

RESISTO

D7.1 – Scenario 1 Test Plan definition



RESISTO

D7.1 – SCENARIO 1 TEST PLAN DEFINITION

Document Manager:	Maria Belesioti	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:	OTE

Document ID N°:	RESISTO_D7.1_200525_01	Version:	1.0
Deliverable:	D7.1	Date:	25/05/2020
		Status:	APPROVED

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

Approval Status	
Prepared by:	Maria Belesioti, Evangelos Sfakianakis, Kostas Chelidonis (OTE)
Approved by: (WP Leader)	Maria Belesioti (OTE)
Approved by: (Coordinator)	Bruno SACCOMANNO (LDO)
Advisory Board Validation (Advisory Board Coordinator)	N.A.
Security Approval (Security Advisory Board Leader)	Paolo DI MICHELE (LDO)

CONTRIBUTING PARTNERS

Name	Company / Organization	Role / Title
Maria Belesiotti Evangelos Sfakianakis Kostas Chelidonis	OTE	Telecommunication Experts
Ioan Constantin, Horia Gunica, Marius Iordache, Carmen Patrascu	ORO	Cyber Security Expert, IP Network Experts, Project Manager
Rodoula Makri, Panos Karaivazoglou, Apostolos Papafragkakis, Athanasios Panagopoulos, Nikolaos Lyras, Anargyros Roumeliotis, Takis Kelefas	ICCS	Senior Researchers, Electrical Engineers, Telecommunication Experts
Luca Lionetti , De Lutiis Paolo	TIM	R&D Engineers
Zhan Cui, Ian Herwono	BTC	R&D Engineers
Michael Skitsas, Antonio Hidalgo, Nicolas Georgiades	ADITESS	Software Engineers, UAV Pilot
José Manuel Sánchez, Javier Valera	INT	R&D Engineers

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	21.01.2020	1-32		Draft ToC
0.2	6.03.2020	1-47		Updated version
0.3	18.03.2020	1-50		Updated version
0.4	28.03.2020	1-50		Updated version
0.5	2.04.2020	1-55		Updated version
0.6	7.04.2020	1-55		Updated version
0.7	22.04.2020	1-63		Refinements
0.8	27.04.2020	1-68		Pre-final version
0.9	28.04.2020	1-64		Final release for SAB
1.0	25.05.2020	All	All	Final version

COPYRIGHT STATEMENT



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

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

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

PROJECT CONTACT



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

RESISTO PROJECT – PUBLISHABLE EXTENDED ABSTRACT

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

EXECUTIVE SUMMARY

The present document is a deliverable of the RESISTO project (Grant Agreement No. 786409) [1]
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 7.1 presents the initial plan to design, implement and deploy the Proof-of-Concepts of the use cases of the Macro Scenario 1, defined in D2.8 [2] "Table-top Read Teaming Results of RESISTO Architecture, Scenarios and Use-Cases" of RESISTO project.

At the same time, this document presents an initial plan for integrating all components of RESISTO platform, developed in the context of other work packages of the project, to all pilot sites as well as the technologies that will be used. There are three pilot sites provided by the partners of the project; OTE, TIM, BTC and an interconnected pilot site provided by ORO. We start by analyzing the steps and the process of each use case, the timeplan of each step as well as the KPI's that will be used to evaluate each use case and the technologies that will be used to access the integrated testbed.

CONTENTS

ABBREVIATIONS	12
1. INTRODUCTION	14
1.1. Scope.....	14
1.2. Relation to Other Work Packages within RESISTO	16
1.3. Document outline	17
2. Description of Use cases corresponding to MACRO-scenario #1 ...	18
2.1. Macro-Scenario 1: Protection and resilience of the Current / existing Telecommunication Critical Infrastructures	18
3. Methodology	20
3.1. Testing Environment	20
3.2. Pilot Planning.....	21
3.2.1. Pilot Execution Time plan	23
4. Use Case 1: Core Network Failure caused by Physical & Cyber Attacks to Telecommunication sites	25
4.1. Scope.....	25
4.2. Test-bed setup	26
4.2.1. Technologies involved	27
4.2.2. Preconditions.....	28
4.2.2.1. Sub Use Case 1 Work flow	29
4.2.2.2. Sub Use Case 2 Work flow	30
4.3. Key Performance Indicators Used to Evaluate the Pilot	32
4.4. ORO's impacted Use case.....	32
4.4.1. Test-bed Interconnection	33
4.4.2. Preconditions.....	35
4.4.3. Interconnection flow diagram	36
5. Use Case 2: Terrorist Attack and Natural Hazards causing network failure and telecommunication congestion	37
5.1. Technologies involved for both sub-scenarios of Use Case 2.....	37
5.2. Sub Use Case 1: Terrorist Attack in telecom asset causes severe network failure	38
5.2.1. Scope.....	39
5.2.2. Test-bed setup	40
5.2.2.1. Preconditions.....	40
5.2.2.2. Sub Use Case 1 Work flow	41
5.3. Sub Use Case 2: Natural Disasters affect telecom assets – network loss and telecommunication congestion	42

5.3.1.	Scope.....	43
5.3.1.1.	Sub Use case 2 Work flow.....	43
5.3.2.	Key Performance Indicators to Evaluate the Pilot.....	45
6.	Use Case 3: Telecommunication sites.....	46
6.1.	Scope.....	46
7.	Use Case 4: Disruption of major sporting event by combined physical & cyber-attack by a terrorist organization	47
7.1.	Scope.....	47
7.2.	Test-bed setup	48
7.2.1.	Technologies involved	49
7.2.2.	Preconditions.....	50
7.2.3.	Use case Work flows	51
7.3.	Key Performance Indicators to Evaluate the Pilot.....	54
8.	Use Case 10: Protection and resilience of tim's network nodes.	55
8.1.	Scope.....	55
8.1.1.	Technologies involved	55
8.1.2.	Preconditions.....	56
8.1.3.	Use case Work flows	57
8.2.	Key Performance Indicators to Evaluate the Pilot.....	59
9.	Users involvement and training (tim).....	60
9.1.	User involvement.....	60
9.2.	Training Plan.....	65
10.	CONCLUSION.....	66

List of Figures

Figure 1 Overall diagram showing the links between the different Work Packages.....	16
Figure 2 – WP7 Overall Action plan	22
Figure 3- Updated timeline with the delays which influence this plan	23
Figure 4: High level OTE Core Lab – Cloud lab topology.....	27
Figure 5. High-level BTC virtual test-bed architecture for multicast and unicast video delivery ..	49

List of Tables

Table 1 Preconditions for the Use Case 1	28
Table 1 – Suggested KPIs to be measured during the pilot activities of Use Case 1	32
Table 3 – Testbed interconnection design choices	34
Table 4 Preconditions for Interconnected Testbeds Use Case	35
Table 5 Preconditions for the Terrorist Attack in telecom Sub Use Case	41
Table 7 – Suggested KPIs to be measured during the pilot activities of Use Case 2	45
Table 8- Preconditions for the Disruption of Major Sporting Event by Combined Physical & Cyber- Attack by a Terrorist Organisation Use Case	50
Table 9 – Suggested KPIs to be measured during the pilot activities of Use Case 4	54
Table 10 -Technologies involved in the TIM sub-scenario.....	56
Table 11- Preconditions for the TIM sub scenario	56
Table 12 - KPI to be referred for the Healthcare scenario	59

ABBREVIATIONS

3G, 4G	Third and fourth generation of mobile phone systems
ACL	Access Control List
API	Application Programming Interface
BNG	Broadband Network Gateway
CBT	Computer Based Training
CCTV	Closed Circuit TV
CI	Critical infrastructure
CPU	Central Processing Unit
DDoS	Distributed Denial Of Service
DoA	Description Of Actions
DoS	Denial Of Service
DMZ	DeMilitarized Zone
DSLAM	Digital Subscriber Line Access Multiplexer
EC	European Commission
HTTPs	HyperText Transfer Protocol Secure
ICT	Information and Communication Technology
ID	Identity
IDS	Intrusion detection systems
IGMP	Internet Group Management Protocol
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion prevention systems
IPTV	Internet Protocol Television
KPIs	Key Performance Indicators
LTCL	Long Term Control Loop
MPLS	Multiprotocol Label Switching
NOC	Network Operations Center
NMAP	Network Mapper

NMS	Network Management System
OS	Operating System
OSINT	Open-Source Intelligence
PC	Personal Computer
PIM	Protocol-Independent Multicast
QoS	Quality of Service
SNMP	Simple Network Management Protocol
SRG	Shared Risk Groups
STCL	Short Term Control Loop
SSM	Source-Specific Multicast
UAV	Unmanned Aerial Vehicle
UC	Use Case
VM	Virtual machine
UEQ	User Experience Questionnaire
VPN	Virtual Private Network
WAN	Wide Area Network
WiFi	Wireless Fidelity
WP	Work Package

1. INTRODUCTION

Protection and resilience of Critical Infrastructures (Cis) has become major issue especially in the last two decades. Many economic, social, political and of course technological reasons have caused a rapid change in the all aspects of Cis, namely organizational, operational and technical. In the past, infrastructures that could be considered as autonomous vertically integrated systems with very few or possibly none points of contact with other infrastructures are now tightly coupled with many dependencies. Consequently, the risk to society due to inadvertent and deliberate CI disruptions has largely increased due to interrelation, complexity, and dependencies of these infrastructures.

The increased use of information and telecommunication technologies (ICT) to support CI functionalities has played a major role to this. The need of providing services without disruption especially when accidental or malicious events occur has become top priority all over the world.

This deliverable, namely D7.1 “Test Plan Definition” is divided in two main parts, Test plan Definition of the Use cases referred to Macro scenario 1 namely “Protection and resilience of the Current / existing Telecommunication Critical Infrastructures” and Users Involvement and Training.

The first part aims is to provide a detailed description of the pilots that will be executed in the context of this project and more specifically the pilots related to Macro scenario 1 as well as the pilot procedures. These pilots are based on the basis of the Use Cases provided in D2.8 [2] and the RESISTO platform reported in D6.1[3] as well as the sensors deployment plan in D4.2 [4]. Therefore, this deliverable shall be considered along with D8.1[5] and D9.1[6], as, together, they provide the overall context in which the Use Cases identified in the RESISTO project will be demonstrated.

As far as Training and Users Involvement are concerned this second part has the objective to build a supporting framework to assist in planning and piloting activities. The organization and dissemination of training initiatives involves the identification of the ongoing training needs related to RESISTO platform and its integration with the testbeds that will be used in the pilots.

Training activities to the entire community of project’s end-users and creating the related content are led by TIM and partners involved are RM3 and LDO. These partners will run different training initiatives for staff and users involved in the pilots of the use cases of the project. To harmonize and more efficiently exploit this potential, this task will produce an inventory of existing training material related to the objective of RESISTO project.

1.1. Scope

The objective of this deliverable is to define the time plans of the actions of the piloted uses cases that will be used to prove the RESISTO added value, in the context of Macro scenario 1 “Protection and resilience of the Current / existing Telecommunication Critical Infrastructures”. In order to achieve that, the consortium will use the use cases, described in D2.8, as a starting point to define

the pilots. Depending on the requirements and description of the test, several partners, will be involved in each pilot.

The Test Plan process has two distinct goals:

- To demonstrate that the RESISTO platform meets the requirements of the operators and that offers added value to their systems.
- To discover incorrect behaviors of the RESISTO platform.

The Test Plan process's objectives to be addressed are the following:

- To describe piloting actions for all the Uses Cases
- To address 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)

The pilots as mentioned in the DoA [1] will have two iterations.

To validate the RESISTO platform, it is very important to have described each use case requirements so as not to have system errors not-detected which could affect the reliability and availability of the RESISTO platform. This work exists in D2.8 [2]. Possible consequences could be:

- More effort and possible delays: If the error is detected in the later stages of piloting (system testing or user testing), it is necessary to check all the components of the system to detect where the problem is
- Business reputation loss: If an error is found while the system is in production, the operator disputes the quality and the reliability of the platform.

WP7 acts as the basis for both WP8, the interconnected testbeds' infrastructures and WP9 which is referred to the envisioned future networks and their protection as this can be demonstrated in the context of the main and impacted Use Cases involved.

1.2. Relation to Other Work Packages within RESISTO

Work Packages 4 is developing tools and algorithms for real time monitoring of threats while WP3 performs cyber –physical risk and resilience assessment and defines the KPIs. WP6 and WP2 are establishing the RESISTO platform and defining the use cases that will be piloted in three validation scenarios. Work Package 5 is developing and implementing algorithms for real time response and mitigation. More specifically, D5.4 [7] “Real Time Response and Mitigation Results”, is the reference for the possible countermeasures to be used in the context of the use cases in the scope of this document. It should be noted that the table in D5.4 is indicative of the demonstrable countermeasures and what will be actually demonstrated will be declared in D7.2 In Task 7.1 the common and detailed planning is described and gives the pilot sites of the first validation scenario the necessary framework to install their hardware testing.

WP7 is related to WP8 and WP9 since they have to progress in parallel with strong interactions.

The most important deliverable which gives the input to D7.1 is D2.8 “Table-top read teaming results of RESISTO architecture, scenarios and use cases”,[2] since it contains the first and main description of the involved use cases to be validated.

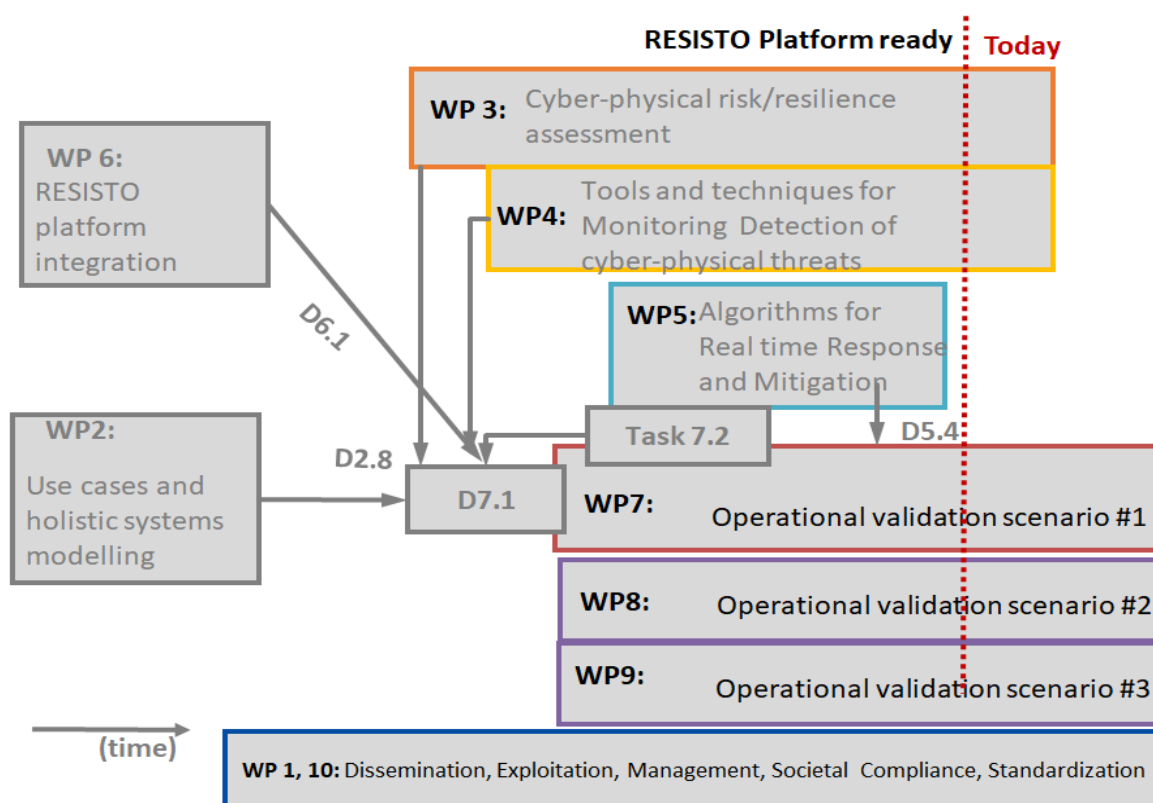


Figure 1 Overall diagram showing the links between the different Work Packages

1.3. Document outline

The present deliverable is structured as follows:

- Chapter 1 – Describes the objectives of Task 7.1 and provides a brief description of the deliverable context.
- Chapter 2 - Presents Macro scenario 1” Protection and resilience of the Current / existing Telecommunication Critical Infrastructures and it’s the specific use cases in the scope of the WP7.
- Chapter 3 - Describes the methodology defined for the Test Plan definition, the macro scenario in scope of WP7 (please note that the same methodology has been used by WP8 and WP9)
- Chapters 4 –5 - Present the test plan for the validation of the OTE and ICCS namely “Core Network Failure caused by Physical & Cyber Attacks to Telecommunication sites” and “Terrorist attacks and natural hazards causing network failure and telecommunication congestion” Use cases
- Chapter 6 – Presents Telecommunication sites Use case.
- Chapter 7 – Presents the test plan for the validation of the BTC use case “Disruption of Major Sporting Event by Combined Physical & Cyber-Attack by a Terrorist Organisation”.
- Chapter 8 – Describes the test plan for the validation of the TIM’s use case “Protection and resilience of TIM’s network nodes.”
- Chapter 9 – This chapter describes the user involvement and the training plan

2. DESCRIPTION OF USE CASES CORRESPONDING TO MACRO-SCENARIO #1

According to the DoA [1] specific main Use cases have been suggested for each Macro-Scenarios, while certain others refer 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.

2.1. 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.

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 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.

Within the DoA [1], 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 and network failure caused by natural (i.e. Earthquake) or man-made (i.e. Terrorist Attacks) hazards (lead by OTE)
- Telecommunication sites (lead by RTV)
- Disruption of major sporting event by combined physical & cyber-attack by a terrorist organization (lead by BTC)
- Protection and resilience of TIM's network nodes (lead by TIM)

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 I 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. METHODOLOGY

Describing a common methodology and making common plans will help all pilot sites to install RESISTO platform and prove the added value it has to offer as described in other project Work Packages. All testbeds of the present deliverable will be connected to the RESISTO platform to demonstrate benefits to telecom operator's systems in terms of new functionality, benefits and efficiencies. The presence of actual testbeds greatly enhances the chances of further exploitation both locally and through worldwide dissemination of results.

3.1. Testing Environment

A testing environment will be set up for each use case pilot. It will be composed of a number of operator devices connected on a network, as well as sensors, cameras etc provided by other partners. As it is extensively described in the Deliverable D4.2 for the various sensors to be used as physical threats detectors within the RESISTO Use Cases, the deployment of the sensing environment towards the execution of each use case pilot is foreseen to be done in three phases: (a) the lab tests of the sensing system for configuration and parametrization to fulfil the technical and user requirements for each case, (b) an execution/testing phase of the pilots using the sensing system integrating them with the RESISTO platform and finally, (c) the deployment of the testing environment and integration of the telecom providers' testbeds with the RESISTO platform according to the Use Case scenarios.

During the execution of lab tests and configuration of system (in progress phase), the sensors are mainly deployed in labs (premises owned by sensors owners) and stand-alone tests are under progress. The second step is the integration of sensors with the RESISTO Platform. This step can be done remotely with the usage of RESISTO VPN infrastructure. The generated events by the detectors will be transferred to the RESISTO platform using the KAFKA broker in the form of JSON messages. Furthermore, for visualization purposes, the sensor's data and alerts will be distributed locally as well. For example, video streams will be available for the HMI media players.

The final execution of pilot will be executed using the testing environment and telecom operators' testbeds of each use case pilot. Detectors will be integrated using the KAFKA broker while the HMI will be launch centrally as a web application.

By this way, a testing environment is being set up that will guarantee adequate performance and debugging, along with testing of the various components of the RESISTO system, before the final execution of the pilots according to the provisions of each Use Case scenarios. Moreover, this will enable us to carry out tests about hardware integration, as well as testing accessibility issues through the foreseen iteration steps.

The set of use cases (as in D2.8 [2]) constitutes the specification of the functional features offered by the platform that must be tested.

Each pilot can be described in a way very similar to use cases:

- Scope: What the user wants from the system
- Preconditions: What is necessary to execute the use case.
- Postcondition: This will be defined by specific KPI's measurement.
- Actors: Users or external systems involved (see D2.8 [2])
- Work Flows: Steps followed in order to get the result he or she expects

The common procedure to carry out each pilot is quite straightforward. First, it must be ensured that the Preconditions hold true for the target user in the testing environment. Then the steps in the Description are executed by a tester, and perhaps other involved actors.

Finally, it must be checked that the Postconditions are met as expected. It is possible, however, that the final tests need to be updated according to the actual implementation of the system, especially the detailed steps of execution in the work flow fields and the potential debugging. Hence, the test definitions will be fully determined on in the following deliverables of WP7.

3.2. Pilot Planning

In the following table an overall timeplan of WP7 is depicted. As per the initial planning and given the complexities involved in the execution of the pilot, we anticipate the following time plan:

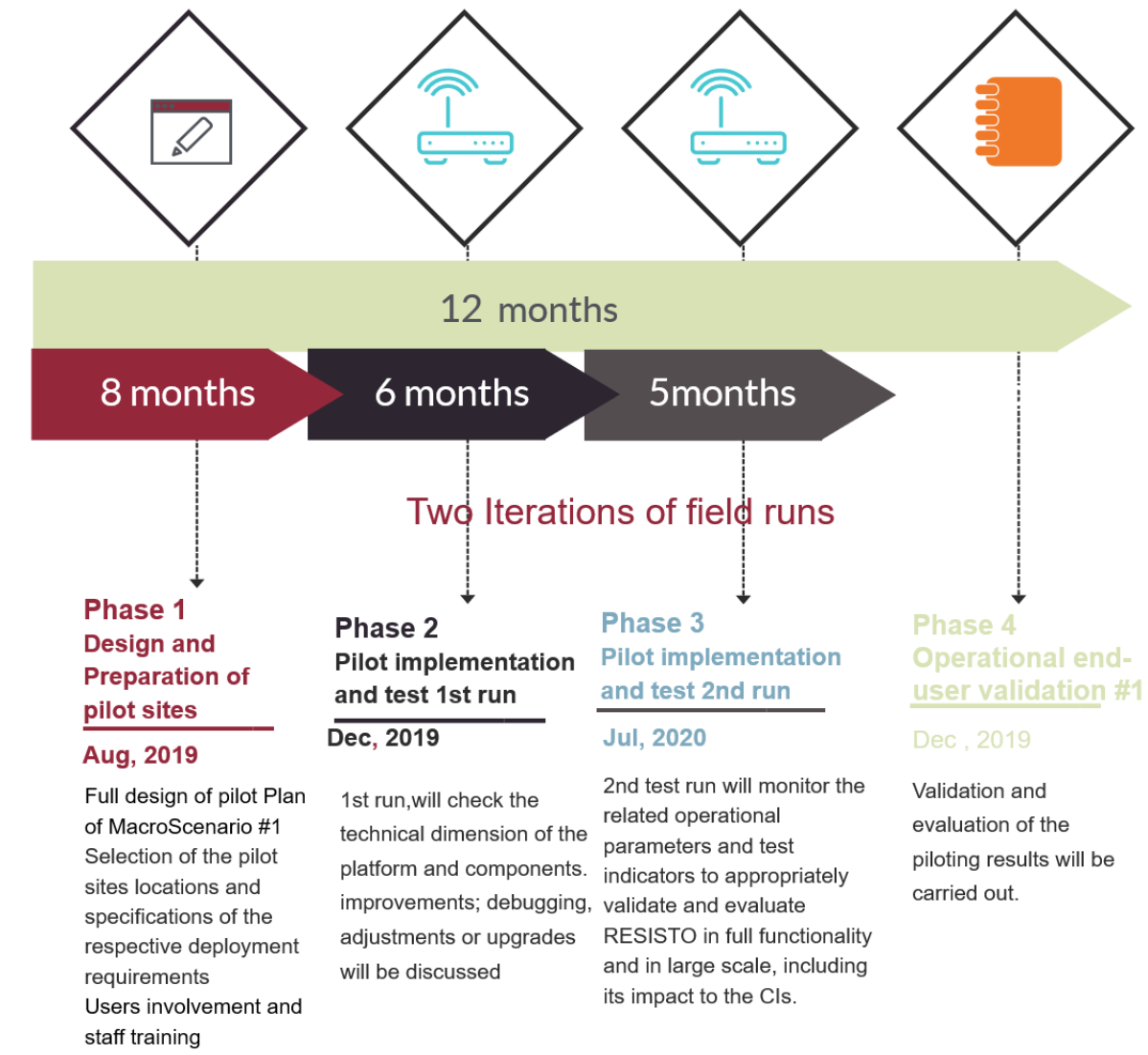


Figure 2 – WP7 Overall Action plan

We have divided the WP actions into four main phases. The operation end-user validation is an ongoing process through the entire Work Package. Phase 1 “Design and preparation of Pilot sites” has started and its ongoing. Phase 2 and Phase 3 will continue in the coming period, due to unexpected delays caused by COVID-19.

- **The pilot sites preparation, users involvement and training requires** two months from T-0 (start of pilots) for the deployment of the necessary connectivity between testbed(s) and the RESISTO components, the dissemination of activities and training for the users of RESISTO. As T-0 to be the date the Scenario planning is complete, each of the activities comprising the pilot execution plan should complete as follows:

- **Pilot implementation and test first run** requires four months starting with T-0 + 2M (following the previous activity) whilst the **pilot implementation and second run** should require additional four months after this
- **The operation end-user validation** is an ongoing process through the entire Work Package.

3.2.1. Pilot Execution Time plan

This plan presents a timeline chart with common actions for WP7 pilot sites.

Individual timelines is not possible to be presented in this deliverable as it was initially planned. In the following deliverables of WP7, maybe some adjustments will take place.

Due to that and as per the initial planning and given the complexities involved in the execution of the pilot, we anticipate that pilot actions will have some delays.

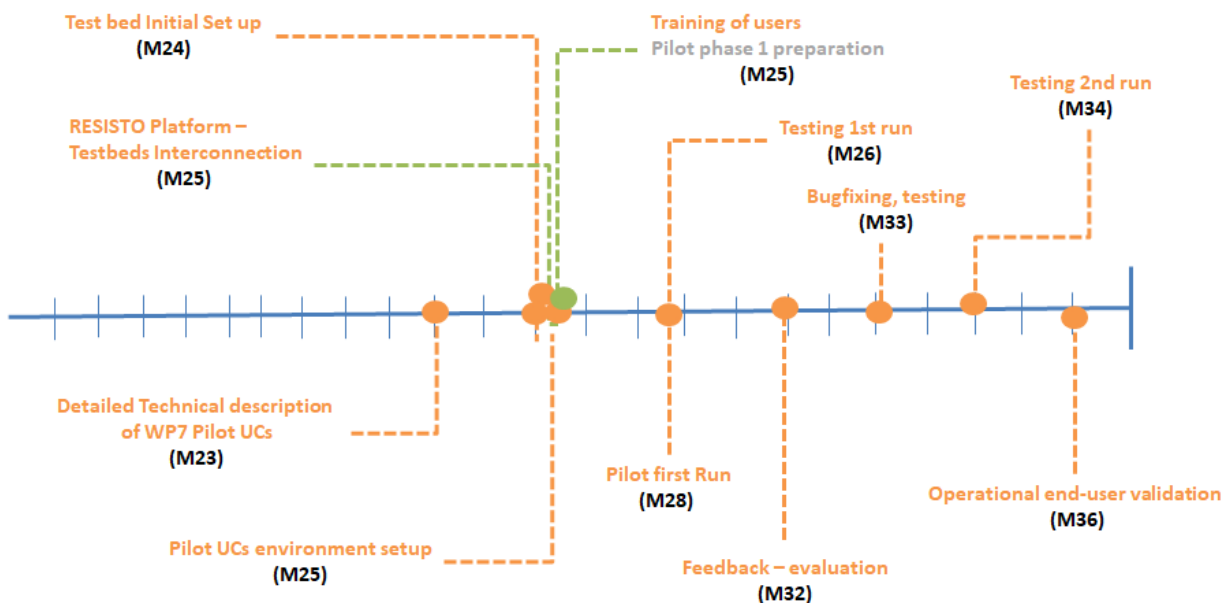


Figure 3- Updated timeline with the delays which influence this plan

All pilots are free to timetable their activities according to their own plan. The main focus is that all the pilot sites need to be connected to the RESISTO platform and running their first implementation by end of June 2020 so as to be able to have enough time to run the tests and to evaluate the RESISTO platform towards the end.

The installation of the Platform components will be different for each pilot Use Case due to their specific architectures and plans.

The long term control loop will be completed at different points throughout the pilot timeline. Before the pilot testing begins, the long term control loop will be completed once to

obtain preliminary, or baseline results. Once the pilot tests are completed, the results will be shared with the long term control loop. This can include improvement measures, or information about the recovery of the testbeds. More accurate values about the times and frequencies would be useful including repair times, or the time until the repairs can start (i.e. a buffer time). The long term control loop can then be completed again and new results can be obtained.

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

Use Case 1 “Core Network Failure caused by Physical & Cyber Attacks to Telecommunication sites” scenarios, as described in D2.8 [2] 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. These combined cyber-physical threats can be triggered either by malicious artefacts (i.e. an airborne threat as a UAV) or by unauthorized attacker against the physical assets of the telecom provider. For this reason, the Use Case 1 will be tested in 2 subcase scenarios.

This physical threat is deliberately meant to enable a security threat in the cyber domain of the telecom provider’s network. It is assumed that in this case of cyber-physical attacks, the consequences for the operator can be significant since it is assumed that a core network and service provision failure takes place as well as side effects; a DoS is initiated, network traffic is caused and / or specific systems of the core network are being attacked and potentially partially shut down. Thus, for this use case, the cyber-physical threat to OTE’s premises will take place considering two sub use cases:

- (a) Using UAVs as a physical threat which is supposed to overcome the physical security of a protected building and connects wirelessly to the wireless network inside, gaining access to a network switch and initiating i.e. a DoS attack, and
- (b) An intrusion by an attacker that breaches the secure perimeter, enters the building, gains access to an unattended computer and installs dormant malware that will be activated at some point in the future.

The 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 both cases, a physical attack has as a result the triggering or activation of a cyber-attack. The steps that will be followed in this use case are described in the following subsections:

4.1. Scope

Both sub use cases of Use Case 1, through a physical attack, initiate an attack in the cyber domain that will cause core network and services provision failure, either directly on the spot or on a later time.

It is assumed that, 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. The physical threats are detected through the additional sensors / detectors introduced by the RESISTO system; the UAV path is captured by the RESISTO Airborne Threat Detection system (offered by ICCS) while the unauthorized attacker’s moves are captured by the RESISTO Audio / Video Analytics system (offered by ADITESS as perimeter protection complementary to the existing security system of the facility). Both systems enable the

detection/classification of the corresponding abnormal activity and issue a separate intrusion event to the RESISTO platform (for each sub use case). 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 cyberattack (malware) is detected a cyberattack 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 in order to meet the needs of service provision. Thus, Use Case 1 demonstrates how the RESISTO platform can detect, identify and mitigate these combined events, compared to the conventional security systems, that are unable to correlate physical and cyber threats. Although both the physical location and the network were already protected by the existing security system of the provider, the correlation between the events identified by RESISTO facilitates the efficient detection of the attack and enables the mitigation in its entirety, since without the RESISTO platform, the combined threats would not even be detected or correlated.

4.2. Test-bed setup

For the implementation of this Use Case, OTE’s facilities will be used as it is described in D2.8 “Table –Top Read Teaming Results of RESISTO Architecture, Scenarios and Use Cases” namely the Core lab and the Cloud lab (as they are depicted in Fig.4). 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 sub use cases’ scenarios of the “physical & cyber-attacks in telecom sites causing DoS or core network failure” of 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.

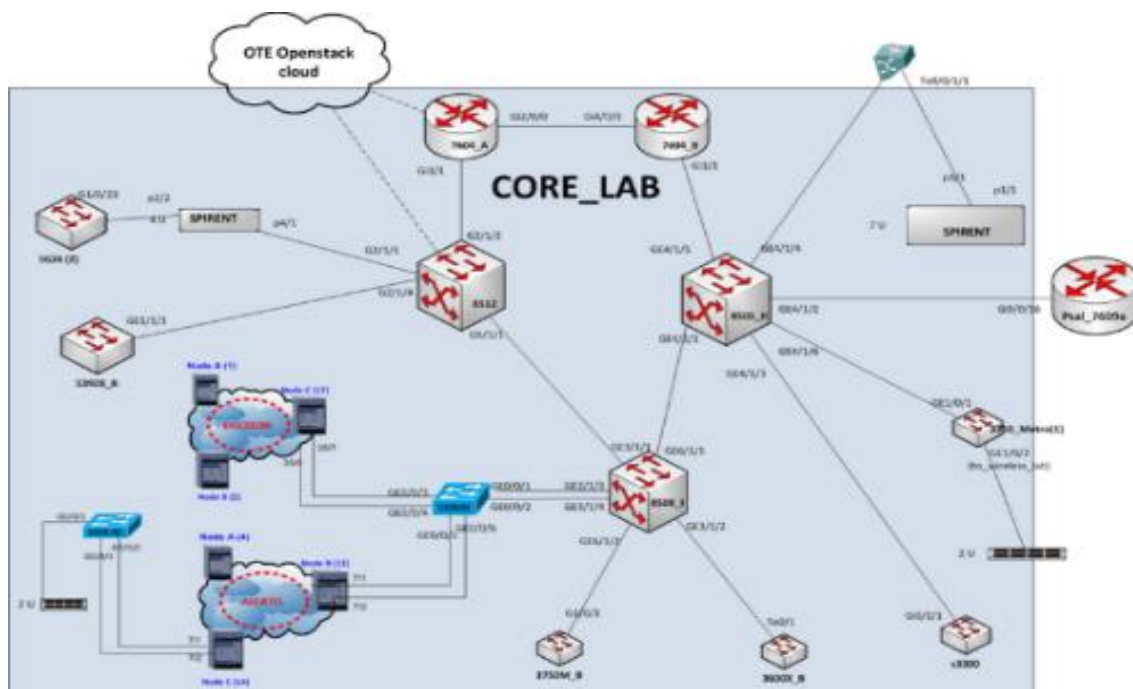


Figure 4: High level OTE Core Lab – Cloud lab topology.

4.2.1. Technologies involved

Technology	Role	Description
Hostile UAV / aerial platforms	Intruder: physical/cyber-attack generator	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.
RESISTO Airborne threat detection system	Technical: detector of airborne threats i.e. small aircrafts and UAVs.	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	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.
RESISTO Platform	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.
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).
Openstack cloud	A cloud slice will be deployed, to host tools and applications	The cloud will be used to host telecom and RESISTO topology components required for the scenario
Streamer (IPTV)		Application server, client, set top box
Cisco PIX 515 firewall		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

4.2.2. Preconditions

		Applicability
P1	Network Connectivity is up and running	Applicable to Scenario 1 & 2
P2	Cloud environment up and running	Applicable to Scenario 1 & 2
P3	NMS installed and running	Applicable to Scenario 1 & 2
P4	Cyber OS Sensors installed and running	Applicable to Scenario 1 & 2
P5	Other cyber security functions installed and running	Applicable to Scenario 1 & 2
P6	Cameras (CCTV) and microphones up and running	Applicable to Scenario 1 & 2
P7	Active and passive sensors (radars and acoustic) up and running	Applicable to Scenario 2
P8	Physical Door Sensors installed and running	Applicable to Scenario 1 & 2
P9	Physical Rack Sensors installed and running	Applicable to Scenario 1 & 2
P10	The RESISTO platform installed and running	Applicable to Scenario 1 & 2
P11	The RESISTO platform is reachable from the test-bed	Applicable to Scenario 1 & 2

Table 1 Preconditions for the Use Case 1

4.2.2.1. Sub Use Case 1 Work flow

The steps that will be followed in this sub use case are described in the following diagram.

Step	Description
1	<p>Configuration of Testbed (Sensors and detection subsystem provided by ICCS, the RESISTO platform's components and OTE labs)</p> <p>OTE will configure the testbed equipment along with ICCS so as to forward event messages to the RESISTO platform. The steps that will be followed are :</p> <p>Testbed setup (networking, cloud, services)</p> <ul style="list-style-type: none"> • NMS Installation • Sensor Installation • NMS – Sensor integration • RESISTO-NMS Integration • RESISTO-Sensor Integration
2	<p>An attacker UAV overcomes the physical protection</p> <p>In this step we assume that a UAV overcomes the secure fence protected by OTE's security system and gains access to a network switch located inside a protected building. (Note: the UAV is provided by ADITESS).</p> <p>The UAV flies over the fence and approaches the building ignoring the physical security of the location, i.e. secure fence and building.</p> <p>We assume that 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 causing service unavailability and affecting the network's resilience.</p>
3	<p>Both attacks (physical and cyber ones) are detected by separate RESISTO sensors/detectors, in place in OTEs infrastructure</p> <p>As the UAV approaches the building, it is detected by the airborne threat detector (radar) provided by ICCS, which issues an airborne threat detection event and sends this event to RESISTO platform.</p> <p>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.</p> <p>When this happens, the OTE's physical equipment will detect a 'port down' instance and will automatically send a syslog message describing this state change to the RESISTO platform. Subsequently, the DoS attack is detected and a cyber-attack event is issued by RESISTO.</p>

	<p>RESISTO recognizes cyber-physical attack</p> <p>The RESISTO platform should be able to collect, parse and correlate the event messages coming from the ICCS detectors and the syslog messages from OTE's testbed and interpret them as DDoS attacks.</p>
	<p>RESISTO correlates the attack information events based on existing system modelling and risk assessments</p> <p>Based on the existing network modelling for OTEs testbed and the impact data pre-provisioned within RESISTO, we expect the Platform to provide immediate and accurate risk and resilience impact assessment taking into account the correlation between the two separate events.</p>
	<p>RESISTO alerts operator and suggests mitigation measures</p> <p>During this phase of the testing scenarios, the RESISTO platform will publish through its cockpit components, the alerts and mitigation measures derived from the correlation of events in the STCL and the information in the LTCL components. The expectation is that the RESISTO cockpit will publish:</p> <ul style="list-style-type: none"> -Real time alerts in a visual manner; -Real time alert notifications by additional methods – e-mail, desktop app notifications etc.; -Real time resilience and impact analysis; -Real time mitigation measures to be taken by OTE's testbed operators in a play-book, step-by-step manner; -Mean time to restoration of functionality (by a pre-existing threshold);
	<p>Attack is mitigated</p> <p>The network services impacted by the events have their functionality restored as is the resilience of the network.</p>

4.2.2.2. Sub Use Case 2 Work flow

Step	Description
	<p>Configuration of Testbed (Audio / Video Analytics system provided by ADITESS, the RESISTO platform's components and OTE labs)</p> <p>OTE will configure the testbed equipment along with ADITESS so as to forward event messages to the RESISTO platform. The steps that will be followed are :</p> <ul style="list-style-type: none"> • Testbed setup (networking, cloud, services) • NMS Installation

	<ul style="list-style-type: none"> • Audio / Video Analytics Installation • NMS – Audio / Video Analytics integration • RESISTO-NMS Integration • RESISTO- Audio / Video Analytics Integration
2	<p>An attacker overcomes the physical protection and intrudes OTE's Premises</p> <p>In this step we assume that an attacker/unauthorized person overcomes the physical protection of OTE's buildings, breaches the secure perimeter and manages to enter OTE's facility (building interior).</p> <p>For the piloting purposes, it is considered that the keycard access system is compromised, allowing the attacker to grant physical access to the building or that a stolen card is being used.</p> <p>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.</p>
3	<p>Intrusion is detected by separate sensors/detectors, in place in OTEs infrastructure</p> <p>The intrusion is detected by the 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.</p> <p>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.</p> <p>The RESISTO system activates various cyber detectors of the provider's network that eventually detect the malware.</p> <p>RESISTO recognizes intrusion</p> <p>The RESISTO platform should be able to collect, parse and correlate the syslog messages coming from the audio/visual analytics system and the OTE testbed and interpret them as intrusion on the cyber-physical domain.</p> <p>RESISTO correlates the attack information events based on existing system modelling and risk assessments</p> <p>Based on the existing network modelling for OTEs testbed and the impact data pre-provisioned within RESISTO, we expect the Platform to provide immediate and accurate risk and resilience impact assessment taking into account the correlation between the two separate events.</p> <p>Attack is mitigated</p> <p>A prevention/mitigation action is suggested and the malware is removed from the network</p>

4.3. Key Performance Indicators Used to Evaluate the Pilot

The Key Performance Indicators (KPIs) to be referred during the evaluation of the Use Case are given in the following Table. The KPIs that were provisionally suggested within D2.8 [2] have been thoroughly analysed within the Deliverable D3.8 [8] which provides the KPIs final shortlist along with the corresponding methods for their validation during the pilots. Thus the suggested KPIs to be measured for this Use Case are updated as follows, while the respective D3.8 section concerning their validation method is indicated as well:

KPI number	KPI Title	D3.8 relevant Section
KPI 1	Number of detected physical threats	Errore. L'origine iferimento non è stata trovata.
KPI 2	Number of detected cyber threats	Errore. L'origine iferimento non è stata trovata.
KPI 3	Detection probability	Errore. L'origine iferimento non è stata trovata.
KPI 4	Time to Detection (average)	Errore. L'origine iferimento non è stata trovata.
KPI 5	Decision-making time (average)	Errore. L'origine iferimento non è stata trovata.
KPI 6	Mitigation Time (average)	Errore. L'origine iferimento non è stata trovata.
KPI 7	Downtime	Errore. L'origine iferimento non è stata trovata.
KPI 9	Financial Impact	Errore. L'origine iferimento non è stata trovata.

Table 2 – Suggested KPIs to be measured during the pilot activities of Use Case 1

4.4. ORO's impacted Use case

ORO's use case "Cyber and Physical Protection of Network and Network Elements Mechanisms used by critical services that impact users" is the impacted use case of WP7 by Use Case 1. It combines cyber threats and physical threats that can be triggered by a malicious actor. The critical services that can be impacted by such threats are voice communications and data communications over 4G, 5G and fixed networks.

ORO has defined two scenarios that will be tested during the RESISTO piloting:

1. **A Distributed Denial of Service Attack and a concurrent Fiber Cut** - 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.
2. **Rogue Access to OROs Core Network and Routing Table Poisoning** - In this scenario, a human actor enters in one of OROs Core Network (ORO's Site in Gara Herastrau 4A, Bucharest – the location of our testbed) 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.

The use case pilot plan is thoroughly analyzed in WP8 –D8.1.[5]

4.4.1. Test-bed Interconnection

For the purposes of the interconnection OTE will use the testbed (Fig. 4) described in D2.8. "Table-top Read Teaming Results of RESISTO Architecture, Scenarios and Use-Cases". The same testbed will be also used in the proof of concept of Use Case 1 namely "Core Network Failure caused by Physical & Cyber Attacks to Telecommunication sites". From ORO's side the testbed that will be used is also presented thoroughly in D2.8 [2].

This interconnection between ORO's and OTE's testbeds can be achieved using various means, each of which induces performance-security tradeoffs. Currently we have chosen the option of interconnecting by using a secure tunnel, namely IPsec [9][10], which is a typical and most secure method of interconnection for such scenarios. If necessary, we may modify the testbed to use another solution for interconnection during the course of the project. The following table summarizes the possible interconnection methods and their properties.

Interconnection Method	Advantages	Disadvantages
Public IPs	Very easy to setup/extend	Requires reachable IPs/ports Low security
Public IPs with firewall	Easy to setup/extend Prevents 3rd parties from joining the network	No confidentiality Some management overhead

VPN	Secure Public IPs are not required, except for VPN server	Management overhead
-----	---	---------------------

Table 3 – Testbed interconnection design choices

4.4.2. Preconditions

No		Applicability
P1	Network interconnection is up and running	Both Testbeds
P2	Virtual environment up and running	Both Testbeds
P3	Physical Security Sensors are installed and functioning	OTE testbed
P4	DDoS Detection capability is functioning	Both Testbeds
P5	Physical Door Sensors installed and running	OTE testbed
P6	The RESISTO platform installed and running	Both Testbeds
P7	The RESISTO platform is reachable from the test-bed	Both Testbeds
P8	Subscriber provisioning and management is up and running	Both Testbeds
P9	Management servers are up and running	Both Testbeds
P10	IPSec Tunnel is Established between OTE and ORO	Both Testbeds

Table 4 Preconditions for Interconnected Testbeds Use Case

4.4.3. Interconnection flow diagram

Step	Description
1	<p>Interconnection Set up</p> <p>In this step we will interconnect the two testbeds. The interconnection, as mentioned will be implemented with IPsec. After that, the roaming user will need to be provisioned from the remote site to the home network. In order to do this, the two management networks will connect through the BGWs to forward the user from the remote site to the home site so that the remote network can service him/her.</p>
2	<p>An attacker overcomes the physical protection and intrudes OTE's Premises</p> <p>A DDoS attack is taking place</p> <p>For this step, that will happen during Use case 1 piloting. During this step;</p> <ul style="list-style-type: none"> • The network segment that is provisioning the user will temporarily become overwhelmed because of malware infection. • The service (video streaming) provided by OTE to the remote user is cut off and service provisioning stops temporarily. • Since the two testbeds will be interconnected servicing of the user will be interrupted until functionality/connectivity is restored. • OTE's NMS will identify that several systems and connections are unavailable and produces notifications and alerts, containing a lot of information, some of which is directly relevant to the occurred event. <p>RESISTO platform recognizes the attack</p> <p>As per the development done in WP6, the RESISTO platform will collect, parse and correlate NMS messages coming from the detectors in OTEs testbed and interpret them as DDoS attacks.</p> <p>During the previous development phases OTE had provided NMAP discovery and SNMP messages from each of the equipment to be used as detectors, in our testbed and the documentation for the specific SNMP messages. Given the existing information, RESISTO platform will detect such attacks once the respective alerts and SNMP messages reach the Platform.</p>
3	<p>Attacks are mitigated</p> <p>The network services impacted by the events have their functionality restored as is the resilience of the network</p>

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

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).

5.1. Technologies involved for both sub-scenarios of Use Case 2

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.

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.
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.

5.2. Sub Use Case 1: Terrorist Attack in telecom asset causes severe network failure

In this sub use case, a non-identified attacker uses a drone (UAV) so as to attack a telecom provider's facility.

A hostile UAV destroys an antenna pillar that supports the backhaul network. The antenna pillar and surrounding facility is not in a metropolitan urban city but it is located to a sub-urban or remote area supporting the backhaul network; thus, its damage, although not causing human casualties, may result in severe network failure. This sub-scenario exploits the current attacking trends, where UAVs or larger drones are used as unmanned attackers with payload meant for surgical bombing or limited but accurate attacks. 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.

The hostile UAV is detected by the airborne threat detector, already installed in the park, which triggers an airborne threat detection event that is send to the RESISTO correlator. 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 and the attack is identified and confirmed. RESISTO responds by selecting and suggesting a suitable mitigation action.

The various steps of the whole attack-mitigation cycle will be described in the sections to follow.

5.2.1. Scope

The scope of this sub use case is to examine cases where terrorism or other incidents occur in a lesser degree without causing devastating consequences in major cities, although affecting severely certain telecom assets that support or are part of the backhaul network; for example, certain telecom assets that are part or support the backhaul network, but they are not located within metropolitan or large urban environments. These cases 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.

However, in remote antenna parks, CCTV or other visual inspection solutions are not usually in place. The provider's NMS identifies the network failure but the telecom provider is not directly aware of the exact situation and what was the cause of the DoS and the network failure. The NMS attempts to reactivate the antennas through software means however, the lack of available information results in keeping the problem persistent and more thorough investigation is needed in order to provide immediate response as early as possible. 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 and after all the potential causes must be thoroughly investigated, 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.

5.2.2. Test-bed setup



This Use case will be piloted in OTE Academy premises as in the photo above, emulating the antenna pillar in sub-urban or remote areas. It will be a real environment pilot and as a consequence the attack will be simulated. UAV platforms that will be provided by ADITESS (as described in Deliverable D2.8 [2]) will have a two-fold role; to provide both the hostile UAV (attacker) and the inspection UAV with surveillance payload (friendly), while the ICCS Airborne Threat detection system will be used as well. The OTE's testbed will emulate the network failure and the telecommunication congestion.

5.2.2.1. Preconditions

		Applicability
P1	Network Connectivity is up and running	yes
P2	Cloud environment up and running	yes
P3	NMS installed and running	yes
P4	Cyber OS Sensors installed and running	yes
P5	Other cyber security functions installed and running	yes
P6	Active and passive airborne threat detector system (radar and acoustic) up and running	yes

P7	Other sensors (friendly UAV payload inspection cameras, connected to audio / visual analytics) installed and running	yes
P8	The RESISTO platform installed and running	yes
P9	The RESISTO platform is connected to the test-bed	yes

Table 5 Preconditions for the Terrorist Attack in telecom Sub Use Case

5.2.2.2. Sub Use Case 1 Work flow

Step	Description
1	<p>Integration of Testbed</p> <p>In this sub use case an actual antenna pillar will be used.</p> <p>The steps that will be followed are :</p> <ul style="list-style-type: none"> • Airborne threat detector installation • Audio / Video Analytics Installation • NMS – Detection and Analytics systems integration • RESISTO-NMS Integration • RESISTO-Sensor systems Integration
2	<p>A third party uses a drone (UAV) to attack a telecom provider's facility.</p> <p>In this step we assume that 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.</p>
3	<p>Intrusion is detected by the airborne threat detector</p> <p>The hostile UAV is detected by the RESISTO airborne threat detector system (offered by ICCS), already installed in the park, which triggers an airborne threat detection event that is send to the RESISTO correlator.</p> <p>Network and service failure events are fed into the RESISTO system</p> <p>The UAV attack renders the telecom asset (antenna pillar) inoperable. Subsequently the telecom provider's network experiences severe network loss in an extended level; mobile services are down at least in a wide area surrounding the antenna pillar / park. Several network and service failure events are fed into the RESISTO system, from the telecom operator's network management Server– NMS.</p> <p>RESISTO recognizes intrusion</p> <p>The RESISTO platform should be able to collect, parse and correlate the</p>

	syslog messages coming from the ICCS airborne threat detector and the telecom operator's Network Management centre (emulated by the OTE's testbed (NMS)).
	<p>RESISTO correlates the attack information and alerts operators: RESISTO "friendly" UAV takes-off</p> <p>Based on the existing network modelling for OTEs testbed and the impact data pre-provisioned within RESISTO, we expect the Platform to provide immediate and accurate risk and resilience impact assessment taking into account the correlation between the two separate events.</p> <p>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 (offered by ADITESS). Thus, the RESISTO "friendly" UAV takes-off and initiates a damage inspection procedure using on-board cameras (connected to the RESISTO audio / visual analytics system) in the vicinity of the airborne threat detection event's location.</p>
	<p>RESISTO suggests mitigation measures</p> <p>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.</p>
	<p>Attack is mitigated</p> <p>A prevention/mitigation action is suggested. The attack and the "destruction" of the telecom asset (antenna pillar) is identified and confirmed. A corresponding event is fed into the RESISTO system.</p>

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

In this use case we consider there is a telecommunication congestion due to network loss caused by a natural disaster that renders a number of assets inoperable. Natural disasters such as severe weather conditions or earthquakes of moderate amplitude can cause damages to telecom assets and facilities located in sub-urban or rural, remote areas. The telecom assets include antenna pillars and buildings containing critical access and routing circuits (DSLAMs, 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 telecommunication congestion in the mobile network.

5.3.1. Scope

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 and the RESISTO "friendly" UAV takes-off using onboard cameras and 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, as the potential cause of the congestion, along with the increased user traffic following the natural disaster occurrence.

The whole action and response is similar to the previous sub-scenario 1 of Use Case 2. 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; the information on the loss of network resources caused by the earthquake or natural disaster wouldn't be correlated with the congestion events without human intervention and the response would be significantly slower compared to the case where the RESISTO system is used to automate the whole procedure.

5.3.1.1. Sub Use case 2 Work flow

Step	Description
1	Integration of Testbed In this sub use case an antenna pillar and buildings containing critical access and routing circuits will be needed. The steps that will be followed are : <ul style="list-style-type: none"> • Natural events (weather and seismic sensing) sensing platform installation • Audio / Video Analytics Installation • NMS – natural events sensing platforms and Audio / Video Analytics integration • RESISTO-NMS Integration • RESISTO-both sensing systems Integration

<p>2</p>	<p>Natural disasters affect telecommunication networks.</p> <p>In this step we assume that due to severe weather conditions (twisters and hurricanes) or due to moderate earthquakes, damages in telecom assets and facilities located in sub-urban or rural remote areas cause network failure, leading to telecommunication congestion in the mobile network.</p> <p>Two reasons can cause this congestion. The first is that some core components are out of order causing heavy traffic to the remaining ones due to existing rerouting rules and the second reason is a burst of traffic that occurs.</p>
<p>3</p>	<p>RESISTO system receives the congestion events</p> <p>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).</p> <p>RESISTO correlates the received information and alerts the operators</p> <p>The RESISTO platform being able to collect, parse and correlate the event messages coming from operator's system, issues a damage inspection order to the RESISTO UAV-based surveillance sensor system. Based on RM3 network modelling for OTEs testbed and the impact data pre-provisioned within RESISTO, we expect the Platform to provide immediate and accurate risk and resilience impact assessment taking into account the correlation between the two separate events.</p> <p>RESISTO "friendly" UAV takes-off</p> <p>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 RESISTO "friendly" UAV platform equipped with optical sensor (daylight and thermal camera) is configured to navigate to the point of interest. The UAV platform is equipped with digital data links for air to ground communication. The UAV Ground Control Station will be integrated with OTE's testbed for real-time video stream transmission. Video analytics will be applied on the stream while any detections will be sent to the RESISTO platform.</p> <p>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 as the potential cause of the congestion, along with the increased user traffic following the natural disaster.</p> <p>RESISTO suggests mitigation measures</p> <p>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 auxilliary network resources.</p>

	<p>Issue is mitigated</p> <p>A prevention/mitigation action is suggested. The “destruction” of the telecom asset (antenna pillar) is identified and confirmed. A corresponding event is fed into the RESISTO system.</p>
--	---

5.3.2. Key Performance Indicators to Evaluate the Pilot

The Key Performance Indicators (KPIs) to be referred during the evaluation of the Use Case are given in the following Table. The KPIs that were provisionally suggested within D2.8 [2] have been thoroughly analysed within the Deliverable D3.8 [8] which provides the KPIs final shortlist along with the corresponding methods for their validation during the pilots. Thus the suggested KPIs to be measured for this Use Case are updated as follows, while the respective D3.8 section concerning their validation method is indicated as well:

KPI number	KPI Title	D3.8 relevant Section
KPI 1	Number of detected physical threats	Errore. L'origine iferimento non è stata trovata.
KPI 2	Number of detected cyber threats	Errore. L'origine iferimento non è stata trovata.
KPI 3	Detection probability	Errore. L'origine iferimento non è stata trovata.
KPI 4	Time to Detection (average)	Errore. L'origine iferimento non è stata trovata.
KPI 5	Decision-making time (average)	Errore. L'origine iferimento non è stata trovata.
KPI 6	Mitigation Time (average)	Errore. L'origine iferimento non è stata trovata.
KPI 7	Downtime	Errore. L'origine iferimento non è stata trovata.
KPI 9	Financial Impact	Errore. L'origine iferimento non è stata trovata.

Table 6 – Suggested KPIs to be measured during the pilot activities of Use Case 2

6. USE CASE 3: TELECOMMUNICATION SITES

This Use Case will not be piloted since it will be using the critical Broadcast network of the infrastructure provider, namely RTV.

The network is based on high tower / high power, with a high capillarity in span and with 3 control centres that can switch or commute functions and management actions in order to fully control the network and therefore the services provided.

6.1. Scope

The main objective is to analysis the procedures a Telco NOC operator must have in order to mitigate a real thread. The operator will analyse the data/message from the Leonardo Platform but need some basic procedures in order to know what to do, what to analyse, who must be involved, and how to mitigate the thread. An operator needs information that is provided by the Leonardo platform but require how is the best way to proceed.

In this use case, based on the threads and architecture, we will set up the procedures an operational NOC must manage the Leonardo platform in conjunction with the equipment, network and of course the most important is the maintenance of the services and the mitigation to others services.

The output of this will be the procedures an operational NOC must follow base on a study case considering all threads and all different architectures.

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

Use Case 4 “Disruption of Major Sporting Event by Combined Physical & Cyber-Attack by a Terrorist Organisation” focuses on potential disruptions of IPTV delivery (i.e. live, linear TV streams) caused by combined physical and cyber-attacks. Although the attacks may not directly target the IPTV delivery itself but since the IPTV service is running over the same network infrastructure as any other IP-based services, such as broadband Internet, any attack on the IP infrastructure could have significant impact on the live TV streams, e.g. of major sporting events, which would affect a huge number of viewers/customers.

An IPTV delivery network typically uses multicast streaming and routing technology for efficient bandwidth utilisation. Unicast transmission is used for delivering on-demand, non-live IPTV streams. The architecture and design of such IPTV network already provides certain level of scalability and resilience in order to deal with high demands, network congestion or geographical-related network delays. In this use case we aim at improving its resilience against cyber-physical attacks by using the RESISTO platform to proactively detect any potential attacks and subsequently trigger or recommend appropriate actions to prevent major service disruption.

7.1. Scope

An IPTV live streaming service will be simulated in the testbed environment. The service will be running over a number of (critical) network nodes that may be subject to cyber-physical attacks. Appropriate cyber sensors are installed on the nodes to monitor system health and report suspicious cyber events. After a physical security breach at one of the critical node sites, the corresponding critical server is compromised and used by the attacker as a platform to launch further cyber-attacks on the other critical nodes in an attempt to cause more severe impacts on the IPTV service. The RESISTO platform continuously monitors each node’s system logs and receive any alerts/events generated by the relevant physical and cyber sensors. By correlating all the information derived from the logs and cyber threat events together and combining them with the relevant risk models the RESISTO platform will provide recommendations to mitigate the impacts, e.g. by re-routing the multicast traffic through unaffected nodes or transcoding any

unicast streams to mobile devices. Once full service has been restored on the affected node the RESISTO platform will indicate to switch the IPTV service back to its normal operation mode.

7.2. Test-bed setup

The BTC's Cyber Security and Research Platform will provide the facilities for building and running the virtual test-beds that will mainly be used to implement and conduct the use case. Where applicable the virtual test-bed will be connected to some physical component, e.g. smart lock system, in order to demonstrate the physical attack. The test-bed setup has already been described in Section 7.2.3 of the Deliverable D2.8 "Table-Top Read Teaming Results of RESISTO Architecture, Scenarios and Use Cases" [2] and is summarised as follows.

As pictured in the Figure 5 the virtual test-bed is composed of the following virtual machines (VM) to represent different type of (critical) network nodes:

- **Core node VM:** This VM represents the core node that is connected directly with IPTV video sources and content server. It is capable of forwarding multicast traffic to adjacent nodes/routers that have registered multicast group members. The node is using the Protocol-Independent Multicast (PIM) as its multicast routing protocol and employs its Source-Specific Multicast (SSM) variant to build the multicast distribution tree. The Internet Group Management Protocol version 3 (IGMPv3) is used by adjacent metro nodes to establish multicast group memberships.
- **Metro node VM:** This VM contains components that replicate the main functions of multicast replicators and unicast IP routers as usually deployed on metro nodes. IGMPv3 protocol is used by adjacent edge nodes to establish multicast group memberships.
- **Edge node VM:** This VM represents the nodes at the edge of the network infrastructure and contain components that replicate the main functions of associated multicast replicators and IP routers. IGMPv3 protocol is used by the connected clients that wish to join the multicast groups and consume the live IPTV streams from the source.
- **Client VM:** This VM contains (software) components that emulate a number of unicast and multicast clients in the network consuming the video streams via unicast and multicast transmission respectively.

Additionally a Controller VM is deployed in the test-bed to aggregate and visualise the system logs and cyber events collected from the network nodes. It will be exchanging information with the RESISTO platform to provide system logs and cyber events, or to receive RESISTO responses in case of potential security breach

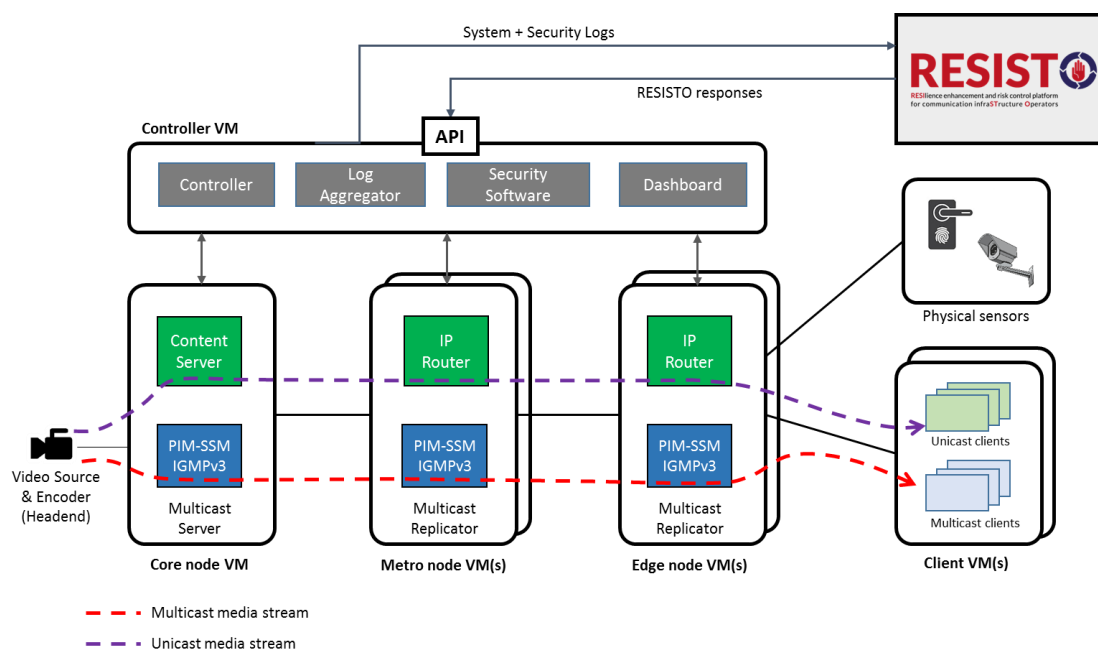


Figure 5. High-level BTC virtual test-bed architecture for multicast and unicast video delivery

7.2.1. Technologies involved

Technology	Role	Description
Video source and content server	Source of IPTV contents	Application server, live video feed.
Video client software	Consumption of IPTV contents	Receives the video streams either via multicast or unicast transmission and plays back the video.
Multicast routing software (PIM-SSM and IGMPv3)	Multicast router	Forwards multicast packets to adjacent nodes and builds multicast group membership tree.
RESISTO Platform	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.
Smart lock	Acquisition of building/room entry data	Part of perimeter protection system. Entry logs (e.g. timestamps) will be collected by the central controller.

Camera (CCTV) - optional	Acquisition of video data	Part of the perimeter protection system. Video footage may be processed by separate analytics component. Alert logs will be collected by the central controller.
ELK (Elasticsearch, Logstash, Kibana) stack	Acquisition, storage and visualisation of system logs and cyber events	Collects the system logs and cyber events from each network node and pushes them to central storage for further analytics and sharing.
RADIOFILTER Cyber sensors	Detection of cyber threats	Detects suspicious cyber threat activities on nodes and generates alerts
IoT Firmware reliability sensors	Detection of modified firmware	Checks the reliability of the installed firmware of the CCTV camera to detect potential compromising
Penetration testing tool	Simulation of cyber-attacks.	Performs a variety of cyber-attacks on victim hosts

7.2.2. Preconditions


No		Applicability
P1	Network Connectivity is up and running	yes
P2	Virtual environment is up and running	yes
P3	Multicast routers are up and running	yes
P3	Physical Security Sensors are installed and functioning	yes
P4	Cyber Detection capability is functioning	yes
P5	The RESISTO platform is installed and running	yes
P6	The RESISTO platform is reachable from the test-bed	yes
P7	Live video stream is up and running	yes
P8	Video content server (on-demand) is up and running	yes
P9	System logs and cyber events feed are up and running	yes

Table 7- Preconditions for the Disruption of Major Sporting Event by Combined Physical & Cyber-Attack by a Terrorist Organisation Use Case

7.2.3. Use case Work flows

The steps that will be followed in this use case are described in the following diagram.

Step	Description
1	<p>Integration of Testbed</p> <p>BTC will deploy and configure the virtual test-bed components and develop the necessary software to forward event messages to the RESISTO platform.</p> <p>This comprises the following activities:</p> <ul style="list-style-type: none"> • Setup of the infrastructure components, i.e. core node, metro node, edge node, servers and clients • Setup of the controller component for system monitoring and control • Testing of the software functionality for small-scale IPTV service, e.g. multi/unicast routing, IPTV streams, etc. • Integration with the RESISTO management platform including communications/message exchange via APIs • Integration with RESISTO sensor (subject to availability)
2	<p>An attacker gains unauthorised entry and compromises a critical node</p> <p>In this step we assume an attacker used a stolen ID card to gain entry to a telco operator's building such as a telephone exchange that hosts a network edge node. The attacker proceeded towards a secured server room inside the building that was protected by smart locks.</p> <p>The attacker bypassed the smart lock security system and connected his laptop to the local network either via local WiFi access point or Ethernet ports available in the room. He then started to explore the local network with the objective to identify the edge node server and any other hosts that has direct connection to a metro node server. After successfully exploiting a vulnerability of the edge node and a router, the attacker injected a malware module into the compromised host and created a cron-job to activate the malware at a specific date/time in the near future. The attacker then left the building.</p> <p>When the attacker entered the secured server room the smart lock system recorded the timestamp of the entry and sent the record to the controller, which forwarded it to the RESISTO (management) platform. Also, in cases where a CCTV camera is used, the footage is also forwarded. However, the attacker may compromise these physical sensors (CCTV camera and smart locks) by performing a Denial of Service (DoS) attack targeting the availability of the sensors. RADIOFILTER cyber sensors will detect this attack and sent an alert to the RESISTO platform. Furthermore, when the attacker tried to gain access to the local network through a Rogue Access Point, RADIOFILTER cyber</p>

	<p>sensors will detect such activity and sent an alert to the RESISTO platform. Another attack that will be detected is the compromising of the CCTV camera installed firmware, which could be used as an alternative way to gain access to the local network. This event will be detected by IoT firmware reliability sensors. Lastly, while the attacker tried to compromise the server, the associated system activities (e.g. user login) were being logged and any suspicious network activity was also monitored by the installed cyber sensor (i.e. Intrusion Detection System). The syslog messages and any detected cyber threat events were then sent to the RESISTO platform (via the controller).</p>
	<p>RESISTO recognises potential threat on edge node</p> <p>The RESISTO platform recognised entry to a secured area inside a building outside working hours, and during the same period of time also received cyber alerts indicating potential security breach on one or more servers at the same location.</p>
	<p>Malware is activated during live stream of a major sporting event</p> <p>A major sporting event was happening and a live IPTV streams were being delivered to a huge number of viewers. During this time the cron-job that had been created by the attacker on the compromised host activated the installed/hidden malware module. The malware was targeting a metro node server that was critical to deliver multicast (as well as unicast) streams to a number of adjacent edge nodes. The cyber sensor installed on the attacked metro node started reporting suspicious network activities resembling a distributed denial of service attack. The threat events were being monitored by the controller and passed on to the RESISTO platform.</p>
	<p>RESISTO correlates the attack information with existing system modelling and risk assessments</p> <p>The RESISTO platform received the alerts from the cyber sensors of a metro node server. At the same time the RESISTO platform observed unusual network and system activities on that particular metro node server, based on transferred syslog messages and/or system metrics, e.g. CPU load, inbound traffic, etc. The platform then correlated all information together with existing risk models.</p>
	<p>RESISTO alerts operator and suggests mitigation measures</p> <p>Following on the outcome of its risk assessment the RESISTO platform informed the IPTV operator about the situation along with details of the metro node server that was potentially under attack. The platform suggested appropriate measures for mitigating the impact of the attack, e.g. by re-routing the multicast and unicast streams via another metro node that was</p>

	<p>known to continue operating under normal condition; in order to avoid traffic congestion and/or system overload on the (fall-back) metro node the RESISTO platform might also suggest to apply appropriate transcoding on affected unicast streams to reduce the bandwidth and resource usage.</p> <p>The relevant countermeasures are indicated into the D5.4.</p>
	<p>Attack is mitigated</p> <p>Depending on the type of recommended mitigation measures, the corresponding actions may either be implemented automatically or by human operators. The IPTV operator was observing the impact of the measure on the live IPTV streams and ensured that the IPTV service was running as expected with minimal disruptions. Once the IPTV operator was happy with the service performance they tried to reinstate the attacked metro node server by e.g. shutting the server down or blocking all incoming traffic.</p>

7.3. Key Performance Indicators to Evaluate the Pilot

The Key Performance Indicators (KPIs) to be referred during the evaluation of the Use Case are given in the following Table. The KPIs that were provisionally suggested within D2.8 [2] have been thoroughly analysed within the Deliverable D3.8 [8] which provides the KPIs final shortlist along with the corresponding methods for their validation during the pilots. Thus the suggested KPIs to be measured for this Use Case are updated as follows, while the respective D3.8 section concerning their validation method is indicated as well:

KPI number	KPI Title	D3.8 relevant Section
KPI 1	Number of detected physical threats	Errore. L'origine iferimento non è stata trovata.
KPI 2	Number of detected cyber threats	Errore. L'origine iferimento non è stata trovata.
KPI 3	Detection probability	Errore. L'origine iferimento non è stata trovata.
KPI 4	Time to Detection (average)	Errore. L'origine iferimento non è stata trovata.
KPI 5	Decision-making time (average)	Errore. L'origine iferimento non è stata trovata.
KPI 6	Mitigation Time (average)	Errore. L'origine iferimento non è stata trovata.
KPI 7	Downtime	Errore. L'origine iferimento non è stata trovata.
KPI 9	Financial Impact	Errore. L'origine iferimento non è stata trovata.

Table 8 – Suggested KPIs to be measured during the pilot activities of Use Case 4

8. USE CASE 10: PROTECTION AND RESILIENCE OF TIM'S NETWORK NODES.

Current Telco infrastructures are the preferred target for DDos attacks and other form of malicious activities. Among the various elements of a Telco network, customers elements are surely the most exposed and easy to select as a potential victim by hackers because they are “outside” the traditional security perimeter and face directly the open Internet. Given the huge number of elements and technologies involved in Telco customers networks, traditional provisioning and assurance processes are under pressure in order to provide to customers protection against cyber threats. Also state-of-the-art WAN technologies, although integrated with modern security features, are suffering an ever increasing number of attacks, and Telco Operators, in case of managed elements, are under huge pressure to protect their services.

In this use case TIM will demonstrate the usefulness of the RESISTO platform in the protection of the customers' network nodes, integrating its ability to correlate information also from OSINT sources with the information related to the configuration of the provided customers network elements.

8.1. Scope

This use case aimed to use RESISTO platform to enhance the security of the Telco customers network nodes. A specific test-bed will be implemented by using the standard WAN technology as the main enabler. Since modern Wide Area Network technology is usually coupled with different security features, such as VPN, firewall, IDS and others, it is common to assume, erroneously, customers networks as well protected from cyber-attacks. Assuming that security tools such as firewall or IDS eliminate the need for other wide-area networking security and resilience best practices is a mistake. In fact WAN elements should not be viewed as a standalone solution that can go untouched for months. It's important to keep the firmware stack updated with the latest security patches. Having the ability to automate patching doesn't alter the fact that changes will be applied frequently. Most organizations may have security software in place, but network engineers are too overwhelmed to actually handle it (or they don't have the necessary security expertise).

One of the main threats against WAN elements is the “outdated” or “unpatched” software. In this regard, one of the most important question is existence of zero-day and known vulnerabilities in the firmware and in other its software modules. Those vulnerabilities provide local facilities and can be exploited by attackers to escalate privileges in the operating system causing any kind of nefarious effects.

8.1.1. Technologies involved

The following table lists the key elements of the TIM sub-use case.

Technology	Role	Description
RESISTO Platform	cyber and physical attack monitoring, detection, response and mitigation system	Monitors the overall functionality of the cyber security, receives threat events, uses specific tools and techniques to identify vulnerabilities, erroneous configurations or intrusion attempts and responds to threats.
WAN element (e.g. router)	The elements will provide the connectivity to the customers	The WAN technology is used only to provide the connectivity to the customers. It is important to note that the focus of the use case is the RESISTO ability to provide additional security services to the Telco customers
PC/System: Windows Server	Several servers will be used in order to simulate the internal network of the customer.	Internal server potentially target of attacks.
WAN elements configuration and description Sensor, named as simply the sensors in this use case	The RESISTO platform has to maintain updated the information about the technology, software level and configuration of the customers elements (e.g. protocols enabled, ACL, etc.)	The sensor will send the configuration information of the WAN nodes to the RESISTO platform via network interface protected by means of encrypted protocol (e.g. HTTPS)

Table 9 -Technologies involved in the TIM sub-scenario

8.1.2. Preconditions

The following table reports the preconditions to be verified before the actual test will be performed.

		Applicability
P1	Network environment up and running	YES
P2	Sensor installed and running	YES
P3	The RESISTO platform is reachable from the test-bed	YES
P4	The RESISTO platform able to correlate OSINT with network elements configuration	YES

Table 10- Preconditions for the TIM sub scenario

8.1.3. Use case Work flows

The steps that will be followed in this sub use case are described in the following diagram.

Step	Description
1	<p>Integration of Testbed (Integration Sensor, RESISTO and TIM WAN elements)</p> <p>TIM will configure the testbed equipment' in order to have an up and running customer network able to provide the needed connectivity to the internal server. The sensor read the main information about WAN nodes configuration, sw level and others and forwards them to the RESISTO platform</p>
2	<p>A specific vulnerability, impacting the WAN elements deployed, has been disclosed. The Threat has been classified as High level by major Threat intelligence organization.</p> <p>In this step we assume the RESISTO platform, by OSINT interconnection, is able to collect and analyse main information related to the cybersecurity and resilience of the Telco Infrastructures (including the customer elements managed by Telcos) it is in charge to protect.</p> <p>Many vulnerabilities are disclosed every day about thousands of different technologies. It is very difficult to keep track of all of them and to focus on the very important ones. It is important to have prioritized alerts, which give a higher level of alert when a certain threat is specific to the telecommunication target sector and coming from specific threat actors that have an interest in attacking customers in the specific country (Italy in our case).</p> <p>RESISTO is able to correlate information about the technologies and configurations used by TIM customers with the emerging threats.</p> <p>A first alarm is sent to the TIM operation center/customers network engineers about the new threats, the risk level and the possible option to resolve it.</p> <p>The WAN platform is not yet upgraded/patched.</p> <p>A specific tool, able to exploit the WAN vulnerability, has been disclosed</p> <p>RESISTO detect that a malicious tool, built to attack network element through the discovered vulnerability, has been published and is available on the dark web. Moreover, OSINT source alerts about a possible attack against TIM customer node elements by using the new malware tool.</p>

<div>3</div>	<p>RESISTO recognizes that the risk level is now critical and helps the operator to solve the issue</p> <p>Given the latest news, the threat is elevated to Critical because the vulnerability has been weaponized.</p>
	<p>RESISTO alerts its operators and suggests mitigation measures</p> <p>Since the WAN nodes are still vulnerable to the vulnerability just discovered, a new event has been sent to the TIM operation center in order to request a reaction asap against the threat.</p> <p>The relevant countermeasures are indicated into the D5.4.</p>
	<p>Threat/attack is mitigated</p> <p>The TIM operation center, after the notification from RESISTO, proceed with the upgrade/patching of the WAN network nodes impacted by the vulnerability.</p> <p>The sensors send to the RESISTO platform the new software level and configuration.</p> <p>The RESISTO platform, given the new information received about the patching/upgrade, reset the alarm.</p>

8.2. Key Performance Indicators to Evaluate the Pilot

The Key Performance Indicators (KPIs) to be referred during the evaluation of the Use Case are given in the following Table. The KPIs that were provisionally suggested within D2.8 [2] have been thoroughly analysed within the Deliverable D3.8 [8] which provides the KPIs final shortlist along with the corresponding methods for their validation during the pilots. Thus the suggested KPIs to be measured for this Use Case are updated as follows, while the respective D3.8 section concerning their validation method is indicated as well:

KPI number	KPI Title	D3.8 relevant Section
KPI 2	Number of detected cyber threats	Errore. L'origine iferimento non è stata trovata.
KPI 3	Detection probability	Errore. L'origine iferimento non è stata trovata.
KPI 4	Time to Detection (average)	Errore. L'origine iferimento non è stata trovata.
KPI 5	Decision-making time (average)	Errore. L'origine iferimento non è stata trovata.
KPI 6	Mitigation Time (average)	Errore. L'origine iferimento non è stata trovata.
KPI 7	Downtime	Errore. L'origine iferimento non è stata trovata.
KPI 9	Financial Impact	Errore. L'origine iferimento non è stata trovata.

Table 11 - KPI to be referred for the Healthcare scenario

9. USERS INVOLVEMENT AND TRAINING (TIM)

Training needs were identified via direct exchange with all other WP leaders and especially with WP8 and WP9 leaders, respectively. As almost all aspects related to RESISTO platform do require training a training procedure and a training plan will be developed.

Key areas, methods of training and time schedule are included and detailed including:

- E-learning materials for presentation
- Formal workshops and Webinars for all partners or subgroups
- One-to-one training of staff for the realization of pilots.
- Material such as glossary for a common understanding of the terminology used, advanced forum for discussions and content creation to facilitate the exchange of information and concepts as well as analytical manuals and tutorials related to RESISTO platform.

Partners responsible for training will be LDO and RM3. TIM will also have a key role since is the partner responsible for the training and the users involvement. Operators and all participants in the pilot will be obliged to provide to the above mentioned partners a list of their staff that will participate in the training.

Mapping of existing training needs was done based on information received from partners and acquired from strategic documents and previously acquired knowledge.

9.1. User involvement

As user needs and use contexts became increasingly important in system framework development, ISO 13407 [11] prescribes the dynamic contribution of users for getting clients and undertaking prerequisites. Karat [12] portrays it in this way: “We don’t consider usability as limited to the display and keyboard interfaces between human and machine, but rather we recognize that it encompasses how any artefact fits into a complex work or home environment”. Along this line, it is obvious that reports are inadequate as sources of information and direct contact with users is urgent to comprehend the various contexts of utilization. Also, in principle, user involvement is most efficient and powerful in the beginning stages of system framework development as the cost engaged with making changes increases during system advancement [13][14].

On the other hand, a clear definition of user involvement is inadequate. It has been utilised synonymously with “focus on users” [15], “consulting end-users” [12], “contacting with system users” [16] and “participation of users” [17]. **Errore. L'origine riferimento non è stata trovata..** User involvement can be seen to be a general term describing direct contact with users and covering many methodologies. For example, in participatory design, users have dynamic and active roles in many design activities, but in other approaches, users are involved as providers of information, commentators or object for observations. The degree of user involvement can be extensively portrayed as being somewhere on the continuum from informative, through consultative to participative [18].

In [19], they recommend classifying the principal approaches to user involvement instead of particular development approaches. The main approaches are user-centred design, participatory design, ethnography, and contextual design. These approaches are represented in Readings in Human-Computer Interaction book [20] and the latter three are considered as frameworks of field research by Wixon and Ramey [21].

User-centric architecture is intended to create useful and functional products. There does not seem to be an accepted definition or mechanism for it [12]. Nevertheless, there is a general acceptance of the concepts Gould and Lewis present in [22]. The principles are:

- Early focus on the users and tasks
- Empirical measurement
- Iterative design

The principles incorporate the possibility of user involvement: Gould and Lewis [22] suggest bringing the design team into direct contact with potential users, as opposed to hearing or finding out about them through human intermediaries. The second principle infers that, early in the development procedure, planned users should use simulations and prototypes to complete real work, and their performance and responses should be observed, recorded and examined.

Usability engineering partially overlaps with user-centred design and the two are frequently used interchangeably (e.g. [23]). Wixon and Wilson [24] characterize usability engineering as a process for defining, estimating and thereby improving the usability of products. Methodological approaches to usability engineering have been presented by several authors such as Mantei and Teorey [25] and Mayhew [26].

According to Damodaran [18] a variety of studies shows that effective involvement in system design yields the following benefits:

1. Improved quality of the system emerging from increasingly accurate user requirements.
2. Avoidance of exorbitant system features that the user did not need or cannot use.
3. Improved degrees of acceptance of the system.
4. Greater understanding of the system by the user resulting in more powerful use.
Increased participation in decision-making within the organization.
5. The list is fairly participatory design focused, but it aptly represents the underlying assumptions regarding the benefits of user-centred design and usability engineering.

Training of the end clients is one of the most significant strides for an effective system usage. The end users can be included in parallel testing, and training needs to be carried out before that. At this point, having the end users involved is also a good way to get them excited about the proposed system because many of them may not been familiar with the project before training. A parallel research assistance will help them plan for the moment when the device goes online. End users in more of a “real world” environment are good at using the system and can determine when process flows are not working. When everyone interested in suing the program is included in the training, they will feel more comfortable about using it when they move into production and the user community can see the implementation when positive. The system may have been checked for functionality and all customizations work properly, but if the end users don’t know how to use it or feel confident with it, then the launch of the new system would be deemed ineffective. The scheduling of end-user training is therefore important and must be scheduled and executed prior to the beginning of the parallel test process to ensure an effective implementation.

There are two potential training approaches. The first is to use project team members to design and implement end-user training and the second is to find a training partner to facilitate end-user training development and implementation, including a training aspect for the trainer. The use of project team members to perform training for the operators would allow end users to be more informed about how and why the system was built.

In her excellent 2006 overview of end-user training, “Plan your end-user experience training strategy before software roll-out” [27], Deb Shinder states the five key points to a successful implementation.

The first goal is setting training goals, that usually coincide with minimizing any productivity losses associated with transition. Firstly, you want the end-user to complete their assignments as quickly as they were doing with the already existing software. In the following phase, the users must do their job more quickly, accurately and securely than before, maybe automizing some features. Obviously, suing a completely new software, such as the RESISTO platform, is very complex and needs time to allow operator to manage it. More important not all software is equal, neither are all operators.

An important step is to assess the technical skill degree of those who will actually use regularly the software. The RESISTO platform will be deployed for the constant use of telecommunication operators, but in several and different companies. Technical novices will require more oriented, step-by-step basic guidance, while more experienced computer users can easily pick up the basics and benefit from further training that teaches them how to use advanced features of the RESISTO platform.

The next move is to determine the methods of delivering the required training. Usually, the suggestion is to use a combination of these:

- Individual hands-on instructor: a teacher will personally guide each user through the process of performing specific task with the RESISTO platform and answer questions. This is the costliest and possibly the most successful tool.
- Hands-on classroom style instructor-led training: a teacher demonstrates to the students how the RESISTO platform operates and how to execute specific tasks in a classroom with users performing the task themselves. Every user or pair of users has a copy of the RESISTO platform where they can practice on.
- Seminar style group demonstration: a teacher demonstrates to the users how the RESISTO platform functions in a live demonstration and how to execute specific tasks.
- Computer Based Training (CBT): virtual self-paced training that enables end users to complete interactive lessons to walk through specific task processes, and software checks them for success and comprehension.
- Book based self-paced training: end users complete workbook tutorials often illustrated with screenshots, about how to execute specific tasks.

End user training is more effective and memorable if it is tailored with the specific use of the software, including common problems users may encounter or security issues related to the platform.

Using a mixture of computer-based training and seminar style training where users can ask questions and practice the skills with teacher guidance, you can get many of the advantages of individualised training without the high costs. CBT has the advantage of scaling up or down depending on the number of users you need to train, so users are able to move at their own speed rather than the rest of the class keeping up or holding back.

For the RESISTO platform, the user involvement is performed through interviews and questionnaires. The content of interviews and questionnaires is related to the potential of the RESISTO platform containing six different scales:

- Attractiveness: do users like the RESISTO platform?
- Perspicuity: Is it easy to know the RESISTO platform? Is learning how to use the RESISTO platform easily?
- Efficiency: Could users solve their tasks without the need for excessive effort?
- Dependability: Does the user feel comfortable with the interaction of the RESISTO platform?
- Stimulation: Is using the RESISTO platform motivating?
- Novelty: Does the RESISTO platform attract the user interests?

Attractiveness is an element of absolute valence. Perspicuity, efficiency, and dependability are goal-directed strategic aspects of quality, while stimulation and novelty are not goal-directed aspects of hedonic quality. For more details on the construction and validation of the User Experience Questionnaire (UEQ), please refer to [28].

The questionnaire is also used as part of a traditional usability study to collect some objective data about participants' opinions of user experience. The best time to hand over the questionnaire is just after they have completed working on the test trials. If the participants fill out the questionnaire after having a long conversation with the individual performing the trials about the RESISTO platform, this would impact the tests. The questionnaire's goal is to capture a user's immediate impression of a feature. Therefore, before you debate with the members, try to get answers to the UEQ.

9.2. Training Plan

The training will be performed using webinars, or eventually workshops. A webinar is a seminar on the web. Webinars are most commonly performed by encouraging key personnel to call into a toll-free phone number or to sign into a website so they can see and hear what is going on. A webinar can also be registered and referenced at a later date. It enables new personnel to study the webinar as if they were already participating.

A webinar is a means for people, before they try it themselves, to learn something different in a group. By giving them the chance to step through a practice run with a specialist, without fear of committing a disastrous error, the anxiety of doing something different is significantly diminished.

Individuals are highly affected by responses from their peers. A webinar is an opportunity for a group of people to hear each other answering questions and feel confident that other people share the same thoughts and curiosities. In reality, people also feel more relaxed engaging online, rather than staring at them as they lift their hand by a hundred people.

Webinars speed up the learning process by improving networking tools, allowing you to provide simulated presentations to a variety of stakeholders at once. The ease of use and affordability of webinars means you can carry out shorter, more regular training sessions which help to keep everyone focused.

For the RESISTO project, we plan to realize the training using webinars, that explains how to use the RESISTO platform in the different use cases. The main goal is to describe the interaction of the RESISTO User Interface. The webinars can include video of the presenter talking, slideshows or any other visual elements. The webinars usually have a Q&A (questions and answers) session, during which the audience can ask questions.

The webinars and the workshops are planned to be prepared before the start date of the pilot demonstrations. There will be also other webinars to assess how the pilots are going and to improve the RESISTO platform in event of troubles and problems.

The webinars are demonstration of the RESISTO platform in the different case studies. They are based on the deliverables that are produced in WP6, especially D6.3 [29].

10. CONCLUSION

The present document describes the initial test plan for the piloting and validation of the use cases involved in the “Protection and resilience of the Current / existing Telecommunication Critical Infrastructures” scenario:

Each test plans have been defined by following a specific methodology (defined in common with WP8 and WP9) consisting of the steps mentioned in section 3 of the current deliverable.

The list of the actual tests that will be performed during the validation of the scenarios will be described analytically into the foreseen deliverables D7.2 and D7.3.of WP7.

Finally the document describes the User Involvement and training plan, focused on the piloting of the use cases and the integration and exploitation of the RESISTO platform.

References

[1]	RESISTO project (Grant Agreement No. 78640)
[2]	RESISTO Deliverable D2.8:Table-top Read Teaming Results of RESISTO Architecture, Scenarios and Use-Cases
[3]	RESISTO Deliverable D6.1 “SW architecture definition”
[4]	RESISTO Deliverable D4.8 “Active and Passive Sensor Deployment Plan”
[5]	RESISTO Deliverable D8.1 “Scenario 2 Test plan definition”
[6]	RESISTO Deliverable D9.1 “ Scenario 3 Test plan definition”
[7]	RESISTO Deliverable D5.4 “Real Time Response and Mitigation Results”
[8]	RESISTO Deliverable 3.8 “KPIs, quantities and metrics for cyberphysical risk and resilience of telecom CI – final”
[9]	https://en.wikipedia.org/wiki/IPsec
[10]	https://www.csoonline.com/article/2117067/data-protection-ipsec.html
[11]	ISO, 13407: Human-centred design processes for interactive systems, Geneva ISO. (1999).
[12]	C.-M. Karat, Cost-Justifying Usability Engineering in the Software Life Cycle, in: Handb. Human-Computer Interact., Elsevier, 1997: pp. 767–778. doi:10.1016/b978-044481862-1.50098-4.
[13]	J.M. Noyes, A.F. Starr, C.R. Frankish, User involvement in the early stages of the development of an aircraft warning system, Behav. Inf. Technol. 15 (1996) 67–75. doi:10.1080/014492996120274
[14]	K. Ehrlich, J. Rohn, others, Cost justification of usability engineering: A vendor’s perspective, Cost-Justifying Usability. (1994) 73–110.
[15]	S. Wilson, M. Bekker, H. Johnson, P. Johnson, Costs and Benefits of User Involvement in Design: Practitioners’ Views, in: People Comput. XI, Springer London, 1996: pp. 221–240. doi:10.1007/978-1-4471-3588-3_15
[16]	J. Grudin, Interactive Systems: Bridging the Gaps Between Developers and Users, Computer (Long. Beach. Calif). 24 (1991) 59–69. doi:10.1109/2.76263.
[17]	T. Heinbokel, S. Sonnentag, M. Frese, W. Stolte, F.C. Brodbeck, Don’t underestimate the problems of user centredness in software development projects there are many!?, Behav. Inf. Technol. 15 (1996) 226–236. doi:10.1080/014492996120157.
[18]	L. Damodaran, User involvement in the systems design process-a practical guide for users, Behav. Inf. Technol. 15 (1996) 363–377. doi:10.1080/014492996120049.
[19]	S. Kujala, User involvement: A review of the benefits and challenges, Behav. Inf. Technol. 22 (2003) 1–16. doi:10.1080/01449290301782

[20]	R.M. Baecker, Readings in Human-Computer Interaction: toward the year 2000, Elsevier, 2014.
[21]	D. Wixon, J. Ramey, Field methods casebook for software design, John Wiley & Sons, Inc., 1996
[22]	J.D. Gould, C. Lewis, Designing for usability: Key principles and what designers think, Commun. ACM. 28 (1985) 300–311. doi:10.1145/3166.3170.
[23]	M. Mantel, A basic framework for cost-justifying usability engineering, Cost-Justifying Usability. (1994)
[24]	D. Wixon, C. Wilson, The Usability Engineering Framework for Product Design and Evaluation, in: Handb. Human-Computer Interact., Elsevier, 1997: pp. 653–688. doi:10.1016/b978-044481862-1.50093-5
[25]	M.M. Mantei, T.J. Teorey, Cost/benefit analysis for incorporating human factors in the software lifecycle, Commun. ACM. 31 (1988) 428–439. doi:10.1145/42404.42408
[26]	D.J. Mayhew, The usability engineering lifecycle, in: Conf. Hum. Factors Comput. Syst. - Proc., ACM Press, New York, New York, USA, 1999: pp. 147–148. doi:10.1145/632716.632805
[27]	https://www.techrepublic.com/article/plan-your-end-user-training-strategy-before-software-roll-out/
[28]	Laugwitz, Bettina, Theo Held, and Martin Schrepp. "Construction and evaluation of a user experience questionnaire." In Symposium of the Austrian HCI and Usability Engineering Group, pp. 63-76. Springer, Berlin, Heidelberg, 2008.
[29]	RESISTO Deliverable D6.3 "HMI definition and Platform integration"