

## RESISTO

### D8.1\_Scenario 2 Test Plan definition



# RESISTO

## D8.1 – SCENARIO 2 TEST PLAN DEFINITION

<b>Document Manager:</b>	Luca LIONETTI	TIM	Editor
--------------------------	---------------	-----	--------

<b>Project Title:</b>	RESilience enhancement and risk control platform for communication infraSTructure Operators
<b>Project Acronym:</b>	RESISTO
<b>Contract Number:</b>	786409
<b>Project Coordinator:</b>	LEONARDO
<b>WP Leader:</b>	TIM

<b>Document ID N°:</b>	RESISTO_D8.1_200525_01	<b>Version:</b>	1.0
<b>Deliverable:</b>	D8.1	<b>Date:</b>	25/05/2020
		<b>Status:</b>	APPROVED

<b>Document classification</b>	<b>PUBLIC</b>
--------------------------------	---------------

Approval Status	
<b>Prepared by:</b>	Luca LIONETTI (TIM)
<b>Approved by: (WP Leader)</b>	Luca LIONETTI (TIM)
<b>Approved by: (Coordinator)</b>	Bruno SACCOMANNO (LDO)
<b>Advisory Board Validation (Advisory Board Coordinator)</b>	NA
<b>Security Approval (Security Advisory Board Leader)</b>	Paolo DI MICHELE (LDO)

## CONTRIBUTING PARTNERS

Name	Company / Organization	Role / Title
Luca Lionetti, Roberto Mancini, Luigi Gallo, Paolo De Lutiis	TIM	WP/Task leader, Cyber Security Expert, IP Network Experts, Project Manager
Ioan Constantin, Horia Gunica, Marius Iordache, Carmen Patrascu	ORO	Cyber Security Expert, IP Network Experts, Project Manager
Luis Moreno Fraile	RTV	Project Manager
Chiara Foglietta	RM3	Senior Researcher
Giuseppe Celozzi, Cosimo Zotti, Antonio Nicoletti, Giovanna Spadaccio	TEI	R&D department
Rodoula Makri, Panos Karaivazoglou, Apostolos Papafragkakis, Athanasios Panagopoulos, Nikolaos Lyras, Anargyros Roumeliotis, Takis Kelefas	ICCS	Senior Researchers, Electrical Engineers, Telecommunication Experts
Jose 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
0.0	17/02/2020	ALL	ALL	Draft ToC
0.1	16/03/2020	ALL	ALL	First stable draft for Emdesk upload Template shared and agreed with WP7 an WP9
0.2	26/3/2020	ALL	ALL	Consolidated draft. Main parts Completed
0.3	06/04/2020	ALL	ALL	Ready for the first review
0.4	09/04/2020	ALL	ALL	First WP8 internal review (to be check “impacted use cases”, “countermeasures” and “user involvement and training”)
0.5	20/04/2020	ALL	ALL	Consolidated version
0.6	28/04/2020	ALL	ALL	Final release
0.9	07/05/2020	ALL	ALL	Final version 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) 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 8.1 contains the plan for the operational validation of the Macro Scenario 2 titled “(improving of resilience of) interconnected Critical Infrastructures” of the RESISTO Project.

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: TIM, ORO and RTV. We start by analyzing the steps and the process of each use case, the time plan 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

<b>ABBREVIATIONS.....</b>	<b>12</b>
<b>1. INTRODUCTION .....</b>	<b>15</b>
1.1. Scope .....	15
1.2. Relation to Other Deliverables within RESISTO.....	16
1.3. Document outline.....	16
<b>2. Methodology .....</b>	<b>17</b>
2.1. Testing Environment.....	17
2.2. Pilot Planning .....	17
<b>3. Description of Use cases corresponding to scenario #2.....</b>	<b>18</b>
3.1. Interdependencies of providers of essential communication services - Interconnected CIs .....	18
<b>4. Use Case 5: PROTECTION OF CLOUD STORAGE SERVICES (TIM) ..</b>	<b>19</b>
4.1. Scope .....	19
4.2. Test-bed setup (sub use case 1 - Healthcare scenario).....	19
4.2.1 Technologies involved.....	21
4.2.2 Preconditions .....	22
4.2.3 Use case Work flows.....	23
4.3. Key Performance Indicators.....	25
4.4. Pilot Execution Time plan.....	26
<b>5 USE CASE 6: Cyber and physical protection of network and network elements mechanisms used by critical services that impact users (ORO). 27</b>	
5.1 Scope .....	27
5.2 Test-bed setup.....	28
5.2.1 Technologies involved.....	29
5.2.2 Preconditions .....	30
5.2.3 Use case Work flows for Scenario 1 .....	31
5.2.4 Use case Work flows for Scenario 2 .....	34
5.3 Interconnected Scenarios and the Impact on OTE's Use-Case(s).....	36
5.3.1 Test-bed Interconnection.....	36
5.3.2 Description of Services impacted by ORO's scenario.....	36
5.3.3 Impact Assessment and KPI measurement.....	37
5.4 Key Performance Indicators to Evaluate the Pilot .....	37
5.5 Pilot Execution Time plan.....	38
<b>6 USE CASE 7: MARITIME SAFETY AND EMERGENCY CASE (RTV) ...</b>	<b>41</b>
6.1 Scope .....	41
6.2 Test-bed setup.....	41
6.2.1 Technologies involved.....	43
6.2.2 Preconditions .....	43



6.2.3	Use case Work flows.....	44
6.3	Key Performance Indicators to Evaluate the Pilot .....	45
6.4	Pilot Execution Time plan.....	46
7	Users involvement and training .....	47
7.1	Training Plan .....	51
8	CONCLUSION .....	52
9	References .....	53

## List of Figures

Figure 1 - High level TIM testing Lab – Cloud Storage System. ....	20
Figure 2 - High Level overview of OROs Testbed .....	28
Figure 3 - High Level overview of RTVs Testbed (1/2) .....	42
Figure 4 - High Level overview of RTVs Testbed (2/2) .....	42

## List of Tables

Table 1 Technologies involved in the healthcare sub-scenario .....	21
Table 2 Preconditions for the Healthcare sub scenario .....	22
Table 3 KPI to be referred for the Healthcare scenario .....	25
Table 4 Technologies involved in the ORO sub-scenario .....	30
Table 5 Precondition in the ORO sub-scenario .....	30
Table 6 KPI to be referred for the ORO scenario .....	38
Table 7 Technologies involved in the RTV scenario .....	43
Table 8 Preconditions for the RTV sub scenario .....	43
Table 9 KPI to be referred for the RTV scenario .....	46

## ABBREVIATIONS

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

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

<b>UAV</b>	Unmanned Aerial Vehicle
<b>VM</b>	Virtual machine
<b>VPN</b>	Virtual Private Network
<b>WP</b>	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 is aimed to provide a detailed description of the plan for the piloting of the use cases executed in the context of the Macro-scenario 2. These pilots are on the basis of the Use Cases provided in D2.8. Therefore, this deliverable shall be considered along with D7.1 and D9.1, 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 have 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.

### 1.1. Scope

This document is aimed to define the plan of each pilot included into WP8 scope, their requirements and design. In particular the document is focused on the Macro-Scenario 2: Interdependencies of providers of essential communication services - Interconnected Cis.

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

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

- To plan, facilitate, demonstrate and provide tangible feedback and evaluation in related cases.

WP8 acts as the liaison between the baseline (formed in WP7) and the envisioned future networks and their protection (WP9) as this can be demonstrated in the context of the main and impacted Use Cases involved.

## 1.2. Relation to Other Deliverables within RESISTO

WP8 is strictly related to WP7 and WP9 and have to be progressed in parallel with strong interactions. The main related deliverables are the following:

- D2.8 RESULTS OF RESISTO ARCHITECTURE, SCENARIOS AND USE CASES, since it contains the first and main description of the involved use cases to be validated.
- D7.1 Test Plan for the Macro-scenario 1: “(improving of resilience of) Current telco Infrastructures”
- D9.1 Test Plan for the Macro-scenario 3: “(improving of resilience of) future 5G telco Infrastructures”

Both D9.1 and D7.1 have been developed in parallel with the D8.1 and follow the same document schema/template, as, together, they provide the overall context in which the Use Cases identified in the RESISTO project will be demonstrated.

- D3.7 KPIs, quantities and metrics for cyber-physical risk and resilience of telecom CI – first
- D3.8 KPIs, quantities and metrics for cyber-physical risk and resilience of telecom CI – final

D3.7 and D3.8 provides the guidelines for the evaluation of the validation of the use cases in the scope of this document.

Finally, the D5.4 “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 D8.2

## 1.3. Document outline

The main part of this document is structured as follows:

- Chapter 1 – Describes the objectives of Task 8.1 and provides a brief description of the deliverable context.
- Chapter 2 – Describes the methodology defined to “evaluate” the macro scenario in scope of WP8 (please note that the same methodology has been used by WP7 and WP9)
- Chapter 3 – Presents the macro scenario in the scope of the WP8.
- Chapter 4 – Presents the test plan for the validation of the TIM use case “Protection of Cloud Storage Services”, in particular the sub use case Health care.
- Chapter 5 – Presents the test plan for the validation of the ORO use case “Cyber and physical protection of network and network elements mechanisms used by critical services that impact users”
- Chapter 6 – Presents the test plan for the validation of the RTV use case “Maritime Safety and Emergency case”
- Chapter 7 – Describes the user involvement and training plan



## 2. 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 functionalities, benefits and efficiencies. The presence of actual testbeds greatly enhances the chances of further exploitation both locally and through worldwide dissemination of results.

### 2.1. 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 such as door sensors and others provided by other partners. Finally, all testbed will be connected to RESISTO platform. The interfaces to the centralized RESISTO platform will be protected by means of VPNs.

This will enable to carry out tests about hardware integration, as well as testing accessibility issues.

The set of use cases (D2.8) 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: System state before the execution of the functionality
- Postcondition: This will be defined by specific KPI's measurement.
- Actors: Users or external systems involved
- Related requirements: What is necessary to execute the use case.
- Workflows: 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. Hence, the test definitions will be fully determined on in the following deliverables of WP8.

### 2.2. Pilot Planning

The validation test will be performed during M26-M32. The actual schedule will be defined in the following deliverables D8.2 and subsequent.

### 3. DESCRIPTION OF USE CASES CORRESPONDING TO SCENARIO #2

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

#### 3.1. Interdependencies of providers of essential communication services - Interconnected CIs

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

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

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

This macro-scenario acts as the liaison between the baseline (formed in the first macro-scenario) and the envisioned future networks and their protection (third macro-scenario) as this can be demonstrated in the context of the main and impacted Use Cases involved.

In this second macro-scenario the following use cases will be taken into consideration:

- Use case 5: Protection of Cloud Storage Services (lead by TIM)
- Use case 6: Cyber and physical protection of network and network elements mechanisms used by critical services that impact users (lead by ORO)
- Use case 7: Maritime Safety and Emergency Case (lead by RTV)

## 4. USE CASE 5: PROTECTION OF CLOUD STORAGE SERVICES (TIM)

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

For Use case 5, in the present document the sub use case-1 Healthcare scenario is envisioned. This choice is made because the Healthcare systems are among the most appealing targets for cyberattacks, as electronic health records (EHR) and all the information regarding patients are very sensitive and are becoming more and more important in the process of managing personal information. Healthcare industry is a particular critical infrastructure, directly affecting people's life. Moreover, hospitals are mostly public facilities, everyone can easily access them and for this reason healthcare systems are representative examples of physically vulnerable systems. Finally, hospital employees (doctors, nurses) generally are not aware about cyber risks.

### 4.1. Scope

The protection of the Cloud Storage is a sort a basic scenario that could be extended to include other CIs infrastructure scenarios. The cloud storage infrastructure is subject to physical and cyber-attacks, that include for example in case of physical attacks, theft of part of servers, unauthorized access to buildings where they are located, and manipulation of facility systems. Cyber-attacks include for example hacking to servers, changing configuration files, virus/worms attacks.

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

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

Another case where the platform may be useful is the detection of a sabotage of the ICT assets and help to make the decision to move services to another site, implement others countermeasure or update the defined threat model, accordingly to the "continuous improvement" paradigm.

### 4.2. Test-bed setup (sub use case 1 - Healthcare scenario)

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

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

The simulated environment will have specific interconnection to a Cloud Storage Provider that offers to the hospital the ability to place and retain data in a secure and protected off-site storage system. The picture below shows a high-level view of such interconnections.

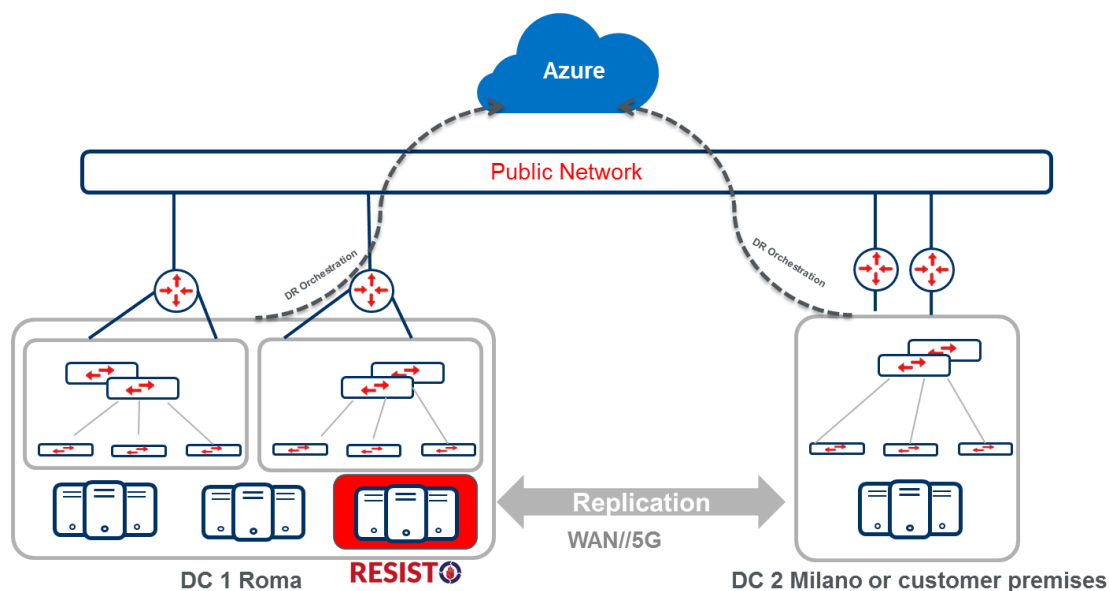


Figure 1 - High level TIM testing Lab – Cloud Storage System.

## 4.2.1 Technologies involved

The following tables lists the key elements of the healthcare sub-use case.

Technology	Role	Description
<b>RESISTO Platform</b>	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.
<b>Rack sensors</b>	Technical: Detection for physical opening of the rack	Monitors and notifies on physical rack opening. Will provide syslog messages on changes to the RESISTO platform when it detects an event.
<b>PC/System: Windows Server 2019</b>	Several servers will be plugged into the rack in order to simulate the Healthcare data room.	The data room is composed by Hyper Converged systems interconnected with remote TIM datacentres. The servers will host ad hoc cyber-sensors connected to the RESISTO platform via Syslog.
<b>Door sensors</b>	The sensor has to detect a physical presence inside a protected area/room	The sensor will send the detected events to the RESISTO platform via syslog
<b>RADIOFILTER cyber sensors</b>	RADIOFILTER sensors that have to detect the presence of a rogue 802.11 AP or unauthorized connection in the protected area	The sensors will send the detected events to the RESISTO platform via syslog
<b>Azure</b>	Disaster recovery Orchestrator	RESISTO, in case of disruptive physical failure, will instruct the recovery procedure by means of Azure platform
<b>Fortigate FG101F</b>	The Fortigate will perform the Firewall and IDS role	The Fortigate will be used to protect the Helthcare network infrastructure. Moreover it will be used to demonstrate the effectiveness as a specific countermeasure.

**Table 1 Technologies involved in the healthcare sub-scenario**

#### 4.2.2 Preconditions

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

		Applicability
P1	Cloud environment up and running	YES
P2	Cyber OS Sensors installed and running	YES
P3	Physical Door Sensors installed and running	YES
P4	Physical Rack Sensors installed and running	YES
P5	Network Connectivity is up and running	YES
P6	The RESISTO platform is reachable from the test-bed	YES
P7	Integrasys sensors installed and running	YES
P8	Fortigate device installed and running	YES

**Table 2 Preconditions for the Healthcare sub scenario**

### 4.2.3 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><b>Integration of Testbed (Sensors provided by Integrasys, RESISTO components and TIM cloud environment)</b></p> <p>TIM will configure the foreseen equipment to forward syslog verbose event messages to the RESISTO connector specifically designed to ingest and parse syslog messages. The equipment consists of the technologies previously mentioned in the table 4.2.1; each of them will act as event detectors and will feed the RESISTO platform, through its connector, both with cyber and physical event information.</p> <p>The testbed setup (networking, cloud, services) will follow the steps below:</p> <ul style="list-style-type: none"> <li>• Sensors Installation</li> <li>• Sensor integration in the test bed</li> <li>• RESISTO Integration: Each sensor has to be able to send event to the RESISTO Platform</li> </ul>
2	<p><b>An intruder physically accesses the control room and tampers with sensitive files (Electronic Health Records).</b></p> <p>In this step we assume that an attacker, who has previously been able to study the structure of the hospital and the habits of employees because it is a public place, enters the protected area of the control room (where there is the actual interconnection to the cloud services).</p> <p>In order to do this, he could previously clone/robbed an admitted badge; moreover, he could know the right moment to do it because he could verify that usually the system administrator leaves the room at a certain time to have a coffee.</p> <p>Once inside the control room, he can tamper with patients' therapies and medical results causing obvious medical problems. Possibly he/she can also try to use an external hard disk in order to copy (PII) data.</p> <p>Before leaving the room, the attacker can install a Rogue Access Point to later access the control room network and repeat the tampering at will without physically accessing the site. Data exfiltration can then be performed which poses a major threat</p>
3	<p><b>The tampering with files is detected by separate sensors/detectors, in place in TIMs infrastructure</b></p> <p>The behaviour described in the previous step triggers at least 3 events detected by the cyber and physical sensors. These events are reported to the RESISTO platform via network interconnections, but individually they do not constitute</p>

	<p>evidence of an ongoing attack:</p> <ul style="list-style-type: none"> <li>Physical access to the control room: at every access, even legit, the platform is notified;</li> <li>Modification of EHRs: at every access, even legit, the platform is notified;</li> <li>Presence of unauthorized Rogue APs and unauthorized ad-hoc connections (even if the device is authorized), leading to data exfiltration.</li> </ul>
	<p><b>RESISTO recognizes that the events are anomalous</b></p> <p>The RESISTO platform shall be able to collect, parse and evaluate the syslog messages coming from the detectors deployed in TIM premises.</p> <ul style="list-style-type: none"> <li>The RESISTO components, algorithms and rules determine that the physical access to the room as soon as the system administrator left is “suspicious”.</li> <li>Modifying EHRs directly from the control room, and not from doctors' applications, is not usual.</li> <li>Finally, the detection by RADIOFILTER cyber sensors of WLAN 802.11 Access Points or connections that are not included in the authorized whitelist.</li> </ul>
	<p><b>RESISTO recognizes the attack by correlating the events</b></p> <p>Based on the existing behavioural models and correlating multiple events, we expect the RESISTO Platform to provide an early warning, a risk impact assessment that first allows the attack to be detected, possibly stopped and then allows the tampered with data to be remedied.</p>
	<p><b>RESISTO alerts its operators and suggests mitigation measures</b></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 different events. The expectation is that the RESISTO cockpit will publish:</p> <ul style="list-style-type: none"> <li>-Real time alerts in a visual manner;</li> <li>-Real time alert notifications by additional methods – emergency call to the system administrator and/or guards;</li> <li>-Real time resilience and impact analysis (e.g. number of tampered files, the moment the tampering took place in order to facilitate the restoring via backups);</li> <li>-Real time mitigation measures to be taken by security operators.</li> </ul>
	<p><b>Attack is mitigated</b></p> <p>Tampering has been averted, medical data has been restored (via backup data in the cloud) and the intruder can be arrested.</p>



### 4.3. Key Performance Indicators

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 have been thoroughly analyzed within the Deliverable D3.8 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 3 KPI to be referred for the Healthcare scenario**

For more information about KPI, please refer to the D3.8 [2] document.

#### 4.4. Pilot Execution Time plan

RESISTO - GANTT (WP 8 Tasks)	2019												2020												2021					
	M12	M13	M14	M15	M16	M17	M18	M19	M20	M21	M22	M23	M24	M25	M26	M27	M28	M29	M30	M31	M32	M33	M34	M35	M36					
Work Packages and tasks																														
Task 8.1 Pilot plan, requirements and Design											D8.1																			
Task 8.2 Pilot Sites preparation; Users involvement and training																														
Task 8.3 Pilot implementation and test first run															D8.2															
Task 8.4 Pilot implementation and test second run																D8.4					D8.3									
Task 8.5 Operational end-user validation of RESISTO platform in scenario #2																					D8.5									

Assuming **T-0** to be the date the Scenario planning is complete, each of the activities comprising the pilot execution plan should complete as follows:

**The pilot sites preparation, users involvement and training requires** two months from T-0 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.

**Pilot implementation and test first run** requires four months starting with T-0 + 2M (following the previous activity) whilst **pilot implementation and second run** should require and additional four months after this

**The operation end-user validation** is an ongoing process through the entire Work Package.

## 5 USE CASE 6: CYBER AND PHYSICAL PROTECTION OF NETWORK AND NETWORK ELEMENTS MECHANISMS USED BY CRITICAL SERVICES THAT IMPACT USERS (ORO)

Use Case 6 – “Cyber and Physical Protection of Network and Network Elements Mechanisms used by critical services that impact users”, 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.

The Interconnected Critical Infrastructure provider for the piloting of ORO’s Use-Case is a Railway Transport Operator based in Bucharest, Romania (SNCF) whose telecommunication infrastructure is provided by ORO. During the piloting of both scenarios, several critical services that SNCF offers to both internal and external customers will be impacted, having the availability and integrity affected by the events impacting OROs infrastructure.

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 simulated MSC functions 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 router acting as border router, access its administrative console and maliciously change a route to one of OROs servers hosting a critical part of OROs Core Network.

### 5.1 Scope

During testing ORO will run attack scenarios combining cybersecurity and physical security threats, affecting both Fixed Services and 4G/5G Services that impact users. ORO’s detectors for these types of threats will trigger the RESISTO platform that, in turn, will associate the detections collected from OROs infrastructure with events and will further correlate those events from both cyber and physical realm. Based on the modelling provided and associated criticality and risk values for the assets, RESISTO will suggest mitigation actions and measures and initiate a disaster recovery plan. During the running of this use-case, several components of the RESISTO platform will be tested:

- Network Resource Monitoring
- Short Term Control Loop – Physical & Cyber Detector (Correlator)
- Short Term Control Loop – Risk (Impact) Predictor
- Knowledgebase – Assets Inventory
- Long Term Control Loop – Risk And Resilience assessment analysis
- Cockpit – Mitigation Module
- Cockpit – Orchestration Module

## 5.2 Test-bed setup

For both scenarios ORO will use the testbed already described in D2.8 – “Table-top Read Teaming Results of RESISTO Architecture, Scenarios and Use-Cases”, specifically Figure 16: Physical Layout of ORO testbed:

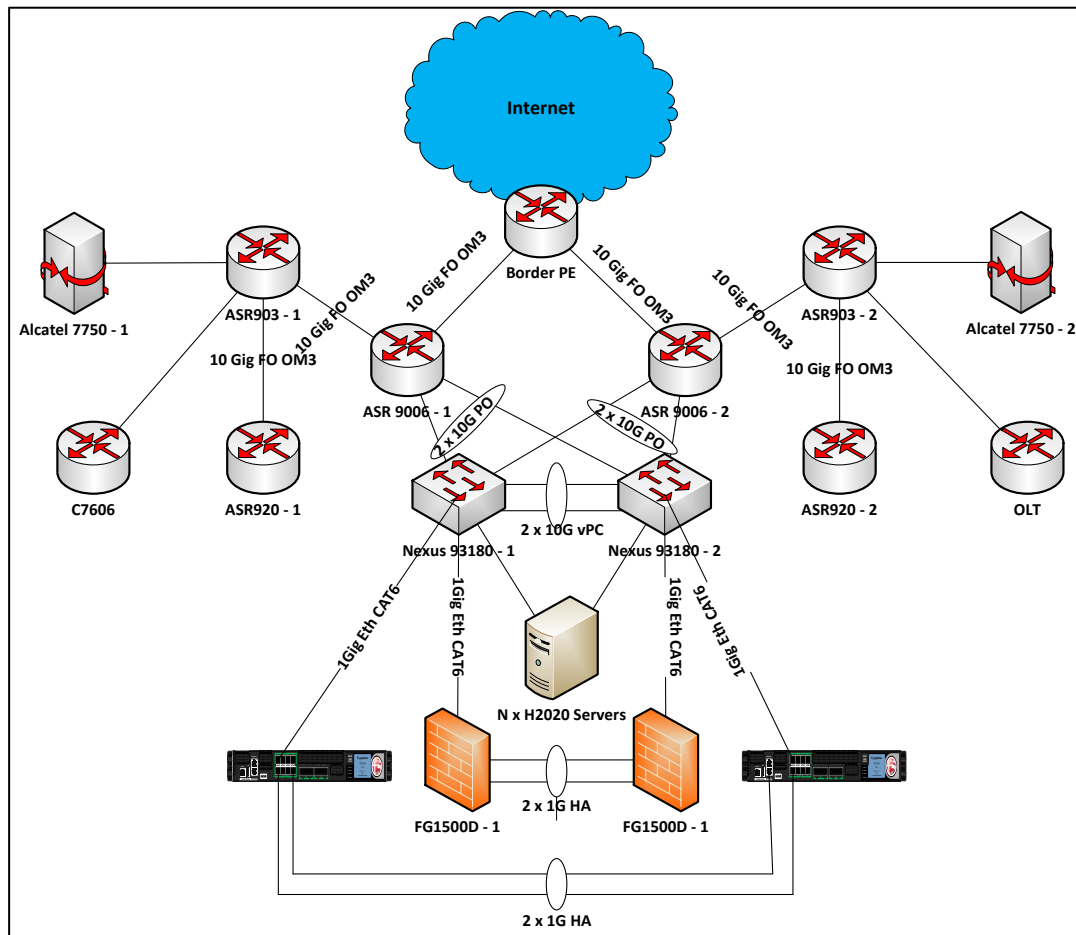


Figure 2 - High Level overview of OROs Testbed

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

ORO's testbed will closely replicate the services offered to SNCF during the piloting of the Use-Cases, applicable to both scenarios. ORO will provision, in the testbed, the following services to SNCF:

- Layer 2/3 Connectivity between ORO's border routers and another similar equipment provisioned inside the testbed for SNCF simulating the communications between:
  - Central Dispatchers and SNCF Train Stations in Romania;
  - Central Dispatchers and Local Dispatches;

- IPsec VPN Tunnels between ORO's border routers and another similar termination equipment provisioned inside the testbed for SNCF simulating the communications between:
  - Application Servers in ORO's Cloud Infrastructure and SNCF Train Stations Terminals;
  - Application Servers in ORO's Cloud Infrastructure and SNCF Central and Local Dispatch Terminals
- Several Virtual Instances of Servers hosted in the Cloud Infrastructure of ORO for SNCF inclusive of:
  - Application Servers for SNCF's Ticketing Platform;
  - Application Servers for SNCF's Fleet Management Platform;

Whilst piloting both scenarios in OROs Use-Case, the availability and integrity of the data and the applications of SNCF, hosted by ORO will be impacted and various KPIs will be affected on both ORO's and SNCF's side

## 5.2.1 Technologies involved

Technology	Role	Description
<b>Arbor DDoS Mitigation Platform</b>	Technical: detector for DDoS and DoS Attacks	A commercial platform with detection and mitigation capabilities for DDoS and DoS Attacks. Will detect the DDoS traffic inbound to OROs border equipment and will send syslog messages to the RESISTO component which it interfaces with.
<b>BNG1</b>	Technical: Broadband Network Gateway Router	Provides gateway services for Broadband subscriber users. Offers advanced services such as automatic subscriber integration and service policing based on AAA server integration. Can also offer CG-NAT services.
<b>Physical Access Monitoring Sensor</b>	Technical: Detection for physical entry	Monitors and notifies on physical access in various areas. Will provide syslog messages on changes to the RESISTO platform when it detects an entry into the data room that hosts OROs test-bed.
<b>RESISTO Platform</b>	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.
<b>Openstack</b>	Technical: Will host various components	Hosts VMs with the components needed for OROs piloting of the Use-Case, such as VMs provisioned for SNCF's Services, VM's provisioned for ORO's Services and VM's hosting RESISTO components.
<b>Monitoring application</b>	Syslog based interface monitoring, alarm triggered	Syslog message generation for loss detection (port down).  The devices that are interconnected via optical fibre detect the loss state on the respective fibre. There are no dedicated devices for fibre cut detection, especially in OROs testbed case, where

		all the devices are directly interconnected. The equipment' ports detect the signal from optical fibre and send traps or syslog messages when loss state is detected.
<b>Orchestration tool</b>	Services and virtual network function instantiation, service monitoring	Instantiate VMs and create services for RESISTO VMs deployment.
<b>IPSec VPN</b>	Technical: Enables a secured connection over the Internet between two or more LAN networks in the Testbed	Enables a Secured connection over the Internet between SNCF and ORO's testbed and provides SNCF and their customers with access to specific resources hosted in the Cloud Infrastructure of ORO

**Table 4 Technologies involved in the ORO sub-scenario**

### 5.2.2 Preconditions

No		Applicability
P1	Network Connectivity is up and running	Applicable to Scenario 1 & 2
P2	Virtual environment up and running	Applicable to Scenario 1 & 2
P3	Physical Security Sensors are installed and functioning	Applicable to Scenario 2
P4	DDoS Detection capability is functioning	Applicable to Scenario 1
P5	Physical Door Sensors installed and running	Applicable to Scenario 2
P6	The RESISTO platform installed and running	Applicable to Scenario 1 & 2
P7	The RESISTO platform is reachable from the test-bed	Applicable to Scenario 1 & 2
P8	Subscriber management is up and running	Applicable to Scenario 1 & 2
P9	Management servers are up and running	Applicable to Scenario 1 & 2
P10	IPSec Tunnel is Established between SNCF LAN and ORO	Applicable to Scenario 1 & 2

**Table 5 Precondition in the ORO sub-scenario**

### 5.2.3 Use case Work flows for Scenario 1

Step	Description
1	<p><b>Integration of RESISTO components and the Cyber and Physical Detectors of ORO is complete and functional</b></p> <p>Following the activities in WP6, specifically Tasks related to the development of RESISTO components (T6.2, T6.3, T6.4) such as the adaptors and risk predictor, as per MS3 – Integration and First Pilot Launch, ORO will configure the testbed equipment to forward syslog verbose event messages to the RESISTO connector specifically designed to ingest and parse syslog messages. The equipment consists of:</p> <ul style="list-style-type: none"> <li>• <b>Border Gateways – CISCO Equipment;</b></li> <li>• <b>DDoS Protection – Arbor Networks Equipment;</b></li> <li>• <b>NG Firewalls – Fortinet Equipment;</b></li> <li>• <b>Network Switches and Routers;</b></li> <li>• <b>Hardware security sensors</b> such as access security toggles (door sensors). Each of these equipment will act as event detectors and will feed the RESISTO platform, through its connector, with event information.</li> </ul>
2	<p><b>An unintentional Fibre Cut occurs on 2 out of the 3 fibres that connect two of OROs MSCs</b></p> <p>In this step we will simulate a disturbance in L1 communications on 2 of 3 high-bandwidth connections in OROs testbed. These are connections between the equipment corresponding to the two MSCs in OROs Production Network. The simulation will incur the physical removing of fibre optics cables and their respective connectors from the physical equipment. This event will impact the functionality of user services such as:</p> <ul style="list-style-type: none"> <li>• Voice and Data Services for Mobile Customers;</li> <li>• Voice and Data Services for Fixed Customers;</li> <li>• Voice and Data Services for SNCF;</li> <li>• Data Communications between SNCF Dispatches and Stations;</li> <li>• Data Communications between SNCF Depots and Dispatches;</li> <li>• Cloud Infrastructure services that host Virtual Resources of SNCF as an interconnected Critical Infrastructure Operator, in turn, impacting the availability of those resources from SNCF's perspective</li> </ul> <p>As this happens, the physical equipment will detect a 'port down' instance and will automatically send a syslog message describing this state change to the RESISTO platform.</p> <p>An unknown attacker starts a DDoS attack against border routers immediately after the fibre cut</p> <p>For this step we will simulate a large-scale DDoS attack against OROs border</p>



	<p>routers that happen immediately after the previous step, further affecting the network KPIs and the network's resilience. In this attack, we will use OROs detectors placed in-line in-traffic to recognize the specific patterns of a DDoS attack. During this testing we will simulate both a Volumetric DDoS Attack, which attempts to saturate the available bandwidth between the target border routers and the internet AND an State-Exhaustion DDoS Attack in which the attacker attempts to consume the connection state tables in the load balancer in 'front' of OROs testbed.</p> <p>This attack will further impact the availability of user services such as:</p> <ul style="list-style-type: none"> <li>• Voice and Data Services for Mobile Customers;</li> <li>• Voice and Data Services for Fixed Customers;</li> <li>• Data Communications between SNCF Dispatches and Stations;</li> <li>• Data Communications between SNCF Depots and Dispatches;</li> <li>• Cloud Infrastructure services that host Virtual Resources of SNCF as an interconnected Critical Infrastructure Operator, in turn, impacting the availability of those resources from SNCF's perspective</li> </ul>
3	<p><b>The DDoS Attack and Fibre Cuts are detected by separate sensors/detectors, in place in OROs infrastructure</b></p> <p>For this scenario the ORO testbed will use its components as detectors for attacks, as follows:</p> <p>The DDoS Attack will be detected by the Netscout Arbor DDoS TMS – Threat Mitigation System. Upon the attack beginning, the Arbor equipment will correlate the information from the incoming traffic, evaluate its impact and try to mitigate the threat by using its 'Traffic Scrubbing' components readily available in the testbed. At the same time, the Arbor DDoS platform will generate syslog event messages containing information pertinent to the detected attack. These messages will be sent to the RESISTO platform.</p> <p>The Fibre Cuts will be detected by the network equipment providing the necessary connectivity. A state change in continuity on the physical ports will trigger a syslog messages generation that contain the appropriate information on the state change for those ports.</p> <p><b>RESISTO recognizes both attacks</b></p> <p>As per the development done in WP6, the RESISTO platform will collect, parse and correlate the syslog messages coming from the detectors in OROs testbed and interpret them as DDoS attacks and Fibre Cuts, respectively.</p> <p>During the previous development phases ORO had sent sample syslog messages from each of the equipment to be used as detectors, in our testbed and the documentation for the specific syslog messages. Given the existing information, RESISTO platform will detect such attacks once the respective syslog messages</p>



	reach the Platform.
	<p><b>RESISTO correlates the attack information with existing system modelling and risk assessments</b></p> <p>Based on the existing network modelling for OROs testbed and the impact data pre-provisioned within RESISTO, the Platform will provide immediate and accurate risk and resilience impact assessment taking into account the correlation between the two separate events.</p>
	<p><b>RESISTO alerts its operators and suggests countermeasures</b></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 Cockpit component will publish:</p> <ul style="list-style-type: none"> <li>• Real time alerts in a visual manner;</li> <li>• Real time alert notifications by additional methods – e-mail, desktop app notifications etc.;</li> <li>• Real time resilience and impact analysis;</li> <li>• Real time resilience and impact analysis on the interconnected Critical Infrastructure (SNCF);</li> <li>• Real time mitigation measures to be taken by OROs NOC/SOC operators in a play-book, step-by-step manner;</li> <li>• Mean time to restauration of functionality (by a pre-existing threshold);</li> </ul>
	<p><b>Attacks are mitigated</b></p> <p>The network services impacted by the events have their functionality restored as is the resilience of the network.</p> <p>Data gathered from the Testbed during and after the initial piloting will be made available to EMI for further improving their modelling application.</p>

## 5.2.4 Use case Work flows for Scenario 2

Step	Description
1	<p><b>Integration of RESISTO components and the Cyber and Physical Detectors of ORO is complete and functional;</b></p> <p>Following the activities in WP6, specifically Tasks related to the development of RESISTO components (T6.2, T6.3, T6.4) such as the adaptors and risk predictor, as per MS3 – Integration and First Pilot Launch, ORO will configure the testbed equipment to forward syslog verbose event messages to the RESISTO connector specifically designed to ingest and parse syslog messages. The equipment consists of:</p> <ul style="list-style-type: none"> <li>• <b>Border Gateways – CISCO Equipment;</b></li> <li>• <b>DDoS Protection – Arbor Networks Equipment;</b></li> <li>• <b>NG Firewalls – Fortinet Equipment;</b></li> <li>• <b>Network Switches and Routers;</b></li> <li>• <b>Hardware security sensors</b> such as access security toggles (door sensors).</li> </ul> <p>Each of these equipment pieces will act as event detectors and will feed the RESISTO platform, through its connector, with event information.</p>
2	<p><b>An attacker enters one of OROs Core Network Sites (Gara Herastrau 4A, Bucharest, the location of OROs test-bed)</b></p> <p>This activity will be simulated by placing physical security access monitoring sensors (door sensors) in the entrance point to the room hosting OROs testbed. This simulates an environment close to that of the production equipment rooms where each door has status monitoring sensors connected to physical security platforms.</p> <p>For this scenario a sensor will be placed on the single door entry in the room, on the interior part of that door and the corresponding detector will be placed in the door frame, whenever the two sensors will move apart the physical security monitoring platform will register a 'door open' respectively 'door closed' status and push a syslog message to the RESISTO platform.</p> <p>The attacker successfully connects to a border router, access its administrative console and maliciously changes a route to one of OROs servers hosting a critical part of OROs core network, making that service unavailable for its users</p> <p>For this part of the scenario, the attacker once inside the server room successfully connects to the administrative interface of one of the main routers in the network and alters the routing table to the OpenStack Infrastructure Servers hosting, amongst others, the ticketing platform backend servers and the fleet management backend servers for SNCF, further affecting their availability</p>

	<p>and rendering SNCFs ticketing and fleet management services unavailable for both internal and external customers;</p> <p>This attack will further impact the availability of user services such as:</p> <ul style="list-style-type: none"> <li>• Voice and Data Services for Mobile Customers;</li> <li>• Voice and Data Services for Fixed Customers;</li> <li>• Cloud Infrastructure services that host Virtual Resources of SNCF as an interconnected Critical Infrastructure Operator, in turn, impacting the availability of those resources from SNCF's perspective</li> </ul>
3	<p><b>The unauthorized entry into the datacentre is detected by OROs Physical Security Systems;</b></p> <p>For this scenario the ORO testbed will use its components as detectors for attacks, as follows:</p> <p>The unauthorized entry into the datacentre is to be detected by the physical security monitoring sensors (the door sensors) that will send a message to a Physical Security Incident and Event Management Platform (P-SIEM) that, in turn, will send a syslog message to the RESISTO platform.</p> <p>The Fibre Cuts will be detected by the network equipment providing the necessary connectivity. A state change in continuity on the physical ports will trigger a syslog messages generation that contain the appropriate information on the state change for those ports.</p> <p><b>The state change in the border router is detected by OROs systems;</b></p> <p>For this to happen, the border router is configured to send an alert in the form of a syslog message every time a status change occurs in the routing table. This includes modification, addition or deletion of routes. The border router will then forward a syslog message containing information on this event, to the RESISTO platform</p> <p><b>RESISTO correlates the attack information with existing system modelling and risk assessments;</b></p> <p>Having pre-existing models in the LCTL component, the RESISTO platform will correlate the separate events (physical and cyber) and conclude that:</p> <p>a) The physical access in the datacentre occurred outside the regular 'baselined' activities usually performed in that room;</p> <p>b) The route change happened in a very short time frame AFTER the physical entry;</p> <p>c) That specific route change will have an impact on the availability of resources and, in turn, on the network's resilience.</p> <p>From these three conclusions RESISTO will generate alerts and suggest</p>

	mitigations on the event of unauthorized modification of the network.
	<p><b>RESISTO alerts its operators and suggests countermeasures</b></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 RESISTO Cockpit will publish:</p> <ul style="list-style-type: none"> <li>• Real time alerts in a visual manner;</li> <li>• Real time alert notifications by additional methods – e-mail, desktop app notifications etc.;</li> <li>• Real time resilience and impact analysis;</li> <li>• Real time resilience and impact analysis on the interconnected Critical Infrastructure (SNCF);</li> <li>• Real time mitigation measures to be taken by OROs NOC/SOC operators in a play-book, step-by-step manner;</li> <li>• Mean time to restauration of functionality (by a pre-existing threshold);</li> </ul>
	<p><b>Attacks are mitigated</b></p> <p>The network services impacted by the events have their functionality restored as is the resilience of the network.</p> <p>Data gathered from the Testbed during and after the initial piloting will be made available to EMI for further improving their modelling application.</p>

### 5.3 Interconnected Scenarios and the Impact on OTE's Use-Case(s)

OTE's Use-Case 'Core Network Failure caused by Physical and Cyber Attacks to Telecommunication sites', piloted in WP7 will be impacted by ORO's Use Case. Voice communication and data communication services provided by OTE to their customers, over fixed and mobile networks will be impacted by the events triggered in ORO's scenarios.

#### 5.3.1 Test-bed Interconnection

ORO's and OTE's testbeds – each described thoroughly in D2.8 'Table-top Read Teaming Results of RESISTO Architecture, Scenarios and Use-Cases', in sections 5.1.8 and 5.1.1 respectively, will be interconnected using and IPSec 'Site to Site' secure tunnel, allowing both testbeds to interface with the various LAN segments in the each other's infrastructure needed for the deployment of the Virtual Machines hosting the software servers and clients required for the provisioning of OTE's services hosted in ORO's Cloud Infrastructure.

#### 5.3.2 Description of Services impacted by ORO's scenario

The interconnected scenarios will challenge Data Communications and Voice Communication Services in OROs and OTEs infrastructure, impacting OTE's customers and ORO's customers as follows:

- a) Voice Services – During the piloting of the interconnected scenarios, ORO customers roaming in OTE's network will have limited or no access to Voice Services initiated through a Session Initiation Protocol (SIP) services, with availability impacted by the running of OTE's scenarios;
- b) Data Services – During the piloting of the interconnected scenarios, OTE's customers will be denied access to a web-based communication service provided by OTE and hosted in ORO's Cloud Infrastructure, in dedicated Virtual Machines. The Availability of the service will be impacted by the running or ORO's scenarios

### 5.3.3 Impact Assessment and KPI measurement

For both situations listed above (5.4.2), various metrics and other measurements can be run both client and server-side, for example measuring latency, throughput and failed and successful attempts at establishing connectivity. These measurements can further be used in the KPI evaluation of the piloting, as it is described in the next section.

### 5.4 Key Performance Indicators to Evaluate the Pilot

The Key Performance Indicators (KPIs) to be referred during the evaluation of this Use Case are given in the following Table. As stated in the previous Use Case, following a thorough analysis within Deliverable D3.8, the final 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 KPI to be referred for the ORO scenario

## 5.5 Pilot Execution Time plan

As per the initial planning and given the complexities involved in the execution of the pilot, we anticipate the following time plan:

Activity	Number of Months necessary from T-0											
	1	2	3	4	5	6	7	8	9	10	11	12
<b>Pilot Sites preparation, users training</b>												
Deployment of virtual instances in the testbed infrastructure – OpenStack Hosts VMs with the components needed for OROs piloting of the Use-Case, such as VMs provisioned for SNCF's Services, VM's provisioned for ORO's Services and VM's hosting RESISTO components	First Two Weeks of M1											
Configuration of Network Equipment in	Third Week of M1											

Testbed as per the two Scenarios to be piloted	
Installation of Physical Security Sensors in the pilot site – Door Activity Sensors in the Data Room	Fourth Week of M1
Validation of the intended functionality for the first run, including testing communication between components and the availability of services	First Two Weeks of M2
Training of the Users involved in the pilot implementation	Third and Fourth Week of M2
<b>Pilot implementation and test first run</b>	<div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div>
Scenario 1: Simulation of Fiber Cuts by physically disconnecting the media links between core routers followed by simulation of an DDoS Attack by using Open-Source traffic generators closely mimicking a DDoS Attack such as DDOSIM and XOIC	Weeks 1-6 of M1-M2. with 3 iterations
Scenario 1: Following the simulation of the physical and cyber security incidents, the Operators will monitor the RESISTO Cockpit for alarms, notifications and remediation procedures. The implementation of the remediation measures provided by RESISTO	Weeks 1-6 of M1-M2, with 3 iterations
Scenario 1: Data gathering from the test first run for the EMI Modelling Tool	Weeks 6-8 of M2
Scenario 2: Simulation of an attacker physically entering the Data Room that hosts OROs Testbed and knowingly accesses the CLI of one core router and 'poisons' – modifies the routing table knowing that the changes will make the destination resources unavailable to the sources.	Weeks 1-6 of M3-M4, with 3 iterations
Scenario 2: Following the simulation of the physical and cyber security incidents, the Operators will monitor the RESISTO Cockpit for alarms, notifications and remediation procedures. The implementation of the remediation measures provided by RESISTO	Weeks 1-6 of M3-M4, with 3 iterations
Scenario 2: Data gathering from the test first run for the EMI Modelling Tool	Weeks 6-8 of M4
<b>Pilot implementation and second run</b>	<div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div>
Scenario 1: Simulation of Fiber Cuts by physically disconnecting the media links between core routers followed by simulation of an DDoS Attack by using Open-Source traffic generators closely mimicking a DDoS Attack such as DDOSIM and XOIC	M1-M2, with 3 iterations
Scenario 1: Following the simulation of the physical and cyber security incidents, the Operators will monitor the RESISTO Cockpit for alarms, notifications and remediation procedures. The implementation of the remediation measures provided by RESISTO	M1-M2, with 3 iterations

Scenario 2: Simulation of an attacker physically entering the Data Room that hosts OROs Testbed and knowingly accesses the CLI of one core router and 'poisons' – modifies the routing table knowing that the changes will make the destination resources unavailable to the sources.	M3-M4, with 3 iterations
Scenario 2: Following the simulation of the physical and cyber security incidents, the Operators will monitor the RESISTO Cockpit for alarms, notifications and remediation procedures. The implementation of the remediation measures provided by RESISTO	M3-M4, with 3 iterations
<b>Operation end-user validation</b>	

Assuming **T-0** to be the date the Scenario planning is complete, each of the activities comprising the pilot execution plan should complete as follows:

**The pilot sites preparation, users involvement and training requires** two months from T-0 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.

**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 an additional four months after this

**The operation end-user validation** is an ongoing process through the entire Work Package.



## 6 USE CASE 7: MARITIME SAFETY AND EMERGENCY CASE (RTV)

The use case 7 is focused in protecting a real isolated Maritime Site from a combined Cyber physical attack. In the use case the main objective is to increase the correlation between physical and cyber alarms to detect faster the attack.

The second objective is to mitigate the action performed by the malicious intruder.

On one hand, everyone can easily access this isolated sites located in the coast. For this reason they are representative examples of physically vulnerable systems. Moreover alarms systems and more precisely physical and cyber are not correlated since most of the time physical alarms systems needs a third party company with special authorizations

For Use case 6 Maritime communications are particular critical, directly affecting possible maritime rescue. Maritime communication are critical to react in time in case of disasters such as big petroleum ships that are near the coast and may suffer an accident.

### 6.1 Scope

Infrastructure providers are basically service providers. The protection of a service is a complex matter that involves different actors in the chain. Moreover the infrastructure for the service selected is subject to physical and cyber-attacks, that include for example in case of physical attacks, unauthorized access to buildings where they are located, and manipulation of equipment and systems. Cyber-attacks include for example hacking to servers, changing configuration files, deny attacks and network sniffing.

These kind of sites are normally protected by a third party system alarm that are connected to the NOC systems. The attacks must be performed in combination of both physical and cyber techniques at the same time, such as an attacker that can gain the access to the inside of the infrastructure. These third party may send the alarm to the NOC but it is not correlated to any other alarm such as cyber attack.

The proposed use cases help to identify changes of configuration of equipment or unusual data traffic in the network that may be suspect of a hacker. The physical sensors implemented help to detect un-authorized access to the CIs site to identify the physical intrusions. Integration between alert of physical sensors and ICT sensors permits, for example, the RESISTO platform to detect a physical intrusion to the CI site with the probable cyber attack and propagation in the network.

Another case where the platform may be useful is the detection of a sabotage of the ICT assets and help to make the decision to move services to another site, implement others countermeasure or update the defined threat model, accordingly to the “continuous improvement” paradigm.

### 6.2 Test-bed setup

The test bed will use real infrastructure. At the point we are we have pre-selected 2 sites one in Vigo another one in Ibiza to do the demonstration. Since we will have at the same a real service going on we need to have a let's say a copy of the real traffic without affecting the service. This will be implementing replicating the IP traffic to another Ethernet point in the router.

The complete architecture of a maritime service is the one show as follow while data and voice communication from maritime service is routed to all the network while at the same time is monitored in the NOC

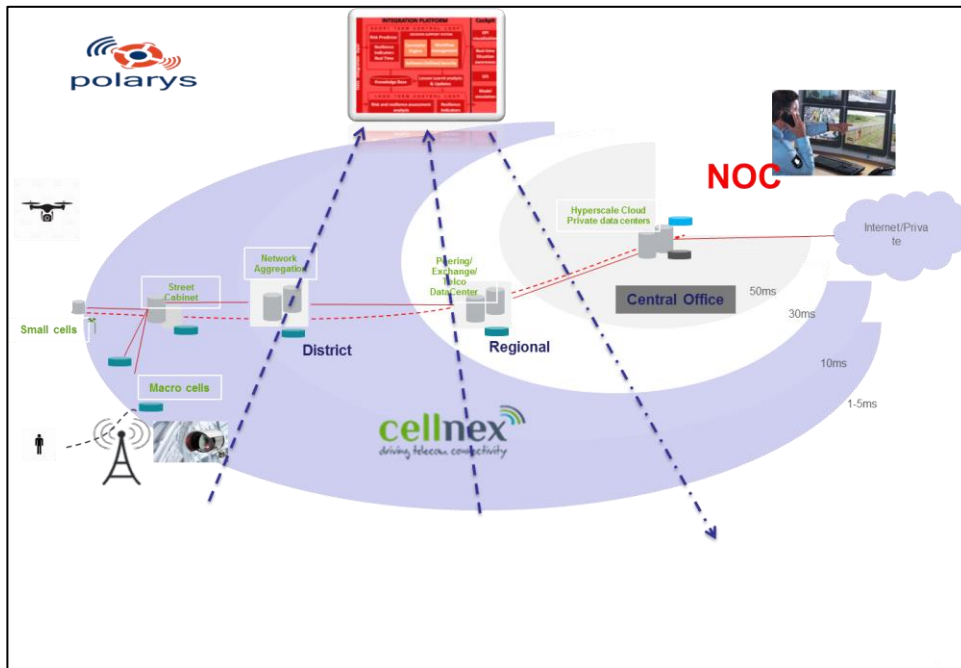


Figure 3 - High Level overview of RTVs Testbed (1/2)

On the other hand the test bed we are going to implement is the following one. We will a copy of the real traffic and will put an AI system with probe and algorithm to analyse the behaviour in the site in terms of IP traffic. This probe will generate message and alarms to the resisto platform.

On parallel physical sensor, drones and the RF analyser will send alarms to the resisto platform.

The resisto platform will correlate both cyber and physical and send the corresponding message to the NOC.

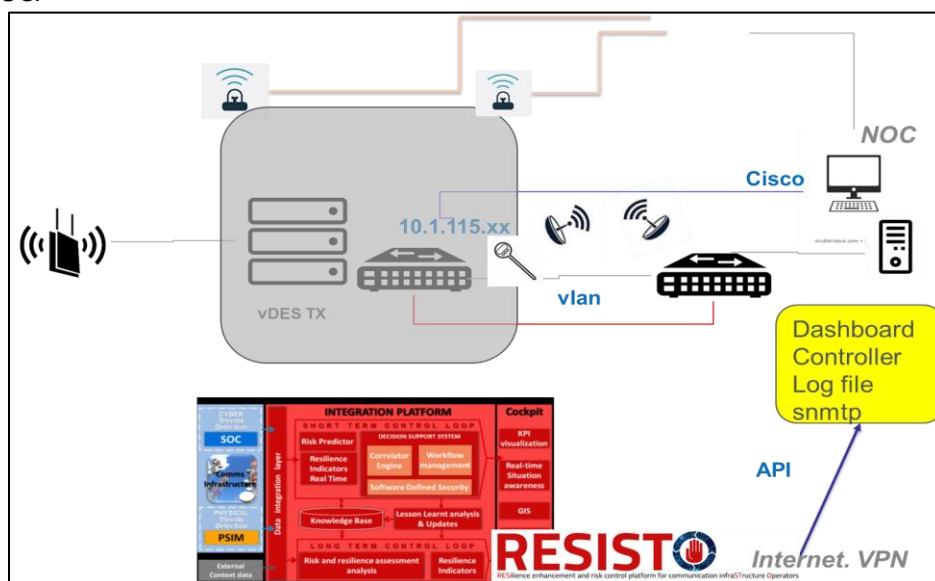


Figure 4 - High Level overview of RTVs Testbed (2/2)

## 6.2.1 Technologies involved

The following tables lists the key elements of the RTV use case.

Technology	Role	Description
<b>RESISTO Platform</b>	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.
<b>Physicals sensors in the site</b>	Detection for physical attack	Monitors and notifies on physical attack. Will provide syslog messages on changes to the RESISTO platform when it detects an event.
<b>Blockchain</b>	Protection of equipment configuration	Implementing blockchain to protect the system configuration of equipment.
<b>AI</b>	AI probe that detect cyber attack	An AI is monitoring the data network and may detect a hacker has entered the network
<b>RADIOFILTER cyber sensors</b>	RADIOFILTER sensors detecting cyber threats and attacks	These passive cyber sensors monitor the wireless traffic and detect anomalous traffic activity, APs and devices representing a cyber threat or attack, such as denial of service
<b>Drone</b>	Drone attack using RF	

Table 7 Technologies involved in the RTV scenario

## 6.2.2 Preconditions

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

		Applicability
P1	Site selection and preparing for demonstration	
P2	AI neuronal network has to learn in a normal situation	
P3	Physical sensors and AI installed	
P4	Integrasys and Drone installed and running	

Table 8 Preconditions for the RTV sub scenario

### 6.2.3 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><b>Integration of Testbed</b></p> <p>RTV will configure the testbed equipment to forward syslog verbose event messages to the RESISTO connector specifically designed to ingest and parse syslog messages. The equipment consists of the technologies previously mentioned; each of them will act as event detectors and will feed the RESISTO platform, through its connector, both with cyber and physical event information.</p>
2	<p><b>An intruder physically accesses the control room of the site and connect in the network</b></p> <p>In this step we assume that an attacker enters the protected site within the control room or equipment room.</p> <p>In order to do this, he may have broken physical sensors.</p> <p>Now he tries different IP or network attacks such as IP sniffing, IP spoofing, denial of service etc...</p>
3	<p><b>The AI algorithm detect the cyber attack.</b></p> <p>The behaviour described in the previous step triggers at least 2 events detected by the cyber and physical sensors. These events are reported to the RESISTO platform as syslog messages, but individually they do not constitute evidence of an attack:</p> <ul style="list-style-type: none"> <li>Physical access to the equipment area.</li> <li>Network unusual traffic and unusual requests.</li> <li>Anomalous over-the air WLAN traffic/activity patterns or messages. Presence of unauthorized WLAN APs or devices</li> </ul> <p><b>RESISTO recognizes that the events are anomalous</b></p> <p>The RESISTO platform should be able to collect, parse and evaluate the syslog messages coming from the detectors</p> <ul style="list-style-type: none"> <li>The RESISTO components, algorithms and rules determine that the physical access to the room as soon as the system administrator left is something strange.</li> <li>Network traffic is not usual.</li> <li>Finally, the detection by RADIOFILTER sensors of unusual WLAN traffic, APs or devices leading to a denial of service or related attacks</li> </ul> <p><b>RESISTO recognizes the attack by correlating the events</b></p> <p>Based on the existing behavioural models and correlating multiple events, we expect the RESISTO Platform to provide an early warning, a risk impact assessment that first allows the attack to be stopped and then allows the tampered with data to be remedied.</p>

	<p><b>RESISTO alerts its operators and suggests mitigation measures</b></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 different events. The expectation is that the RESISTO cockpit will publish:</p> <ul style="list-style-type: none"> <li>-Real time alerts in a visual manner;</li> <li>-Real time alert notifications by additional methods – emergency call to the system administrator or NOC operators;</li> <li>-Real time resilience and impact analysis (e.g. number of equipment, network propagation);</li> <li>-Real time service impact in maritime communication.</li> <li>-Real time mitigation measures to be taken by NOC operators.</li> </ul>
	<p><b>Attack is mitigated</b></p> <p>Tampering has been averted, medical data has been restored and the intruder can be arrested.</p>

### 6.3 Key Performance Indicators to Evaluate the Pilot

The Key Performance Indicators (KPIs) to be referred during the evaluation of this Use Case are given in the following Table. As stated in the previous Use Cases, following a thorough analysis within Deliverable D3.8, the final 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 9 KPI to be referred for the RTV scenario

## 6.4 Pilot Execution Time plan

Assuming **T-0** to be the date the Scenario planning is complete, each of the activities comprising the pilot execution plan should complete as follows:

**The pilot sites preparation, users involvement and training requires** two months from T-0 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.

**Pilot implementation and test first run** requires four months starting with T-0 + 2M (following the previous activity) whilst **pilot implementation and second run** should require and additional four months after this

**The operation end-user validation** is an ongoing process through the entire Work Package.

## 7 USERS INVOLVEMENT AND TRAINING

The objective of user-centred design is the development of usable frameworks [17][22]. One of the principles of user-centred design is the early continual spotlight on users, and it is generally accomplished that usability is achieved through the inclusion of potential clients in framework structure [22][36][7].

As user needs and use contexts became increasingly important in system framework development, ISO 13407 [20] prescribes the dynamic contribution of users for getting clients and undertaking prerequisites. Karat [22] 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 artifact 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 [15][32].

On the other hand, a clear definition of user involvement is inadequate. It has been utilised synonymously with “focus on users” [36], “consulting end-users” [32], “contacting with system users” [18], and “participation of users” [19]. 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 [12].

Regardless of whether client contribution is commonly endorsed, the outcomes were to some degree contradictory and demonstrated that user participation does not necessarily prompt users’ progressively uplifting mentalities toward the innovation or market success.

On the other hand, the advantages of usability engineering have been demonstrated in [8] and in [22]. In general, for a given project the cost-benefit analysis identifies the costs associated with the usability work for the project and attempts to quantify the potential sources of benefit. The distinction between the expenses and the advantages exhibits the value that usability engineering brought to a project [26].

It was stated before that user involvement has been inexactly interpreted as “direct contact with users” thus covering many approaches. For example, Muller *et al* [28] includes different framework approaches like Joint Application Design “JAD” [11], Soft System Methodology (SSM) [33], and ETHICS [30]. Bekker and Long [7] reviewed the similarities and differences between the five of these “practices”. They did not compare the handiness or adequacy of these approaches, possibly because this data is not accessible.

In [24], 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 [6] and the latter three are considered as frameworks of field research by Wixon and Ramey [37].

User-centric architecture is intended to create useful and functional products. There does not seem to be an accepted definition or mechanism for it [22]. Nevertheless, there is a general acceptance of the concepts Gould and Lewis present in [17]. The principles are:

1. Early focus on the users and tasks
2. Empirical measurement
3. Iterative design



The principles incorporate the possibility of user involvement: Gould and Lewis [17] 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. [26]). Wixon and Wilson [38] 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 [27].

Participatory or co-operative design is a methodology of Scandinavian origin[16][14]. Designers and workers have worked together on understanding users and their tasks when planning and structuring new business strategies and interfaces. Users participate by analysing the organizational requirements and by arranging suitable social and technical structures to help both individual and organizational needs. Democratic participation and skill upgrade are significant highlights of participatory design [14]. The early work has been supplemented in other nations and the methodology has been applied in a few research projects of the in-house or contract development type, and in product development. Kuhn and Muller [29] state that outside of Scandinavia, the field is increasingly varied, with some theorists and experts seeking after a locally adjusted type of democratic decision-making, and others underlining powerful information acquisition and product quality.

Ethnomethodological ethnography is a sociological methodology that is likewise used to inform the design of systems. It is generally powerful within the research communities of computer-supported co-operative work (CSCW), but also progressively in Human-Computer Interaction (HCI) research [13]. It has become a shorthand or simplification to talk about ethnography rather than ethnomethodology in CSCW, while inside sociology and anthropology themselves ethnography means rather little [34]. Ethnography portrays human exercises and culture with attention on the social parts of human co-operation. Bloomberg *et al* [10] characterize it with four principles:

1. It happens in natural settings.
2. It depends on the principle of holism, that is particular behaviours must be understood in the respective context.
3. It creates descriptive understanding as opposed to prescriptive.
4. It is grounded in a member's point of view. The primary techniques are observation and video-analysis.

In a design context, ethnography aims to build up a careful understanding of current work practices as a reason for the design of computer support [9] [35]. Kensing *et al*'s [23] MUST-method joins the use of ethnographic procedures and intervention within the participatory design tradition in the context of in-house/custom development.

Contextual design is centred around considering people in their work [39][40]. Users, usually one-at-a-time, are watched and talked with about their work while working in their environment. The idea is to examine the work processes and to portray and redesign them by changing the role structures, supporting assignments, robotizing and eliminating superfluous steps. The approach includes a general way of thinking of visiting users. The approach incorporates a general philosophy of visiting users. Beyer and Holtzblatt [39] themselves describe the contextual design as a way to deal with designing products.

Task analysis covers a wide range of techniques to break down a system function in terms of user objectives and the sub-objectives characteristic in performing the task [21][5]. A significant part of the task analysis literature is devoted to the analysis of information, but task analysis also includes the users as sources [41]. Moreover, task analysis may be utilized as a part of larger design strategies.



To genuinely understand user involvement, we should have an comprehension of the advantages such involvement achieves. The expected benefits of user involvement therefore serve as hypotheses to be tested.

According to Damodaran [12] 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.
5. Increased participation in decision-making within the organization.

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”<sup>1</sup>, 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

---

<sup>1</sup> <https://www.techrepublic.com/article/plan-your-end-user-training-strategy-before-software-roll-out/>

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 [43].

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.

## 7.1 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. [42]

## 8 CONCLUSION

The present document describes the initial test plan for the piloting and validation of the three use cases involved in the “Interconnected Critical Infrastructures” scenario:

- Use case 5: Protection of Cloud Storage Services (lead by TIM)
- Use case 6: Cyber and physical protection of network and network elements mechanisms used by critical services that impact users (lead by ORO)
- Use case 7: Maritime Safety and Emergency Case (lead by RTV)

Each test plans have been defined by following a specific methodology (defined in common with WP7 and WP9) consisting of the following steps:

- Scope: What the user wants from the system
- Preconditions: System state before the execution of the functionality
- Postcondition: This will be defined by specific KPI’s measurement.
- Actors: Users or external systems involved
- Related requirements: What is necessary to execute the use case.
- Work Flows: Steps followed in order to get the result he or she expects.

The list of the actual tests that will be performed during the validation of the scenarios will be described into the foreseen documents D8.2 and D8.4

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.

## 9 REFERENCES

[1] RESISTO – Grant Agreement. Project Starting Date: May, 1 <sup>st</sup> 2018
[2] RESISTO - D3.8 “KPIs, quantities and metrics for cyberphysical risk and resilience of telecom CI - final”
[3] RESISTO - D2.8 RESULTS OF RESISTO ARCHITECTURE, SCENARIOS AND USE CASES
[4] RESISTO - D5.4 Real Time Response and Mitigations Results
[5] J. Annett, N.A. Stanton, Task analysis, CRC Press, 2000.
[6] R.M. Baecker, Readings in Human-Computer Interaction: toward the year 2000, Elsevier, 2014.
[7] M. Bekker, J. Long, User Involvement in the Design of Human—Computer Interactions: Some Similarities and Differences between Design Approaches, in: People Comput. XIV — Usability or Else!, Springer London, 2000: pp. 135–147. doi:10.1007/978-1-4471-0515-2_10.
[8] R.G. Bias, D.J. Mayhew, Cost-justifying usability: An update for the Internet age, Elsevier, 2005.
[9] J. Blomberg, L. Suchman, R.H. Trigg, Reflections on a work-oriented design project, Human-Computer Interact. 11 (1996) 237–265. doi:10.1207/s15327051hci1103_3.
[10] J. Bloomberg, J. Giacomi, A. Mosher, and P. Swenton-Wall (1993)“Ethnographic Field Methods and their Relation to Design,” Schuler Namolda Particip. Des. Perspect. Syst. Des. Lawrence Erlbaum Hillsdale, NJ. (n.d.) 123–155.
[11] E. Carmel, R.D. Whitaker, J.F. George, PD and joint application design: A transatlantic comparison, Commun. ACM. 36 (1993) 40–48. doi:10.1145/153571.163265.
[12] 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.
[13] P. Dourish, G. Button, On “technomethodology”: foundational relationships between ethnomethodology and system design, Human-Computer Interact. 13 (1998) 395–432. doi:10.1207/s15327051hci1304_2.
[14] P. Ehn, Scandinavian design: On participation and skill, Particip. Des. Princ. Pract. 41 (1993) 77.
[15] K. Ehrlich, J. Rohn, others, Cost justification of usability engineering: A vendor’s perspective, Cost-Justifying Usability. (1994) 73–110.
[16] C. Floyd, W.M. Mehl, F.M. Reisin, G. Schmidt, G. Wolf, Out of Scandinavia: Alternative Approaches to Software Design and System Development, Human-Computer Interact. 4 (1989) 253–350. doi:10.1207/s15327051hci0404_1.
[17] 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.
[18] J. Grudin, Interactive Systems: Bridging the Gaps Between Developers and Users, Computer (Long. Beach. Calif). 24 (1991) 59–69. doi:10.1109/2.76263.
[19] T. Heinbokel, S. Sonnentag, M. Frese, W. Stolte, F.C. Brodbeck, Don't underestimate the problems of user centredness in software development projectsthere are many!?, Behav. Inf. Technol. 15 (1996) 226–236. doi:10.1080/014492996120157.

[20] I. ISO, 13407: Human-centred design processes for interactive systems, Geneva ISO. (1999).
[21] P. Johnson, Supporting system design by analyzing current task knowledge, Task Anal. Human-Computer Interact. (1989) 160–185.
[22] 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.
[23] F. Kensing, J. Simonsen, K. Bødker, MUST: A Method for Participatory Design, Human-Computer Interact. 13 (1998) 167–198. doi:10.1207/s15327051hci1302_3.
[24] S. Kujala, User involvement: A review of the benefits and challenges, Behav. Inf. Technol. 22 (2003) 1–16. doi:10.1080/01449290301782
[25] M.M. Mantel, 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] M. Mantel, A basic framework for cost-justifying usability engineering, Cost-Justifying Usability. (1994) 9
[27] 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
[28] M.J. Muller, J.H. Haslwanter, T. Dayton, Participatory Practices in the Software Lifecycle, in: Handb. Human-Computer Interact., Elsevier, 1997: pp. 255–297. doi:10.1016/b978-044481862-1.50077-7
[29] M.J. Muller, S. Kuhn, Participatory design, Commun. ACM. 36 (1993) 24–28. doi:10.1145/153571.255960
[30] E. Mumford, The Participation of Users in Systems Design: An Account of the Origin, Evolution, and, Particip. Des. Princ. Pract. (1993) 257
[31] J. Nielson, J. Landauer, A mathematical model of finding the usability problem. Proceedings of the CHI 93 proceedings of the Interact conference on human factors in computing systems, Espac. Trab. Matemático. Quinto Simp. Int. (1993) 206–213. doi:10.1145/169059.169166.
[32] 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
[33] J. Scholes, P.B. Checkland, Soft systems methodology in action, Chichester, Wiley. 876 (1990) 910
[34] D. Shapiro, The limits of ethnography: Combining social sciences for CSCW, in: Proc. 1994 ACM Conf. Comput. Support. Coop. Work. CSCW 1994, Association for Computing Machinery, Inc, New York, New York, USA, 1994: pp. 417–428. doi:10.1145/192844.193064
[35] J. Simonsen, F. Kensing, Using Ethnography in Contextual Design, Commun. ACM. 40 (1997) 82–88. doi:10.1145/256175.256190
[36] 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
[37] D. Wixon, J. Ramey, Field methods casebook for software design, John Wiley & Sons, Inc., 1996



[38] 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
[39] H. Beyer, K. Holtzblatt, Contextual design, Interactions. 6 (1999) 32–42. doi:10.1145/291224.291229.
[40] K. Holtzblatt, H. Beyer, Making customer-centered design work for teams, Commun. ACM. 36 (1993) 92–103. doi:10.1145/163430.164050.
[41] R. Jeffries, The Role of Task Analysis in the Design of Software, in: Handb. Human-Computer Interact., Elsevier, 1997: pp. 347–359. doi:10.1016/b978-044481862-1.50080-7.
[42] RESISTO D6.3 “HMI definition and Platform integration”
[43] 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.