validation, verification and evaluation process will be performed i.e. through metrics, indicators and KPIs and online technical assessment, questionnaires etc. in order to objectively assess the piloting results but also to capture the users' feedback and recommendations for the RESISTO platform improvements, triggering post releases.

The above will be discussed and defined in all their implementation details within the framework of the respective WP 7, 8 and 9 and the respective Deliverables.

3.6.1. Key aspects of the validation process of the Use Cases

From the description of the Use Cases that follows it will be seen that quite many issues concerning the implementation and operational validation of the RESISTO platform are already stated per Use Case. At this point, where the general guidelines of the validation framework are being described in a preliminary level, the main principles that govern the design and planning of the RESISTO pilot deployment and validation can be summarised in the following, in order to provide herein an initial roadmap for the overall implementation:

Step by step approach: The main strategy for the RESISTO pilot validation and evaluation framework follows a step by step approach, so that the overall system is gradually tested and implemented in all its dimensions; starting from the technological components up to all processes and procedures needed at the telecom operators for the foreseen resilience improvements in their telecom assets and critical telecom infrastructures.

Use of test-beds and emulations of threats and vulnerabilities: It has already been made clear that the real, operational, telecom network of the involved telecom providers / end-users, cannot be employed for obvious reasons; since it is the backbone for the provision of all telecom services and the interruption of this services for testing purposes would significantly risk customers' SLAs. To this respect, test-beds to emulate the network performance are being employed by all telecom providers for the conductance of the Use Case implementation are already described. These test-beds will be fed with real or realistic data of threat incidents, in order to emulate the effects on the network of real incidents or threats according to the so far experience on security events anticipation gained by the telecom providers through their network usage.

On the other, even emulations of threats might be impossible to be implemented in certain cases: for example, UAV/s drone flights are not allowed in urban areas or are under specific legislation. This dictates the UAV flight and attack detection to be held in a remote area or in specialised test sites for that purpose, while the detected potential intrusion events will be interfaced with the test-beds at the telecom operator's central facilities. These are examples on how the deployment and operational validation will be held from the technical point of view in certain Use Cases, while more details on the deployment plans are described in the relevant Deliverable D4.2 [6].

The above are just paradigms to indicate that appropriate solutions are meant to be used to emulate the real telecom network functionalities and the threat effects on it along with the RESISTO system added value on enhancing the telecom asset's resilience. However, it has to be emphasized that the main aspect that will govern all suggested or selected solutions of this kind is that ***from the technical standpoint the quality of the expected results of the involved tools and modules including the test-beds and emulations of the telecom network will not be affected.***

Technical validation measurements, metrics and KPIs: Specific metrics and KPIs have already foreseen to assess the technical functionalities of the Use Case scenarios and specifically proof the concept and the added value of the RESISTO platform. The specific KPIs to be measured per Use Case have already been attributed in the relevant Sections. A more detailed analysis of the measurement methods concerning the metrics and KPIs is given within Deliverable D3.8 [4].

Validation based on the described Use Cases: The Use Cases described in this Deliverables consist of the **main core** of the experiments that will be held within RESISTO. The operational functionality of the RESISTO solution will be tested following the quite many scenarios that were defined herein. Furthermore, other, additional experiments and scenarios may emerge based on those Use Cases described herein, including their variations or combinations and they will be tested as well i.e. in the framework of interconnected CIs, so that all macro-scenarios are addressed and examined. The above depend greatly on the initial feedback to be gathered and processed.

RESISTO Short Term Control Loop Response: The RESISTO short term control loop provides the real-time (or almost) real time response to an identified threat. Almost in every Use Case described in this Deliverable, the Short Term Response of the RESISTO system is being identified and described in order to prove its added value towards the enhancement of resilience in telecom assets. In summary, the RESISTO short term response consists of the following features:

- Activation of modern, more sophisticated and low cost counter-measure solutions in case of severe physical threats, based on equally sophisticated sensing and detection systems and correlation of events and threat incidents with the assets' failures
- Response in lesser time than the conventional security systems would need to react
- Reduced human intervention; the security staff could evaluate and examine the response results instead of consuming time and resources to search and identify the threat and the cause of the failure in the first place
- Suggestion of immediate protection and mitigation actions

All the above will be evaluated and assessed through metrics and KPIs during the pilot operational validation process.

RESISTO Long Term Control Loop Response: Especially for the Long Term Control loop, the following is summarized in the below section.

3.6.2. *RESISTO Long Term Control Loop response through the Use cases*

As already denoted, the RESISTO Long Term Control Loop (LTCL) mainly refers to the “risk and resilience analysis and management tool” that is developed within WP3. The LTCL works offline and concentrates all potentially detected vulnerabilities and threats within the telecom infrastructures in order to analyse them in respect to the assets affected as well as the provided services to the customers in order to provide at regular times integrated mitigation recommendations for the whole facility or network. By that way a new iteration of mitigation measures is provided, and a new cycle of prevention is being initiated.

The main output of the Long Term Control Loop (LTCL) applying the risk and resilience analysis management process, are interventions to improve the CI resilience.

The aim of the LTCL is to identify and evaluate risks and suggest improvement and mitigation strategies, which will improve the resilience of the CI.

The new Resilience Indicators taking into account the identified strategies will be evaluated, in order to measure the improvement of the resilience from the CI.

Since the LTCL works offline, it could follow the two validation iterations described previously; in each, the LTCL could be activated before and after the conductance of the Use cases in order, through that comparison, valuable results to be extracted for the overall resilience of the infrastructure, taking into account the threat or attack impact.

The use cases will be deployed to verify the analysis of the LTCL. If the implementation of the use cases indicate shortcomings, the knowledge from the use cases will be applied to improve the LTCL. To evaluate each use case, the following steps are performed:

1. Implementing the test-bed topology in the CaESAR simulation tool for the Use cases
2. Defining and implementing the dependencies in the Critical Infrastructure within the CaESAR simulation tool (e.g. Power, Buildings)
3. Actors and detection tools involved in the use cases will be implemented (e.g. Attacker/Hacker, Camera, Aerial Surveillance System, Hostile UAV...)
4. Simulation of threats described in the use cases will be simulated in the CaESAR simulation tool. Further, a combination of the different threats presented in the use cases will be considered and simulated.
5. The critical pairs of system functions and threats will be identified. The critical pairs are identified with a correlation matrix. The next picture shows a generic correlation matrix. The Resilience quantification (curves) will be performed for critical couples Performance/Threat

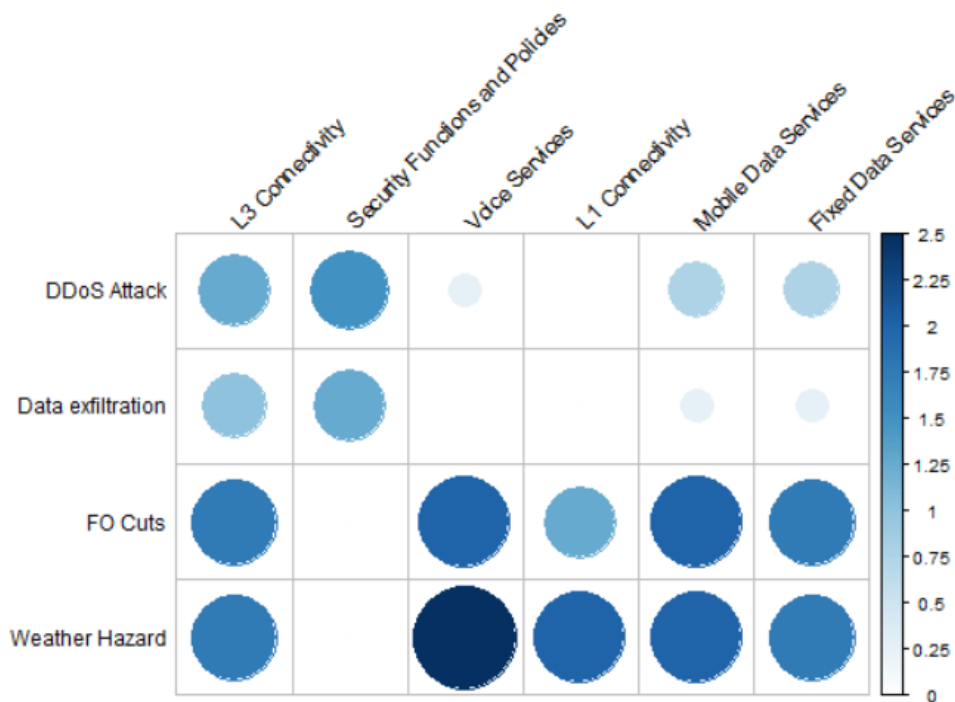


Figure 3: Exemplary correlation matrix of system functions and threats. It should be noted, that the entries in the correlation matrix are not normalized but rather refer to a connection strength in arbitrary units

- Expected impact on the network in terms of service performance loss will be computed. As explained in the deliverable D3.6 section 3.3.1 various performance metrics are given for a telecommunication network. For each threat and for each provided service, the expected impact will be calculated. Further, a resilience curve will be computed for each combination of disruptive potential event (threat) and service performance metric (see Figure 4).

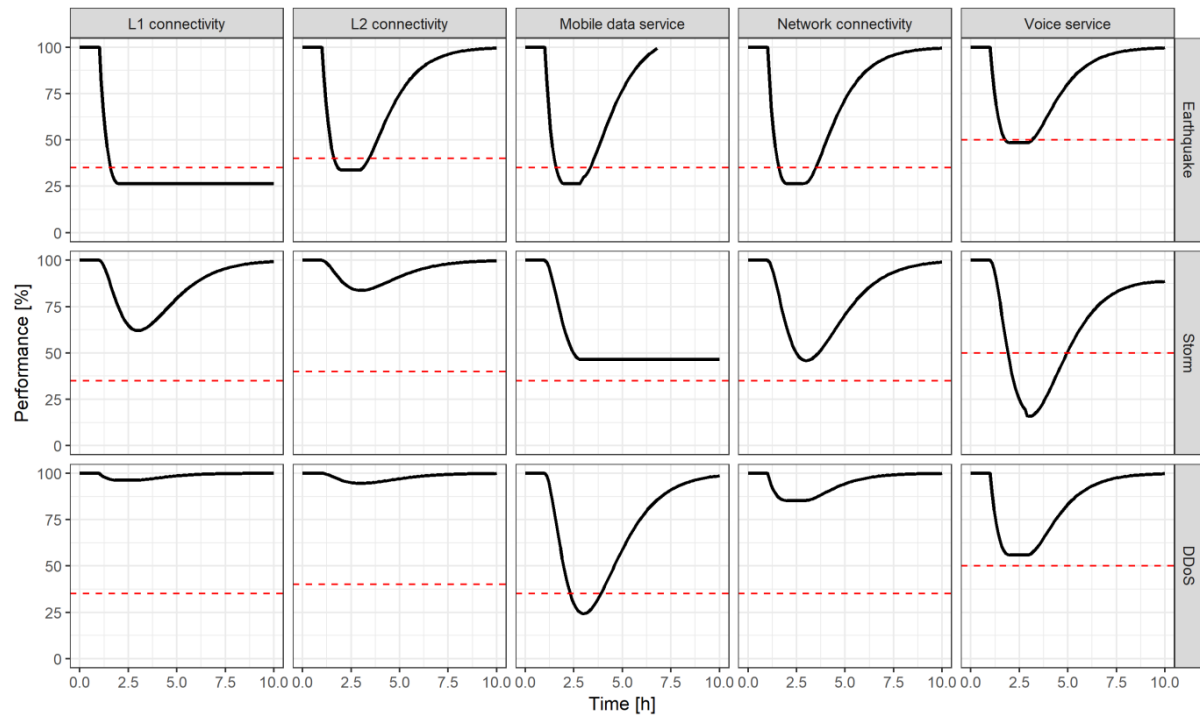


Figure 4: Exemplary visualization of a resilience matrix (performance metrics vs threats). The performance functions and threats are taken from actual inputs but the curves are not realistic, i.e. not based on real data or a realistic simulation

- Resilience indicators (RI) for each couple of thread/performances will be computed and stored in the knowledge base (see Table 1). The objective of the RI's is to allow a continuous Critical Infrastructure resilience monitoring and improvement. (see D3.6 section 5.3)) These RI's will be compared with the new RI's evaluated taking into account improvement interventions (see point 9.)

Telecommunication Infrastructure Network	Ddoss Attack	Fiber Cut	Data Exfiltration	Weather Hazard
Voice Services					
L1 Connectivity					
Mobile Data Services					
Fixed Data Services		Estimated RI(1;i;j) RI(2;i;j) RI(3;i;j) RI(4;i;j)			
L3 Connectivity					
Security Functions and policies					
Throughput					
Delay					
Loss Packet					
Jitter					
....					

Table 1 – Storage format of RIs in the Knowledge Base of the RESISTO platform, based on the matrix structure of potential events and performance functions.

8. The critical components of the system will be pointed out.
9. Finally, mitigation strategies will be proposed, and the new resilience of the CI will be evaluated, taking in account the chosen mitigation strategies. This will enable an analysis of the potential resilience improvement from these strategies. After the new Resilience evaluation, the new RI's will be stored in the knowledge base.

3.7. Interconnected CIs validation

The Operational validation of the Interconnected CIs constitute the whole WP8.

The RESISTO Use cases are meant to demonstrate attacks, threats and vulnerabilities that may affect the existing framework of the telecom CIs and the added value of the RESISTO platform in dealing with more sophisticated kinds of threats, especially the combined cyber-physical ones.

Certain Use cases may not directly foresee cascade effects and interdependencies with other critical infrastructures in the vicinity. However, the threats could be used by specific RESISTO tools (such as CISIAPro and tools dealing with propagation effects) to develop and implement experiments on the potential impacts imposed to other interconnected critical infrastructures supposed to be affected by the specific Use Case.

To this respect, the Use Cases that will be described in the following should not be seen as independent to each other; at least certain of them can be “interconnected” to each other

providing the opportunity and opening the floor for studying respective threat propagation and cascading effects. This kind of interconnection scenarios between the various Use cases that are described herein, will be the subject of the Macro-Scenario 2 in the framework of WP8. Thus, the pool of Use cases that are selected within the present D2.8 will be used for testing more interlinked scenarios.

As indicative examples the following can be said at this point:

- As a first example, the combined cyber-physical threats in Use Case 1 that follows, could affect the internet connectivity of financial and banking services or the telemetry network of power grids, since telecom networks (fibers, WLANs, cables etc.) are an important factor for the operation of other critical infrastructures.
- Another example would be the interconnection between OTE's and ORO's Use cases: OTE's and ORO's RESISTO labs (test-beds) can become interconnected through the use of a VPN tunnel, in order to run a DoS attack scenario with cascading effect. For this scenario a remote ORO user/customer will be provisioned through OTE network (roaming customer). During a DoS attack at ORO's network some services will be destabilized or stop working for some time (service disruption), so the provisioned user over OTE, will experience this instability or may temporarily suffer loss of connectivity / loss of availability for some services provided by ORO, as a result of cascading effect. This indicative example will demonstrate the cascading effect on interconnected telco infrastructure and will be elaborated in the framework of WP8.

Similar studies of threat propagation and cascading effects are currently being examined within the framework of **D4.4 :“Complete propagation analysis” [8]**, and are not being repeated herein, so the reader may refer there for more information.

The above are particularly true when connected and dispersive scenarios are considered and dependencies on Information and Communication Technologies play a key role. In order to understand the CI behaviour, identify their vulnerability and protect them against increasing level of propagated threats, a modelling framework of the related test-beds conducted through tools such as the RESISTO CISIAPro would be valuable and challenging at the same time. Such a framework for assessing CI flow efficiency, robustness, reconfiguration and resilience under cyber-physical threats aims at increasing telecom and other CIs operators awareness, providing real time optimization of CI flows at different dispersion levels over wide geographic areas (national, regional, urban).

In this context, RESISTO can also build upon the Use cases studied within the ATENA project and extract valuable outcomes that could be adjusted and advanced through the RESISTO system.

The ATENA Use cases could be exploited since they deal with: the electricity domain (grid transmission and distribution, customer site – smart home, smart neighbourhood operation and physical protection of the electrical grid and customer site); Gas domain (distribution and automatic load-shedding management); Water domain (water distribution and treatment); ICT domain (premises network, field network, corporate network and inter-domain services).

By this way, well-known security issues, addressed in ATENA³ project, generated by both the presence of CI interdependencies (e.g., threat propagation and cascading effects) or SCADA complexity (e.g., presence of interconnected/inter-operable distributed devices, sensors and actuators) could be used as baseline.

Moreover, new challenges arise from the growth of the interconnection among these infrastructures with the telecom ones through the development of IIoT aspects. Thus, the relevant ATENA³ results can be more expanded through RESISTO in the field of detection and risk assessment, in order to assure the achievement of the desired security level in normal operational modes.

4. USE CASE 1: CORE NETWORK FAILURE CAUSED BY PHYSICAL & CYBER ATTACKS TO TELECOMMUNICATION SITES

4.1. Introduction and Background

Telecom networks as critical infrastructures are meant to provide multiple types of services with predefined and guaranteed Quality of Service. Mobile network operators focus on protecting their existing networks and telecom infrastructures from attacks originating from outside.

In the most devious attacks, rather than trying to gain full access into the system, an attacker may only want to open up a few strategic holes to the cyber domain of a network that will cause severe problems or failures to the offered services either immediately or at a later time. In the latter case, the attackers may perform reconnaissance and preparatory work on the digital front, before moving to actually perform the attack. Thus, the attackers can exploit vulnerabilities in the physical domain of an infrastructure, to gain access to the cyber domain.

These physical intrusions (such as unauthorized access to a building without obvious, direct or severe damage on the telecom infrastructure) may be initially seen as physical assaults of a lesser importance in respect to their consequences on the cyber domain, especially when correlation between the physical and cyber intrusion events is hardly performed by the telecom operator's existing security system. Thus, both events may not be given the proper attention.

Based on the above, the present Use Case is a representative example of how seemingly unimportant physical intrusions can facilitate very severe assaults in the cyber domain, creating combined threats (physical threats enabling cyber ones) in existing telecom infrastructures. Thus, Use Case 1 provides the perfect opportunity to demonstrate how the RESISTO platform can detect, identify and mitigate these combined events, demonstrating the added value of the RESISTO system compared to the conventional security systems, that are unable to correlate physical and cyber threats.

4.2. Overall Description of the Use Case 1

Use Case 1 will be implemented by OTE as the main telecom operator with the assistance of modern detection tools offered by other consortium partners (ICCS and ADI).

In this Use Case, a cyber-physical attack takes place, targeting network equipment in a specific location that is physically protected by the telecom provider's security system. The physical intrusion (either by an airborne threat or by an attacker) is performed against the physical assets of the telecom provider. This physical threat is deliberately meant to enable a security threat in the cyber domain of the telecom provider's network. The telecom facilities are protected by the provider's existing security system, while the RESISTO platform, with its additional new sensors for detection, is also deployed by the provider.

Two relevant subcases (scenarios) are envisioned, indicating the RESISTO added value to the telecom provider's security systems:

- a) **In the first subcase**, the attackers use a UAV to overcome the physical protection and execute the cyber-attack. The RESISTO system, deploying its sensors (i.e. radar for airborne threat detection), detects the UAV and identifies a potential security threat in the cyber domain, activating the provider's cyber detectors, which detect and neutralize the threat.
- b) **In the second subcase**, an unauthorized person gains entry into a protected building and it is detected using data from the provider's security sensors (i.e. cameras and microphones), which are integrated into the RESISTO system and augmented with sophisticated detection algorithms

provided by RESISTO. Thus, a potential security threat in the cyber domain is identified and subsequently detected and eliminated by the provider's cyber detectors and prevention mechanisms activated by RESISTO.

In both cases, a combined, cyber-physical, attack is executed by a third party targeting the provider's network and it is being detected and neutralized by the unique capabilities of the RESISTO system; that is the integration of old (existing) and new (from RESISTO) sensors along with the advanced data processing and the decision making mechanisms offered by the RESISTO system. ***Although both the physical location and the network were already protected by the physical and cyber detectors of the provider, without the RESISTO platform, the threats would not even be detected, let alone neutralized.***

In the following paragraphs, each subcase story scenario will be described.

4.2.1. Sub Use case 1 – Storytelling

- In subcase 1, a UAV is supposed to overcome the physical security (i.e. secure fence protected by OTE's security system) and gain access to a network switch located inside a protected building. The UAV flies over the fence and approaches the building ignoring the physical security of the location, i.e. secure fence and building.
- As it approaches the building, it is detected by the airborne threat detector (radar) of RESISTO, which issues an airborne threat detection event.
- The drone connects wirelessly to the wireless network from the exterior of the building, gaining access to a network switch and initiating i.e. a DoS attack, which targets the switch.
- Having detected the potential airborne threat, the RESISTO system identifies the cyber assets in the location as "compromised" and initiates different cyber detectors of the provider's network in order them to detect potential threats in the cyber domain.
- Subsequently, the DoS attack is detected and a cyber attack event is issued by RESISTO.
- Finally, RESISTO suggests a prevention / mitigation action, i.e. deactivation of the switch and redirection of normal traffic.

4.2.2. Sub Use case 2 – Storytelling

- In subcase 2, an unauthorized person breaches the secure perimeter and tries to gain access to the interior of the building.
- It is detected by RESISTO's sensors for video and audio analytics and a perimeter breach event is issued. Moreover OTE's assets in the vicinity are identified as "compromised" by RESISTO.
- The unauthorized person enters the building, gains access to an unattended computer and installs dormant malware that will be activated at some point in the future.
- Meanwhile, the RESISTO system activates various cyber detectors of the provider's network that eventually detect the malware.
- A prevention/mitigation action is suggested and the malware is removed from the network.

Both subcases represent realistic cyber-physical attacks targeting critical telecommunication infrastructure and cannot be detected and mitigated efficiently by conventional security systems already used by telecom providers. Although separate physical and cyber security mechanisms may

be in place, ***the correlation between the events identified by RESISTO facilitates the efficient detection of the attack and enables its mitigation in its entirety.***

4.3. Analysis of the Use Case 1 Sub Use cases

In both sub use cases of Use Case 1, the relevant physical attacks will take place in OTE's premises in Athens. The indicative location is being shown in the following photo.

The basic concept of Use Case 1 is to consider that a physical threat or intrusion in a telecom operator's infrastructures can impose important threats in the cyber domain of a telecom network. By this way, combined cyber-physical threats can be emulated and tested. The physical threat can impose a cyber threat that is either activated directly or is meant to be activated after a period of time. Thus, the main challenge is the RESISTO platform to be able to make this correlation in the short term and activate the respective response and mitigation actions.



Figure 5: Attack location in OTE's premises, subcases 1 & 2

In the Use Case 1 scenarios, these combined cyber-physical threats can be triggered either by malicious artifacts or by an attacker as a person. For this reason, the Use Case 1 will be tested in 2 subcase scenarios. The concept exploits the newest trends in airborne attacks, as found in literature search or the web, where airborne platforms such as UAVs, drones or small aircrafts are used by attackers not only to make malicious actions (i.e. bombing) but also to create undesired electromagnetic signals that could affect a wireless infrastructure; wireless interference of this kind could impose viruses or similar cyber threats by having the drone wirelessly intruding and penetrating to the wireless network of an infrastructure. By that way, this subcase scenario would perfectly fit an urban environment, where drones or UAVs are used for commercial purposes: and thus, this kind of attack would be concealed behind an everyday activity that would not potentially create any kind of suspicion.

Regardless of the manner that the physical intrusion is caused (either by an airborne or impersonal attacks) the cyber threat imposed **can result in core network failures** and similar major consequences in the telecom network.

Thus, for this use case, the physical attack to OTE's premises will take place considering two cases: (a) using UAVs and b) an intruder by an attacker. Both physical attacks are considered to impose a major issue in the cyber domain of the telecom network (either directly on the spot or to be activated after a time period). All attacks are considered to take place in a protected critical building and assets (i.e. one of the company's main data located in the city of Athens, Greece).

This attack will have an immediate impact to telecommunication systems and the offered services. The attacks can result to core network's failure since certain main routers are been damaged through the imposed attack in the cyber domain.

The steps that will be followed in this use case are the following:

- **1st subcase:** A UAV (drone) is attacking OTE's facility (building). **Airborne threat detection** system will provide information about the path followed by the UAV and issues an intrusion event to the RESISTO platform.
- **2nd subcase:** An attacker / unauthorized person manages to enter OTE's facility (building). It is considered that the keycard access system is compromised, allowing the attacker to grant physical access to the building / or a stolen card is being used. An **Audio / Video Analytics system** (as perimeter protection complementary to the existing security system of the facility) is in operation for the detection/classification of this abnormal activity and issues an intrusion event to the RESISTO platform.
- **Objective of both intrusion subcases:** Both intrusions initiate an attack in the cyber domain, as described previously, that would potentially cause a core network failure, either directly on the spot or on a later time.
- **Malware (active or dormant)** can be loaded onto a switch initiating a DoS and / or to a server cluster. Thus, network traffic is being caused and / or specific systems of the core network are being attacked and potentially partially shut down.
- Having detected the potential physical threats, **the RESISTO platform** identifies the cyber assets as "compromised" and initiates different cyber detectors to detect potential threats in the cyber domain, upon the relevant correlation of the cyber-physical threat events. When the cyber attack (malware) is detected a cyber attack event is issued by RESISTO.
- Finally, RESISTO suggests prevention / mitigation actions and measures, i.e. deactivation of the switch and redirection of normal traffic (traffic rerouting) as well as a disaster recovery plan in order to meet the needs of service provision.

4.3.1. Telecom Assets affected

Based on the above analysis, the telecom **assets that are affected** by the cyber – physical attacks in both subcases of Use Case 1 are the following:

- Selected nodes serving core network traffic
- WiFi networks of the telecom building that are accessed (hacked) wirelessly by the UAV.
- Physical domain of the telecom operator: Building's access system and / or perimeter protection system that are breached by the attacker who tries to gain access to the interior

of the building. Other OTE's assets in the vicinity that can be identified as "compromised" by RESISTO.

- Cyber domain of the telecom network: datacenters with network monitoring / unattended computers / services and management operations, as a result of the (aerial or ground) attacks.

4.3.2. *RESISTO tools involved*

During the RESISTO piloting activities, the two scenarios of the Use Case 1 will be emulated through the implementation of specific RESISTO tools and processes as follows:

- The OTE's test-bed located in OTE premises in Athens, Greece will be used to emulate the telecom network affected by the imposed cyber-physical threats. For the simulation of traffic overload, a traffic generator will be used to flood the Core network test-bed. The OTE test-bed functionalities for the specific Use Case are depicted in section 4.3.5.
- The Airborne threat detection system will be provided by ICCS (radar / passive and active sensors, as described in Deliverables D4.1 [5] and D4.2 [6].
- The UAV platforms will be provided by ADITESS (as described in Deliverables D4.1 and D4.2.
- The Audio / Video Analytics system and algorithms as perimeter protection and surveillance systems will be provided by ADDITESS as well (as described in Deliverables D4.1 and D4.2)
- The RESISTO platform and especially the Short-Term Control Loop and its correlator engine

for both scenarios of Use Case 1. The exact details of the implementation (duration, span of DoS or network failure etc.) will be defined during the piloting framework of WP7.

4.3.3. *Impact of threats foreseen in Use Case 1*

The expected impact involves the following aspects:

Operational: Risk of connectivity loss, denial of service and service delivery failure which would also potentially affect PPDR / emergency services as well, if the imposed cyber-attacks are not detected. The direct physical attacks affect the existing security systems (access or entrance breaches) which would need immediate attention and change of protocols.

Technical: Network connectivity failure / data corruption / telephony (fixed, mobile) & internet services (wired / wireless) at risk depending on the severity of the imposed cyber-attacks consequences. In case of core network failure (severe damage), services could be restored through traffic rerouting or secondary resilience centers until the problems are solved. However, this may also affect the networks in the surrounding areas near OTE's premises, especially when other critical infrastructures are in the vicinity.

Economic: Apart from the damage in building security, large economic impact would be created due to the loss (partially or wholly) of network functionalities for the telecom provider since SLAs are at risk due to service delivery failure.

Societal: If the imposed cyber-attacks remain undetected, this would cause severe problems in the wider telecom network and the customers' telecom services (telephony, fixed or mobile & internet services wired or wireless or WLANs / private networks).

In case that the correlation between the combined cyber-physical threats remains undetected and mitigated, this would cause constantly impacts of the above kinds in the future that would need much more time and costs before they are finally identified and confronted, since the core of their creation would have remained undetected.

4.3.4. Other consequences - Interconnected Critical infrastructures

Use Case 1 (and its two subcases) is meant to demonstrate attacks, threats and vulnerabilities that may affect the existing framework of the telecom CIs and the added value of the RESISTO platform in dealing with more sophisticated threats, especially the “combined cyber-physical” ones. Neither of the two Use Case 1 scenarios directly foresees cascading effects and interdependencies with other critical infrastructures in the vicinity.

However, specific experiments based on the proposed Use Case can be carried out in order to assess the potential effects on interconnected critical infrastructures using specific RESISTO tools (such as CISIAPro) to model the threat propagation effects. As indicative example, the combined cyber-physical threats in Use Case 1 could affect the internet connectivity of financial and banking services or the telemetry network of power grids, since telecom networks (fibers, WLANs, cables etc.) are crucial to the operation of other critical infrastructures.

4.3.5. Deployment Topology Example – Test-bed setup

For the implementation of this scenario two of OTE’s labs / test-beds will be used; the Core lab and the Cloud lab. The two labs are closely located and interconnected, but a separate common network domain will be implemented between the two labs for running the two scenarios of the “**physical & cyber-attacks in telecom sites causing DoS or core network failure**” Use Case 1.

OTE’s Core Lab main responsibilities are the provision of a reliable environment for testing and measurement of OTE’s new services and products, with regard to the Core Network. The Core Lab is equipped with the appropriate network infrastructure in order to simulate the actual OTE live core network and the corresponded services. OTE’s Core Lab retains a great range of routers (from small- and medium-size to carrier routers) and switches which can be used for the implementation of complex network topologies and scenarios. Such scenarios include inter-alia: Metro Ethernet services over MPLS infrastructure; MPLS based VPNs, and QoS and Traffic Engineering test-beds.

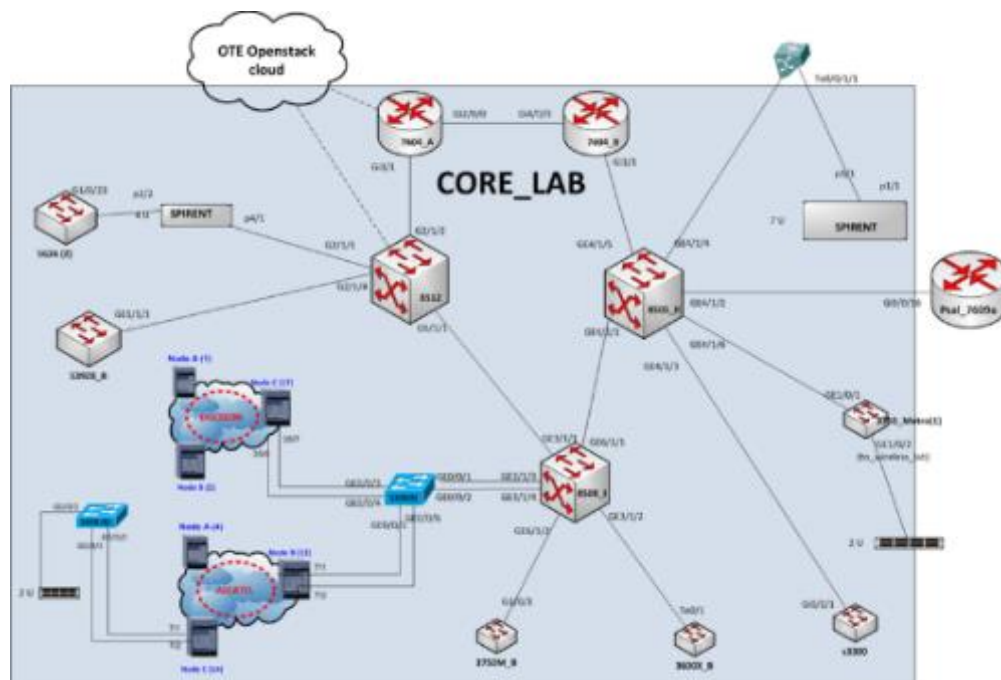


Figure 6: High level OTE Core Lab – Cloud lab topology.

Furthermore, Ethernet-over-SDH services are implemented and tested in that Lab. Additionally, Lab's network interconnection to other OTE's labs (such as Access Lab and VoIP Lab) provide the opportunity to test various scenarios and network services (i.e.: Fast Internet, VoIP, IPTV, IMS). Finally, the Lab is equipped with a state-of-the-art traffic generator and analysis tool (Spirent Test Center) in order to "conduct" the necessary experiments and testing for equipment, network topologies and proposed service scenarios.

Core lab's interfaces are mainly 10G and 1G both fiber and copper. Among others, there is a major commercial traffic generator which is the Spirent test Center and has direct/physical connection to other components with cable (fiber for data and copper for management). All metro Ethernet Switches (distributors) are Huawei connected with Layer 2 and L3 VPN connections to distant sites while locally are connected through cable (both fiber and copper). All BNG Routers are CISCO and are considered core network. They have connections to other components with cable (fiber and copper) and indirect connections to other components located in other sites through Layer 2 and L3 VPN connections. Regarding security the lab has firewalls enabled through ACLs (Access Control Lists).

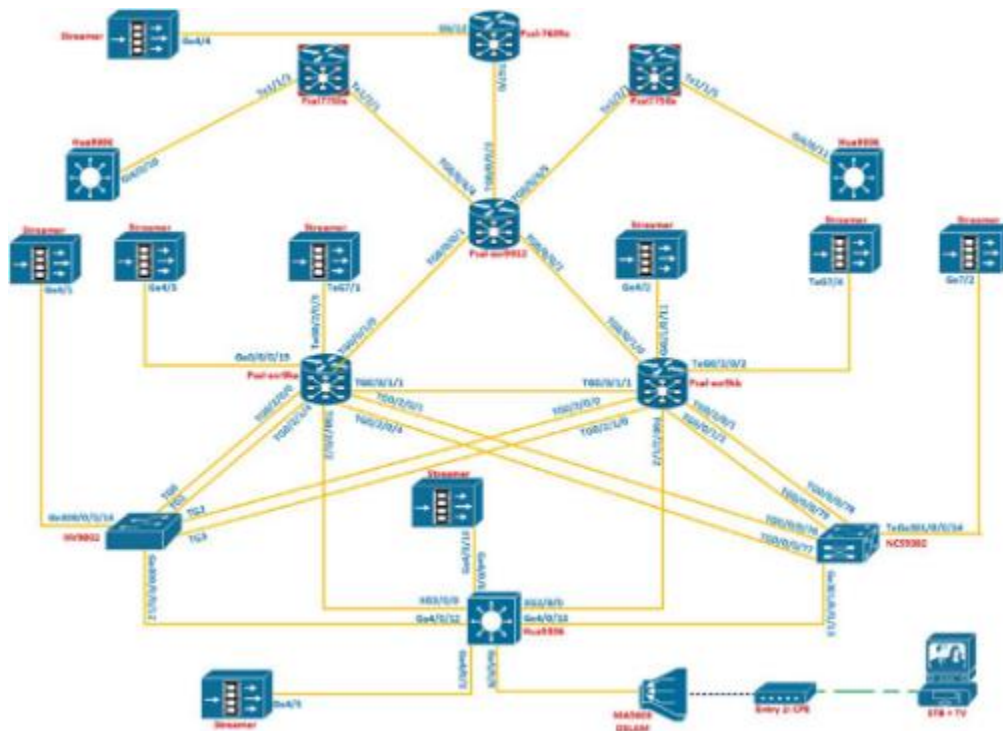


Figure 7: RESISTO slice Core Lab Description

The OpenStack test-bed can be customized or upgraded based on project's specific requirements. The test-bed can be utilized for new technologies experimentation, either for Proof of Concept (PoC) or for field trials. The cloud setup is currently based on Openstack Queens (Ubuntu Server 16.04 LTS) and can be made available for providing compute and storage resources directly, or for hosting relevant services for the project as e.g. a CI/CD platform, monitoring, provisioning or even network attack tools. The setup can be split into one or more controller and compute nodes of various sizes to match project's needs, either in bare metal or virtualized form. The whole infrastructure now contains mostly 10GBps fiber/copper interconnections.

The whole setup is behind a Cisco PIX 515 firewall, which provides NAT and which is forwarded to a Gateway server, where a VPN has been set up, which once connected to, provides access to the other Openstack hosts and the running VMs as well. Capability of federation with other external test-beds can also be provided, depending on the requirements and a limited range of public IPs can be made available as well.

4.4. Actors and detection tools involved

In the context of this Use Case, the below roles are identified and described in the following table:

Actor	Role	Description
Hostile UAV / aerial platforms	Intruder: physical/cyber-attack generator (1 st subcase scenario)	A hostile UAV performs perimeter breach - physical intrusion to a physically protected telecom building, gaining access to the operator's wireless network, performing cyberattacks disrupting services and creating network failures.
Attacker/Hacker	Intruder: physical/cyber-attack generator (2 nd subcase scenario)	An unauthorized person, exploits vulnerabilities in the physical security system to perform cyber attacks on network components, software and middleware, in order to gain access to resources or to change the intended use of the systems.
RESISTO Airborne threat detection system	Technical: detector of airborne threats i.e. small aircrafts and UAVs (1 st subcase scenario, ICCS)	Active and passive sensors (i.e. radar and acoustic ones) to detect direction path of airborne threats. This is a physical threat detection module that provides potential intrusion events to the RESISTO platform.
RESISTO Sensors for audio and video analytics & monitoring tools	Technical: detector of intruders and perimeter breaching (2 nd subcase scenario, ADI)	Video/audio analytics based on pattern recognition algorithms (uses existing CCTVs or deploys new video and audio sensors). This is a physical threat detection module that provides potential intrusion events to the RESISTO platform.
Network/system specialist/administrator	Technical: network and system operator (configures the test-bed that emulates the provider's network-OTE)	Telecom provider's personnel that configures the test-bed for the various test scenarios.
Information & physical security platform-The RESISTO system	Technical: cyber and physical attack monitoring, detection, response and mitigation system	Monitors the overall functionality of the physical and cyber security, receives threat events, uses specific tools and techniques to identify vulnerabilities, erroneous configurations or intrusion attempts and responds to threats.
Service Provider	Business: communication service provider (OTE)	The telecom provider (OTE) that provides communication services and consumes network resources
Customer (hypothetical)	Business: service consumer	An entity that consumes one or more telecommunication services, affected by the DoS.

Table 2 – Identified actors in the “physical & cyber-attacks in telecom sites” Use Case 1

Sensor	Role	Description
Microphone	Acquisition of acoustic data	Part of perimeter protection system. Audio signals will be processed by the audio analytics component
Camera (CCTV)	Acquisition of video data	Part of the perimeter protection system. Video signals will be processed by the video analytics component.
Active and passive radar (electromagnetic and acoustic)	Acquisition and processing of electromagnetic and acoustic data	RESISTO Airborne threat detection system, signal processing and extraction of potential intrusion events (i.e. hostile UAVs).

Table 3 – Detection Sensors that will be used in Use Case 1

4.5. RESISTO response and Added Value

The main objective of the Use Case 1 (both subcases scenarios) is to enhance the resilience of the existing communication infrastructures towards both the domains of physical security and cyber protection. The focus is to advance the processes of detection and response and thus to result in new additional measures for mitigation and prevention, confronting threats that would have not been identified without the RESISTO system.

To this respect, modern sophisticated by also realistic cyber-physical attacks against the existing critical telecommunication infrastructures have been envisioned so that by correlating the interdependencies between the two domains to proof that it would be possible to detect the consequences of these combined threats and attacks in advance or in short response time and to use joint counter-measures.

However, it should be pointed out that these kinds of threats are not possible to be detected, correlated and identified by the conventional security systems already used by telecom providers; instead these threats would be identified separately as only physical or only cyber ones respectively. Thus, RESISTO performs the correlation between the two domains (Cyber+Phy), a feature not implemented by conventional security systems.

This feature is also enabled by additional sensors and algorithm systems introduced by RESISTO facilitating an effective detection of the attacks along with the RESISTO decision making mechanisms enabling their response and mitigation seen as a combination of threats.

The detection through these modern tools and sensors that are adjusted for RESISTO platform is hardly taking place so far to conventional security systems and thus it can act complementary to them. Of course these more sophisticated detection tools follow the more sophisticated types of attacks that are envisioned as current and future trends in attacking telecom CIs (imposed cyber attacks through “wireless hacking” by drones/UAVs or other physical intruders or even combined with attack on cloud data services etc.).

4.5.1. RESISTO Short Term response

Based on the above the RESISTO Short Term Response consists of the following:

- Detection: Having received the alert events by the sensors (for the airborne and intruder threats), the RESISTO platform issues the relevant physical threat detection events.
- Response: Based on its correlation engines rules, the RESISTO system, in both subcase scenarios, identifies the cyber assets in the location as “compromised” and initiates various cyber detectors

- of the provider's network to detect the cyber malware and generally potential threats in the cyber domain. As soon as the cyber attack is detected, a cyber attack event is issued by RESISTO.
- Response: Countermeasures are potentially triggered by the RESISTO platform, i.e. providing emergency signals or notifying the security operation center of the telecom provider of the telecom operator or notifying the management and decision making mechanisms.
 - Prevention / Mitigation: RESISTO suggests short term (or immediate) prevention / mitigation action, i.e. deactivation of the switch and redirection of normal traffic so that the malware is removed from the network. RESISTO ensures communication continuity in the end.

4.5.2. RESISTO Long Term response

The outcomes and the implementation results of both subcase scenarios of Use Case 1 will be used as input for an iteration of the LTCL. The proposed, by the tool, mitigation and prevention measures could include best practices and/or creation of redundancy / resilience / disaster centers in respect to the assets affected by the cyber – physical threats tackled within Use Case 1.

4.5.3. Innovation addressed

Based on all the above analysis, it can be highlighted that through RESISTO the following innovations are addressed with the implementation of Use Case 1:

- New types of security incidents (Cyber+Phy, combined) have been identified and will be implemented through the Use Case 1 scenarios' piloting. Use Case 1 attempts to exploit new trends on various kinds of attacks discussed in the literature.
- New, complementary to the conventional security systems, physical threats detectors are meant to be implemented; attempting to provide a suite of additional tools for detection and prevention of combined threats. Thus, new technologies for physical threats detection/protection/response may emerge from the use of the specific sensing tools.
- New challenges are posed in terms of the technological evolution, since it is expected that new innovative processing, measurement and analysis methods may be derived in order to efficiently process and analyze the data acquired during the piloting activities.
- Mindset evolution: the combination of the above may lead to new procedures and/or changes in the organization's (telecom operator's) security approach, while new standards in physical & cyber security may emerge.

4.5.4. Suggested KPIs for Use Case 1 validation

Apart from the contribution of this Use Case to the overall RESISTO implementation statistical data that will be gathered, the following metrics / KPIs are suggested to be measured:

KPI number	Title / Description
K1	Number of detected physical threats
K2	Number of detected cyber threats
K3	Detection probability
K4	Time to detection
K5	Average decision-making time
K6	Average mitigation time
K7	Human intervention/Automated response

Table 4 – Suggested KPIs to be measured during the pilot activities of Use Case 1

5. USE CASE 2: TERRORIST ATTACK AND NATURAL HAZARDS CAUSING NETWORK FAILURE AND TELECOMMUNICATION CONGESTION

5.1. Introduction and Background

Mobile communications are rapidly evolving into complex systems both in terms of the network architecture and the types of connected devices. This increasing complexity naturally results in an increasing number of security threats. It is well known that these networks support a large number of services that go beyond traditional voice and short messaging traffic to include high bandwidth data communications. Despite the tremendous capacity and system enhancements implemented by LTE, cellular networks are in general vulnerable to security attacks [9].

As all critical infrastructures, telecom assets and facilities are vulnerable to malicious attacks intending their destruction as well as to natural disasters like earthquakes and severe weather conditions, where significant direct and indirect consequences emerge caused by the effects that loss functionality might have on large communities.

The cost of lost connectivity obviously varies with the time and duration of the outage, but the temporal pattern may be complex and may differ by sector. Dynes et al. (2007) [10], in their study of Inter-net outages affecting single firms, found that firms in some sectors could continue operation for days before the outage would be fully identified and begin to have a material effect. Furthermore, in terrorist risk assessment, the main challenge is to estimate the probability of a terrorist attack. Some specialists believe that probabilistic measure is not adequate for the terrorist risk assessment since terrorist attack is not a stochastic event but a deliberate action based on the preparation made by terrorists regarding their skills and capabilities and the system's vulnerabilities.

Thus, since both these kinds of actions (deliberate terrorist attacks and natural disasters) are practically unpredicted in their exact time and place details, the important aspect is to be able to react and response as soon as possible, in order to save time and resources. Thus, in the framework of Use Case 2, the RESISTO system will be used, through its detection, correlation and analysis features, to provide a faster response in these cases of hazards, in respect to the conventional security systems and response and mitigation actions of the existing systems.

5.2. Overall description of the Use Case 2 sub Use Cases

In this Use Case, a physical attack (sub-scenario 1) or a natural disaster (sub-scenario 2) affects severely the telecom provider's network. The difference with Use Case 1, is that this type of scenarios can be classified as physical events that greatly affect the cyber domain, for example by degrading throughput. Even in such cases, the RESISTO system can detect the related events using data from a diversity of sensors and through complex processing, identify and assess potential cascading effects, suggesting appropriate mitigation actions.

The Use Case 2 will again be implemented by OTE as the main telecom operator with the assistance of modern detection tools offered by other consortium partners (ICCS, TEI and ADI).

Compared to Use Case 1 and depending on the case examined, additional sensing and processing tools may be used. Unlike the Use Case 1, where different physical intrusions enable similar types of cyber threats within a telecom operator's system, in Use Case 2, physical threats may result in network service unavailability, but with different causes (either man-made or natural disaster), that may require different mitigation measures. To this respect, the two sub-scenarios of Use Case 2 will be described separately in the following:

5.2.1. Sub Use Case 1 - Storytelling: Terrorist Attack in telecom asset cause severe network failure

In sub-scenario 1, a third party uses a drone (UAV) to attack a telecom provider's facility.

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

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

Without the RESISTO system, the telecom provider may become aware of the situation when a series of events have happened, leaving very short response time or when a network or service failure is unavoidable, at least for a short time. Since there is no other information available, all the potential causes must be thoroughly investigated in order to identify the real one and suggest a suitable mitigation action, resulting in increased costs in both time and resources. Even if more information was available, a mechanism to correlate all this different types of information in order to efficiently identify and mitigate the threats, would still be necessary. The RESISTO system offers both the increased information by integrating a diversity of sensors/detectors and the correlation mechanism to efficiently detect and mitigate such threats.

5.2.1.1. Analysis of the Use Case 2: Sub Use Case 1

Many scenarios have been carried out by public or private agents (LEAs, Civil Protection Public Authorities, major CI operators etc.) in case of major terrorists' attacks in metropolitan centers and highly urban areas. Considering that these terrorist events include bombing or similar sabotage actions causing human casualties and hitting important civil targets (i.e. representative buildings of political and economic life or with symbolic value such as the Parliament, Central Banks main ports, metro or athletic centers etc.) even with little or no warning, response scenarios and counter measures have already been planned involving even military reactions.

The complexity, scope, and potential consequences of these terrorist threats require that there be a rapid and decisive level of coordination among law enforcement, criminal investigation, protective activities, emergency management functions, and technical expertise across all levels of

administration, which are struggling to maintain consistent prioritized communications. Generally, response actions in these major cases are being coordinated centrally by the State.

As far as communications assets are involved, these might have or have not been destroyed due to these major incidents. However, congestions in Internet, Public Switched Telephone Network (PSTN), private / public LANs are likely to be experienced within a wider area surrounding the attacks theater and rapid surges that cellular infrastructures are inundated with need to be considered, as people seek information on the attacks, trying to call relatives, receive calls, and send pictures or videos from their mobile devices including through the use of WiFi networks. Immediately following the incident, news media reports would likely create alarm among the general population and also spur a sharp increase in cellular communications. Generally, nationwide broadband communications infrastructure, broadcast radio, and television (public and private) would be remain operational and fully functional, despite potential damages.

To anticipate devastating scenarios of the above kinds but also to tackle potential network failures caused by other reasons (i.e. network damages or design faults and losses) the telecom providers have already foreseen and already launched resilience or even disaster centers acting as already existing redundant solutions to the core network management.

Depending on each country's geographical topology mostly dictating the backhaul paths, in the most usual cases, Network Management Centers (NMC) are located in the operator's headquarters in i.e. the capital city. Secondary NMCs with the same functionalities are already established in other metropolitan cities far from the main one (supposing i.e. Athens and Thessaloniki for Greece).

Thus, if, due to a major incident, the main NMC in the capital goes down, the network management is **automatically redirected** to the second NMC that takes over immediately acting as resilience node, so that the nationwide backhaul network is maintained in its majority.

However, cases where terrorism or other incidents occur in a lesser degree without causing devastating consequences as above, although affecting severely certain telecom assets that support or are part of the backhaul network, have not been given adequate attention so far and their protection and emergency response lies directly on the telecom operators responsibility (and not transferred to the civil protection and response of public agencies). In these cases, the RESISTO system can fill-in the security gaps as examined in the present sub-scenario.

Let us consider, certain telecom assets that are part or support the backhaul network, but they are not located within metropolitan or large urban environments, as in the following figure.

On the backhaul path, sometimes functioning as connecting junctions, there are telecom assets that support other urban areas or rural areas. These assets are not necessarily placed in urban locations (building rooftops); instead they may be located in mountains near urban areas or serially connected to each other (route tails). These can be antenna parks involving antenna pillars each one equipped with antennas and wireless devices supporting almost all services i.e. in their majority cellular services with base stations and wireless links for mobile and fixed telephony wireless backhaul. Furthermore, in certain locations, the same antenna pillars are used for broadcast (i.e. DIGEA) and radio transmissions purposes simultaneously.



Figure 8: Example location of a telecom asset in remote sub-urban areas⁵

In certain such cases, the telecom operators have also foreseen redundant solutions at the local level at the antenna parks. For example, in certain antenna parks for wireless backhaul, fiber optics terminals are also foreseen as fallback to the wireless connection; but this is not always the case in all pillars especially in remote and rural areas considering also the lack of automated rerouting. Moreover, UPS and battery banks are foreseen so that, if the central power supply is interrupted, the service remains in operation at least for a certain time. However, if the pillar is destroyed or severely damaged given a certain reason, all backup and redundant solutions are destroyed as well.

According to the specific sub-scenario 1, a hostile UAV destroys an antenna pillar that supports the backhaul network as described previously. This sub-scenario exploits the current war attacking trends, as seen from recent conflicts (i.e. in Syria), where UAVs or larger drones are used as unmanned attackers with payload meant for surgical bombing or limited but accurate attacks. This creates a precedent on that current and future terrorists may attack with drones / UAVs, or drone swarms carrying explosives.

In the present case, the antenna pillar is destroyed by the hostile UAV. Partially or total damage of the facility will result in interruption of services and since this asset supports the wireless backhaul, the telecom service goes down, especially the mobile communications. Thus, network failure and a general DoS at the broader vicinity surrounding the antenna park takes place and the respective users experience total lack of service or telecommunication congestion. Even more, in case that this antenna pillar is a part of a serial sequence of similar assets within the backhaul path, the network failure caused by the damaged antenna pillar is propagated.

In major incidents like the terrorists' attacks in urban environments described earlier, immediate information on what happened is given both by the media as well as crowd sourcing and first responders. However, in remote antenna parks, CCTV or other visual inspection solutions are not usually in place. The provider's NMC identifies the network failure and the DoS while it acknowledges that a set of antennas is not operational (i.e. transmitting) for some reason. Thus, the telecom provider is not directly aware of the exact situation and what was the cause of the DoS and the

⁵<https://www.kathimerini.gr/1051127/article/oikonomia/ellhnikh-oikonomia/strofh-twn-ependytnw-se-thlepikoinwniakes-ypodomes>

network failure. The NMC attempts to reactivate the antennas through software means however, the lack of available information results in keeping the problem persistent and more thorough investigation to be needed, which is time and resources consuming in order to provide immediate response as early as possible. LEAs of course will proceed the incident's scene to investigate the causes, which will impose more time before restorations begun. In the end, technical echelons must inspect the location for final mitigation actions.

The RESISTO contribution in this sub-scenario consists of the following:

- Direct detection and identification of the cause of the attack (hostile drone) through the RESISTO airborne threat detection system
- Timely inspection of the devastated area as friendly drones are available to establish a remote surveillance system (through the friendly UAV platform with surveillance payload that is launched by RESISTO)
- Correlation of both events (the cause of the attack and the network failure) in time
- Localization and selection of suitable response and mitigation actions in a prioritized manner for a more effective decision making.

As response actions RESISTO could suggest the following: appropriate redirection of the network traffic (i.e. mobile services), to other base stations nearby or activation of auxiliary antennas/pillars. Replacement of the antenna pillar may seem the optimum final solution however, depending on the severity of the problem and the critical level of the specific antenna pillar to the backhaul path, the replacement may not be performed immediately, but at a time convenient for the telecom provider in terms of cost and resources, especially when the rest of the response actions successfully tackled the network failure. In case of severe network failures, where the specific antenna park seems to be critical for the backhaul path, mitigation and protection actions in the long term, could include replacement or redundant solutions for the whole park.

5.2.1.2. Telecom assets affected

Based on the above analysis, the telecom **assets that are affected** within the first sub Use Case of Use Case 2 are the following:

- 1) Wireless assets (antennas, pillars and parks) in remote locations and the networks that they support (backhaul paths and consumer cellular networks). Telecom sites for backhaul links, 3G/4G towers, antennas, sites for broadcast and radio transmissions.
- 2) Physical domain of the telecom assets: fencing and / or perimeter protection system that are bypassed and breached by the airborne attack.
- 3) Telecom network: network failure and especially for mobile communications and potential congestion in the vicinity. Selected nodes serving core network traffic.

5.2.1.3. RESISTO tools involved

During the RESISTO piloting activities, the sub-scenario 1 of the Use Case 2 will be emulated with the implementation of specific RESISTO tools and processes as follows:

- The OTE's test-bed located in OTE premises in Athens, Greece will be used to emulate the telecom network affected by the terrorist attack in a similar way described previously in Use Case 1. The OTE test-bed functionalities for the specific Use Case are depicted in Section 4.3.5. Furthermore, OTE possesses various antenna parks in various urban and remote locations, so their specific technical characteristics can be emulated during the relevant implementation.
- The Airborne threat detection system will be provided by ICCS (radar / passive and active sensors, as described in Deliverables D4.1 [5] and D4.2 [6].

- The UAV platforms will be provided by ADITESS (as described in Deliverables D4.1 and D4.2). Important notice: Herein these UAV platforms would have a two-fold role; to provide both the hostile UAV (attacker) and the inspection UAV with surveillance payload (friendly)
- The RESISTO platform and especially the Short-Term Control Loop and its correlator engine

The exact details of the implementation (duration, span of DoS or network failure etc.) will be defined during the piloting in the framework of WP7.

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

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

The various steps of this sub-scenario are the following:

- A natural disaster, i.e. very severe weather conditions causing twisters and hurricanes or an earthquake, damages telecom assets and facilities located in sub-urban or rural, remote areas. The telecom assets include antenna pillars and buildings containing critical routing circuits (switches, routers etc.) supporting part of the backhaul network. A network failure is caused by the damage on the pillar and the building, leading to a telecommunication congestion in the mobile network.
- The RESISTO system receives the congestion events from the provider's monitoring tools, along with an earthquake or natural disaster event from the RESISTO natural events sensing platforms (weather and seismic sensing).
- RESISTO responds by issuing a damage inspection order to the RESISTO UAV-based surveillance sensor system.
- The RESISTO "friendly" UAV takes-off and initiates a damage inspection procedure using onboard cameras, inspecting the provider's premises affected by the natural disaster. The UAV sends an extensive building and asset damage event after detecting extensive damage at the provider's telecom assets.
- The RESISTO system identifies the damage, since it contains a number of critical network assets (switches, routers etc), as the potential cause of the congestion, along with the increased user traffic following the natural disaster occurrence.
- Correlating the loss of specific network resources with the congestion events, the RESISTO platform suggests suitable mitigation actions to be imposed as early as possible, i.e. traffic redirection and or activation of auxiliary network resources.

Without the RESISTO system, the increased user traffic would be identified as the primary cause of the congestion. Even though a mitigation action could be initiated, it wouldn't be the optimal one, since the information on the loss of network resources caused by the earthquake wouldn't be correlated with the congestion events without human intervention. Even in this case, the overall response of the network and the application of the mitigation strategy would be significantly slower compared to the case where the RESISTO system is used to automate and facilitate the whole procedure.

5.2.2.1. Analysis of the Use Case 2: sub Use Case 2

This sub-scenario seems a variation of the previous sub-scenario 1 since again telecom assets such as antenna pillars are affected. However, unlike the sub-scenario 1 where the cause of the destruction was a man-made malicious action, herein the cause is a natural disaster. Although in deliberate man-

made attacks there is enough room for prevention and mitigation, the severity of natural disasters cannot be predicted adequately.

Furthermore, in sub-scenario 2 it is assumed again that the natural disaster occurs in sub-urban or rural and remote areas and that they present a moderate level of severity. That is because, in case that this kind of events occur in metropolitan or large urban environments they will be felt instantly and in case of large severity they will trigger the involvement of public agencies as first responders and LEAs. In other words, they will have the outcomes that were described in the previous sub-scenario 1 for major terrorist incidents in capital cities. This way, the RESISTO impact would have been overlooked. Finally, all the technical features presented earlier in the previous sub-scenario 1 concerning the antenna pillars are still valid, while the telecom assets affected herein include also building facilities.

A telecommunication congestion usually occurs when a huge traffic is held in the whole or part of a telecom network. This can be the consequence of a network failure that leads to overload or, in the most usual cases when a sharp increase in mobile phone usage takes place. The latter is seen either regularly in particular events (i.e. New Year's Eve) or suddenly following major incidents resulting in major damages (i.e. earthquakes) where communications infrastructures are seeing rapid surges in usage as people seek information or are trying to call relatives. In regular events the operators, having known the problem already, can assign more capacity for this specific short period of time while, the users recently focus more on texting (sms, viber etc.) and thus congestion is hardly experienced any more. However, following major incidents of natural disasters, congestion still remains unpredicted with practically no immediate solution.

Following major disaster events of broad impact, cellular communications could spike within minutes, initially in the proximity to the incidents and then to outer regions, stressing local telecommunications carriers' network capacity. As users would experience prolonged delays in completing voice calls, critical public and private national security and emergency communications would be affected as well during this period of wireless congestion. Depending on the events, especially the cellular communications as well as the inbound enhanced emergency lines could be saturated with calls from citizens trying to reach relatives, get information or requiring emergency assistance trying to reach first responders. In general, a low percentage or lack of service is experienced for quite some time following the severe incident, which is slowly restored in the next hours.

However, telecommunication congestion can also happen directly after natural disasters with even low severity, depending either on the impact they cause or if the network behind is affected. For example, earthquakes with rather low magnitudes can cause telecommunication congestion as this did happen in the recent earthquake in Athens (19 July 2019).

Greece is a seismic territory while earthquakes with maximum 6 – 6,5 magnitude have been experienced historically. Thus, countermeasures have been imposed over the years in buildings and for public safety and protection. The recent earthquake in July 2019 in Athens had a 5,1 magnitude, thus it was rather moderate in intensity and no damages in building or human casualties were reported. However, the earthquake's epicenter was very near Athens and since Athens is the largest metropolitan city in Greece with residents of around half the Greek population, both the earthquake was strongly felt and almost immediately a telecommunication congestion took place lasting over an hour resulting in service loss. During that earthquake, communications assets have not been destroyed, but telecom network was inundated; everybody tried to call relatives and friends, to seek information and send pictures or videos from their mobile phones, so that a huge surge in the system

occurred, while both fixed telephony and mobile services were down as well as texting. The telecom network was congested as people were seeking information from both mobile and WiFi networks.

From the telecom's operator point of view, in the following diagrams the increase in network traffic as well as the network drop calls rate just after the earthquake are depicted:

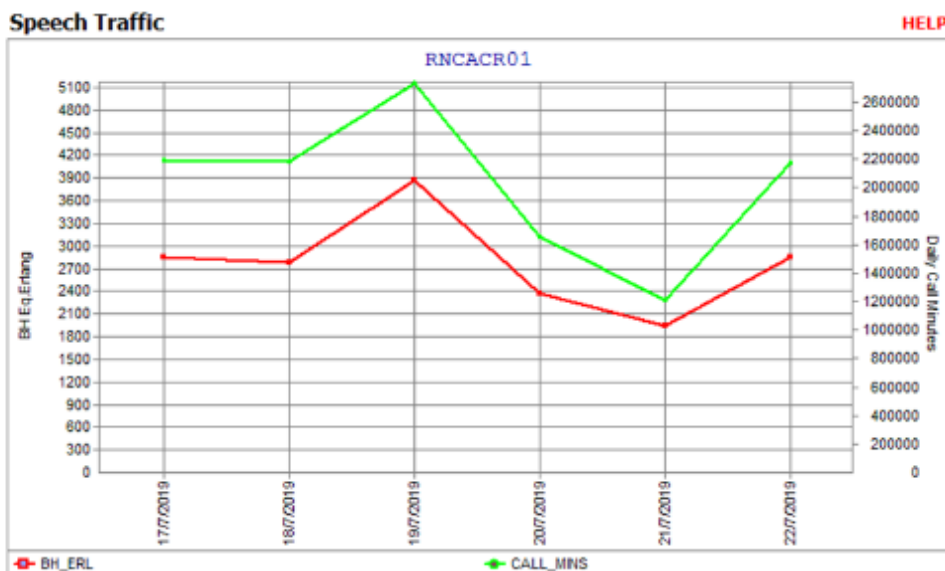


Figure 9: Traffic at 19/7/2019 during earthquake

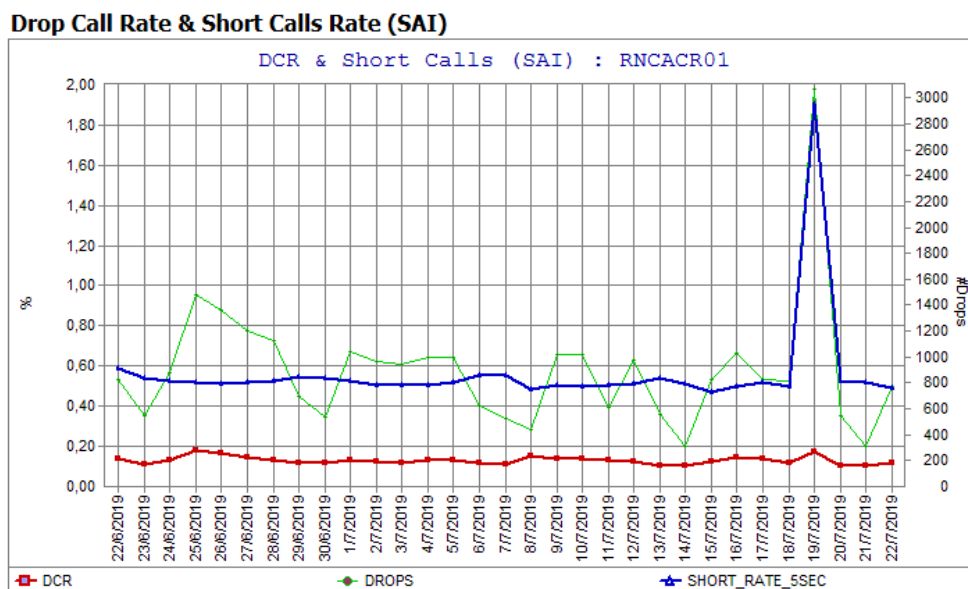


Figure 10: Drop Call & short Calls Rate

It is obvious that in order to keep an adequate quality of service, traffic rerouting was necessary as well as disaster recovery mechanisms needed to be enabled.

The above telecom related results from the earthquake and the post seismic sequence that followed, provided a perfect opportunity to understand the congestion consequences that an earthquake can cause to the performance of telecom infrastructure systems, and to analyze issues affecting the post-earthquake assessment and management of telecom networks. By this way, the above network results during the July 5,1 earthquake in Athens will be used to feed the OTE's test-bed when emulating the present sub-scenario 2.

Apart from the earthquakes, other natural disasters i.e. hurricanes or severe weather may have similar telecommunication congestion outcomes as those described above for the earthquake.

On the other hand, telecommunication congestion can also occur when whole or part of the network is down i.e. due to incurred damages. In this sense, a natural disaster (i.e. earthquake or very strong wind or severe weather conditions), may not completely destroy a telecom asset like an antenna pillar but it can incur damages that result in lower quality of service. For example, severe weather or earthquake may throw away, disturb or move the directional axis of the antennas mounted upon the pillar resulting in changes of main lobe directivity or complete lack of the specific antenna upon the pillar. Moreover, these disasters may cut or move redundant circuits i.e. fiber optics or damage the small cages with routing circuits just below.

The above can be outcomes of natural disasters with even moderate severity; not necessarily causing large-scale catastrophes. Moreover, the natural disasters may cause both types of events (both damages in network assets or services and sharp surges in the telecom services buy the users) to result in telecommunication congestion. However, during large-scale natural disasters with wide impact, the congestion caused by the huge number users' calls is more dominant and thus could not easily indicate the RESISTO added value. Thus, the above are the main rationale behind the description of the specific sub-scenario 2.

Based on all the above analysis, the sub-scenario 2 foresees the following:

It is assumed that a natural disaster (i.e. very severe weather causing twisters and hurricanes or even an earthquake) damages telecom assets (antenna pillar and accompanying small building containing routing circuits, supporting part of the backhaul network. These telecom assets are placed in a remote area in the country where small cities and urban areas are in the vicinity and are supported by this telecom asset.

It is also considered that the natural disaster is of a moderate kind, i.e. a local wind twister with large speed (but with no devastating effects) or an earthquake of a magnitude around 5. It is also assumed that the telecom asset and the affected area are near the epicenter of the natural events in both cases. Thus, the scenario assumes that no physical destruction to the communications infrastructure happens, however, damages at this asset are caused by the natural disaster leading to network failure and a subsequent telecommunication congestion in the mobile network at the local area, potentially also affecting part of the backhaul leading to lack of broad communications. Broadcasting also (TV or radio) may be affected as well.

Although, immediately after the natural disaster event, local users inundate the cellular network with calls and mobile phone use; however despite causing lower quality service in a local level, this cannot be regarded as the main cause of the telecommunication congestion noticed by the Network Management Center (NMC) of the telecom provider. But, the NMC cannot distinguish the real cause and, since the damages at the telecom assets are not known yet; the NMC is informed that the antenna pillar is not transmitting or suddenly turns into lower quality of service (as this was described in the previous sub-scenario 1, in case that RESISTO is not present). On a wider area, although the Internet, Public Switched Telephone Network (PSTN), and private / public networks

experience the effects of the congestion at the place of the disaster, they remain partially operational.

The RESISTO system interfaces with specific natural events sensing platforms such as weather and seismic / earthquake sensing ones. Thus, RESISTO is aware of the natural disaster and simultaneously receives the congestion events from the provider's NMC and monitoring tools and responds by "ordering" a "friendly" UAV to make a damage inspection at the telecom assets in the area that the disaster and congestion occurred. The friendly UAV surveils the area and informs regarding the extensive damages at the telecom asset (antenna pillar and small building underneath). RESISTO identifies the affected critical network assets (antennas, switches, routers etc.) as the potential cause of the congestion, and correlating the loss of the network resources with the congestion events, RESISTO suggests suitable mitigation actions to be imposed as early as possible, i.e. traffic redirection and or activation of auxiliary network resources.

Thus, in this sub-scenario, RESISTO provides additional information to the telecom provider for the primary cause of the congestion and in less time than through conventional, human intervened, responses.

The RESISTO contribution in this sub Use Case consists of the following:

- Direct detection and identification of the cause of the congestion (network failure through damaged telecom circuits and antennas) through the RESISTO natural events sensing platforms
- Timely inspection of the affected area as friendly drones are available to establish a remote surveillance system (through the friendly UAV platform with surveillance payload that is launched by RESISTO)
- Correlation of both events (the cause of the congestion and the network failure) in time (and in less time than without the RESISTO system)
- Mapping and suggestion of suitable response and mitigation actions for a more effective decision making (i.e. traffic redirection and or activation of auxiliary network resources or as described in the previous sub-scenario 1).

5.2.2.2. Telecom Assets Affected

Based on the above analysis, the telecom **assets that are affected** within the second sub Use Case of Use Case 2 are the following:

- 1) Wireless assets (antenna pillars) in sub-urban locations, their accompanying buildings with routing circuits (buildings and facilities that are affected by the natural disasters and are partly or wholly damaged but not fully destroyed) and the networks that they support (backhaul paths and consumer cellular networks), and sites for broadcast and radio transmissions.
- 2) Telecom network: network failure and DoS especially for mobile communications, telecommunication congestion in the local area of impact.

5.2.2.3. RESISTO tools involved

During the RESISTO piloting activities, the sub-scenario 2 of the Use Case 2 will be executed using specific RESISTO tools and processes as follows:

- The OTE's test-bed located in OTE premises in Athens, Greece will be used to emulate the telecom network affected by the natural disasters as described in the previous Section 4.3.5. Furthermore, OTE possesses various antenna parks in various urban and remote locations, so their specific technical characteristics can be emulated during the piloting activities. Since for the specific Use Case scenario, a natural disaster of moderate magnitude will take place, for example, similar to the earthquake that occurred in Athens in July 2019, the test-bed will be

configured properly and fed with the real congestion data gathered during that specific earthquake. This setup will be used to emulate the congestion in sub-scenario 2.

- The RESISTO natural events sensing platform (weather and seismic sensing), which will be provided by TEI (as described in Deliverable D4.3 [7]).
- The inspection UAV platform with surveillance payload (friendly), which will be provided by ADITESS (as described in Deliverables D4.1 [5] and D4.2 [6]).
- The RESISTO platform with its correlator engine

The exact details of the implementation (duration, span of network failure for congestion etc.) will be defined during the piloting in the framework of WP7.

5.2.3. *Impact of threats foreseen in Use Case 2*

The expected impact involves the following aspects:

Operational: Risk of Service delivery and network failure especially for mobile communications which would also potentially affect PPDR services as well, if the problem is not quickly restored. Local users would experience prolonged delays in completing voice calls through cellular services, leading to an experience of wireless congestion. The local users may also experience lack of broadcast (TV or radio services) if the antenna pillar incorporates relevant transmission infrastructure. In addition, communication interoperability is scarcely available, accounting for low percent of service and repairs are urgently needed.

Technical: Telecommunications and data connectivity are at risk; network connectivity failure / telephony & internet services face severe problems; especially cellular communications are lost, initially in the proximity to the incident and then in a wider area and routes, especially if the problems caused by the attack or the natural disaster remains unrestored for a significant time period. Heightened usage could stress local telecommunications carriers' network capacity and could result in periods of network congestion on public cellular infrastructure at least in a local level. Congestion could also increase switched-circuit use within the region, leading to "all circuits are busy" messages. In the regions surrounding the most impacted area, communications would likely operate after significant time or be restored through resilience / disaster centers, with the exception of communications facilities that directly rely on the damaged / destroyed underlying infrastructure located in the impacted area.

Economic: A direct impact is the loss of facilities and infrastructure for the telecom provider. Additionally, a significant economic impact is the consumption in time and resources attempting to tackle and restore the problem with the conventional manner (i.e. without the RESISTO system implementation). Although the scenarios are unlikely to create widespread service outages, the surge in demand could impede local commercial or private network customers from accessing and using the network as they would under normal conditions. The precise levels of network failure resulting from both these scenarios would depend on the nature, duration, and exact locations of the events; nonetheless, the network user experience would be substantially reduced in the local level.

Societal: Critical public safety issues, needing further investigation, arise by the facts that on the one hand, an airborne threat hit and destroyed a telecom asset even in a remote location and on the other hand, that a natural disaster damaged the same facility; both incidents would initiate central civil protection actions by the state. The potential scale of public safety coordination could also incorporate other separate public safety agencies. Apart from that, as in all similar Use Cases, the network disruption or failure could impact other critical infrastructures that may happen to be on the vicinity; offices and homes could suffer significant damage as well. If the problem remains unrestored

for a significant period of time, it would cause severe problems in the wider telecom network of the area and the customers' telecom services, while TV and radio may be affected as well.

5.2.4. Other consequences - Interconnected Critical infrastructures

As in the previous Use Case 1, the sub Use Cases of Use Case 2 are meant to demonstrate attacks, threats and vulnerabilities that affect the existing framework of the telecom CIs. Thus, they do not directly foresee cascade effects and interdependencies with other CIs.

However, this kind of Use Cases, are potentially ideal for examining and emulating interconnections with other critical infrastructures in the local area or in surrounding regions and respective cascade effects. Since other telecom providers may rely on the specific provider's (i.e. OTE's) fiber infrastructure or wireless network, the telecommunications services in general for i.e. at least the wider territory, will be severely affected, and other CIs assets in the vicinity can be identified as "compromised" by RESISTO.

To this end, the results of the Use Case 2 could be used by specific RESISTO tools (such as CISIAPro and propagation effects tools) to develop and implement experiments on potential effects in other interconnected critical infrastructures supposed to be affected by the specific.

Both incidents would also put into motion the full range of public safety and emergency response activities across all levels of administration. Critical public safety tasks would include maintaining command and control of public agents participating in the response, activating emergency alert and notification systems. The complexity, scope, and potential consequences of these threats require that there be a rapid and decisive level of coordination among them. However, in the earthquake variation scenario, cumulative effects could include fires, collapsing structures, flooding from broken water mains, exposed electrical hazards or leaking fuel, landslides and ground ruptures affecting other CIs in the wider area, depending on the severity of the attack or disaster events.

5.2.5. Deployment topology example

The test-bed that will be used is the same as in Use Case 1. As already mentioned, the OTE's test-bed located in OTE premises in Athens, Greece, will be used to emulate the sub Use Cases of the Use Case 2, as this test-bed was described in the previous Section 4.3.5.

OTE possesses various antenna parks in various urban and remote locations, so their specific technical characteristics can be emulated or taken into account during the relevant implementation through the test-bed. Furthermore, considering that a natural disaster of moderate magnitude takes place, then OTE's test-bed can be fed with the real results for congestion obtained from the recent Athens earthquake. This setup will be used to emulate the congestion in the whole Use Case 2.

5.3. Actors and detection tools involved

In the context of this use case, the below roles are identified, as shown in the following table:

Actor	Role	Description
Hostile UAV / aerial platform	Intruder: physical (terrorist) attack generator	A hostile UAV attacks OTE's infrastructure, destroying a critical telecom asset and disrupting services creating severe network failure
RESISTO Airborne threat detection system	Technical: detector of airborne threats i.e. small aircrafts and UAVs (1 st sub-scenario, ICCS)	Active and passive sensors (i.e. radar and acoustic ones) to detect direction path of airborne threats. This is a physical threat detection module that provides potential intrusion events to the RESISTO platform.
RESISTO friendly UAV platform	Technical: damage inspection module (both sub-scenarios, ADITESS)	Aerial UAV platform equipped with video cameras for the real-time inspection of remote areas.
RESISTO natural events sensing platform	Technical: weather and seismic sensing platforms (2 nd sub-scenario, TEI)	Sensing modules and processing software for weather and seismic incidents. This is a natural hazard events processing module of the RESISTO system.
Network/system specialist/administrator	Technical: network and system operator (configures the test-bed that emulates the provider's network-OTE)	Telecom provider's personnel that configures the test-bed for the various test scenarios.
Information & physical security platform-The RESISTO system	Technical: cyber and physical attack monitoring, detection, response and mitigation system	Monitors the overall functionality of the physical and cyber security, receives threat events, uses tools and techniques to identify vulnerabilities, erroneous configurations or intrusion attempts and responds to threats.
Service Provider	Business: communication service provider (OTE)	The telecom provider (OTE) that provides communication services and consumes network resources
Customer (hypothetical)	Business: service consumer	An entity that consumes one or more telecommunication services, affected by the network failure.

Table 5 – Identified actors for Use Case 2

Sensor	Role	Description
Active and passive sensors (electromagnetic radar and acoustic)	Acquisition and processing of electromagnetic and acoustic data	RESISTO Airborne threat detection system, signal processing and extraction of potential intrusion events (i.e. hostile UAVs).
UAV-platform surveillance sensors	Damage inspection	Optical and thermal cameras mounted on a UAV along with the corresponding algorithms for damage inspection
RESISTO natural events sensing platform	To provide natural disasters events	weather and seismic processing platforms for relevant incidents, to be correlated with network failure events.

Table 6 – Detection Sensors that will be used in Use Case 2

5.4. RESISTO response and Added Value

The main objective of the Use Case 2 (both sub-Use Cases) is to enhance the response and mitigation actions of the existing communication infrastructures towards protection against man-made physical threats and natural disasters. The focus is to advance the processes of detection and response and thus to result in measures for mitigation and prevention, **in a shorter time** than the time that would be needed in conventional responses (without the RESISTO system).

To this respect, modern detection systems are being used along with surveillance and inspection capabilities to prove that it would be possible to detect, correlate and identify the consequences of physical threats and natural disasters early enough and in short response time and to use joint counter-measures and mitigation techniques. Without RESISTO the relevant causes and accompanying risk of the consequences would not be possible to be detected and correlated early enough by the conventional security systems already used by telecom providers; and it would take much longer time until they are identified and eventually tackled and resolved.

Thus, RESISTO performs correlation enabled by additional modern tools, sensors and algorithm systems facilitating an effective detection along with the RESISTO decision making mechanisms to result in faster response and mitigation.

5.4.1. RESISTO Short Term response

Based on the above the RESISTO Short Term Response consists of the following:

- Detection: Having received the alert events by the sensors (from the airborne threat and natural disaster), the RESISTO platform issues the relevant physical threat detection events.
- Response: the RESISTO system, in both sub-scenarios, triggers counter-measures such as launching friendly drones to monitor and inspect the damaged asset.
- Response: based on the events correlation the RESISTO platform, provides emergency signals and notifies the security operation center of the telecom provider of the telecom operator concerning the damages.
- Prevention / Mitigation: RESISTO suggests short term (or immediate) prevention / mitigation action, i.e. redirection of normal traffic activating the decision making mechanisms. RESISTO ensures communication continuity in the end.

5.4.2. RESISTO Long Term response

In a similar way to Use Case 1, the RESISTO Long Term mitigation (LTCL - “risk and resilience analysis and management tool”) concentrates all detected vulnerabilities and threats within the telecom infrastructures in order to analyse them in respect to the assets affected as well as the provided services to the customers. Based on that, the outcomes and implementation results of both sub-scenarios of the present Use Case 2 will contribute to reiterating another cycle of long-term mitigation and prevention measures through i.e. best practices or creation of redundant / resilience solutions.

5.4.3. Innovation addressed

Potential innovation for Use Case 2 can be summarized as follows:

- New, physical threats detectors are implemented and new technologies for physical threat detection/protection/response may emerge through the use of these sensing tools.

- New challenges are posed in terms of the technological evolution, since it is expected that new innovative processing, measurement and analysis methods may be derived in order to efficiently process and analyze the data acquired during the piloting activities.
- Mindset evolution: the combination of the above may lead to new procedures/changes in the organization's (telecom operator's) security policy, while new standards may emerge.

5.4.4. Suggested KPIs for Use Case 2

Apart from the contribution of this Use Case to the overall RESISTO implementation statistical data that will be gathered, the following metrics / KPIs are suggested to be measured:

KPI number	Title / Description
K1	Number of detected physical threats
K2	Number of detected cyber threats
K3	Detection probability
K4	Time to detection
K5	Average decision-making time
K6	Average mitigation time
K7	Human intervention/Automated response

Table 7 – Suggested KPIs to be measured during the pilot activities of Use Case 2

6. USE CASE 3: TELECOMMUNICATION SITES

6.1. Introduction and Background

Telecom Broadcast as critical infrastructures are meant to provide multiple television and radio broadcast types of services with predefined and guaranteed Quality of Service.

A simulated attacker may only want to open up a few strategic holes to the cyber domain of a network that will cause severe failures to the offered services either immediately or at a later time. Thus, the attackers can exploit vulnerabilities both in the cyber and physical domain of an infrastructure, to gain access to the cyber domain.

These physical intrusions may be initially seen as physical assaults of a lesser importance in respect to their consequences on the cyber domain.

From the Infrastructure provider is not only important to detect but know how to react on such kind of attacks in **order to mitigate it**.

The main objective is to produce a complete procedure to establish or determine the operational decision support system actions. We will be based on our Telecommunication architecture and network with a complete risk analysis in order to define the actions to be carried out by the operational support system based on RESISTO recommendations. The objective of the use case is to help developing IA algorithms on RESISTO platform.

The operator that is using monitoring the network needs to have some operational guides in order to automatise the process of reaction.

This use case will be based on the real Telecom infrastructure network but will not simulate real attack. The idea is to analyse all the possibilities in an attack, in order to recommend operational reaction in order to mitigate to be propose to the operator.

6.2. Overall Description of the Use Case

Typical Broadcast Sites are covering large areas providing services that have very restrictive Service Level of assurance. The key point is to maintain the Service on air in a certain percentage of the country while assuring 100% of availability. Any physical-cyber-attack may have direct impact on broadcasting the signal and on maintaining the SLA.

Usually, the Broadcast network integrates in parallel redundant systems and must be switched on as soon as possible.

The typical use case will be the following:

- Resisto platform introduce the complete architecture.
- Resisto long term block integrate the operational procedures stated.
- Simulating alarms or events in the NOC and Resisto recommends how to continue considering all the equipment affected.
- In this hypothetic case 1, someone is detected while approaches and entering the site building. It is detected by the security threat detector such as video or present detector.
- Having detected the potential attacker threat, the NOC system identifies the cyber assets in the location as “compromised” and initiates different cyber detectors of the provider’s network in order them to detect potential threats in the cyber domain.

- The attacker starts performing a cyber attack, is detected and a cyber attack event is issued by RESISTO.
- Finally, RESISTO suggests a prevention / mitigation action, i.e. deactivation of the switch and redirection of normal traffic. sw

The idea is to analyze all the possible intrusion detection, cyber-attack and determine the operational procedure to react. The idea is to feed the long term response block.

We will consider that Physical detection could come from any physical detector and cyber detection may come from any kind of cyber-attack, not only considering DoS.

6.2.1. Assets Affected

We are considering **TV and Radio broadcast sites** where we are transmitting commercial signals. In a broadcast site we are just considering the cyber part. Power supply, antenna are not considered.

In any case, in any cyber-attack all the network may be affected, considering all the equipment and services.

Once the attacker is in the network some others components may be affected:

Equipment in the site:

- **TV Headend:** Source of the linear TV streams, coders, multiplexor and others are the main equipment in the Broadcast chain.
- **Access interconnect:** Point of interconnection to the Infrastructure Provider's access network (e.g. fibre-based access network). Different routers, switches etc. that may interconnect others services or networks.

Equipment from the Network:

- **TV Headend:** Source of the linear TV streams, coders, multiplexor and others are the main equipment in the Broadcast chain.
- **Access interconnect:** Point of interconnection to the Infrastructure Provider's access network (e.g. fibre-based access network). Different routers, switches etc. that may interconnect others services or networks.
- **Monitoring center NOC.**

6.2.2. Impact of the foreseen threats - Interconnected Critical infrastructures

The impact should be considered depending also on the kind of response and protocol to follow. Possible affected infrastructures may be other TV or radio sites, the service or services and finally the complete network.

- At the first moments the potential attack may affect the service provision in that zone.
- Secondly the propagation of the effects may affect others services in that site.
- Moreover the propagation may affect other sites and others services.
- Finally the attack could have an impact in the complete network.

6.2.3. Deployment Topology Example – Test-bed setup

The use case will be using the critical Broadcast network of the infrastructure provider. The network is based on high tower / high power, with a high capilarity in span and with 3 control centers that can switch or connute functions and management actions in order to fully control the network and therefore the services provided.

The test bed will not be piloted but will use the real network and infrastructure of the Television broadcast.

6.3. Actors and detection tools involved

The infrastructure provider in coordination with the RESISTO platform developer are the main actors involved in defining the correct IA algorithm behaviour according to a real procedure.

The main actor will be the operator in the NOC that must know the best praticices in order to mitigate the attack. A complete procedure will be detailed and traduced to long term response.

6.4. RESISTO response and Added Value

The objective is to describe the procedures to mitigate and response in an efficient way to any kind of attack at any Broadcast site. The main issue is to provide a guide to the operator in order to facilitate the more appropriated answer.

The operational procedure must be translated to the long term response algorithm in order to mitigate.

- Mitigation
- Response

6.4.1. RESISTO Short Term response

The objective of the implementation is the RESISTO platform to establish the appropriate procedures in order to have a real time response and mitigate the attack. The RESISTO Short Term Control Loop should implement the algorithm dictated by the procedures while reacting in real time. RESISTO should first provide the corresponding alert message to the corresponding profiles and Decision mechanisms and moreover certain recommendations on how to proceed to avoid the shut-down of the service. The Short Term Control Loop should be responsible for assessing redundant systems while preparing the first step in reaction to the attack.

- RESISTO analyzes the information and creates a dashboard for real-time recognition and proper action to be taken, including site attacked, propagation or network affected and estimation of response.
- RESISTO orchestrates threat mitigation by automating responses.
- The Operational team takes decisions about high risk events and operates the decisions, based on the actions suggested by RESISTO AI algorithms.

6.4.2. RESISTO Long Term response

The RESISTO may automatically configure the parameters of the algorithms and set up alerts to users and decision boards. The long term response (Long Term Control Loop) may propose optimization in

the algorithms, analyze the effects produced and assess the future countermeasures on how to proceed.

- RESISTO aggregates the threats information into a database collection ('knowledgebase') for future pattern attack recognition and prediction with AI algorithms.
- RESISTO AI algorithm Identifies business critical assets and implements best-practice protection and resilience.

6.4.3. Innovation addressed

The objective of the use case is to integrate the procedures established by Cellnex (RTV) in the RESISTO platform, aiming at mitigating with AI the response and anticipate it:

- RESISTO to analyze the information and create a dashboard for real-time recognition and proper action to be taken, including site attacked, propagation or network affected and estimation of response.
- RESISTO to create appropriate algorithms based on real procedures.
- Long term control loop recommends the best procedure considering the architecture.

6.4.4. Suggested KPIs for Use Case 3

Apart from the contribution of this Use Case to the overall RESISTO implementation statistical data that will be gathered, the following metrics / KPIs are suggested to be measured:

KPI number	Title / Description
K1	Number of detected physical threats
K2	Number of detected cyber threats
K3	Detection probability
K4	Time to detection
K5	Average decision-making time
K6	Average mitigation time
K7	Human intervention/Automated response

Table 8 – Suggested KPIs to be measured during the pilot activities of Use Case 3

7. USE CASE 4: DISRUPTION OF MAJOR SPORTING EVENT BY COMBINED PHYSICAL & CYBER-ATTACK BY A TERRORIST ORGANIZATION

7.1. Introduction and Background

In a major sporting event such as Olympics or World Cup football championships, smooth delivery of live, linear TV streams to a variety of IP devices such as digital TV boxes, tablets or smartphones can be a challenge for the underlying communication infrastructures due to the expected high number of users/viewers and the huge growth in video to mobile devices. Currently, TV delivered via the public Internet is almost exclusively delivered in a unicast fashion. Such Over-the-Top (OTT) services use unicast delivery for both on-demand and live simulcast streaming, where the connection from client (consumer's device) to server is unmanaged and across the open Internet. Without a guaranteed network quality of service noticeable variation in performance and throughput, and hence quality of experience for the consumer may occur.

Multicast distribution is used to overcome quality of service issues and better deal with anticipated network congestions. Instead of being addressed to a single client IP address, multicast packets are addressed to a multicast group address. Clients use the Internet Group Management Protocol (IGMP) to express interest to their nearest router in receiving packets addressed to one or more multicast groups.

Both technologies (unicast and multicast) employ IP networks to deliver their content to end users. Depending on the types of content and end-devices, both technologies are usually supported by IPTV service/platform providers and share the same underlying (IP-based) telecommunication infrastructures. The Figure below shows the typical transmission paths, number of network nodes and protocol stacks used for (data plane) unicast and multicast distribution. The following network nodes are involved:

- **TV Headend:** Source of the linear TV streams; typically one primary and one secondary location.
- **Core node:** Primary network sites in major locations, which may also house metro and access interconnect points. Each core node hosts a Content Distribution Network (CDN) node in order to manage and deliver the contents to authorized end-users based on their geographic locations.
- **Metro node:** Network nodes in major metropolitan cities.
- **Access interconnect (edge node):** Point of interconnection to the Infrastructure Provider's access network (e.g. fibre-based access network).

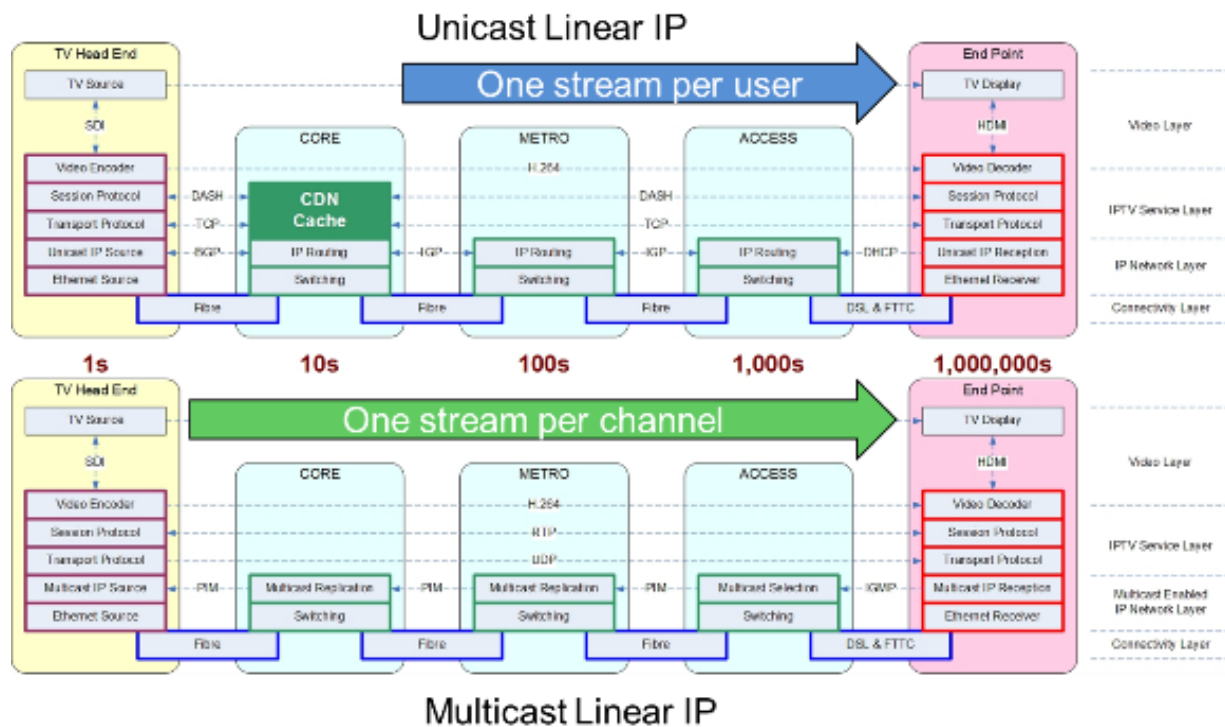


Figure 11: Support of Unicast and Multicast technologies for TV content delivery (data plane)

7.2. Overall Description of the Use Case

This use case will mainly focus on disruptions and resilience during major sporting events on communication infrastructure by studying IPTV delivery over IP networks. As IPTV delivery uses the same IP networks of Internet, all cyber-physical attacks will affect IPTV services. Thus log data whether mentioned or not in this document may be provided for cyber-physical attack analysis as well as resilience analysis to evaluate RESISTO platform and capabilities.

The following figure shows BTC's network infrastructure for unicast and multicast services and includes key components for IPTV delivery. Details could be accessed from ⁶.

BT IPTV delivery at core network consists of tens of Core Routers. They are connected through fully meshed VPN tunnels. There are two Multicast Access Routers (MARs), hundreds of Multicast Service Edge (MSE) nodes and Multi Service Core (MSC) nodes. Thousands of Layer 2 Switches (L2S) on the access networks are delivering multicast services to homes by DSLAMs and PONs.

⁶ <https://www.btplc.com/SINet/sins/pdf/511v2p0.pdf>

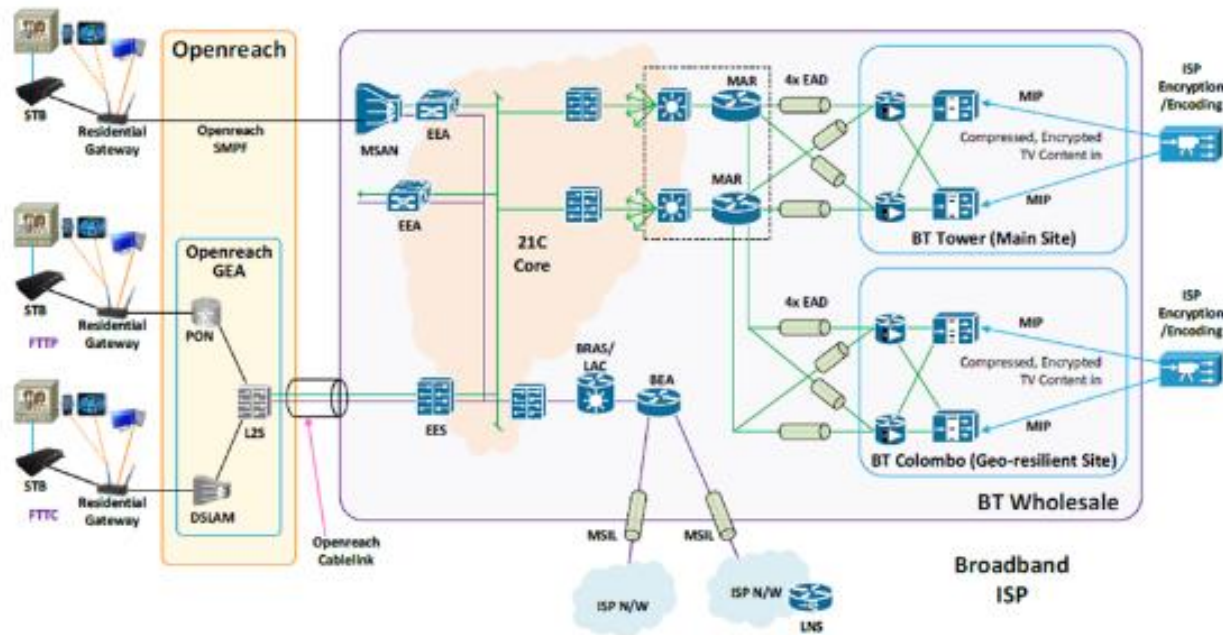


Figure 12: UK network infrastructure for unicast and multicast services

All the components in the above infrastructure could be targeted by cyber-physical attacks. The major threats during major sporting events include terrorist attacks on BT Tower and BT Geo-resilient site, i.e. the TV headend. For the TV headend disruption, RESISTO's long term control loop could research and develop resilience to see how 5G could support TV content streaming to deliver video sources to MARs. In case of cyber-attacks such as the ones causing congestions via DDoS to multicast routers, RESISTO could discover where the DDoS attacks are coming from and then block the attacks closer to the attack sources to minimize disruptions or via unicast over the core infrastructure or mobile networks such as 4G/5G networks for maintaining services.

If the end user devices are used to launch DDoS attacks, RESISTO could use logs from the end user devices to identify abnormal activities over several devices by disabling these devices or by traffic pattern analysis to discover these attacks. It's possible to simulate some network traffics based on real traffic to send certain alerts generated by alerts received by BT security platform.

Due to its one-to-many relationship between a video source and a set of clients/end-devices multicast transmission typically uses the User Datagram Protocol (UDP), which has no built-in retransmission mechanism (in contrast to Transmission Control Protocol (TCP)) and favours low latency over reliability. In order to ensure continuous uninterrupted playback of a multicast video stream, a mechanism at application layer is used to recover lost packets from a dedicated retransmission server which holds or buffers a copy of the video stream. In case of a targeted cyber-attack such as DDoS on a critical multicast router during a major sporting event, a sudden flood of packet retransmission requests will be received by the retransmission server. Since the lost packets are retransmitted to a huge number of end-devices within the same time using unicast (one-to-one) transmission, it may unbalance and overload the core network which may lead to interrupted video delivery. This will also have cascading negative impacts on other IP-based services relying on the same core network.

Exceptionally high volume of multicast packet retransmission requests combined with relevant system and security logs should be detected as anomalous event by the RESISTO's in-built correlation engine. RESISTO's short term control loop engine should make recommendations in terms of actions to be taken by the service/network provider in order to deal with the multicast service disruption and to prevent any cascading effects that may seriously affect the whole network performance. Some of the example recommendations are briefly described later on.

7.2.1. Assets Affected

As discussed earlier, there are many components in delivering IPTV services. The following list indicates some key assets affecting IPTV networks.

1. TV headend, e.g. BT Tower
2. Multicast routers deployed on core/metro/edge nodes, e.g. telephone exchange, cabinets
3. Consumer devices, e.g. IPTV set top boxes, mobile end-devices, TVs
4. Network assets including network bandwidth, intermediate systems such as routers or firewalls
5. Service assets
6. Contents and CDN servers

7.2.2. Impact of threats foreseen in Use Case 4

Operational: Risk of linear TV service loss (unavailable service), degradation of quality of service, unbalanced network loads (network congestion)

Technical: Unicast or multicast nodes running at maximum capacity, corrupted multicast packets, high multicast transmission error rates

Economic: Breach of SLA with end-users and wholesale customers which may lead to financial loss due to compensation arrangement

Societal: Loss of good reputations of the IPTV providers and loss of consumer data such as identity and transactions, etc.

7.2.3. Deployment Topology Example – Test-bed setup

We envisage the implementation of a test-bed with the initial architecture shown in the Figure below. This test-bed should represent the typical network infrastructure for delivering video streams using multicast and unicast transmissions to different types of video clients or end-devices.

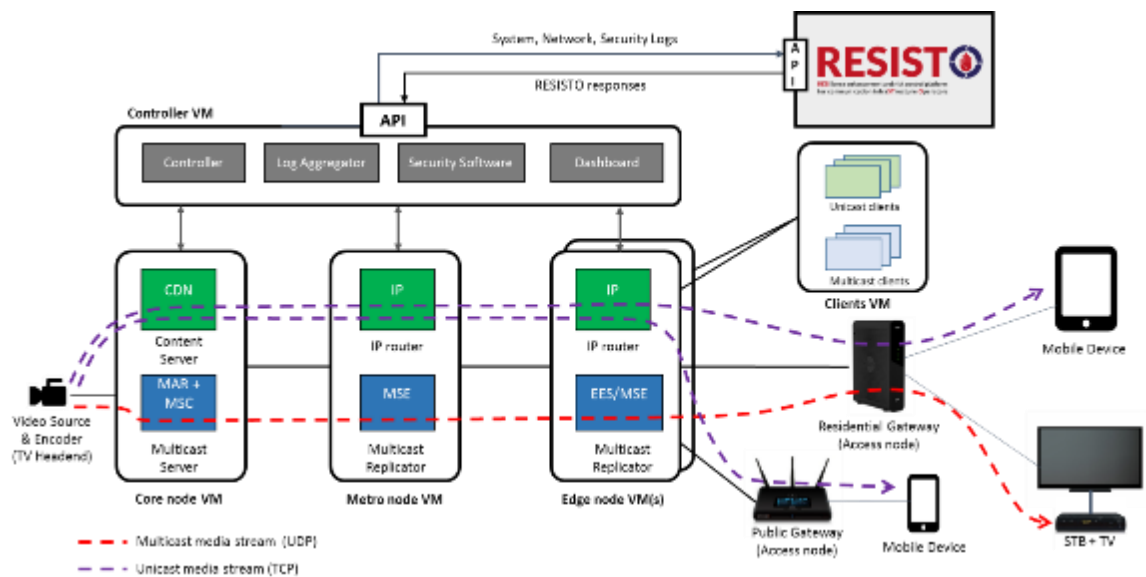


Figure 13: BTC test-bed (initial) architecture for multicast and unicast video delivery

The majority of the test-bed components will be deployed in a virtualized environment, i.e. BT Research Platform, which could be connected to some physical components such as WiFi router or mobile phones depending on the test scenarios. We strive to integrate the TV headend as physical device into the test-bed in order to provide live video stream into the delivery network. In particular the following virtual machines (VM) should be deployed to represent the network infrastructure:

- **Core node VM:** This VM will contain components that replicate the main functions of a multicast server (i.e. MAR and MSC) as well as of a content server that holds a copy of the video stream that can be transmitted to client devices using unicast route. The content server also acts as a retransmission server for handling the requests to retransmit lost multicast packets. CDN responsible for authenticating users/devices and verify clients have the rights to access the contents
- **Metro node VM:** This VM will contain components that replicate the main functions of multicast replicators and unicast IP routers as usually deployed on metro nodes.
- **Edge node VM:** This VM will represent the nodes at the edge of the network infrastructure and contain components that replicate the main functions of associated multicast replicators and IP routers. Depending on the test scenarios there may be more than one edge node VMs deployed in the test-bed. During the design and implementation phase we will examine further whether or not to co-locate the edge and metro node functions together in order to simplify the test-bed architecture.
- **Clients VM:** This VM will contain (software) components that simulate a number of unicast and multicast clients in the network consuming the video streams (simultaneously) via unicast and multicast transmission respectively.

In addition to the virtual machines described above we envisage the deployment of a Controller VM which (among others) should comprise the following components:

- **Controller:** This component acts as a hub to control the main operation of multicast and unicast transmission in the test-bed. It is the one that will handle the requests and responses of the RESISTO platform.
- **Log Aggregator:** This component collects the relevant system, network and security logs produced within the test-bed and provides them to the RESISTO platform. The RESISTO platform will continuously monitor the provided logs and takes actions based on the outcome of its internal correlation engine.
- **Security Software:** This component represents the threat monitoring and detection service of the network infrastructure. Essentially its main function is to produce security logs and alerts in the case of suspected cyber-attacks on the network infrastructure. Such cyber-attacks may either be simulated or carried out using external penetration testing tool.
- **Dashboard:** This component provides a graphical interface showing the current state of the network, e.g. network health, traffic statistics, security alerts, etc.

The controller VM is exchanging information with the RESISTO platform via their respective APIs, e.g. to provide network and security logs, or to receive RESISTO responses in case of network or security incidents.

During normal operation a live or recorded video stream is transmitted from the TV Headend; the video content is encoded according to service requirements and sent to both the content and multicast servers. In order to reduce network loads the video is streamed to multicast group addresses and replicated by the multicast-capable (software) routers deployed at core, metro and edge node VMs. Any multicast-capable end-devices such as set top boxes (STB) or multicast clients that have joined or subscribed to the multicast group via IGMP will receive the video stream as multicast packets.

Consumers on mobile devices are using apps to select the video event and stream the video using unicast transmission. In some cases, video delivery via home or public access nodes (gateway) can be done using multicast transmission too.

In case of unicast transmission, the video quality (i.e. encoding scheme) can be chosen dynamically by consumers based on their personal preferences, device capability (e.g. processing power) and channel quality. If multicast packets get lost during transmission, e.g. due to noises in the channel or network failures, the multicast device will request for packet retransmission from the content server. Such packet retransmission happens at the application layer and uses unicast delivery method.

Alerts and log data from the platform could be provided by columns and values formats, JSON or syslogs as appropriate.

7.3. Actors involved and detection tools involved

In the context of this use case, the below roles are identified to be involved, as shown in the following table:

Actor	Role	Description
Customer	Business: TV Service Customer (end-user)	Consumes an IP TV Service
Wholesale Customer	Business: TV Content Customer (reseller)	Distributes IP TV Content to its own end-users
IPTV Service Provider	Business: IPTV Service Provider	Provides an IP TV Service Consumes Network Infrastructure Services
CDN Service Provider	Business: CDN Service Provider	Provides CDN service
Network Infrastructure Provider	Business: Network Operator	Provides Network Infrastructure Service (including virtual network) to IPTV Service Provider
Internet Service Provider	Business: Internet Service Provider	Provides Internet Service to End-Users (Customer)
Access Network Provider	Business: Network Operator	Provides a Physical Network Access to End-Users (Customer)
Attacker/Hacker	Technical: Cyber and physical attacks generator	Attempts to exploit vulnerabilities in system components' software, hardware and middleware in order to gain access to resources and information or to change the intended use case of the systems Can also cause physical damage to systems, cut off power
Network/system specialist/administrator	Technical: Network/system and services configurator	Configures the test-bed infrastructure and services for different test scenarios
Information Security/Cyber Security Specialist	Technical: Cyber and physical attacks monitor/detect and respond	Monitors the overall functionality of the cyber security systems, uses specific tools and techniques to detect vulnerabilities, malware, erroneous configurations or intrusion attempts and responds to threats.
Physical Security	Video/Audio surveillance system	Building/Area perimeter video and audio surveillance tools for the detection of illegal intruders and/or unauthorized personnel in an area of interest

Table 9 – Actors of Use Case 4

7.4. RESISTO response and Added Value

In order to respond to major multicast service disruption some of the following actions may be recommended by RESISTO:

- Re-route the multicast streaming for affected routers or end-devices
- Reject packet retransmissions for selected group of end-devices to ease the network congestion
- Request the change of encoding scheme at source/headend (i.e. to degrade the video quality from 4K to HD/SD) in order to reduce the network traffic in general
- Request the change of encoding schemes at content server (i.e. to degrade the video quality) in order to reduce unicast traffic to every single end-devices, i.e. both multicast-capable (e.g. STB) or unicast-only devices
- Request the (unicast) receivers to switch to public access node (e.g. public WiFi) nearby (if available) if multicast streaming can be activated on that particular access node
- Request the video source to switch to high-speed radio networks (e.g. LTE-A or 5G) for streaming

The risk control and resilience objectives are not much different from communication infrastructure. During the major sporting events, terrorists could disrupt by attacking TV head end for contents productions, attacking core routers/CDN servers by injecting wrong contents, and DDoS attacks causing major congestions. The following lists some risks which RESISTO could try to address.

- Terrorist attacks and physical damages to TV head end, access network assets, and cable cuts
- Cyber-attacks on core nodes and metro nodes, and CDN servers
- DDoS attacks using end user devices.
- Injecting wrong video contents for terrorist propaganda
- Unauthorized access or modification of messages
- Theft of subscriber or transaction information

7.4.1. RESISTO Short Term response

The BTC test-bed will have interfaces to send alerts and receive responses from RESISTO platform. There will be various action handlers to process RESISTO responses, and then invoke various action handlers to execute mitigation actions. Detailed implementation will be developed as the project progresses.

The RESISTO platform will receive security events/alerts from the test-bed. If required, it's also possible to send simulated events including cyber and/or physical security events based on BT operational IPTV networks.

Examples of short-term responses are:

- Re-route the multicast streaming for affected routers or end-devices
- Reject packet retransmissions for selected group of end-devices to ease the network congestion

- Request the change of encoding scheme at source/headend (i.e. to degrade the video quality from 4K to HD/SD) in order to reduce the network traffic in general
- Request the change of encoding schemes at content server (i.e. to degrade the video quality) in order to reduce unicast traffic to every single end-devices, i.e. both multicast-capable (e.g. STB) or unicast-only devices
- Request the (unicast) receivers to switch to public access node (e.g. public WiFi) nearby (if available) if multicast streaming can be activated on that particular access node
- Request the video source to switch to high-speed radio networks (e.g. LTE-A or 5G) for streaming

7.4.2. *RESISTO Long Term response*

The RESISTO platform has received BT operational platform network diagrams and BTC test-bed. Any long term responses for network resilience will be tested if possible on BTC test-bed. BTC test-bed dashboard will display any long term responses from RESISTO platform, and any long term modelling tools if available will be made available in the dashboard to network managers and decision makers.

Specifically, the RESISTO long term responses could consider:

- Improvement to BT IPTV delivery network architecture as shown in the earlier sections.
- Terrorist attacks and physical damages to TV head end, access network assets, and cable cuts
- Cyber-attacks on core nodes and metro nodes, and CDN servers
- DDoS attacks using end user devices.
- Injecting wrong video contents for terrorist propaganda

7.4.3. *Innovation addressed*

IPTV is delivered mainly with multicast. This is very different from unicast where security issues at lower OSI layers are better understood. This offers RESISTO opportunities to develop new ways to identify additional security issues and propose new methods and contributing to IPTV standards. Below are some potential innovations to be considered by RESISTO:

- Multicast is delivered to group addresses. Everyone on the group will receive the streaming data. This could potentially be used to launch attacks. RESISTO long term control loop could potentially identify vulnerabilities in multicast networks.
- Detect unauthorized access to data. Detecting authorized users using traffic patterns especially true at layer 2 switches.
- Traffic logs and alerts could be used to discover new threats.
- Identify issues for using unicast for loss packets retransmissions
- New measures for network protections
- Multicast TV head end protection and resilience
- Injecting wrong contents during the broadcast. Is there a way to detect other than analyze video content, e.g. end customers reporting problematic video streams.

- Home network protection end user home could be used to spreading worms, virus, Trojan and stealing contents.
- Detects unusual number of channel requests. RESISTO could provide ways such as simply hold those requests for a second or two and that will prevent the server from busying out. Take suspected problem users off the network
- Long term control loop recommends new architecture how IPTV could be securely delivered.

7.4.4. Suggested KPIs for Use Case 4

Apart from the contribution of this Use Case to the overall RESISTO implementation statistical data that will be gathered, the following metrics / KPIs are suggested to be measured:

KPI number	Title / Description
K1	Number of detected physical threats
K2	Number of detected cyber threats
K3	Detection probability
K4	Time to detection
K5	Average decision-making time
K6	Average mitigation time
K7	Human intervention/Automated response

Table 10 – Suggested KPIs to be measured during the pilot activities of Use Case 4

8. USE CASE 5: PROTECTION OF CLOUD STORAGE SERVICES

8.1. Introduction and Background

TIM's use case related to protection Cloud Storage Services is part of Macro scenario 2 which is entitled "Interconnected/Interdependent CIs and cascade effects and Macro scenario 3: "CI evolution towards the future 5G networks and the emerging IoT world".

The main objective of the use case is to simulate the attack on a system architecture and its storage system, and to use a correlation between physical and cyber alarms, in order to mitigate the action performed by a malicious intruder on a critical infrastructure. The events recorded by the platform will be used to determine the actions needed to help the operational team to make the right decision in order to resume and support the normal service function.

8.2. Overall Description of the use Case

The use case is described based on a general system that needs to save information on Cloud Storage.

The protection a Cloud Storage is a sort a basic scenario that could be extended to include other CIs infrastructure scenarios.

The cloud storage infrastructure is subject to physical and cyber-attacks, that include for example in case of physical attacks, theft of part of servers, unauthorized access to buildings where they are located, and manipulation of facility systems. Cyber-attacks include for example hacking to servers, changing configuration files, virus/worms attacks.

Some of the attacks can be performed also in combination of both physical and logical techniques at the same time, such as an attacker that can gain the access to the network/storage infrastructure by using the data/credentials gathered from stolen devices or stolen authentication tokens.

The proposed use cases help to identify changes of configuration or of data of critical assets and help to implement best-practices to protect the information on Secure Storage. The physical sensors implemented help to detect un-authorized access to the CIs site to identify the physical intrusions. Integration between alert of physical sensors and ICT sensors permits, for example, the RESISTO platform to detect a physical intrusion to the CI site with the probable theft of an ICT asset.

Another case where the platform may be useful is the detection of a sabotage of the ICT assets and help to make the decision to move services to another site, implement others countermeasure or update the defined threat model, accordingly to the "continuous improvement" paradigm. In addition, a block-chain based security module installed on the nodes will be able to detect attacks aiming at modifying/deleting its SW or configuration data and to report the unauthorized events.

RESISTO platform will receive alerts from physical and ICT sensors, and showing situation in RESISTO dashboard, predicts possible impacts, suggests mitigation actions such as an intervention of security group or guard. RESISTO could also contribute to identify how several assets of cloud storage infrastructure should be protected and help to develop an integration of security vision that should be in places for different scenarios.

Physical security considered in our use cases is related to threats, risks, and countermeasures to protect site facilities and data where secure storage is deployed.

This involves authorized entry methods, environmental procedures, ICT procedures. Some of the topics covered include:

- Access to restricted areas, authorization methods to access to a protect environment
- Physical sensors, ICT Sensors installed on servers
- Security guards
- OSINT

Correlating the domains of physical security systems, cyber domain and OSINT information permits to take advantage of interdependencies between such domains. Hence it is possible to detect in advance threats and attacks and to adopt the opportune actions to implement mixed cyber and physical counter-measures.

Significant damage issues to critical infrastructure could be impacting on the level of services that the same CIs are offering or could create, for example, a serious damage to communication infrastructure. In some cases, a latent risk could not be easily evaluated and hence is difficult to determine its impacts and its propagations on infrastructure.

-The following attack scenarios are taken into consideration:

- Tampering of sensitive information on “Secure storage”, such as firmware of devices or PII data stored on the infrastructure.
- Un-authorized access to physical site.
- Change of system configuration.
- Change of Hardware configuration of system.
- Power outage.
- Temperature out of range.

For Use case 5, two scenario / sub use cases are envisioned; each one with various tests and experiments. The first sub use case is related to healthcare services and the other to manufacturing. In the following each one will be presented:

8.2.1. Sub Use Case 1 – Healthcare

The healthcare systems is one of the most appealing targets for cyberattacks, as electronic health records (EHR) and all the information regarding patients are very sensitive and are becoming more and more important in the process of managing personal information.

The hospitals are increasingly dependent on their ICT systems, the use of connected medical devices and networked systems for normal medical activity expose those systems to both cyber and physical attacks, where the scope is to disrupt the service or to steal sensitive information that could be used for other types of attacks.

The healthcare sector must face several cybersecurity-related issues. Among the others, it is important to consider malware infections that compromise the integrity of systems and privacy of patients, but also denial of service attacks that block hospital ability to provide patient care. While other critical infrastructures have experienced these attacks as well, the healthcare industry is particular because the damages caused by an attack can have consequences beyond financial or privacy losses, but impact directly the life of the patients. Many data breaches events have been

reported in the healthcare sector. That can be caused by many different types of incidents, such as credential theft or directly disgruntled employees disclosing confidential information.

Personal Identifiable Information (PII) managed by hospital is usually very valuable, hence there is a higher incentive for cyber criminals to target medical databases. Denial of service attacks are usually performed by sending huge amount of data toward a specific server, overwhelming its resources till it is not able to provide any services. But DoS can be caused also by malware⁷ able to infect and consequently block the normal behaviors of e.g. electronic medical devices that prevents victims from accessing part of their file-system or data base by encrypting all the data unless they pay a certain amount of money. Finally, the BYOD strategies as well, by allowing personal mobile devices to be regularly used, generate more potential access points for unauthorized users, actually expanding the attack surface.

8.2.1.1. Test 1 - Detect tampering on files containing sensitive information after physical access to site

Considering a layered approach to physical security, one the most important and maybe the first-one to starts with is the request and validation of access credentials prior to entering at the datacenter.

Type of Threat: Man-made threats

Case Type: Cyber-physical.

Security Threats:

- Unauthorized access to physical site.
- Unauthorized application launch
- Unauthorized changes in system configurations
- Tampering with files containing sensitive information (configuration files) or PII information.
- Tampering with a file by modifying the creation time. This kind of modification is related to anomaly behaviors associated with an hacking or a malware attack.

Sensors: Rack/Door sensor, ICT sensor, BlockChain (KSI Guardtime) WiFi sensors (from Integrasys)

Type of sensors used:

- ICT sensors - will be implemented on every Windows servers,
- Physical sensors - Rack or door sensor (binary sensor) will be implemented on rack where TIM's test-bed servers will be mounted.

High level description of the temporal events:

Rack or door sensors detect a first event about a physical access and consequently send an alarm to the RESISTO platform.

The intruder, by using previously stolen credentials, can now access into a critical system and try to launch a program or change the system/network configuration.

The intruder could also install a rogue Access Point (WiFi device) physically connected to the management LAN (e.g. directly to the switch used in the restricted area). In this manner the intruder

⁷ <http://healthitsecurity.com/news/understanding-ransomware-and-healthcare-data-security>

could access to the LAN without being in the restricted area. The WiFi Sensors detect such a rogue AP and send an alert to RESISTO.

ICT System monitoring sensors detect the anomaly in specific running processes or a configuration changes and send an alert to RESISTO. RESISTO platform, by collecting and correlating the events, can detect the anomaly and send an alarm to the security guard. RESISTO can send also an alarm to the SOC team that can restore the tampered with file and resume the normal operation. Eventually, the security guard has to check for the presence of the rogue AP as well.

The tampered with file can be, for example, a network configuration or a file related to a device firmware or other sensitive data related to PII stored in the Cloud. In case the creation time of a file has been modified by a process and the executable path is not %Windir% or ProgramFiles (for the Windows platforms) but, for example a specific folder like /tmp, the sensor sends an event to RESISTO platform that in turn can send an alert to IT Security group.

During the testing of this use case, the following activities will be performed:

1. Implementation of physical detector for supervision of physical access to protected area or rack where ICT systems are located.
2. Monitoring logon accesses to servers
3. Monitoring of processes that start from some folders that are considered "restricted"
4. Generation of security alerts for cyber and physical events, simulating a physical and a cyber attacks
5. Correlation through RESISTO platform of security generated events

Use case steps:

- Physical: An unauthorized cybercriminal access a protected area
- Cyber: attacker access to one system with a theft credential
- Cyber: Start a program from a privilege folder or temporary folder of system to change one or more information stored on system:
 1. Data contained on sensitive files (system configuration, firmware of router etc.)
 2. time of creation of sensitive files

8.2.1.2. Test 2: HW configuration system change

Type of Threat: Man-made threats

Case Type: Cyber-physical.

Sensors: Rack or door sensors, ICT sensors

Type of sensors used:

- ICT sensors - will be implemented on every Windows servers,
- Physical sensors - Rack or door sensors (binary sensor) will be implemented on rack where TIM's test-bed servers will be mounted.

Security Threat:

- physical intrusion, unauthorized access to a physical site

- Unauthorized hw configuration changes, like removing (theft) an hard drive or adding an external memory drive.

High level description of the temporal events:

The rack sensors detects the opening of the rack and the change of node HW/configurations, it sends an alert to RESISTO. RESISTO platform in turn sends an alarm to the security guards and IT/SOC personnel. If the attacked system is the hypervisor, RESISTO move the impacted resources to a different node whereas if the attacked system is a single virtual machine, RESISTO sends an alert to ICT team to evaluate the option to restore of a prior snapshot.

During the testing of this use case, the following activities will be performed:

1. Implementation of physical detector for the supervision of the rack where ICT systems are located.
2. Monitoring of all the system events related to the servers
3. Generation of security alerts for cyber and physical events, simulating a physical attack aimed at removing a hard drive or adding an external flash drive.
4. Correlation through RESISTO platform of security generated events

Use case steps:

1. Physical: An unauthorized access to a protected area
2. Physical: Removal of a hard drive of one of the monitored systems
3. Cyber: Monitoring systems behavior to detect an anomalous change and send the related event to RESISTO

8.2.1.3. Test 3: Disaster response and recovery

Case Type: Cyber-physical, political motivated threats, natural disasters

Sensor: RESISTO OSINT, ICT sensors

High level description:

In case of a natural or others kind of threats able to cause service outage, or that could prevent a correct treatment of the threats, the RESISTO platform, previously alerted by OSINT or temperature sensors (e.g. in case of fire), can: send an alert to a guard for perimeter controls and, in some case, migrate automatically a service to a secondary site, alert IT team personnel to initiate the recovery process and provide support for a fast recovery of all involved services in an alternate and safer site. Moreover, it can help personnel to switch all network connections to 5G connections or vice versa.

8.2.1.4. Test 4: Data exfiltration

Security Threat description: large amount of data has been extracted from the storage system and transferred to a different location/logical area; that event indicates a possible data exfiltration. The PSIM detects an event caused by the opening of the rack meanwhile the ICT sensor detects an external device (e.g. external memory stick) connected to the system where some data are copied.

The intruder, instead of transferring the data to another location/drive, could also encrypt the data using a Ransomware injected into the system through the external device (e.g. external memory stick).

Type of Threat: Man-made threats

Case Type: Cyber-physical

Sensor: ICT sensor, physical sensor

High level description:

The sensors alerts the RESISTO platform about the physical and IT events just detected; the physical intrusion will be handled by security guards alerted by RESISTO; the IT alerts are sent also to ICT Team for the appropriate checks. The system involved will be moved to another node, with support of RESISTO platform, in this manner the external connections will be dropped automatically.

In case the Ransomware started to encrypt files, the ICT personnel can restore data with backups.

8.2.2. Sub Use case 2 – Smart Manufacturing

Smart factories and warehouses bring a new and complex set of requirements. As the number of remote-control and autonomous robots and automated guided vehicles (AGVs) on the factory floor increase, manufacturers are demanding: reliability, so mobile solutions remain connected no matter where they are in the factory: density to accommodate many devices communicating within a small area; predictable latency for quick reaction times. New wireless connections and services increase value, reduce waste and overcome the pain points of a fixed network. Which is why connectivity is the foundation of the smart factory.

The answer to the requirements and the KPIs listed above is given by the 5G network, able to provide the requested wireless connectivity that enables mobility for connected devices, agility in operations and an ever-increasing level of device density. Cellular technology wirelessly connects widespread assets and processes in real time, allowing plants to integrate workflows—by being able to locate moving assets and portable tools, for instance. In this case, for instance, it is possible to implement the concept of virtual robot control, where various parts of a robot's motion control calculation can be outsourced to a cloud (or edge cloud) system instead of locating them in the robot itself.

To this extent the protection against cyber-attacks of the nodes where the control modules are located is of fundamental importance (see Fig. 11). RESISTO platform is able to put under control the SW and configuration data of those nodes and is able to detect unauthorized events and generate the correspondent alarm and propose the relevant countermeasure able to mitigate the attack effects.

8.2.2.1. Test 1: Cyber attach to the Manufacturing remote control node

A cloud-based robot remote control system over 5G network for smart manufactory, which enables remote users to control geographically distributed robots and then realizing intelligent production is considered. Robot control systems are responsible for sensing, motor driving, and movement functions that require sophisticated algorithms. A robotic production line involves many aspects beyond the robots, some of which can be challenging. There are actuation controls, sensing, data

processing, and operational intelligence that may present issues around system integration, machine-to-machine communication, and information integration.

Smart manufacturing based on IoT, smart robots, cyber-physical systems, and big data technologies introduce additional layers of complexity. The complexity can be greatly reduced by the modular design of industrial robots with limited computational capacity located in the robot itself and placing most of the requested rising level of “intelligence”, needed to allow them to adapt to the changing conditions and to be able to respond in real time to changes in customer demands, in a cloud, making it possible for affordable, minimal-infrastructure smart robot systems with unlimited computing capacity to evolve.

On the other end in that distributed architecture the integration of these innovative technologies with industrial systems leads to new challenges related to securing smart manufacturing systems in order to avoid costly breaches due to the massively increasing of the scope for attack from adversaries aiming at industrial espionage and sabotage. The potential outcome of these attacks ranges from economic damage and lost production, through injury and loss of life, to catastrophic nation-wide effects.

Security threat description: Data Tampering attack: an unauthorized access to the end-user local cloud where the robot control SW is stored. If the stored data are modified that event is detected by RESISTO platform and managed as a potential data tampering attack.

Type of Threat: Cyber threat

Sensor: Keyless Signature Infrastructure (KSI) module, a blockchain based tool provided by Guardtime

High level description:

Keyless Signature Infrastructure (KSI) is a technology that aims to support the integrity of the data that are put under control. Data Integrity is about ensuring that data is recorded exactly as intended and upon later retrieval ensure the data is the same as it was when it was originally recorded. In short, data integrity aims to prevent and detect changes to information by malicious or unintentional intent.

One or more nodes of the local end-user cloud (see Figure 11) are put under control using the KSI module that is able to monitor it and detect any changes to the data. When an unauthorized event is detected an alarm is sent to the RESISTO platform that will determine the actions needed to help the operational team to make the right decision in order to verify the root cause of access to the files monitored to guarantee normal service function;

8.2.2.2. Test 2: Cyber attach to the 5G network used to connect the remote robots to the centralized control node

Security threat description: man in the mean attack: an unauthorized access to one or more of the nodes of the 5G network used to connect the robots to the remote control system.

If the configuration data of the nodes are modified the link among the remote robots and the control unit can be lost, causing the lock of the factory activities.

Type of Threat: Cyber threat

Sensor: Keyless Signature Infrastructure (KSI) module, a blockchain based tool provided by Guardtime.

High level description:

Keyless Signature Infrastructure (KSI) is used to put under control the configuration data of the nodes, ensuring its integrity. Any changes is detected and an alarm is sent to the RESISTO platform to determine the actions needed to mitigate the attack.

8.2.3. Assets Affected

- Premises where systems are located;
- Servers and storage;
- Node of networks serving end-users;
- Data stored with consequence impact on related services;

8.2.4. Impact of the threats foreseen in this Use Case

Apart from the obvious technical and societal impact (breach of access and damage to files and personal data) the above threats also affect the business operation since an incident can generate reputational, financial and stakeholders' impacts. Also compliance issues with regulations and standards may be created.

8.2.5. Deployment Topology Example – Test-bed setup

The focus of this use case is enhancing the resilience of secure Cloud and storage services support for CIs infrastructure as the Telco communication infrastructures.

In the following figures a high level schema of test-bed is represented.

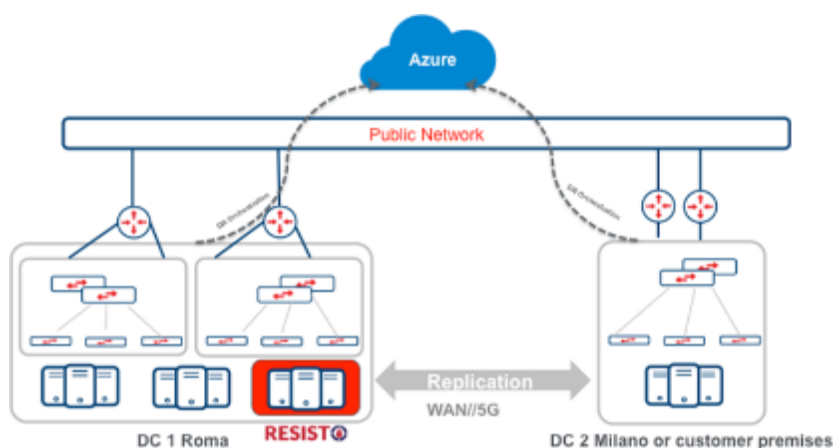


Figure 14: TIM Cloud storage critical infrastructure Healthcare Scenario

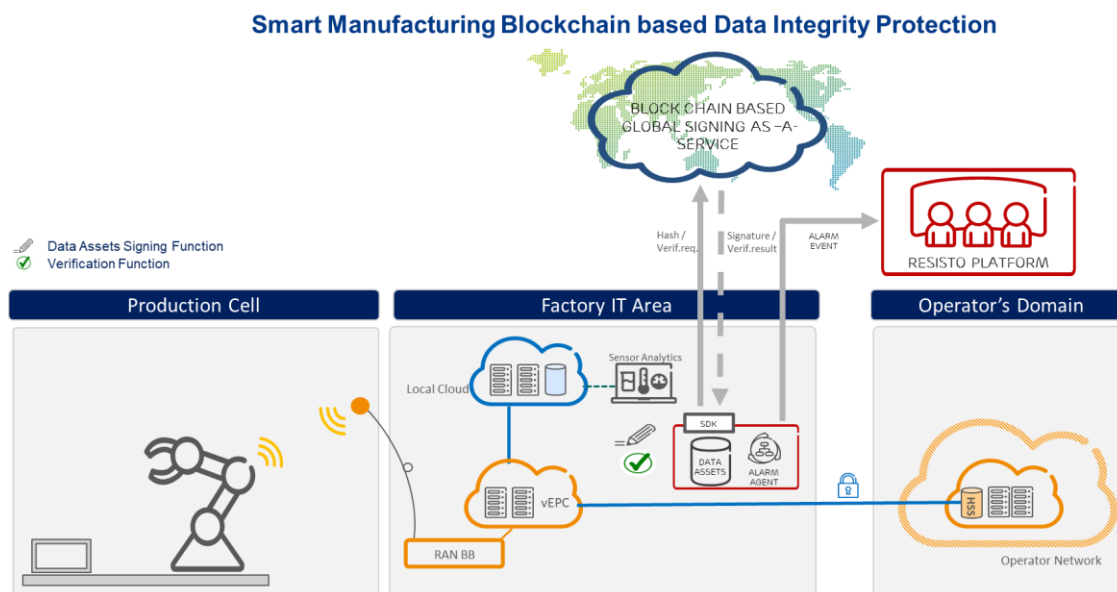


Figure 15: Critical infrastructure Smart Manufacturing Scenario

TIM's test-bed Lab main responsibilities are the provision of a Cloud and Storage facilities for testing services and to detect cyber and physical threats, to provide information and alerts to the RESISTO platform enabling the correlations of generated alerts.

8.3. Actors and detection tools involved

The scenarios were based on the analysis of typical scenarios of attack basically starting from the idea of integration and correlation of cyber and physical alerts.

Stackholders	Player / Organization involved
Public	Public sector, hospitals, health care provider. All these public stakeholders may be give incentives to develop applications or set regulations for better developing secure cloud and 5G services.
Commercial	<ul style="list-style-type: none"> - Vendors: manufactures and suppliers of devices (e.g. IoT devices, smart objects, gateways); security devices (e.g. Firewall, Intrusion Prevention, Web Application Firewall, anti DDoS systems) - Service providers: companies that aim to provide high critical services for a citizen such as home health care support or monitoring. - Utility companies: public or private companies that generate or distribute energy, companies that distribute water. - Telecom providers: obviously telcos that provide the backbone connections for services, mobile connection such as 4G and 5G.
Private	- Citizen and organizations, generally End-User.

Table 11 – Use Case 5 stakeholders

The stakeholders can be grouped into three main categories:

- public,
- commercial,
- private.

More details about the players that are involved in each category can be found in following table.

In the context of the following use case, the actors that are identified to be involved are shown in the following table:

Actor	Actor type	Actor description
End-User (EU)	Person/organization	An individual that may have physical custodianship or access to site, services responsibility.
Sensors	Device	The scenarios anticipate several types of sensors: opening sensors of doors or rack, ICT sensor to detecting anomalies or attack on servers, power supply and temperature sensors, OSINT sensor, Blockchain sensors.
Un-authorized person/Attacker	Person - threat agent	An individual may be the end-user or a threat agent (e.g. contractor, employee) who intends to manipulate the system or access to site or both and is not authorized to carry out these actions.
Guards	Person	An individual that has the responsibility to control the physical access to site, and react in emergency situations
ICT Team	Person	Configure the test-bed infrastructure and services for different proposed scenario
SOC	Person	Team of Cyber Security Operation Center (SOC), experts monitoring the overall security of the test-bed and related services

Table 12 – Use Case 5 actors

Sensors and detectors involved:

The sensors will be implemented on TIM ICT systems, on physical site furthermore will be used the OSINT process (RESISTO sensor) to detect some threats than could represent an issue for the resilience of the infrastructure.

Physical Sensors: The physical sensor used in this use case are:

- Contact sensors to detect a physical access, e.g. the opening action of doors or racks.
- Power grid sensors to detect anomalies on electric power supply.
- Temperature sensors to detect an out of range temperature.
- Wifi sensors used to detect the presence of an unauthorized wireless device in protected areas. (in collaboration with IntegrasyS)

ICT Sensors

- The ICT sensors will be implemented on servers of Cloud Storage Services and will be useful to detect some attack attempts listed on the framework MITRE ATT&CK⁸ relevant for our use cases. The ATT&CK framework, in conjunction with the physical threats considered in our use cases, with related sensors, will be used to build a specific threat model for the cyber-physical domain.
- Hardware and software related logs sent to a centralized collector server

8.4. RESISTO response and Added Value

Taking into account the above-mentioned scenarios, the following modules from RESISTO platform could be evaluated during Use Case demonstration:

- During the attack RESISTO platform detect alarms and anomalies to permit evaluation the impact on infrastructure with **CISIAPro** and could use **Risk Predictor and Orchestrator** in order to select and apply the best mitigation strategy or send an alarm to group of personnel to perform a specific action related to the incident.
- In case of Power Outage scenario, appropriate information is sent to **Cockpit** and by using **Risk Predictor (CISIAPro)** the resilience of overall infrastructure will be evaluated

8.4.1. RESISTO Short Term and long term response

For the short term:

- Identify how a combined incident came to light,
- identify affected systems and suggest how to mitigate or block the incident,
- have an indication about a level of resilience of overall systems
- have one-point where gathering the main evidence and analyze it to:
 - determine the root cause,
 - assess the impact on CIs infrastructure.
- available of an timeline of Cyber-physical security event

For the long-term response, this Use case contributes as well to the overall risk and resilience analysis cycle in order to examine the level of resilience of overall systems.

8.4.2. Innovation addressed

- Identify new threats derived detecting a combination of Cyber and physical threat.
- Mitigation and prevention Mitigation and prevention of cyber-physical threat.
- Define new guideline or suggest integration of controls in actual Cyber Security framework.
- Orchestration of threat mitigation by automating responses or speed-up human intervention.

⁸ <https://attack.mitre.org>

- Build a knowledgebase of controls and countermeasure for combined threats.
- Identify the reliability of services and network connections are fundamental for of all CIs. In this test case will be implemented fixed and 5G connections to permit infrastructure connection between two or more site and for orchestration of services offer.

8.4.3. *Suggested KPIs for Use Case 5*

Apart from the contribution of this Use Case to the overall RESISTO implementation statistical data that will be gathered, the following metrics / KPIs are suggested to be measured:

KPI number	Title / Description
K1	Number of detected physical threats
K2	Number of detected cyber threats
K3	Detection probability
K4	Time to detection
K5	Average decision-making time
K6	Average mitigation time
K7	Human intervention/Automated response

Table 13 – Suggested KPIs to be measured during the pilot activities of Use Case 5

9. USE CASE 6: CYBER AND PHYSICAL PROTECTION OF NETWORK AND NETWORK ELEMENTS MECHANISMS USED BY CRITICAL SERVICES THAT IMPACT USERS


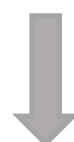
9.1. Introduction and Background

The Cyber and physical protection are driven by human and non-human threats that affect telecommunication networks and endanger the safety and wellbeing of humans by impacting critical services functionality. The critical services in-scope of this Use Case are:

- Voice communications over 4G/5G and fixed networks;
- Data communications over 4G/5G and fixed networks;


The ORO test-bed is built in a redundant architecture closely simulating the production networks of Orange Romania. Most resources are doubled, both physical equipment and virtual machines. The ORO Test-bed closely simulates the real-life usage of OROs production networks, albeit in a scale-down manner and includes most of the monitoring capability and capacity of the production networks. During the testing of OROs Use Case, the Test-bed will behave and output data as close as a real-life production network as possible.

During the testing of OROs Use Case, the following activities will be performed:

- 
1. Implement physical network access protection to limit the intrusion possibilities. Integrate RESISTO with the physical network access control platform for supervision of unwanted physical access;
 2. Protect traffic between highly sensitive information nodes in the network using encryption and anti-replay protection;
- 
3. Generate security events, both cyber and physical, by using traffic generators and event simulators (training mode) with impact on the security perimeter of ORO. The following types of attacks and events will be generated and later used in various correlations for the development of the testing scenarios:

No	Type	Description
1	Cyber	DDoS attack on border router A Distributed Denial of Service attack on a border router point, stemming from OROs networks (both fixed and mobile will be tested).
2	Cyber	DDoS attack on peering point (in conjunction with partner TELCO) A DDoS attack on a peering router used for interconnection with another ISP/TELCO.
3	Cyber	Routing Table Poisoning on Core Network A modification of the routing table(s) of network equipment used in OROs networks (both fixed and mobile will be tested) that re-routes legitimate traffic from the legitimate destination(s)
4	Cyber	Botnet C2C server communication from internal network end-points Communication between infected end-points inside OROs security perimeter to a known Command and Control (C2C) server used by a Bot Network.
5	Physical	Link Disruption (Cable cut)

		A simulation of a fiber cut between MSC Sites – in the Test-bed this will be performed by physically disconnecting the equipment
6	Physical	Rogue access to MSC Site (break in) Unauthorized access to a MSC Site by breaking through the physical security perimeter, gaining access to the equipment hosted in the site. In the Test-bed this will be performed by accessing the server room that hosts the testing infrastructure in OROs principal building. Entry and movement sensors will be triggered
7	Physical	Rogue access to OROs Core Network Datacenter(s) Unauthorized access to OROs Core Network Datacenter(s) by breaking through the physical security perimeter, gaining access to the equipment hosted in the site. In the Test-bed this will be performed by accessing the server room that hosts the testing infrastructure in OROs principal building. Entry and movement sensors will be triggered
8	Physical	Power Outage in MSC Site (unintentional) The interruption of power delivery to a MSC Site due to severe weather breaking the power lines. In the Test-bed this will be simulated by opening circuit breakers and engaging UPS devices.

- 
4. Use ORO IP/RAN/Core/Cyber Security and Physical Security / Access Control elements for relevant information collected from generally named “sensors” for malicious events recognition (cyber, human, non-human);
 5. Sensors will be implemented at every network boundaries e.g. IDS/IPS, DDoS mitigation platform, WAF, roaming end-points, Sites and Buildings (access monitoring);
 6. ORO SOC connects to RESISTO and publishes relevant information reg. cyber-events detection;
 7. ORO physical sensors (motion detection, access control) connects to RESISTO and publishes relevant information req. physical events detection;
 8. RESISTO aggregates the threats information into a database collection (‘knowledgebase’) for future pattern attack recognition;
 9. RESISTO Analyze the information and creates a dashboard for real-time recognition and proper action to be taken, including orchestrating threat mitigation (i.e. – on the physical side – automatic failover to back-up UPSs and Diesel Generators, automatic locking of access doors or –on the cyber security and network ops site -: ‘black holing’ DDoS traffic, isolating network ports, dumping ‘bad’ traffic, disabling compromised user accounts from A.D/LDAP/RADIUS);
 - 10. Operational team takes decisions about high risk events and operates the decision based on the actions suggested by RESISTO**
 11. Identify business critical assets and implement best-practice protection and resilience;
 12. Extrapolate the scenario of cyber & physical security as a driver for next generation virtualized/sliced 5G networks.

9.2. Overall description of the Use Cases and test-beds setup

Fixed Services tests scenario

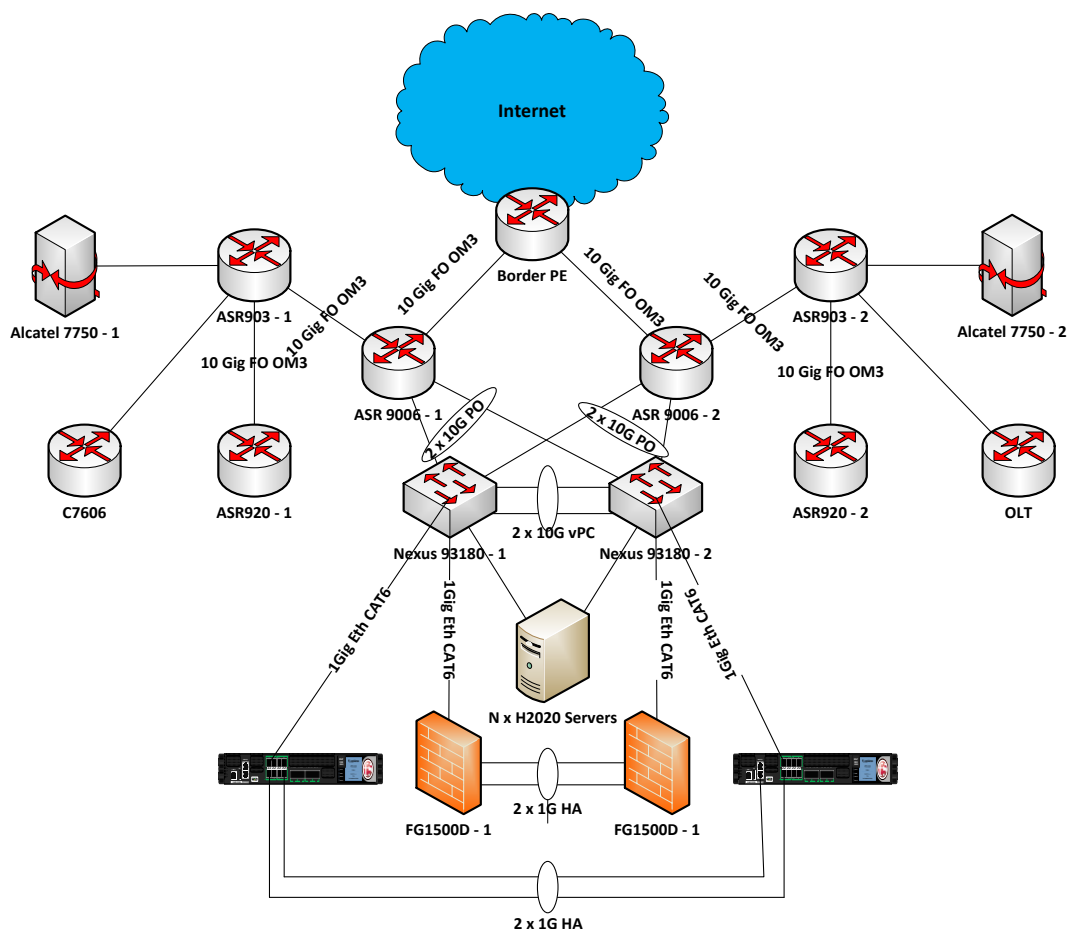


Figure 16: Physical layout of ORO test-bed

Access routers and border/core routers are directly interconnected, in order to assure the testing of Fiber-cut scenario, which is very often encountered in our production network and is included in the Hazards Excel Template. Moreover other physical security scenarios that imply damage of physical connections could be tested using this design. The test-bed also includes various servers which run VMWare and Openstack hypervisors for virtualized solutions and datacenter services emulation.

Most RESISTO components (COCKPIT, some parts of SHORT TERM CONTROL LOOP, LONG TERM CONTROL LOOP) will be deployed in a virtualized environment over Openstack or VMWare – giving the test engineers the possibility to scale-out different components both vertically (grow a single VMs resources) and horizontally (deploy more instances of the same type of VM).

5G Tests scenario

This section describes the Cyber Security use case running on ORO test-bed related to next generation 5G slice networks deployed over the virtualized environment.

The test-bed setup is based on Figure 15, Openstack based and orchestrated through OSMv5.

Through the automation deployment tool there are different network slices deployed, sharing the same physical cluster servers' infrastructure, but dedicated VNFs, isolated in relation to the communication and accessibility from other network slices.

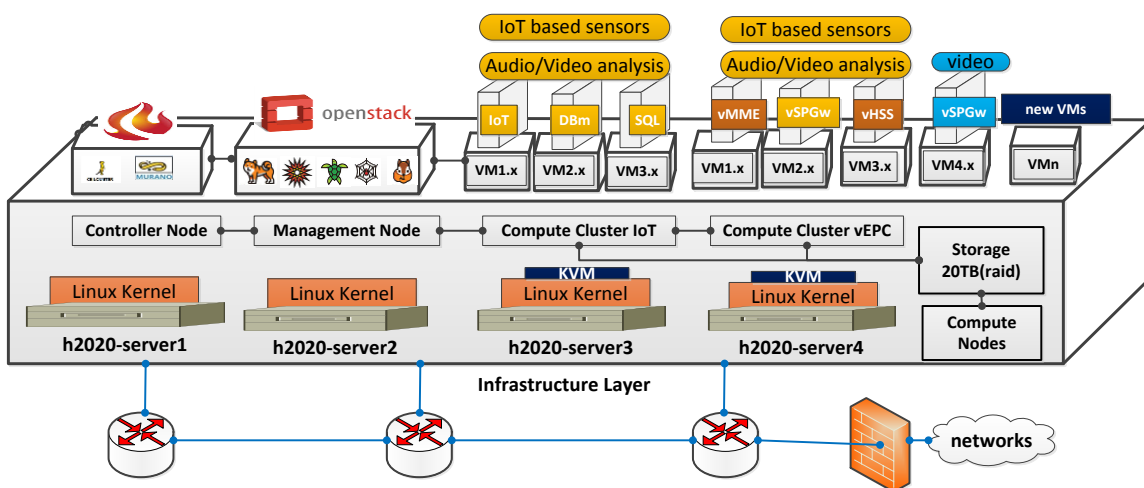


Figure 17: 5G test-bed- physical layout

A 5G network slice is a logical network that provides specific network capabilities and characteristics, for different use cases and application, as described by NGMN

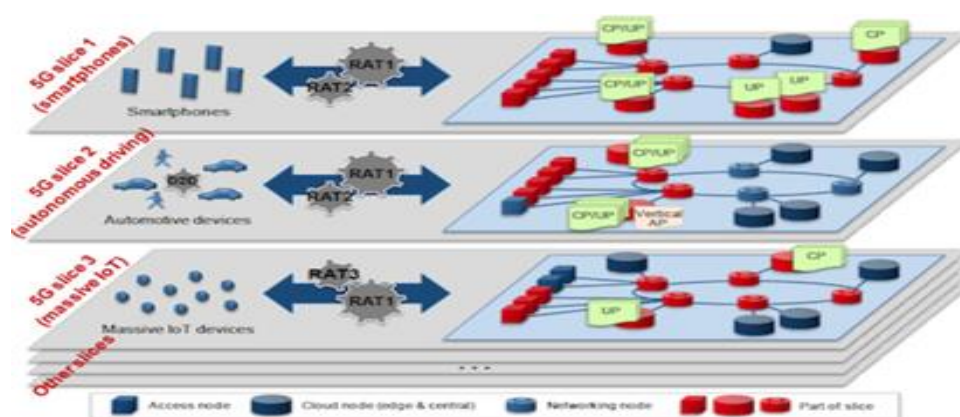


Figure 18: 5G Network Slicing NGMN

The 5G slicing concepts envisaged for this case are based on several 5G-PPP concepts, related to: (1) 5G domain slicing resources shared between different network components, Radio, Transport, Core

Network; (2) Vertical in the loop customizing sliced capable networks for a given vertical customer specifications; (3) Network slice capabilities Life Cycle Management, activities of service preparation, subscription, run-time; (4) Network Slice Physical/Virtual Network Functions belong to Access (AN) and Core (CN), logical network characteristics.

The analytical case for cyber & physical security may determine if in the context of 5G network slicing virtualization, a network component within a slice is subject to a security attack, based on metrics collected during the system functioning. The metrics collected refer to the: (1) CPU; (2) Link bandwidth; (3) RAM consumption; (4) Linux Syslog.

To realize the model, a network slice is deployed over the test-bed, using the proper NFV/VNFs: RAN; EPC; HSS; IoT platform. All this VNFs are Linux based VMs. One of the most exposed platform of the System, the IoT VNF, is used to for system testing. The metrics are collected through Prometheus and then extracted to be further processed. The VM syslogs are basic Linux logs. The data is generated using an IoT simulator, configured to control the messages send to the IoT platform. Prometheus server collects the metrics from server's agent over HyperText Transfer Protocol (HTTP), and then stores them locally or remotely and displays them back in the Prometheus server.

Tests scenario and involved RESISTO components

The following diagram exemplifies ORO's test scenario.

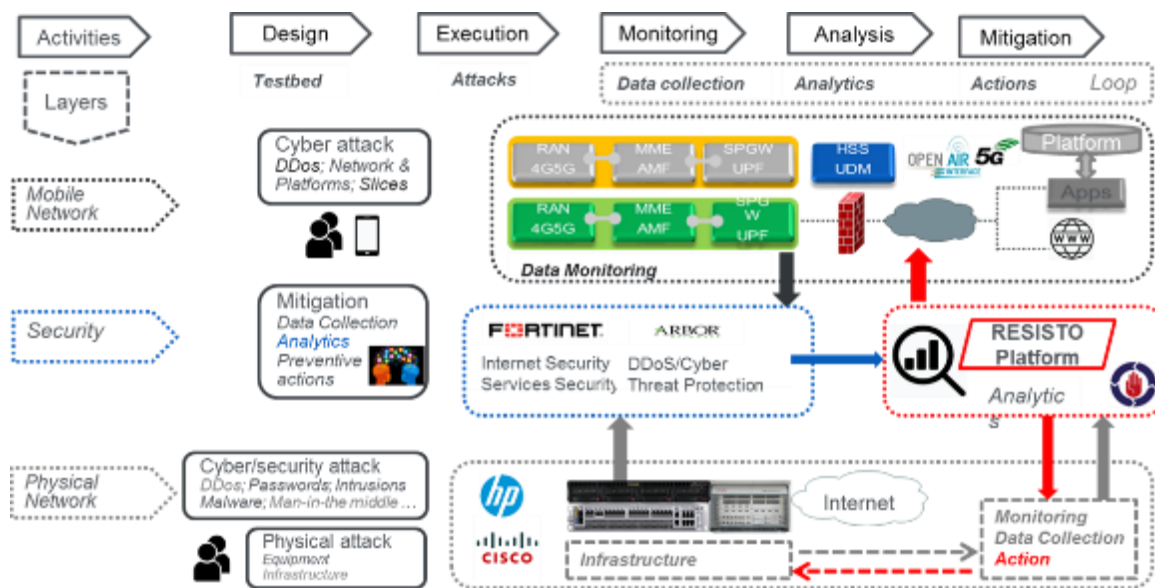


Figure 19: ORO Use Case - testing diagram

The test infrastructure contains various network elements, ranging from high speed backbone routers to mobile and B2B access routers and dedicated virtualized infrastructure, Openstack based and ETSI MANO orchestrated, supported by several capable compute nodes and shared storages. On the virtualized infrastructure there are deployed specific mobile core network components and IoT platforms, in an initial phase 4G network elements and later the new and novel 5G CN. The deployed

virtualized infrastructure will allow to connect several UEs and IoT and OT devices to the network, enabling the ORO to deploy the attack scenarios described below.

During testing ORO will run attack scenarios combining cybersecurity and physical security threats, affecting both Fixed Services and 4G/5G Services that impact users.

5.9.1.1 Scenario 1		DDoS Attack and Fiber Cut	
Description	In this scenario, an unintentional fiber cut resulting from civil works will sever the connections between the two MSCs represented in ORO’s Test-bed. The fiber cut will be followed shortly by a large-scale DDoS attack on one of OROs border routers		
Impact on services functionality	This scenario will impact the voice and data functionality of OROs network as one of the two MSCs will be isolated from the network and the remaining one will be subjected to a large-scale DDoS attack, vastly impacting on the availability of network resources for data and voice communications.		
	Detection		Correlation
	a) SNMP traps will be sent from the NEs indicating the loss of connectivity (Fiber Cut) b) Syslog Messages will be sent from the Anti-DDoS equipment, signaling an ongoing attack		RESISTO will correlate these two events and derive the impact on performance from the data modeled in CISIAPro, in the context of the resources of ORO’s network being already affected by the fiber cut.
	RESISTO Components Tested		
	<ul style="list-style-type: none">• Network Resource Monitoring - Polling Connector in the Data Integration Layer that will receive Syslog Messages from Anti-DDoS• Network Resource Monitoring- SNMP Traps• Short Term Control Loop – Physical & Cyber Detector (Correlator)• Short Term Control Loop – Risk (Impact) Predictor• Knowledgebase – Assets Inventory• Long Term Control Loop – Risk And Resilience assessment analysis• Cockpit – Mitigation Module• Cockpit – Orchestration Module		
	In conjunction with this testing, in this scenario ORO will also test the detection and response capacity of RESISTO to the detection of a Bot Net Inside the Fixed Network of ORO that actively targets a DDoS attack on one of OROs edge routers. A power failure will also be tested in this scenario in conjunction with the fiber cut severing the connectivity between MSCs.		

Table 14 – Use Case 6: Sub Use Case 1

5.9.1.2 Scenario 2 Rogue access to OROs Core Network and Routing Table Poisoning		
Description	In this scenario, a human actor enters in one of OROs Core Network (OROs Site in Gara Herastrau 4A, Bucharest – the location of our test-bed) and attempts (successfully) to connect to a border router, access its administrative console and maliciously change a route to one of OROs servers hosting a critical part of OROs Core Network.	
Impact on services functionality	This scenario will impact the voice and data functionality of OROs network for both B2C and B2B customers as the core network will not be able to effectively verify subscriber profiles against the Core Network Service (HSS)	
	Detection	Correlation
	c) The border router will send a message (syslog) for a successful administrative login d) A network monitoring tool will send a message indicating the down state (unavailable) of the server hosting the Core Network Component e) The Access Sensor installed in ORO's Core Network Site will send a MQTT message to the Physical Resource Monitoring component indicating a state change	RESISTO will correlate these three events and derive the impact on performance from the data modeled in CISIAPro.
	RESISTO Components Tested	
	<ul style="list-style-type: none"> • Network Resource Monitoring - Polling Connector in the Data Integration Layer that will receive Syslog Messages from Anti-DDoS • Network Resource Monitoring- SNMP Traps • Short Term Control Loop – Physical & Cyber Detector (Correlator) • Short Term Control Loop – Risk (Impact) Predictor • Knowledgebase – Assets Inventory • Long Term Control Loop – Risk And Resilience assessment analysis • Cockpit – Mitigation Module • Cockpit – Orchestration Module 	

Table 15 – Use Case 6: Sub Use Case 2

9.2.1. Assets Affected

- Nodes serving network traffic;
- Equipment serving end-users;
- Public WiFi networks serving end-users;
- Datacenters with network monitoring, services and management operations

9.2.2. Impact of the threats foreseen in Use Case 6

Operational: Risk of connectivity loss, Service delivery failure.

Technical: Connectivity Failure, Data Integrity Corruption, Data Confidentiality Corruption. Impacted areas will deal with loss of connectivity to voice and/or data services

Economic: SLAs will be breached for most customers

Societal: Telephony, Internet Services will be affected in large areas causing disruption of normal social interactions in both Consumer and Business areas

9.2.3. Other consequences - Interconnected Critical infrastructures

ORO provides communication services to various Critical Infrastructure Operators in Romania that rely on such services for operations including coordination of activities. A major disruption in availability of service and resource could have cascading effects for operators in the banking and financial sector, transportation sector or the energy sector

9.3. Actors involved

ORO RESISTO team members will assure all the necessary roles for testing the scenarios described in the use case. In the test scenarios defined, different roles can be played by different team members or different roles can be played by the same person.

Actor	Role	Description
Customer	Telecommunication Service Customer	Consumes a Communication Service
Hacker	Cyber and physical attacks generator	Attempts to exploit vulnerabilities in system components' software, hardware and middleware in order to gain access to resources and information or to change the intended use case of the systems
Network specialist	Network and services configurator	Configures the test-bed infrastructure and services for different test scenarios
Information Security/Cyber Security Specialist	Cyber and physical attacks monitor/detect and respond	Monitors the overall functionality of the cyber security systems, uses specific tools and techniques to detect vulnerabilities, malware, erroneous configurations or intrusion attempts and responds to threats.

Table 16 – Use Case 6 actors involved

9.4. RESISTO response and Added Value

As seen from the above description, the RESISTO added value in Use case 6 refers to Detection aspects, Response as this will be output to the ORO SOC and Prevention and Mitigation issues. More specifically, taking into account the above-mentioned scenarios, the following modules from RESISTO platform could be evaluated during Use Case demonstration:

- Before the attack/incident: **Cockpit** will monitor/display the network KPIs and alarms, presenting Run-time situation awareness.
- During the attack/incident, the change of specific KPIs and the correlated alarms/anomalies are indicated, the operators could evaluate the impact on infrastructure with **CISIAppro** and could use **Risk Predictor and Orchestrator** in order to select and apply the best mitigation strategy for the respective incident. Network elements affected are indicated and also network elements that will be affected in the mentioned interval, in case the incident is not mitigated, are shown.
- In case of Power Outage scenario, the following information will be displayed: the time of running on the alternative energy source and the impact on network (services) if the affected network element ceases to function.

9.4.1. Innovation addressed

Potential innovation for Use Case 6, can be summarized as follows:

- A new approach in cyber security based on the convergence of cyber security technology and PSIM tools, may emerge
- The application of a complete risk and resilience management process to a “real-life” test-bed and through a holistic system modelling
- Mindset evolution: the combination of the above may lead to new procedures/changes in the organization’s (telecom operator’s) security policy, while new standards in Physical and Cyber Security may emerge.

9.4.2. Suggested KPIs for Use Case 6

Apart from the contribution of this Use Case to the overall RESISTO implementation statistical data that will be gathered, the following metrics / KPIs are suggested to be measured:

KPI number	Title / Description
K1	Number of detected physical threats
K2	Number of detected cyber threats
K3	Detection probability
K4	Time to detection
K5	Average decision-making time
K6	Average mitigation time
K7	Human intervention/Automated response

Table 17 – Suggested KPIs to be measured during the pilot activities of Use Case 6

10. USE CASE 7: MARITIME SAFETY AND EMERGENCY CASE

10.1. Introduction and Background

The use case dealt with cyber and physical protection. Threats may affect telecommunication networks and services in different areas but in the use case we will analyze and protect maritime and emergency communications.

Maritime sites are located in rural area where control access are easy to bypass. An attacker may have enough time to analyze the site and observe the weak point.

These physical intrusions, such as unauthorized access to a building may be initially seen as physical assaults of a lesser importance in respect to their consequences on the cyber domain.

The attackers may perform reconnaissance and preparatory work on the physical and later in digital front, before moving to actually perform the attack. Thus, the attackers can exploit vulnerabilities to gain access to the complete network.

Based on the above, the present Use Case is a representative example of how seemingly unimportant physical intrusions can facilitate very severe assaults in the cyber domain, creating combined threats (physical threats enabling cyber ones) in existing Maritime telecom infrastructures. Thus, Use Case 7 provides the perfect opportunity to demonstrate how the RESISTO platform can detect, identify and mitigate these combined events, demonstrating the added value of the RESISTO system compared to the conventional security systems, that are unable to correlate physical and cyber threats.

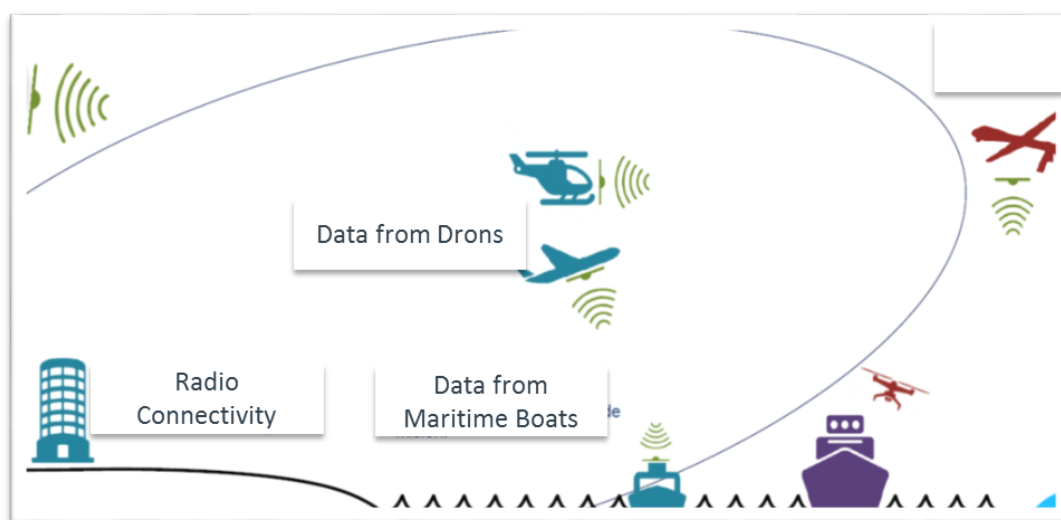


Figure 20: Use case 7 Topology

10.2. Overall Description of the use Case

In this Use Case, a cyber-physical attack takes place, targeting network equipment in a specific maritime location that is physically partially protected. The physical intrusion is performed against the physical assets of the telecom provider. This physical threat is deliberately meant to enable a security threat in the cyber domain of the telecom provider's network. New additional sensors for detection will be deployed for cyber detection. The physical detection will rely on existing physical sensor already deployed by the Infrastructure provider.

An unauthorized person gains entry into a protected building and it is detected using data from the provider's security sensors (i.e. cameras and microphones), which are integrated into the RESISTO system and augmented with sophisticated detection algorithms provided by RESISTO. Thus, a potential security threat in the cyber domain is identified and subsequently detected and eliminated by the provider's cyber detectors and prevention mechanisms activated by RESISTO.

A combined, cyber-physical, attack is executed by a third party targeting the provider's network and it is being detected and neutralized by the capabilities of the RESISTO system; that is the integration of old (existing) and new (from RESISTO) sensors along with the advanced data processing and the decision making mechanisms offered by the RESISTO system.

Although the physical was already protected by the physical detectors of the infrastructure provider, without the RESISTO platform, the combined threats would not even be detected, neither neutralized.

In the use case we will use critical maritime infrastructure to integrate:

- Implement physical network access protection to limit the intrusion possibilities.
- Collect from generally named "sensors" for malicious events recognition.
- Implement traffic information in the network using data probes.
- Integrate RESISTO with our network access control platform for supervision of unwanted access.
- Generate propagation event error to limit the attack in the network and recover the service as soon as possible.
- Generate security events, both cyber and physical, by using traffic generators and event simulators.

10.2.1. Assets Affected

In this use case we propose to protect critical asset that are located in rural areas where the response time is low due to the distance and some time to the kind of accessibility. In this use case we propose to use maritime sites located in the coast line. In any case we are considering a cyber-attack where all the network may be affected.

- **Maritime transmitter:** Transmitter, power supply.
- **Maritime head-end:** Complete end-to-end service
- **Access interconnect:** Point of interconnection to the Infrastructure Provider's access network (e.g. fibre-based access network). Different routers, switches etc...that may interconnect others services or networks.
- **Monitoring center NOC.**

10.2.2. Deployment Topology Example – Test-bed setup

The architecture will be in a general way described with the next diagram which is based on a real Emergency Service provided. The attack may affect different networks depending on the physical connection.

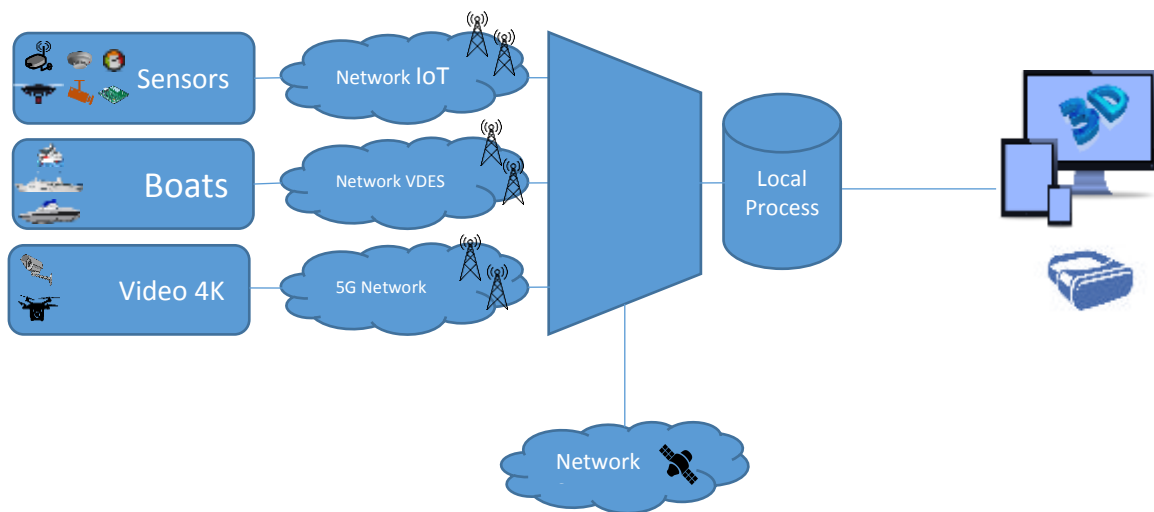


Figure 21: Use case 7 Topology of Emergency service provision

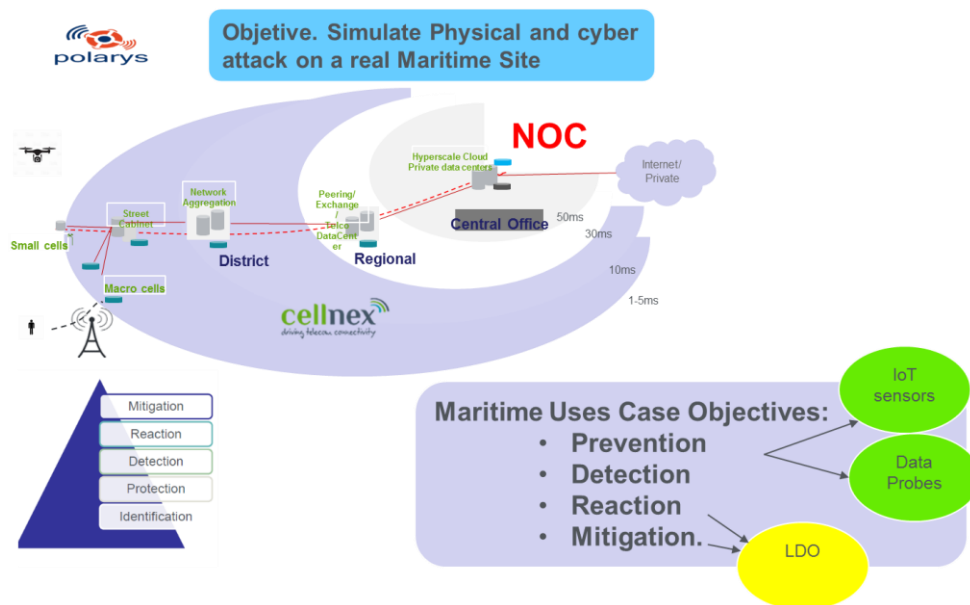


Figure 22: Use case 7 Topology of Maritime Use Cases

10.2.3. Impact of the threats foreseen in this Use Case - Interconnected Critical infrastructures

The impact should be considered in the kind of answer and protocol to follow. Possible affected infrastructures may be other TV or radio sites, the service or services and finally the network completely.

- In a first moment the possible attack may affect the service provide in that zone.
- Secondly the propagation may affect others services in that site.

- Moreover the propagation may affect other sites and others services.
- Finally the attack could have an impact in the complete network.

10.3. Actors and detection tools involved

The main actors to be involved in the use case are:

- Infrastructure providers. Maritime sites
- Physical probes manufacturers.
- Cyber prober manufacturers.
- Drones manufacturers.
- Satellite equipment providers.
- RESISTO platform configuration/set up IA algorithm.

10.4. RESISTO response and Added Value

The RESISTO added value in this Use Case can be summarized in the additional functionalities that are provided towards Detection, Response and Mitigation. The detection functionalities have been described through the scenarios presentation above, while for those concerning Response and Mitigation, the following can be noted:

10.4.1. RESISTO Short Term response

The objective of the integration with RESISTO platform is to have a real time response in order to mitigate the attack. The RESISTO Short Term should detect the physical attack as soon as possible in order to avoid the cyber-attack. A combination of cyber and physical attack may be detected too. RESISTO should provide first the corresponding alert message to the corresponding profiles and moreover some recommendations on how to proceed to avoid the shut-down of the network.

The short term should be responsible of assessing redundant system while prepare the first step in reaction to the attack.

10.4.2. RESISTO Long Term response

This Use case will also contribute to the risk and resilience tool being incorporated to the database while considering the mitigation path. LTCL may also consider equipment and network affected as well as different profiles of users. The long term response will set up and update the configuration files for the short term response and determine the strategies for responding the attacks along with evaluating future countermeasures.

10.4.3. Innovation addressed

The objective of the use case is to integrate both Cellnex (RTV) and RESISTO platforms aiming at:

- RESISTO Analyze the information and creates a dashboard for real-time recognition and proper action to be taken, including site attacked, propagation or network affected and estimation of response.
- RESISTO to orchestrate threat mitigation by automating responses.
- RESISTO aggregates the threats information into a database collection ('knowledgebase') for future pattern attack recognition and prediction with AI algorithms.
- Operational team takes decisions about high risk events and operates the decision based on the actions suggested by RESISTO IA algorithms.
- RESISTO IA algorithm to identify business critical assets and implement best-practice protection and resilience.

10.4.4. Suggested KPIs for Use Case 7

Apart from the contribution of this Use Case to the overall RESISTO implementation statistical data that will be gathered, the following metrics / KPIs are suggested to be measured:

KPI number	Title / Description
K1	Number of detected physical threats
K2	Number of detected cyber threats
K3	Detection probability
K4	Time to detection
K5	Average decision-making time
K6	Average mitigation time
K7	Human intervention/Automated response

Table 18 – Suggested KPIs to be measured during the pilot activities of Use Case 7

11. USE CASE 8: PPDR VIRTUAL OPERATOR

11.1. Introduction and Background

From a user perspective, 5G is inherently different to any of the previous mobile generations. Machine-type communication, enabled by 5G, is widely anticipated to become the strategic difference and unique selling point of 5G in the long run. 5G networks will serve as critical infrastructures to facilitate the digitization, automation and connectivity to machines, robots and transport solutions etc. Thus, there is significant value at stake and, so too, a significantly different tolerance for risk. 5G marks the beginning of a new era of network security with the introduction of IMSI encryption. All traffic data which is sent over 5G radio network is encrypted, integrity protected and subject to mutual authentication e.g. device to network

On one hand, actual technologies such as 4G can be hacked. In new technologies such as 5G it has been stated to be more reliable but introducing aspects like MEC may **open new doors for hacking systems**.

On the other hand, frequencies are very expensive and new business model propose **sharing frequencies**. Commercial services may share frequency with critical services.

This use cases deals with critical services protection from commercial services combining MEC services while sharing frequency.

Additionally, it deals with cyber protection. Threats may affect telecommunication networks and services in different areas but in the use case we will analyze and protect next 5G networks.

11.2. Overall description of the Use Case and Test-beds setup

Basically, the core network can provide a number of services to subscribers that are connected via the access network into the core, such as telephone calls and data connections. The transport network keeps the access network connected with the core, and the base stations within the radio access network connected with each other. The interconnect network connects different core networks with each other. Telecommunication networks transfer voice and data across the globe with high quality and consistency. User devices such as mobile phones can stay connected regardless of time and place, which is all possible thanks to standardized signalling systems and interfaces.

Each network part can be subdivided further into three so-called network planes, each of which carries a different class of traffic: signalling traffic, user payload traffic and management traffic. The signalling plane transports messages that are used to control user sessions, e.g. establishing a call or data session. The contents of a call or web page is referred to as user plane or user payload. The management plane includes management of monitoring, troubleshooting, configuration and optimization of networks.

All planes are of interest for threat actors for varying reasons:

Signaling – the metadata which supports the networks is targeted to obtain information such as the geographical position of a subscriber. Modification of signaling traffic may be attempted to re-route calls or intercept SMS messages of a target for eavesdropping purposes or denying service. Today's security risks are far more developed and complex compared to previous generation technology. As such, signaling of previous generations, such as 2G, was developed with a reduced focus on security. This was owing, in part, to a high level of trust in signaling peers. Now we know better. Telecom

signaling is regularly attacked and sometimes exploited on a daily basis. In current 5G 3GPP standardization, security is now taking a central role across all aspects.

User payload traffic contains the actual data that is transferred for the user. Without appropriate security measures, the privacy of the user and the confidentiality of enterprise or government data would be at risk. So far, integrity protection for user payload traffic has been seen as necessary.

The management layer is needed to ensure that the service provider's business performs optimally. The management plane is an attractive target for hackers to gain access to network resources, where they can manipulate and disturb network traffic and data. Mitigation of network management related risks and threats requires security policies and several security controls to be implemented, such as access control and security monitoring, in the right places (section 4).

In the use case we will use critical infrastructure to simulate an attack using the **signaling** plane. In this use case we will integrate the following aspects:

- Implement network Slicing protection to reduce the intrusion from one private network to another private network sharing frequency.
- Implement traffic information in the network using data probes.
- Integrate RESISTO with our network access control platform for supervision of unwanted access.
- Generate security events, both cyber and physical, by using traffic generators and event simulators.
- Generate propagation event error to limit the attack in the network and recover the service as soon as possible.

The objective of the use case is to integrate both Cellnex (RTV) and RESISTO platforms aiming at:

- RESISTO Analyze the information and creates a dashboard for real-time recognition and proper action to be taken, including slice or service attacked, propagation or network affected, time/period of the attack, and estimation of response.
- RESISTO to orchestrate threat mitigation by automating responses.
- RESISTO aggregates the threats information into a database collection ('knowledgebase') for future pattern attack recognition and prediction with AI algorithms.
- Operational team takes decisions about high risk events and operates the decision based on the actions suggested by RESISTO AI algorithms.
- RESISTO AI algorithm to identify business critical assets and implement best-practice protection and resilience

In the use case we will use 5G infrastructure to increase the security and mitigate the cyber- attack while:

- Implement 5G network with Slicing and Virtualization
- Collect data from traffic from the network and Implement traffic information in the network using data probes.
- Integrate RESISTO with our network access control platform for supervision of unwanted access.
- Generate propagation event error to limit the attack in the network and recover the service as soon as possible.
- Generate security events, both cyber and physical, by using traffic generators and event simulators.

In one site we may have more than one service running associated to different MNO. One user active may use GTP protocol to try to access services running in the MEC from another operator.

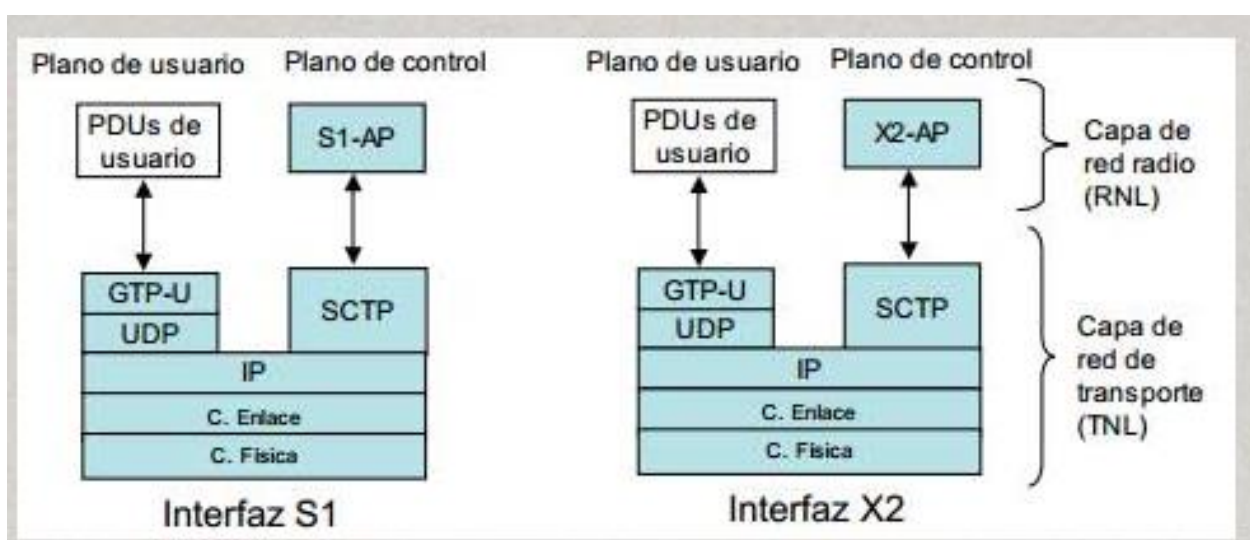


Figure 23: Use case 8-Attacks on Services and protocols

One user may know that a certain service in a concrete IP is served from the MEC for slice 2 of another operator. In that case the user is using a service not allowed to.

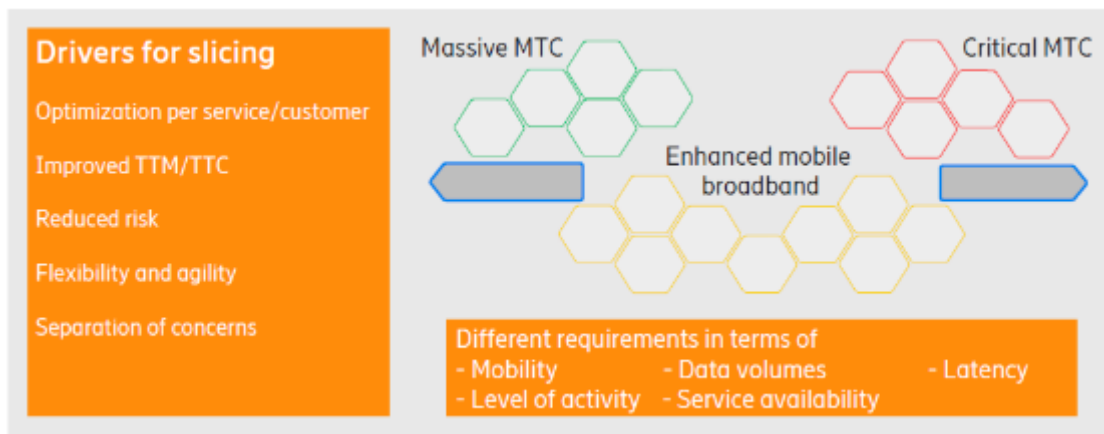


Figure 24: Use case 8 network slicing

We will implement a service running in a 5G MEC architecture. The service is running in a slice while and due to the criticist is in redundancy. Each slice runs the service deployed in a Virtual machine.

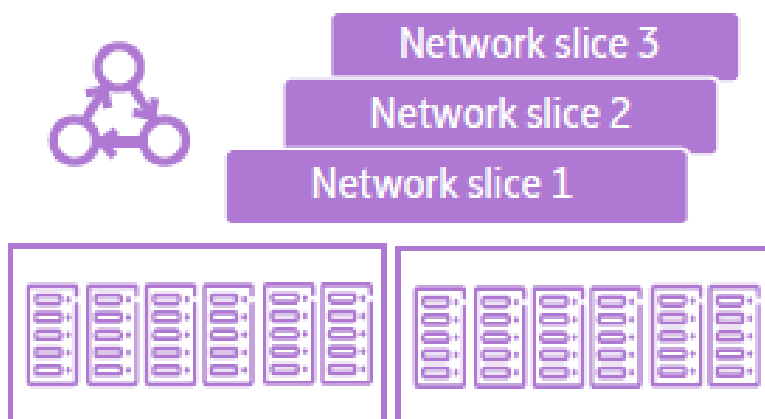


Figure 25: Use case 8 5G MEC architecture slices

The proposed architecture is the following one. The key point is the MEC virtualized managed by the orchestrator and the interconnection between orchestrator and RESISTO.

Future Network Uses Case: Scheme

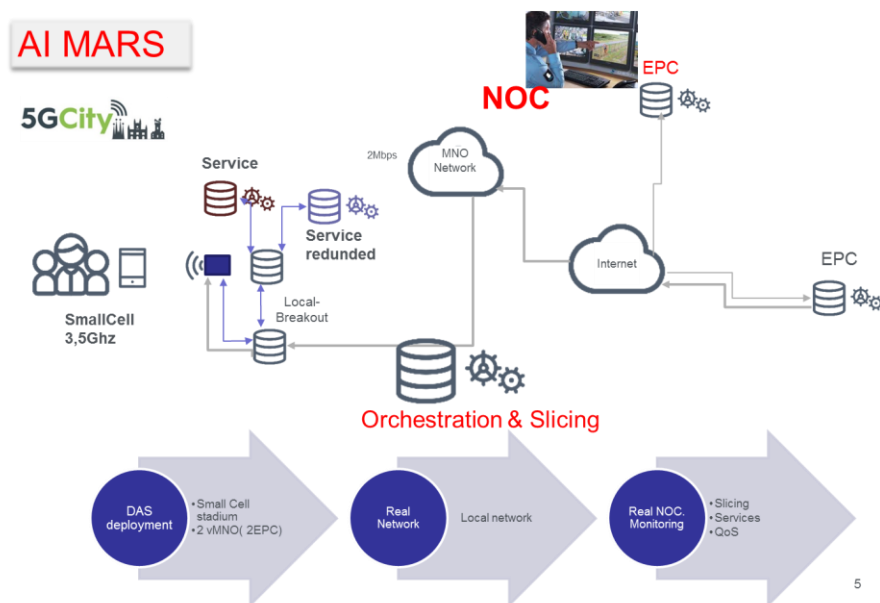


Figure 26: Use case 8 proposed architecture

The MEC Virtualization architecture that will be implemented is shown below:

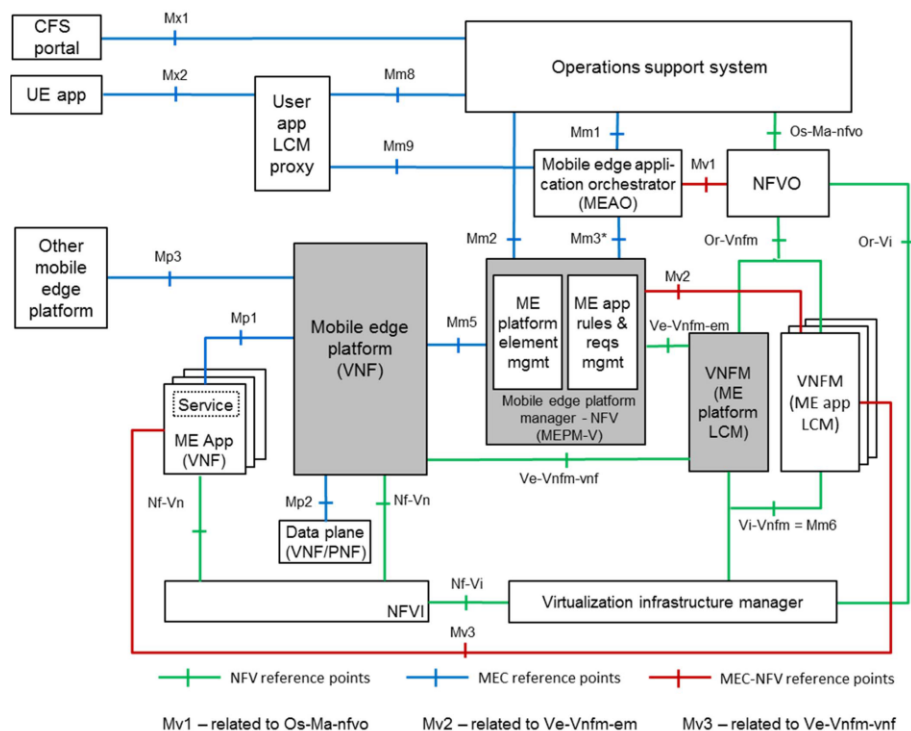


Figure 27: Use case 8 MEC Virtualization architecture

11.2.1. Assets Affected

In this use case we propose to protect 5G assets and more precisely the virtualization part included of the services in the MEC. The architecture will be in a general way described with the next diagram: Cell, eNode will be a common part in order to guarantee services and slicing. SGW will be also shared by the different MNOs or service providers. The idea is to guarantee that other MNO or services providers are not affected by any attack using the common part. Here not only the network may be affected but others services are to be monitored and secured.

Mobile Network Sharing Options

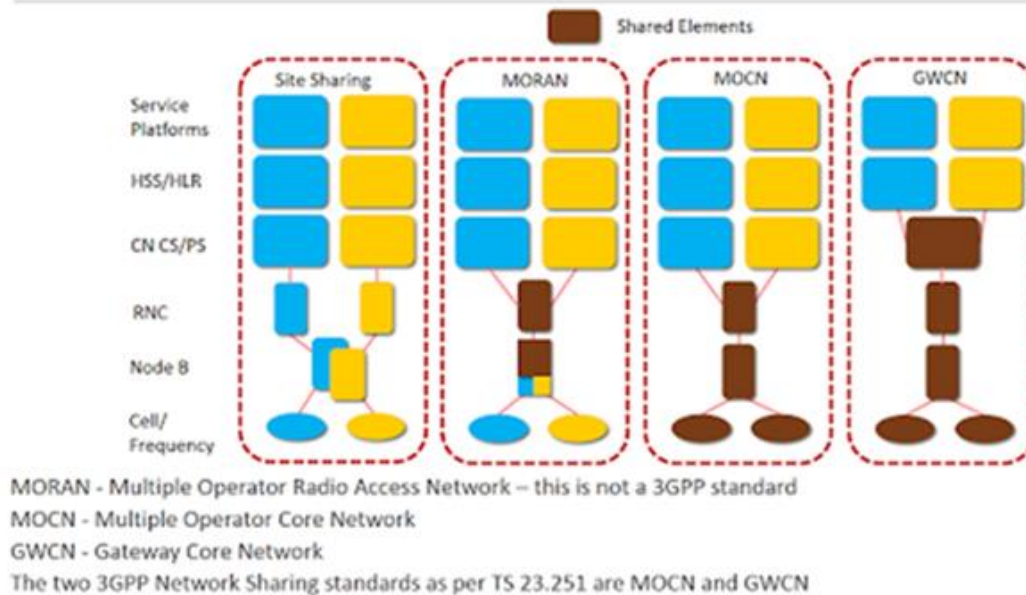


Figure 28: Use case 8 assets affected

11.3. Actors and detection tools involved

The main actors to be involved in the use case are:

- Infrastructure neutral provider with slicing
- Cyber probes manufacturers
- RESISTO platform configuration/set up IA algorithm.
- Virtualization
- MEC services

11.4. RESISTO response and Added Value

The RESISTO added value in this Use Case can be summarized in the additional functionalities that are provided towards Detection, Response and Mitigation. The detection functionalities have been described through the scenarios presentation above, while for those concerning Response and Mitigation, the following can be noted:

11.4.1. RESISTO Short Term response

The objective of the integration with RESISTO platform is to have a real time response in order to mitigate the attack. The RESISTO Short Term should detect the cyber-attack as soon as possible in order to avoid the negation of service.

RESISTO should provide first the corresponding alert message to the corresponding profiles and moreover some recommendations on how to proceed to avoid the shut-down of the network.

11.4.2. RESISTO Long Term response

This Use case will also contribute to the risk and resilience tool being incorporated to the database while considering the mitigation path. LTCL may also consider equipment and network affected as well as different profiles of users. The long term response will set up and update the configuration files for the short term response and determine the strategies for responding the attacks along with evaluating future countermeasures.

11.4.3. Innovation addressed

The objective of the use case is to integrate both Cellnex (RTV) and RESISTO platforms aiming at:

- RESISTO Analyze the information and creates a dashboard for real-time recognition and proper action to be taken, including site attacked, propagation or network affected and estimation of response.
- RESISTO to orchestrate threat mitigation by automating responses.
- RESISTO aggregates the threats information into a database collection ('knowledgebase') for future pattern attack recognition and prediction with AI algorithms.
- Operational team takes decisions about high risk events and operates the decision based on the actions suggested by RESISTO IA algorithms.
- RESISTO IA algorithm to identify business critical assets and implement best-practice protection and resilience.

11.4.4. Suggested KPIs for Use Case 8

Apart from the contribution of this Use Case to the overall RESISTO implementation statistical data that will be gathered, the following metrics / KPIs are suggested to be measured:

KPI number	Title / Description
K2	Number of detected cyber threats
K3	Detection probability
K4	Time to detection
K5	Average decision-making time
K6	Average mitigation time
K7	Human intervention/Automated response

Table 19 – Suggested KPIs to be measured during the pilot activities of Use Case 8

12. USE CASE 9: 5G NETWORK RESPONSE TO A SECURITY BREACH

12.1. Introduction and background

5G networks are not just a quantitative evolution similar to previous transitions, such as higher bitrate, lower latency and more devices, but rather a qualitative leap forward to meet the demands of a fully networked society. From a security viewpoint, 5G introduces new challenges that require attention and have been discussed in the literature [11]. Because 5G will connect every aspect of life to communications networks, the security challenges are quite diversified and include [12]:

- Flash network traffic: a high number of end-user devices and new things (IoT);
- Security of radio interfaces: radio interfaces encryption keys are sent over insecure channels;
- User plane integrity: there is no cryptographic integrity protection for the user data plane;
- Mandated security in the network: service-driven constraints on the security architecture lead to the optional use of security measures;
- Roaming security: user-security parameters are not updated with roaming from one operator network to another, leading to security compromises with roaming;
- DoS attacks in the infrastructure: there are visible network control elements and unencrypted control channels;
- Signalling storms: distributed control systems require coordination;
- DoS attacks on end-user devices: there are no security measures for operating systems, applications, and configuration data on user devices.

The Figure below from [12] summarizes the threat landscape for 5G network scenarios.

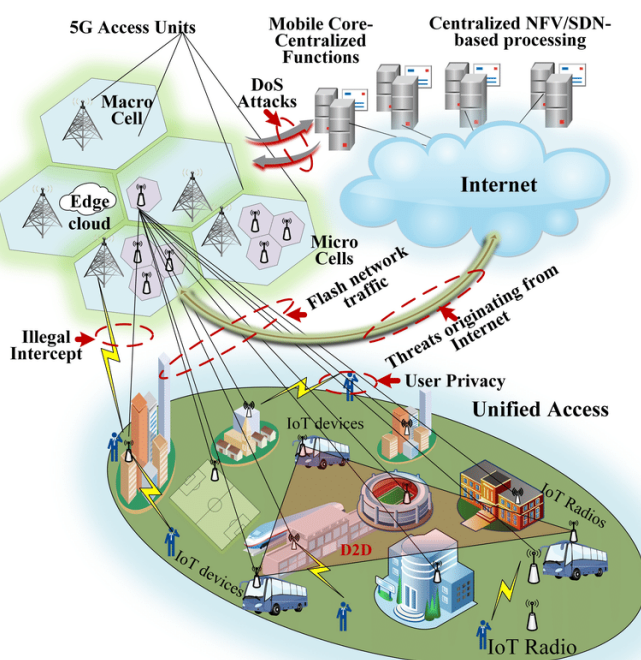


Figure 29: Threat landscape for 5G network scenarios

The complexity added by 5G requires traditional (i.e. preconfigured) security solutions to be supplemented and reinforced with dynamic mechanisms, instantiated and deployed by AI-based systems[13]. Early and integrated threat detection is a key requirement. Complex mechanisms based on a combination of big data and ML can be used to identify threats not spotted by conventional solutions supported by basic filters.

In addition, prompt reaction is also a key requirement. 5G provides a number of tools to avoid or mitigate the effects of security and resilience threats, which are mainly related to the capability to detach network functions from the infrastructure and flexibly control the lifecycle of network services. The independence between network and infrastructure, which strictly speaking is not enabled by 5G, but rather the virtualization of network resources, paves the way to the definition of innovative security use cases. Network slicing is the main enabler and catalyst to properly deliver those use cases.

The combination of AI-based detection tools with network slicing provides new possibilities to prevent or mitigate many of the security and resilience threats in telco infrastructures, especially for 5G, and is likely to represent a relevant research topics in the next few years. The use case described in this section hopefully illustrates the synergies that can be obtained through the combination of these two technological trends.

12.2. Overall Description of the Use Case

Network slicing is an important tool to provide isolated networks, each optimized for specific types of traffic characteristics. One such characteristic could be related to security and safety requirements - by means of slicing, it will be possible to dynamically confine the impact of security requirements to single slices, rather than the whole network. In addition, new recovery mechanisms are enabled by network slicing, especially the capability to establish network resources on-demand.

The proposed use case comprises a mission-critical scenario based on a 5G telecommunication mobile network in which the probability of an ongoing cyber/physical attack or equipment failure is assessed by continuous analysis of specific parameters (e.g. temperature) or abnormal behaviour, making use of machine learning techniques. The use case definition is based on the execution of different actions depending on the perceived probability of equipment failure.

Initial State

The initial state of the use case is represented in the figure below.

The SP (also playing the role of NSP, see description of these roles above) builds and operates a network slice based on own resources – core network, core DC (hosting the majority of the 5G Core components), coloured black in the figure, as well as resources leased from an independent Network Slice Subnet Provider (NSSP A) – C-RAN and edge components, coloured green in the figure.

In that specific edge geographical area, the SP has a business relationship with a second NSSP (NSSP B, not represented in the figure), also able to provide C-RAN and edge components if/when needed (e.g. for reasons of malfunction or quick traffic growth), but not active by default.

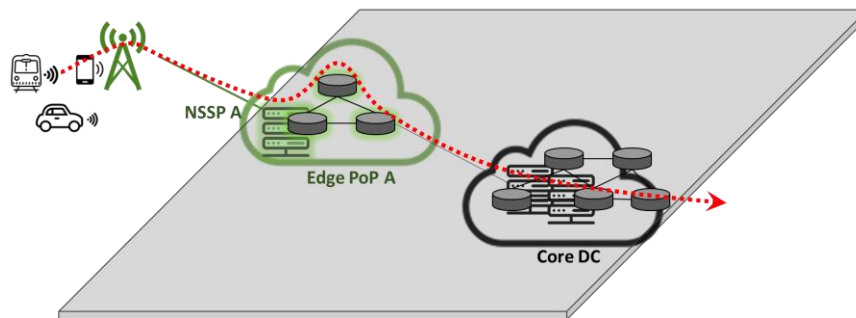


Figure 30: Use case 9 initial state

Phase 1 - Preparation

The use case is triggered when the probability of service loss affecting resources run by NSSP-A goes above a certain threshold, e.g. 35% (possible cause – temperature rising in Edge PoP). The event may be accidental, caused by a natural event, or by a malicious action.

At this stage, the risk is classified as low to medium. The preparation of a smooth transition from NSSP-A to NSSP-B is started through the creation of a slice subnet (C-RAN, Edge, x-haul) dimensioned according to the number of users. Recovery mechanisms (e.g. equipment restart) if available and feasible, are attempted.

The SP requests NSSP-B to instantiate an edge slice subnet, in case a relocation of resources from NSSP-A proves to be necessary as a result of the identified issue.

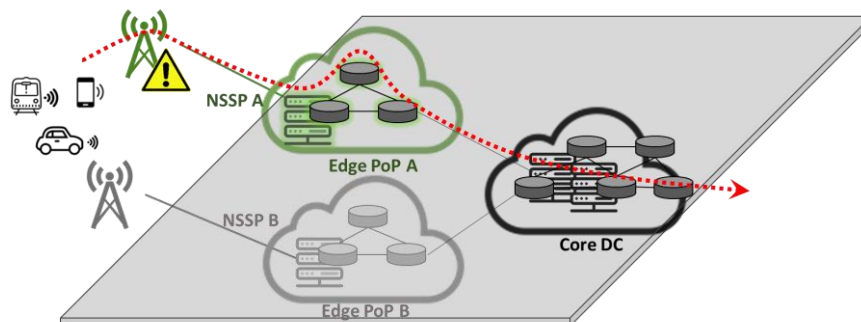


Figure 31: Use case 9 phase 1 (preparation)

Phase 2 - Activation

The second phase of the use case is triggered when the service loss probability goes above a second threshold (e.g. 50%). At this point, the risk is classified as high. The slice subnet that had been instantiated in the previous step is activated at this point (colored blue in the figure below). This

includes the activation of all VMs/containers, as well as the virtual links. At the same time, non-essential resources are shutdown.

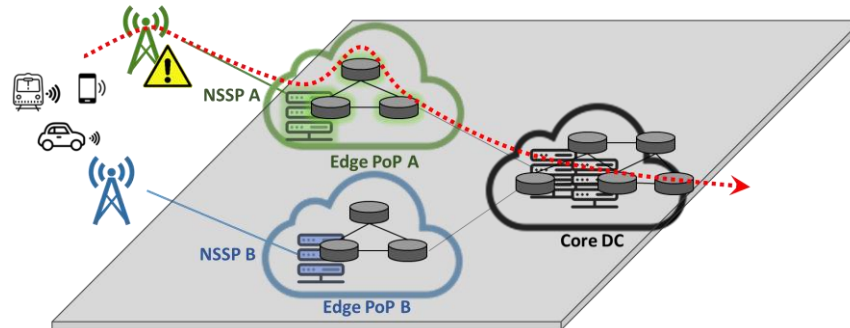


Figure 32: Use case 9 phase 2 (activation)

Phase 3 - Migration

The third phase corresponds to actuation/mitigation and is triggered when a third service loss probability threshold (e.g. 65%) is exceeded. The affected C-RAN and edge components are relocated from NSSP A to NSSP B; however, from the customer perspective, the impact should be as minimal as possible (ideally, no perceived impact). This is illustrated in the figure below.

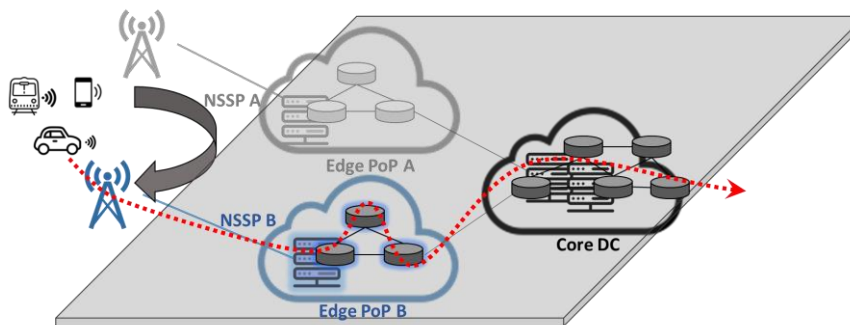


Figure 33: Use case 9 phase 3 (migration)

In a 5G environment, the actuation phase takes advantage of network slicing and the capability to deploy network services on demand. In this case, the affected resources (i.e. those provided by NSSP A) should be deactivated and replaced by different resources in such a way that service continuity can be guaranteed.

12.2.1. Assets Affected

In this use case, the assets affected are the NSSPs and, as a consequence, the SP.

12.2.2. Deployment Topology Example – Test-bed setup

The following Figure illustrates the topology of the test-bed that will support the 5G use case, as well as the main components. The physical resources will be deployed in two sites, Altice Labs headquarters and the Institute of Telecommunications, both of which are located in the city of Aveiro, separated by roughly 2 km. The transport network infrastructure providing connectivity between the two physical sites is based on NGPON-2 technology.

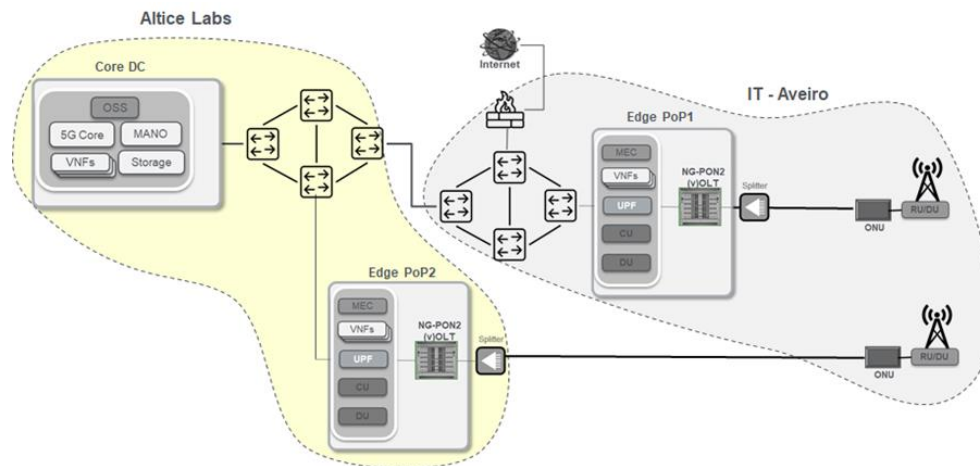


Figure 34: Use case 9: 5G use case topology and basic components

12.3. Actors and detection tools involved

In the context of this use case, four main roles are involved, as shown in the following table:

Actor	Role	Description
Customer	Communication Service Customer	Consumes a Communication Service
Service Provider(SP)	Communication Service Provider	Provides a Communication Service Consumes Network Slice(s)
Network Slice Provider (NSP)	Network Operator	Provides a Network Slice Consumes Network Slice Subnet(s) ⁹
Network Slice Subnet Provider (NSSP)	Network Operator	Provides a Network Slice Subnet

Table 20 – Use Case 9 - Actors Related to 5G

⁹ In this context, a subnet corresponds to a set of network functions and the resources for these network functions which are arranged and configured to form a logical network [15].

The Service Provider (SP) is the key role in the use case storyline. The SP provides communication services to end-users, supported by network slices. The SP is also supposed to provision of the network, thus it also plays the Network Slice Provider (NSP) role.

A network slice can be composed of multiple network slice subnets (e.g. core, edge). Each slice subnet may be owned and operated by the SP, or by an independent NSSP (Network Slice Subnet Provider).

The security threat vectors in 5G will be multi-dimensional, as 5G networks will connect infrastructures, interconnect societies and industries, providing anything-as-a-service, and integrate new models of service delivery. Since 5G has higher flexibility and agility, Network Functions Virtualization (NFV) and Software Defined Networking (SDN) play a vital role in 5G[14].

The virtualization of network resources, and especially network slicing, enable the definition of new business models based on new stakeholders and roles. In this context, the definition of any 5G use case should be understood under a specific business ecosystem, where different players are responsible for playing different roles. A detailed analysis is provided in 3GPP TR 28.801 [15].

The following figure, copied from 3GPP TR 28.801 [15], illustrates possible relationships between these roles. It is important to note that multiple scenarios can be defined – different roles can be played by different players, or different roles can be played by the same player.

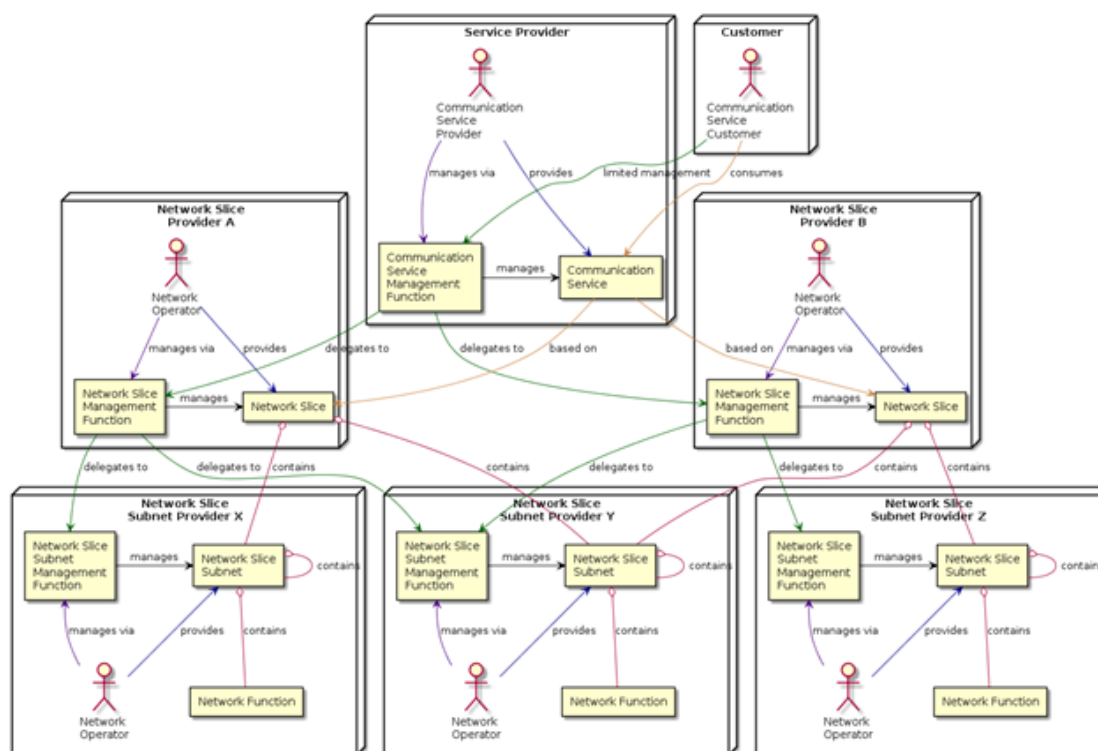


Figure 35: Use case 9: General example of network slicing management functions [15]

The use case described is based on novel 5G business models enabled by NaaS and the separation of service providers and (virtual) infrastructure providers. In addition, the possibility of sharing mobile access/edge network resources among competitor operators under certain circumstances (e.g. natural events such as forest fires affecting the availability of the mobile network in a certain zone)

has been suggested for possible implementation as a way to avoid loss of communication, which is often a cause for aggravation of the effects of this kind of events.

12.4. RESISTO response and Added Value

The use case demonstrates how the RESISTO platform can be used to mitigate the following risks, among others:

- Service delivery failure in a geographical area, as a result of intentional malicious actions (e.g. cyber-physical attacks, motivated either by terrorism and economic sabotage), equipment malfunctions or natural events (e.g. forest fire, potentially endangering significant components of the network infrastructure physically located on that zone).
- Financial losses, both to operators (loss of income, customer churn) and end users (especially businesses for which communication is a critical requirement).
- Damages caused by network disruptions, especially in emergency scenarios, potentially exposing human lives to risk.

The most significant contribution of RESISTO is on the **Decision-making process** as seen below:

12.4.1. Short term control loop

Although a detailed analysis of the RESISTO short term loop components is out of the scope of this document, a general overview of the actions performed by each component during the execution of the use case is attempted in the figure below.

The use case will be based on a data set provided by Altice, related to fixed and mobile infrastructures, which feeds the RESISTO correlator AI engine. The data set includes alarms of KPI threshold violations, alarms of network element failures (partial, total), trouble tickets and inventory of network elements.

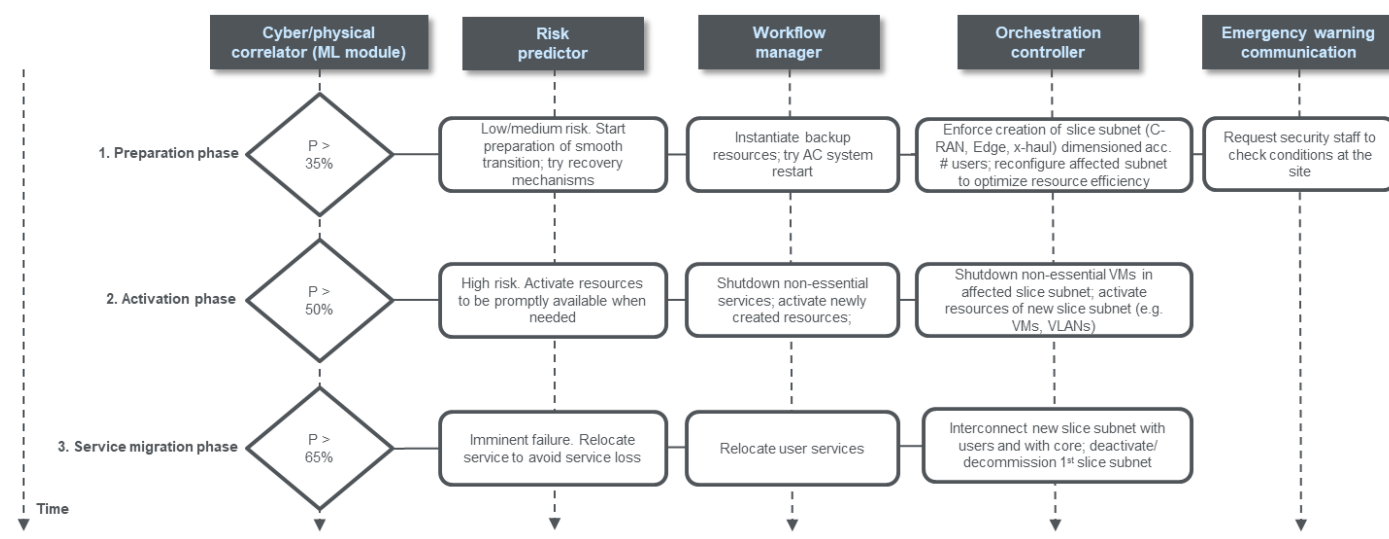


Figure 36: Use case 9: Overall use case decision making by RESISTO short term loop

Based on ML/AI techniques, network element failures are predicted by the cyber/physical correlator. A root cause analysis is performed with a view to identifying potential security breaches (by the risk predictor) and defining adequate actuation strategies to mitigate the impact of the security incident (by the workflow manager), to be enforced by the orchestration controller. Optionally, the emergency warning communication module intervenes to alert the security staff, if manual actuation is considered necessary to mitigate or avoid the security event.

12.4.2. Long term control loop

A Long Term Control Loop cycle is performed on a periodic basis or when particular events take place (new threats or discovery of previously undetected vulnerabilities) [D6.1] [16]. In this particular use case, several actions taken by the long term control loop can be defined, with a view to continuously improving infrastructure resilience.

The evolution of the short term loop process outlined above is guided by the failure probability estimated by ML/AI algorithms. However, there a number of variables that must be adjusted to optimize the efficiency and the effectiveness of the process. The fine tuning of these variables is supposed to be done by the long term control loop, based on the observation of the results of the short term control loop. Examples are:

- Failure probability levels – the objective is to optimize the prompt reaction to suspicious events, while at the same time minimizing the reaction to “false positives” and avoiding the implementation of unnecessarily complex and intrusive mitigation actions.
- Alternate mitigation actions – before applying the “last resort” action (i.e. to relocate the service to a different infrastructure), less intrusive actions can be attempted, either automated (e.g. system restart) or manual (e.g. request support staff to verify conditions on site). Depending on the observed effectiveness of these actions, different strategies can be defined.
- Timers – several actions included in the process are bounded by timers (e.g. maximum time to instantiate a new virtual subnet, maximum time for manual staff intervention). These timers should be dynamically adjusted by the long term control loop based on the observation of the system under failure conditions.

12.4.3. Innovation addressed

The innovations of this use case are mainly related to the combined use of two types of tools for security threat detection and mitigation, respectively:

- AI/ML-based detection mechanisms for early detection of security threats;
- Network automation and programmability, enabled by 5G cornerstones such as network virtualization, software defined networking and network slicing.

This use case is expected to evaluate and demonstrate the preparedness of the RESISTO platform to handle the specific challenges of 5G and the ability to exploit the 5G features mentioned above in scenarios of cyber-physical attacks or natural events.

12.4.4. Suggested KPIs for Use Case 9

Apart from the contribution of this Use Case to the overall RESISTO implementation statistical data that will be gathered, the following metrics / KPIs are suggested to be measured:

KPI number	Title / Description
K2	Number of detected cyber threats
K3	Detection probability
K4	Time to detection
K5	Average decision-making time
K6	Average mitigation time
K7	Human intervention/Automated response

Table 21 – Suggested KPIs to be measured during the pilot activities of Use Case 9

13. TRACEABILITY MATRICES - KPIS AND REQUIREMENTS MAPPING

The use of key performance indicators (KPI) has become a recognized practice in measuring performance. In this section, an effort has been made to map the already identified KPIs (included in D3.7 [3] and D3.8 [4]) and user requirements that are applicable and addressed by the described RESISTO use cases.

13.1. KPIs Mapping

KPI's \ Use Cases	UC 1	UC2	UC 3	UC 4	UC5	UC 6	UC7	UC8	UC 9
K1: Number of detected physical threats	X	X	X	X	X	X	X		
K2: Number of detected cyber threats	X	X	X	X	X	X	X	X	X
K3: Detection probability	X	X	X	X	X	X	X	X	X
K4: Time to detection	X	X	X	X	X	X	X	X	X
K5: Average decision-making time	X	X	X	X	X	X	X	X	X
K6: Average mitigation time	X	X	X	X	X	X	X	X	X
K7: Human intervention/Automated response	X	X	X	X	X	X	X	X	X

Table 22 – KPI's mapping to RESISTO use cases

13.2. User Requirements addressed by the RESISTO Use cases

The described Use cases address the following User Requirements (selected from the User requirements extracted in D2.1).

Requirement Identity Code	Requirement Description
RES_FUN_0005	RESISTO shall exploit the outcomes of the cyber security and the physical security systems of the TLC infrastructures (if existing).
RES_FUN_0006	RESISTO shall provide physical intrusion detection based on a variety of sensors, such as audio/video/radar and other passive and active sensors.
RES_FUN_0030	RESISTO shall be able to receive, collect and process alert events relev. to physical detection.
RES_FUN_0070	RESISTO shall suggest to the operator the necessary steps to mitigate the effect of a cyber/physical attack.
RES_FUN_0100	RESISTO shall collect non-authorized personnel access to the telecom facility if prov. by the operator.
RES_FUN_0390	RESISTO shall have a whitelist with all authorized radio devices inside the telecom facility.
RES_FUN_0400	RESISTO shall have a list of all authorized cells or base stations and their operating frequency range in a target area.
RES_FUN_0550	The <i>Mitigation Module</i> shall provide automated or semi-automated mitigation responses based on pre-defined templates.
RES_FUN_0560	The <i>Risk (Impact) Predictor</i> shall also include a network impact as well.
RES_FUN_0570	The <i>Risk and resilience assessment analysis</i> shall also take into consideration network single point of failure nodes, using network metrics such as:
	<ul style="list-style-type: none"> • Link state protocol databases for alternative IGP routes
	<ul style="list-style-type: none"> • BGP secondary paths for EGP routes
	<ul style="list-style-type: none"> • HSRP/VRRP/GLBP statuses for gateway redundancy
RES_FUN_0585	RESISTO shall provide a mitigation action at run-time when any backup resource will not be available anymore.
RES_FUN_0660	The <i>Vulnerability Disclosure Framework</i> shall be able to authenticate users and security researchers.
RES_FUN_0670	The <i>Vulnerability Disclosure Framework</i> shall be able to provide users with functionalities to define the scope for testing, rewards for different types of threats.
RES_FUN_0680	The <i>Vulnerability Disclosure Framework</i> shall be able to allow Security Researchers to submit findings.

RES_FUN_0690	The <i>Vulnerability Disclosure Framework</i> shall be able to reward Security Researchers based on a matrix of rewards defined by users.
RES_FUN_0700	The <i>Vulnerability Disclosure Framework</i> shall be able to help Security Researchers and users to monitor vulnerabilities reported through the whole cycle:
	<ul style="list-style-type: none"> report the finding,
	<ul style="list-style-type: none"> confirm/reject/request additional information from the security researcher,
	<ul style="list-style-type: none"> notify the stakeholders,
	<ul style="list-style-type: none"> patch the finding,
	<ul style="list-style-type: none"> confirm from the security researcher that the issue was fixed, reward the security researcher, if appropriate.
RES_FUN_0870	RESISTO shall be able to produce a report for each attack / mitigation action set containing relevant elements such as duration of the attack, types of traffic or sensors that triggered the attack for security insight, etc.
RES_FUN_1040	RESISTO shall support the distribution of human-readable reports in industry-standard formats such as .PDF or .HTML.
RES_FUN_1105	The RESISTO platform shall ensure user access authentication acc. to the security requirements.
RES_FUN_1106	All users of the RESISTO platform shall be authenticated.
RES_FUN_1107	The RESISTO system shall be able to order the seamless relocation and restoration of virtualized network resources in the event of failure or cyber/physical attack if provided by the operator control system, such that service continuity can be guaranteed.
RES_FUN_1108	The RESISTO system shall maintain updated information of compute, storage and network resources within the relevant infrastructure domain.
RES_IMP_0010	The Smart Spectrum Surveillance shall provide an interface in the Cockpit in order to change settings for the tools developed.
RES_INT_0230	Network interfaces of the Virtual Machines that host RESISTO components shall offer full support for both IPv6 and IPv4 TCP stacks.
RES_INT_0240	Network interfaces shall support standardized IEEE 802.3 Ethernet technol. for interoperability.
RES_SEC_0105	The integrity of the relevant information sent by the security sensors in the system shall be protected by the RESISTO system.
RES_SEC_0110	Access to the RESISTO system shall be granted using the principle of “Least Privilege”, meaning that any program, any interface, any debugging and testing console and every user of RESISTO should operate using the least set of privileges necessary to complete the job.
RES_SEC_0120	Each user shall be identified by a unique user identity so that users can be linked to and take responsibility for their actions.
RES_SEC_0160	RESISTO shall support the User’s user access / segregation of duty requirements i.e. it supports set up of standard and group profiles.

RES_SEC_0245	RESISTO shall support remote login using encrypted protocols, such as HTTPS and SSH with only TLSv1.2 or above algorithms.
RES_SEC_0280	All staff and third parties who access the RESISTO network remotely shall only be authenticated using the approved remote access authentication mechanism.
RES_SEC_0435	RESISTO shall use services for protecting integrity and confidentiality of the data.
RES_SEC_0440	RESISTO shall transmit all passwords over a secure connection.
RES_SEC_0640	Access to Confidential, Personal and security data shall be logged.
RES_SEC_0650	RESISTO shall provide the user with the ability to import and export data from other systems in standard formats such as CSV, XML, XLS (e.g. “physical security alerts of a selected time interval”).
RES_SEC_0720	User and system data shall be stored in a data store with adequate access control measures/policies.
RES_SEC_0730	Direct access to the platform’s data store shall only be allowed to users with privileged access rights (such as system administrators).
RES_OPR_0125	RESISTO shall be able to run on OSs and/or Virtualization environments offering “snapshot” mechanism in order to provide immediate reverse in case of major fault.

Table 23 – Requirements as described in D2.6 [1]

14. ETHICAL AND SOCIETAL SCIENCE FEEDBACK ON THE USE CASES

At this point of the project, the use cases have been defined and require an early ethical and societal feedback. For this purpose, the responsible partners for each use case provided input on some questions related to the societal impact of the implemented use case. There are two aspects to this; first, the impact on the participating personnel, related to the (monitoring and/or detection) techniques used. For all use cases homogeneously highly trained personnel, between 0 and 8 people, will be involved. The following Table 24 presents the use case owners' input on this.

Secondly, in a more general view, the impact the results of the use cases could have. Here, the RESISTO platform and its purposes have to be kept in mind as well: if the implemented use cases and test-beds in the platform show enhancements in preparedness or coping capabilities of telecommunication service providers, how is this affecting society? Also, a first query of the potential impact on policy making has been made. Here, 5G is one of the potential topics to be considered by policy makers, due to unsolved issues (see use case no. 9). Table 25 displays the use case owners' input on the issue.

This - being a first feedback on societal and ethical issues - can't be considered as the final analysis of the societal impact of the use cases. Their implementation in the RESISTO platform and the impact on potential decision support and resilience enhancement might show more or other ethical aspects.

Use case no.	Use case name	Involved detection techniques	Involved monitoring techniques	Involved personnel / persons (approx. number and kind of)
1	Core Network Failure caused by Physical & Cyber Attacks to Telecommunication sites	for physical intrusion: audio and visual analytics, active and passive sensors (radar and acoustic). For cyber intrusion: NOC's software detecting cyber attacks. (the exact use depends on the type of intrusion to be considered)	audio and visual analytics, NOC's software detecting cyber attacks	2 R&D Engineers, 2 telecom experts, 1 IP/Core Network Engineer, 1 security expert
2	Telecommunications congestion caused by natural (Earthquake) or man-made (i.e. Multiple Terrorist Attacks) hazards in Athens	active and passive sensors (radar and acoustic), audio and visual analytics, UAV platform	audio and visual analytics, active and passive sensors, UAV platform, NOC's software detecting cyber attacks	2 R&D Engineers, 2 telecom experts, 1 IP/Core Network Engineer, 1 security expert
3	Telecommunication sites	Any or all detection techniques	Procedures to be implemented in the algorithm detection	1 person to implement algorithm. 1 person to monitor the response

Use case no.	Use case name	Involved detection techniques	Involved monitoring techniques	Involved personnel / persons (approx. number and kind of)
4	Disruption of major sporting event by combined physical & cyber-attack by a terrorist organization	<p>Correlating alerts to detection patterns of potential attacks using ML/AI techniques.</p> <p>Analyzing delivery networks to suggest long term resilience measures. Using alternatives such as mobile eg. 4G/5G, Satellite to provide seamless resilience to end customer experiences.</p>	<p>Logs from key network components, develop normal traffic patterns.</p> <p>The testbed will provide multicast routers logs and will simulate/generate many other logs based on past events BTC cyber security platform received as well end user device logs and CDN server logs.</p> <p>Most of the logs are captured and processed for analysis so most of the logs will be provided in database table formats in CSV, JSON, etc formats. Some of the logs could be syslogs</p>	<p>Not sure how much resources will be required at the moment. We need experts to build a virtual multicast testbed; planning to use BT TV set top box to show multicast videos, and linking up with other testing facilities. Some IPTV experts will be required. Minimum resources will be two persons.</p>
5	Protection of Cloud Storage that impact critical infrastructure services	Physical sensors and ICT sensors.	<p>Cyber: Firewall, Intrusion detection, system logs</p> <p>Phisycal: Sensors, surveillance cameras</p>	<p>1 x Cloud expert</p> <p>1 x cyber security expert</p> <p>1 x network expert</p> <p>1 x Project manager</p>

Use case no.	Use case name	Involved detection techniques	Involved monitoring techniques	Involved personnel / persons (approx. number and kind of)
6	Cyber and physical protection of network and network elements mechanisms used by critical services that impact users	The Network Elements and Cybersecurity detectors 'sensors' will use proprietary technologies and methods for detection of threats. Once a detection occurs, the 'sensors' will generate events pushed through Syslog Data and/or SNMP messages deployed (traps). Some of the physical event detection devices will use lightweight protocols such as MQTT to relay detection event information to RESISTO	For Cybersecurity Events , ORO's testbed uses in-line monitoring for incidents and threats at OSI Layer 3 to 7 level - Firewalls, DDoS Mitigation Tools, Application Control Monitoring, Network Activity Monitoring, Network Performance Monitoring and Assets Monitoring (such as endpoints and servers up/down time) For Physical Security Events , ORO's testbed uses hardware devices with status update capabilities such as motion sensors, perimeter access sensors, continuity sensors (for cable/fiber cuts). These sensors will push status information at regular times and will push detection event information when a detection is triggered.	8 Persons: 1 x Cyber Security expert 2 x Information Security experts, 2 x IP/Core Network experts 3 x Development and Innovation experts
7	Maritime Safety and Emergency Case	Physical sensors and data probe sensors	Physical Attack: Alarms for physical sensors. Cyber Attack: KPI from data probes.	Sensor provider for physical and cyber attack. Monitoring person in order to detect the attack.
8	PPDR Virtual Operator	Any or all detection techniques	Alarms, trouble tickets	2 R&D Engineers, 2 telecom experts, 1 IP/Core Network Engineer, 1 security expert
9	5G network response to a security breach	Machine learning techniques	Alarms, trouble tickets	Strictly speaking, no personnel is required (use case based on fully automated procedures). Optionally, network operations support staff may be involved (1-2 people)

Table 24 – Use case owners' input on involved techniques and personnel

Use case no.	Use case name	Who profits from the enhanced security?	Are there implications for policy makers? (E.g. best practices)	Real parts (actual events)	Virtual parts
1	Core Network Failure caused by Physical & Cyber Attacks to Telecommunication sites	it's a win win situation. Both the customers and the Telecommunication Provider	no	Physical intrusion to OTE core lab that will cause deliberate network malfunction - Camera detection - Testbed physical connections exist	Simulated Events generated during testing: - some virtual network connections may be disrupted or disabled temporarily - rerouting of virtual connections may be applied -some VMs may be disabled/disconnected temporarily
2	Telecommunications congestion caused by natural (Earthquake) or man-made (i.e. Multiple Terrorist Attacks) hazards in Athens	It's a win win situation. Both the customers and the Telecommunication Provider /Public safety and emergency response agencies	no	In sub scenario #1 we will deliberately flood the network with traffic by using traffic generators. Traffic rerouting will take place. Physical lab connection exist. - In sub scenario #2 real data from the recent earthquake in Athens will be used.	Simulated Events generated during testing: - DDoS and DoS attack on the infrastructure using open-source software and custom scripting; - rerouting of virtual connections may be applied
3	Telecommunication sites	Sites infrastructure providers	yes	Sites and platform	monitor and algorithm

Use case no.	Use case name	Who profits from the enhanced security?	Are there implications for policy makers? (E.g. best practices)	Real parts (actual events)	Virtual parts
4	Disruption of major sporting event by combined physical & cyber-attack by a terrorist organization	All stakeholders in IPTV such as customers, operators and service providers	Unlikely, but depend on what RESISTO could come up in resilience	Components on the testbed will generate some real events such as multicast routers logs. Other simulated logs will be based on real logs captured in the network, but sanitised to remove customers and sensitive data.	Components on the testbed will generate some real events such as multicast routers logs. Other simulated logs will be based on real logs captured in the network, but sanitised to remove customers and sensitive data.
5	Protection of Cloud Storage that impact critical infrastructure services	End user Customer and Cis infrastructures	No policy changes	Physical entry to datacenter, or secondary site. Hardware changes in systems, Logical modification of servers configurations, changes in data files. Switch of services infrastructure between sites.	Simulated cyber attack against cloud and storage systems. Unavailability of datacenter services. Unavailability of network connectivity with switching to 5g connection.

Use case no.	Use case name	Who profits from the enhanced security?	Are there implications for policy makers? (E.g. best practices)	Real parts (actual events)	Virtual parts
6	Cyber and physical protection of network and network elements mechanisms used by critical services that impact users	Both the customers and the Tele-communication Provider (End-User of RESISTO)	No changes in policies or best practices	Real Events generated during testing: <ul style="list-style-type: none"> - Physical entry into a datacenter in one of OROs buildings by a malicious actor; - Physical disconnect of several NE s from the testbed; - Physical connection to several NE s in the testbed to a rogue laptop computer; - Modification of several routes in the routing table of the NEs in the testbed by the malicious actor. 	Simulated Events generated during testing: <ul style="list-style-type: none"> - DDoS and DoS attack on the infrastructure using open-source software and custom scripting; - Botnet activity simulation using open-source software and custom scripting.

Use case no.	Use case name	Who profits from the enhanced security?	Are there implications for policy makers? (E.g. best practices)	Real parts (actual events)	Virtual parts
7	Maritime Safety and Emergency Case	Sites infrastructure providers	yes	Sites and platform	
8	PPDR Virtual Operator	Sites infrastructure and service providers	yes	Sites, network and platform	Monitor and slices
9	5G network response to a security breach	The easy / obvious answer is - the users and the operator. If we want to highlight the societal value, we may think of specific scenarios where communication is critical (e.g. first responders to natural disaster).	The use case is based on novel 5G business models enabled by NaaS and the separation of service providers and (virtual) infrastructure providers, for which, to a large extent, regulation is still needed. In addition, apart from 5G, the possibility of sharing mobile access/edge network resources among competitor operators under certain circumstances (e.g. natural events such as forest fires affecting the availability of the mobile network in a certain zone) has been suggested for possible implementation as a way to avoid loss of communication, which is often a cause for aggravation of the effects of this kind of events.	The use case is based on real data from Altice operational network infrastructure.	The use case is based on real data. However, there may be a need to "tailor" the data set to be sure that it drives the envisioned sequence of use case steps. This requires further study.

Table 25 – Use case owners' input on potential societal impact

15. CONCLUSION

An overall description of the RESISTO Use Cases has been presented in the framework of this Deliverable, serving as a “reference document” for all 3 implementation work packages (WP7, 8 and 9) of the RESISTO project.

Detection and identification of threats, implementation and the response and mitigation aspects have been covered for each Use case, addressing the User Requirements, while certain validation aspects (i.e. KPIs) have been attributed.

The Use cases also address the three macro-scenarios as starting point, and identification of the involved actors’ role for validation was given.

However, the present Deliverable should be seen in combination with other Deliverables already elaborated such D2.6 [1] and D2.7 [2] for the RESISTO architecture, as well as D4.2 [6] for the sensors deployment plan and D3.7 [3] and D3.8 [4] for analyzing the validation measurements through KPIs.

The convergence of all these Deliverables including the present one will be the subject of the 3 operational validation WPs namely WP7, WP8 and WP9 where the RESISTO solutions will be tested, validated and evaluated to prove its added value towards the overall protection cycle of the telecom critical infrastructures.

16. REFERENCES

- [1] RESISTO, "D2.6: RESISTO platform and tools reference architecture - first" 2019. [Online]. Available: http://www.resistoproject.eu/wp-content/uploads/2019/09/Attachment_0-7.pdf
- [2] RESISTO, "D2.7 RESISTO platform and tools reference architecture - final," 2020. [Online]. Available: <http://www.resistoproject.eu/resources/> . [Accessed August 2020].
- [3] RESISTO, "D3.7 KPIs, quantities and metrics for cyberphysical risk and resilience of telecom CI - first," 2019. [Online]. Available: http://www.resistoproject.eu/wp-content/uploads/2019/09/Attachment_0-11.pdf . [Accessed August 2019].
- [4] RESISTO, "D3.8 KPIs, quantities and metrics for cyberphysical risk and resilience of telecom CI - final," 2020. [Online]. Available: <http://www.resistoproject.eu/resources/> . [Accessed August 2020].
- [5] RESISTO, "D4.1 Active and Passive Sensor Definition," 2019. [Online]. Available: http://www.resistoproject.eu/wp-content/uploads/2019/09/Attachment_0-12.pdf . [Accessed August 2019].
- [6] RESISTO, "D4.2 Active and Passive Sensor Deployment Plan," 2020. [Online]. Available: <http://www.resistoproject.eu/resources/> . [Accessed August 2020].
- [7] RESISTO, "D4.3 Techniques and Procedures for cyber/physical threats Detection" 2020 [Online]. Available: <http://www.resistoproject.eu/resources/> . [Accessed August 2020].
- [8] RESISTO, "D4.4 Complete propagation analysis," 2020. [Online]. Available: <http://www.resistoproject.eu/resources/> . [Accessed August 2020].
- [9] Traynor, P. McDaniel, and T. La Porta, "On attack causality in internet-connected cellular networks," in Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium , 2007, pp. 21:1–21:16
- [10] Dynes, S., Johnson, M. E., Andrijcic, E., and Horowitz, B. Economic costs of firm-level information infrastructure failures: estimates from field studies in manufacturing supply chains. International Journal of Logistics Management, 18, 3, 2007, 420–442.
- [11] "5G security - scenarios and solutions", Ericsson White Paper, 2017 Available: <https://www.ericsson.com/49d571/assets/local/publications/white-papers/wp-5g-security.pdf>
- [12] "Overview of 5G Security Challenges and Solutions", Ijaz Ahmad, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, and Andrei Gurtov, IEEE Communications Standards Magazine, March 2018.
- [13] "The Evolution of Security in 5G" - 5G Americas White Paper, July 2019.
- [14] "A Comprehensive Guide to 5G Security", Editors: Madhusanka Liyanage Ijaz Ahmad Ahmed Bux Abro Andrei Gurtov Mika Ylianttila, 2018.
- [15] 3GPP, "TR 28.801 Technical Report Technical Specification Group Services and System Aspects; Telecommunication management; Study on management and orchestration of network slicing for next generation network (Release 15)," 2018.
- [16] RESISTO, "D6.1 SW architecture definition," 2019. [Online]. Available: <http://www.resistoproject.eu/resources/> [August 2019, Restricted].