

# **RESISTO**

## **D9.1\_Scenario 3 Test Plan definition**

# RESISTO

## D9.1 –SCENARIO 3 TEST PLAN DEFINITION

<b>Document Manager:</b>	Luis MORENO	RTV	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>	RTV

<b>Document ID N°:</b>	RESISTO_D9.1_200525_01	<b>Version:</b>	1.0
<b>Deliverable:</b>	D9.1	<b>Date:</b>	25/05/2020
		<b>Status:</b>	APPROVED

<b>Document classification</b>	<b>Public</b>
--------------------------------	---------------

Approval Status	
<b>Prepared by:</b>	Luis MORENO (RTV)
<b>Approved by: (WP Leader)</b>	Luis MORENO (RTV)
<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
Paolo De Lutiis	TIM	R&D Engineer
Jose Manuel Sánchez, Javier Valera	INT	R&D Engineers
Jorge Carapihna	ALB	R&D Engineer
Luis Moreno	RTV	R&D department
Cosimo Zotti, Giuseppe Celozzi, Giovanna Spadaccio, Antonio Nicoletti	TEI	R&D department – Senior System manager, senior project manager, senior test manager, senior software developer

## DISTRIBUTION LIST

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

## REVISION TABLE

Version	Date	Modified Pages	Modified Sections	Comments
0.1	17/03/2020	ALL	ALL	Draft ToC
0.2	31/03/2020	ALL	ALL	TEI and RTV contribution
0.3	02/04/2020	ALL	ALL	ALB contribution
0.4	29/04/2020	ALL	ALL	Final contributions different partners
0.6	04/05/2020	ALL	ALL	ALB comments
0.7	05/05/2020	ALL	ALL	INT contribution
0.9	07/05/2020	ALL	ALL	Final release for SAB
1.0	25/05/2020	ALL	ALL	Final version

## COPYRIGHT STATEMENT



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

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

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

## PROJECT CONTACT



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

## RESISTO PROJECT – PUBLISHABLE EXTENDED ABSTRACT

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

## EXECUTIVE SUMMARY

The present document is a deliverable of the RESISTO project (Grant Agreement No. 786409) 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.

WP9 deals with increase the resilience of 5G network, covering the whole chain: Distributed backhaul, Cloud Storage and platform system, RF communication head-end along with Applications and data, Services provided and a wide variety of users.

Deliverable 9.1 presents the initial plan to design, implement and deploy the Proof-of-Concepts of the use cases of the Macro Scenario 3, defined in D2.8 "Table-top Read Teaming Results of RESISTO Architecture, Scenarios and Use-Cases" of RESISTO project.

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

## CONTENTS

<b>ABBREVIATIONS</b>	<b>9</b>
<b>1. INTRODUCTION</b>	<b>12</b>
1.1. Scope	13
1.2. Document outline	14
<b>2. Methodology</b>	<b>15</b>
2.1. Pilot Description	15
2.2. Pilot Planning	15
<b>3. Description of Use cases corresponding to macro scenario #3</b>	<b>17</b>
<b>4. Use Case 5 sub-case 2: PROTECTION OF CLOUD STORAGE SERVICES Smart Manufacturing</b>	<b>18</b>
4.1. Scope	18
4.2. Test-bed setup	18
4.2.1. Technologies involved	19
4.2.2. Preconditions	20
4.2.3. Use case Work flows	20
4.3. Key Performance Indicators to Evaluate the Pilot	22
4.4. Pilot Execution Time plan	22
<b>5. USE CASE 8: PPDR Virtual Operator</b>	<b>23</b>
5.1. Scope	23
5.2. Test-bed setup	24
5.2.1. Technologies involved	24
5.2.2. Preconditions	25
5.2.3. Use case Work flows	25
5.3. Key Performance Indicators to Evaluate the Pilot	27
5.4. Pilot Execution Time plan	27
<b>6. USE CASE 9: 5G NETWORK RESPONSE TO A SECURITY BREACH</b>	<b>28</b>
6.1. Scope	28
6.2. Test-bed setup	29
6.2.1. Technologies involved	31
6.2.2. Preconditions	32
6.2.3. Use case Work flows	32
6.3. Key Performance Indicators to Evaluate the Pilot	34
6.4. Pilot Execution Time plan	34
<b>7. Users involvement and training</b>	<b>35</b>
7.1. User involvement	35
7.2. Training Plan	38
<b>8. CONCLUSION</b>	<b>40</b>

## 9. References ..... 41

### List of Figures

Figure 1 Overall diagram showing the links between the different Work Packages.....	14
Figure 1 – Basic use case scenario .....	29
Figure 2 – Altice Labs 5G testbed (as of March 2020) .....	30
Figure 3 – Altice Labs 5G testbed: topology to run the use case .....	30
Figure 4 - Main technological building blocks .....	31
Figure 5 – Basic use case workflow.....	33

### List of Tables

Table 1 Technologies involved UC7 .....	20
Table 2 Preconditions UC7.....	20
Table 3 KPI UC7 .....	22
Table 4 Technologies involved UC8 .....	25
Table 5 Preconditions UC8.....	25
Table 6 KPI UC8.....	27
Table 7 Technologies involved UC9 .....	32
Table 8 KPI UC9.....	34
Table 9 Work Plan Gantt.....	34



## 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

In the past, infrastructures may be considered almost impossible to be attacked. Different risks have raised these decades and the impact of them on the society have reached critical levels.

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 and Protection and resilience of Critical Infrastructures (Cis) has become major issue.

Moreover not only the danger has raised also but the coupled with many dependencies. Infrastructure was thought as autonomous vertically integrated systems with very few or possibly none points of contact dependencies but complexity and dependencies are very and their impact in others services and systems are critical.

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.

Consequently, the risk to society due to inadvertent and deliberate CI disruptions has largely increased due to interrelation, complexity, and dependencies of these infrastructures.

This deliverable, namely D9.1 “Test Plan Definition” is divided in two main parts, Test plan Definition of the Use cases referred to Macro scenario 3 for the protection and resilience of the future Telecommunication Critical Infrastructures and Users Involvement and Training.

3 Main Scenario Use Cases are planned to be implemented, addressing future networks, as described in Section B1.3.6 of DoW.

1. Smart Manufacturing Data Integrity Protection using a block-chain based mechanism (lead by TIM)
2. PPDR Virtual Operator (lead by RTV)
3. 5G network response to a large scale natural disaster in Lisbon (lead by ALB)

First a detailed description of the pilots that will be executed in the context of this project and more specifically the pilots related to Macro scenario 3 are described. These pilots are based on the basis of the Use Cases provided in D2.8 and the RESISTO platform reported in D6.1. Moreover, this deliverable shall be considered along with D7.1 and D8.1, as, together, they provide the overall context in which the Use Cases of all Macro Scenarios are 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.

Training activities to the entire community of project’s end-users and creating the related contented are led by TIM and partners involved are RM3 and LDO. These partners will run different training initiatives for staff and users involved in the pilots of the use cases of the

project. To harmonize and more efficiently exploit this potential, this task will produce an inventory of existing training material related to the objective of RESISTO project.

## 1.1. Scope

WP9 particular objectives are:

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

This document is aimed to define the Plan of the pilot, its requirements and design. In particular the document is focused on the Macro-Scenario 3.

Such a macro-scenario focuses on addressing essential future communication services and related cascade effects in the network and services caused by indicative threat cases in Telecom infrastructures through sufficient responding and innovative protection measures. Relation to Other Work Packages within RESISTO

All the Work Packages are linked and follow a methodological path in order to develop the project. Many descriptions and deliverables are defined in others sections or work package while they will used and mentioned here.

Work Packages 4 is developing tools and algorithms for real time monitoring of treats while WP3 performs cyber –physical risk and resilience assessment. WP6 and WP2 are establishing the RESISTO platform and defining the use cases that will be piloted in three validation scenarios. Work Package 5 is developing and implementing algorithms for real time response and mitigation. **In Task 9.1 the common and detailed planning is described and gives the pilot sites of the 3 validation scenarios the necessary framework to install their hardware testing.**

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

The most important deliverable which gives the input to D9.1 is D2.8 “Table-top read teaming results of RESISTO architecture, scenarios and use cases”, since it contains the first and main description of the involved use cased to be validated.

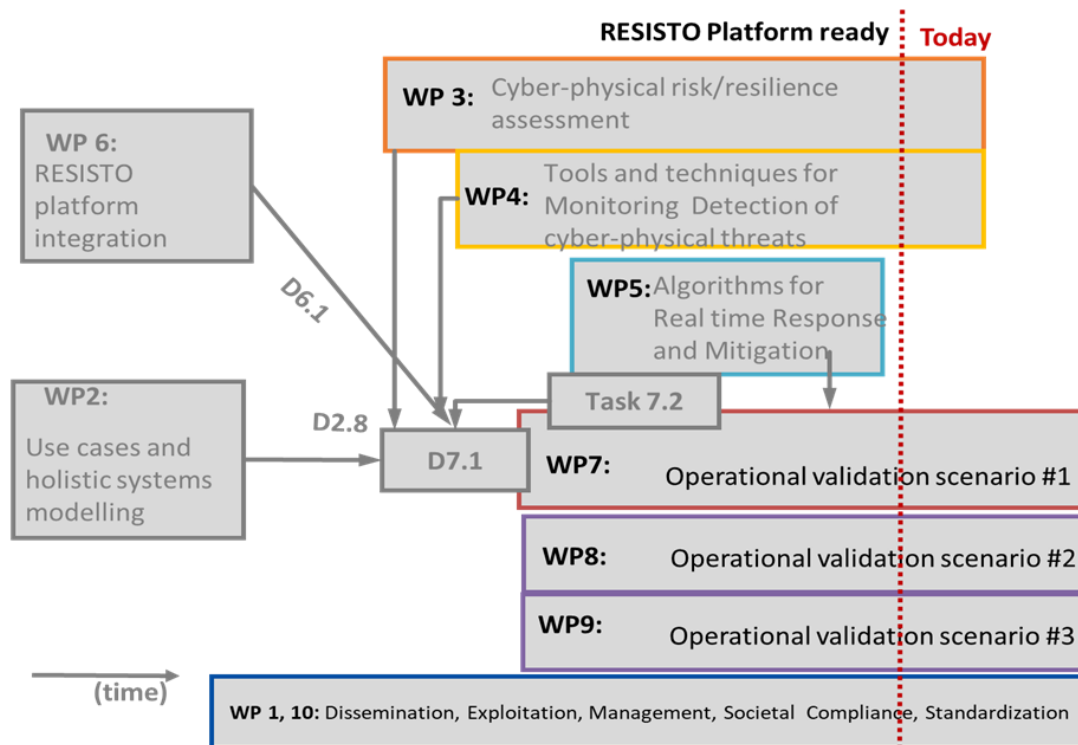


Figure 1 Overall diagram showing the links between the different Work Packages

## 1.2. Document outline

The present deliverable is structured as follows:

- Chapter 1 – Describes the objectives of Task 9.1 and provides a brief description of the deliverable context.
- Chapter 2 - Describes the methodology defined for the Test Plan definition the macro scenario in scope of WP9 (please note that the same methodology has been used by WP7 and WP8)
- Chapter 3 - Presents Macro scenario 3 to Protection the future Telecommunication Critical Infrastructures and it's the specific use cases in the scope of the WP9.
- Chapters 4 - Present the test plan for the validation of the TIM namely " Smart Manufacturing "
- Chapter 5 – Presents Telecommunication sites Use case. PPDR Virtual Operator leaded by RTV
- Chapter 6 – Presents the test plan for the validation of the ALB use case "5G NETWORK RESPONSE TO A SECURITY BREACH".
- Chapter 7 – This chapter describes the user involvement and the training plan

## 2. METHODOLOGY

### 2.1. Pilot Description

WP9 focuses on addressing cyber and physical attacks on future network and the impact of Interconnected/Interdependent CIs and cascade effects caused by indicative threats. Through sufficient responding and innovative protection measures, WP9 objectives are aligned with WP7 and WP8. The main objectives to be addressed are the following:

At a technological point of view:

- 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 measure through KPI indicators the level of countermeasures responses.
- To derive lessons learned and best practices of the comparative analyses and end user validation.

At a high level point of view:

- To conclude the best 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.

### 2.2. Pilot Planning

As per the initial planning and given the complexities involved in the execution of the pilot, the time plan for WP9 is the following:

we have divided the WP actions into 4 main phases. The operation end-user validation is an ongoing process through the entire Work Package. Phase 1 “Design and preparation of Pilot sites” has started and it is ongoing. Phase2 and phase 3 will have some delays .

1. **The pilot sites preparation**, starting at T0 of the WP9 the pilot site preparation is the initial and more critical for the WP. Installation of all the equipment and connectivity of all the component is necessary to be carried out correctly.

2. **Pilot implementation and test first run** requires four months starting when deployment has been finished (following the previous activity) whilst the **pilot implementation and second run** should require an additional four months after this.
3. **The operation end-user validation** is an ongoing process through the entire Work Package as explained already. It is a task that last all the WP9 duration.
4. **Users involvement and training requires** two months since (start of pilots) the deployment of the necessary connectivity between testbed(s) and the RESISTO components. The dissemination of activities and training for the users of RESISTO are also included.



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

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.

Future communication infrastructures - towards 5G Macro-Scenario 3 is meant to be examined in the framework of WP9.

This third macro-scenario focuses on improving of resilience of future 5G telco Infrastructures , involving IoT and 5G networks based UCs, able to demonstrate the readiness of RESISTO platform to support the new 5G envisioned network nodes, promoting applicability in a very challenging UCs. . The main objectives to be addressed are the following:

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

This macro-scenario acts as the liaison between the baseline (formed in the first macro-scenario) and the envisioned future networks and their protection (third macro-scenario) as this can be demonstrated in the context of the main and impacted Use Cases involved. Thus, setting the basis for the functional interconnections of the Scenario pilots through established federation aspects. In this third macro-scenario the following use cases (see D2.8 [ref 3]) will be described:

- Use case 5 sub-case 2: Protection of Cloud Storage Services: Smart Manufacturing (lead by TIM)
- Use case 8: PPDR Virtual OperaTor (lead by RTV)
- Use case 9: 5G NEtwork Response to a large sacale natural disaster in lisbon (lead by ALT)

## 4. USE CASE 5 SUB-CASE 2: PROTECTION OF CLOUD STORAGE SERVICES SMART MANUFACTURING

### 4.1. Scope

This UC intent is to address the validation and trialing of RESISTO platform applied to 5G-enabled SMART MANUFACTURING vertical applications developed by a key agent of that specific industry sector, COMAU, and the plan is to carry out the validation activities on Industry 4.0 use cases at his factory premises in Turin area, where the ICT-17 Platform of H2020 5G EVE project is available for supporting that process.

In a smart factory (industry 4.0) the number of remote-control and autonomous robots and automated guided vehicles (AGVs) on the factory floor increase, and manufacturers are demanding mobility, reliability, density to accommodate many devices, predictable latency for quick reaction times: the 5G network, that is able to provide the requested wireless connectivity is the solution to implement the concept of virtual robot control, where various parts of a robot's motion control calculation are be outsourced to a cloud (or edge cloud) system instead of located in the robot itself. To this extent the UC demonstrate that RESISTO platform is able to provide protection against cyber-attacks of both the nodes of the 5G network and the ones where the ROBOT control modules are located, detecting unauthorized events like changes of installed SW or of configuration data and generating the correspondent alarm and proposing the relevant countermeasure able to mitigate the attack effects.

For this use case, the cyber attack will take place considering two cases:

- (a) an attach to the 5G nodes, comprising the data link;
- (b) an attack to the end-user application stored in the local cloud, comprising the robot functionalities;

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

### 4.2. Test-bed setup

For the implementation of this Use Case, COMAU and TIM facilities will be used, namely the Core lab and the Cloud lab described in Fig. 4.1. The COMAU lab located in Turin will host both the cloud infrastructure where the end user application (robot remote control) is installed and the nodes needed to implement the 5G connection between the user application and the remote robots. The TIM lab locate in Milan will host the RESISTO platform.

TIM 5G responsibilities are the provision of a reliable environment for testing and measurement of industry 4.0 applications. Ericsson responsibility The Core Lab is equipped with the appropriate network infrastructure in order to simulate the actual OTE live core network and the corresponded services. OTE's Core Lab retains a great range of routers (from small- and medium-size to carrier routers) and switches which can be used for the implementation of complex network topologies and scenarios. Such scenarios include inter-alia: Metro Ethernet services over MPLS infrastructure; MPLS based VPNs, and QoS and Traffic Engineering test-beds.

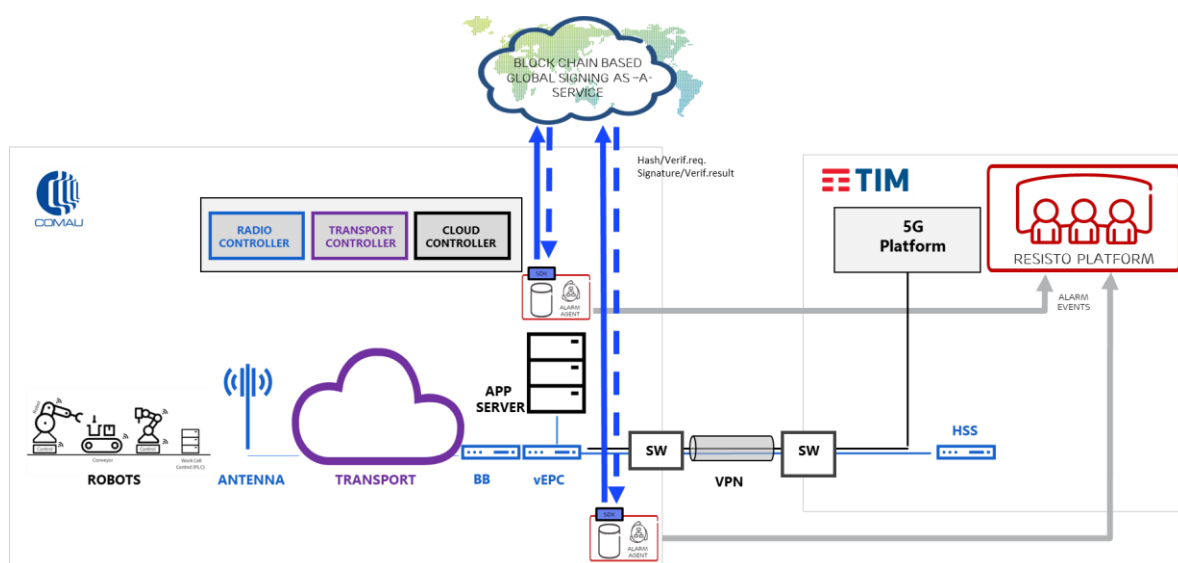


Figure 4.1: High level COMAU and TIM Labs topology.

## 4.2.1. Technologies involved

Technology	Role	Description
Robotic line		Production line including robots and other systems which will be remotely controlled.
App Server		Server platform running COMAU applications devoted to build the digital twin of the robotics line to be shown on the display in real time
Antenna System		Ericsson antenna system for 5G NR
Controllers		Server where radio, transport, and cloud controllers run
Transport		Wired connection (in the specific case it is just a point to point link) between the antenna system and the vEPC, through a baseband system
vEPC		Ericsson Virtual Evolved Packet Core providing core radio functionalities on COMAU premises
Switches		Terminals of the connection between the COMAU site and the TIM site
HSS		Home Subscriber Server
RESISTO Platform	cyber and physical attack monitoring, detection, response and mitigation system	Monitors the overall functionality of the physical and cyber security, receives threat events, uses specific tools and techniques to identify vulnerabilities, erroneous configurations or

		intrusion attempts and responds to threats.
<b>Global Signing-as a service</b>		Guardtime Blockchain based application for remote secure KS storage
<b>KSI Agent</b>	Sensor for Cyber threat detection	Keyless Signature Infrastructure (KSI) module, a blockchain based tool provided by Guardtime

Table 1 Technologies involved UC7

#### 4.2.2. Preconditions

		Applicability
P1	5G Network Connectivity is up and running	
P2	Cloud environment up and running	
P3	APP server installed and running	
P4	KSI module installed and running on vEPC, BB and APP server	
P5	Global Signing-as a service module up and running	
P6	Global Signing-as a service linked to the KSI agent installed in COMAU site	
P7	Other cyber security functions installed and running	
P8	The RESISTO platform installed and running	
P9	The RESISTO platform is reachable from the test-bed	

Table 2 Preconditions UC7

#### 4.2.3. Use case Work flows

Step	Description
1	<p>Integration of Testbed: sensors (KSI agent) provided by Guardtime, 5G network provided by TEI and TIM, remote robot controller provided by TEI, Robotic line provided by COMAU, RESISTO components</p> <p>COMAU/TIM/TEI will configure the testbed equipment so as to have an up and running 5G based remote controlled robotic line. The KSI agent will be installed by Guardtime on both Application server and BB/vEPC 5G nodes. The link among the KSI agents and RESISTO platform/the Global Signing-as a service module will be set-up.</p> <p>The steps that will be followed are:</p> <p>Testbed setup robotic line, networking, cloud, services)</p> <p>5G network Installation</p> <p>Robotic line installation</p> <p>Application server installation</p>

	<p>Robotic line/application server link up and running (remote control up and running)</p> <p>KSI agent Installation on relevant nodes</p> <p>KSI- integration- Global Signing-as a service module integration</p> <p>RESISTO-Sensor (KSI) Integration</p>
2	<p>An cyber attack to perform an authorized change to the vEPC/BB configuration</p> <p>In this step we assume that an attacker overcomes the secure login to the vEPC/BB nodes using an admin profile and gain access to the network configuration data.</p> <p>We assume that the configuration data are put under control, in order to assure its integrity, i.e ensuring that data is recorded exactly as intended and upon later retrieval ensuring the data is the same as it was when it was originally recorded, preventing and detecting changes to information by malicious or unintentional intent.</p> <p>To guarantee data integrity the KSI agents perform a check-sum of the configuration data and store it in the remote Global Signing-as a service module. The checksum is then periodically recalculated and compared with the stored one.</p>
3	<p>Cyber attack is detected by KSI agent, in place in involved node</p> <p>As the data configuration changes is detected by KSI and alarm is raised to RESISTO platform.</p> <p>The RESISTO system identifies the cyber assets in the location as “compromised” and initiates different cyber detectors of the provider’s network in order them to detect potential threats in the cyber domain.</p> <p>RESISTO recognizes attack</p> <p>The RESISTO platform should be able to collect, parse and correlate the syslog messages coming from the KSI detectors and interpret them considering the node involved in the attack.</p> <p>.</p> <p>RESISTO correlates the attack information with existing system modelling and risk assessments</p> <p>Based on the existing network modelling for COMAU/TIM testbed and the impact data pre-provisioned within RESISTO, we expect the Platform to provide immediate and accurate risk and resilience impact assessment taking into account the correlation between the event and the involved node.</p> <p>RESISTO alerts operator and suggests mitigation measures</p> <p>During this phase of the testing scenarios, the RESISTO platform will publish through its cockpit components, the alerts and mitigation measures derived from the correlation of events in the STCL and the information in the LTCL components. The expectation is that the RESISTO cockpit will publish:</p> <ul style="list-style-type: none"> <li>-Real time alerts in a visual manner;</li> <li>-Real time alert notifications by additional methods – e-mail, desktop app notifications etc.;</li> </ul>

	-Real time resilience and impact analysis; -Real time mitigation measures to be taken by COMAU/TIMs testbed operators in a play-book, step-by-step manner; -Mean time to restauration of functionality (by a pre-existing threshold);
	Attack is mitigated The network services impacted by the events have their functionality restored as is the resilience of the network

### 4.3. Key Performance Indicators to Evaluate the Pilot

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

Table 3 KPI UC7

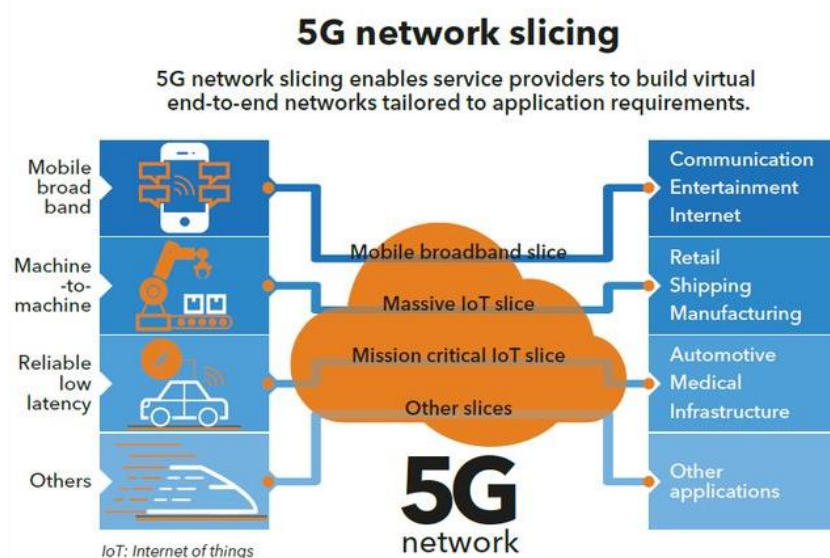
### 4.4. Pilot Execution Time plan

Activity	Number of Months necessary for each Task Implementation											
	1	2	3	4	5	6	7	8	9	10	11	12
Pilot Sites preparation, users training												
Pilot implementation and test first run												
Pilot implementation and second run												
Operation end-user validation												

## 5. USE CASE 8: PPDR VIRTUAL OPERATOR

This UC address the service of PPDR in 5G. PPDR services are dedicated for critical services such as special police or emergency or for private network. These services needs for an special quality of service assuring the coverage and availability 100%.

In 5G in order to provide different quality of service the ETSI has defined the slicing as a technological way of differentiate services. Each network slice is an isolated end-to-end network tailored to fulfil diverse requirements requested by a particular application. Next generation of Tetra service for example will rely on this kind of technologies in order to deploy their services. It is assumed that 5G will be efficient in the way of use of the spectrum and we will not deploy specific wireless networks for specifics network but on the contrary commercial and critical services will share the spectrum.



Slicing will rely on virtualization and on MEC technologies to be implemented. Virtualization creates virtual resources based on real hardware while MEC provides services with lower latency and higher throughput.

For this use case, the cyber attack will take place considering two cases:

- (a) an attack to the 5G nodes, in the MEC where a dedicated service for a dedicated slice is running;
- (b) an attack to the end-user application or service in the slice;

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

### 5.1. Scope

Infrastructure providers are preparing themselves for the arrival of the first commercial 5G networks. One of the most innovative aspects of the 5G architecture will be its reliance on 5G network slicing, which will let operators provide portions of their networks for specific customer uses cases — whether that use case is the smart home, the Internet of Things (IoT) factory, the connected car, or the smart energy grid.

Each use case receives a unique set of optimized resources and network topology — covering certain SLA-specified factors such as connectivity, speed, and capacity — that suit the needs of that application



Network slicing is a type of virtual networking architecture in the same family as software-defined networking (SDN) and network functions virtualization (NFV) through the partitioning of network architectures into virtual elements. In essence, network slicing allows the creation of multiple virtual networks on top of a shared physical infrastructure.

In this virtualized network scenario, physical components are secondary and logical (software-based) partitions are paramount, devoting capacity to certain purposes dynamically, according to need. As needs change, so can the devoted resources. Using common resources such as storage and processors, network slicing permits the creation of slices devoted to logical, self-contained, and partitioned network functions.

## 5.2. Test-bed setup

The scheme of the test bed is based on a deployment in a real infrastructure site. In that site we will deploy a 5G network plus a MEC platform for delivery of local services. In the MEC a local breakout equipment will route traffic to/from the local MEC or either from the core of the MNO.

From the orchestrator we will configure different services or application running on different slices in order to emulate 2 different MNOs with different quality of services running in the same radio frequency.

2 devices set up in the 5G radio network will be used to simulate the cyber attack. Attack to small cell service availability will be simulated by a wired jammer and a wired IMSI-catcher.

### 5.2.1. Technologies involved

Technology	Role	Description
<b>MEC</b>		Service or application running in the edge near the 5G transmitter such as CDN services for video delivery
<b>Slicing</b>		Server platform running MEC
<b>Antenna System</b>		antenna system for 5G NR
<b>Controllers</b>		Server where radio, transport, and cloud controllers run
<b>Transport</b>		Wired connection (in the specific case it is just a point to point link) between the antenna system and the vEPC, through a baseband system
<b>vEPC</b>		Virtual Evolved Packet Core providing core radio functionalities
<b>RANMONITOR sensors</b>	Detect jamming and IMSI-catchers attacks/threats to the service	Monitors signals coming from cells and jammers to detect threats/attacks to the availability of the service



<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.
-------------------------	---	--

Table 4 Technologies involved UC8

### 5.2.2. Preconditions

		Applicability
P1	5G Network Connectivity is up and running	
P2	Slicing configured	
P3	MEC APP server installed and running CDN or video delivery caching service	
P4	Other cyber security functions installed and running	
P5	The RESISTO platform installed and running	
P6	The RESISTO platform is reachable from the test-bed	

Table 5 Preconditions UC8

### 5.2.3. Use case Work flows

Step	Description
1	<p>Integration of Testbed:</p> <p>RTV will configure the testbed equipment so as to have an up and running 5G network.</p> <p>The steps that will be followed are:</p> <p>Testbed setup robotic line, networking, cloud, services)</p> <p>5G network Installation in real sites</p> <p>MEC Application server installation</p> <p>Preparation of 2 slices</p> <p>Configuration of 2 SIMs, only one authorized to use the service</p> <p>RESISTO- Integration</p>

<p>2</p>	<p>An attacker with the use a cyber attack to perform an unauthorized use of the service that is running in the MEC.</p> <p>A SIM non authorized knows from an authorized SIM service IP and tries to access this service.</p> <p>Another attack consists in accessing control of the MEC platform. In this step we assume that an attacker overcomes the secure login MEC node using an admin profile and gain access to the network configuration data.</p> <p>In the same manner, a SIM non authorized knows from an authorized SIM service IP and tries to get access to the MEC platform and gain root access.</p> <p>In relation to the attack to the service, another attack/threat will be detected where the attacker targets the base station node providing the connectivity, thus negatively affecting service availability by using direct methods (jamming) or indirect methods (IMSI-catcher)</p>
<p>3</p>	<p>Cyber attack is detected by MEC, in place in involved node.</p> <p>Jamming or IMSI-catcher threats/attacks are detected by RANMONITOR sensors.</p> <p>Alarm is raised to RESISTO platform.</p> <p>The RESISTO system identifies the cyber assets in the location as “compromised” and initiates different cyber detectors of the provider’s network in order them to detect potential threats in the cyber domain.</p> <p>RESISTO recognizes attack</p> <p>The RESISTO platform should be able to collect, parse and correlate the syslog messages and interpret them considering the node involved in the attack.</p> <p>.</p> <p>RESISTO correlates the attack information with existing system modelling and risk assessments</p> <p>Based on the existing network modelling for COMAU/TIM testbed and the impact data pre-provisioned within RESISTO, we expect the Platform to provide immediate and accurate risk and resilience impact assessment taking into account the correlation between the event and the involved node.</p> <p>RESISTO alerts operator and suggests mitigation measures</p> <p>During this phase of the testing scenarios, the RESISTO platform will publish through its cockpit components, the alerts and mitigation measures derived from the correlation of events in the STCL and the information in the LTCL components. The expectation is that the RESISTO cockpit will publish:</p> <ul style="list-style-type: none"> <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 mitigation measures to be taken by operators, step-by-step manner;</li> <li>-Mean time to restoration of functionality (by a pre-existing threshold);</li> </ul>

	<p>Attack is mitigated</p> <p>The network services impacted by the events have their functionality restored as is the resilience of the network</p>
--	---

### 5.3. Key Performance Indicators to Evaluate the Pilot

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

Table 6 KPI UC8

### 5.4. 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 de **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.

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

One of the differentiating aspects of 5G compared to previous mobile generations is the massive deployment of IT infrastructure at the edge. This is motivated by multiple factors, including the virtualization and centralization of gNB components, the low latency requirements by many emerging applications and the need to avoid the massive growth of traffic load injected in the network transport and core segments. As a result of this trend, a significant part of the network infrastructure is likely to become distributed through a high number of physical locations, which makes global network security and dependability much more challenging to achieve.

In this context, the traditional solutions for protection of the infrastructure against disruptive events, either as a result of accidental technical failure or intentional cyber/physical attacks, are no longer adequate to guarantee the fulfilment of carrier-grade reliability target numbers, therefore new solutions are required.

Recent technical advancements have contributed to provide new solutions to cope with the new challenges raised by 5G:

- Machine Learning has enabled new possibilities to enable autonomous network management, towards the materialization of self-configuration, self-optimization and self-healing.
- Network slicing provides a solution for on-demand creation of dedicated network and computation resources by leveraging network function virtualization (NFV) and software-defined networking (SDN) techniques.

Use case #9 illustrates how recent advancements in these two areas can be leveraged to address 5G security and reliability related challenges, particularly in the network edge. Machine learning enables the precocious diagnosis of network failures, malfunctions and cyber/physical attacks. On the other hand, network slicing and virtualization enable the on-demand instantiation and reconfiguration of network resources to mitigate the potential effects of failures and minimize the impacts.

### 6.1. Scope

The proposed use case, described in detail in D2.8 [3], comprises a mission-critical scenario based on a 5G telecommunication mobile network in which the probability of equipment failure is assessed by continuous analysis of specific parameters or abnormal behaviour, making use of machine learning techniques. The use case definition is based on the execution of different actions depending on the perceived probability of equipment failure.

Three management roles are associated with the use case, in line with the model defined by 3GPP in TR 28.801 for 5G network slicing enabled networks, as described in Section 12.3 of D2.8 [3] – the Service Provider (SP, responsible for the end-to-end communication service, built from one or more network slices), the Network Slice Provider (NSP, responsible for building and operating network slices, built from one or more network slice subnets) and the Network Slice Subnet Provider (NSSP, responsible for building and operating network slice subnets). No specific business relationship is implicit between the players of these roles, which could be

played by the same entity (e.g. a single network operator) or different entities (e.g. a SP using infrastructure from multiple NSPs and/or NSSPs).

In the specific scenario of the use case, the SP provides network services based on a network slice, which is partly built from C-RAN and edge components with two NSSPs in a specific geographical area, who provide C-RAN and edge components – NSSP-A (primary, active by default) and NSSP-B (backup, activated if/when needed).

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

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

The second phase is triggered when the service loss probability goes above a second threshold (e.g. 50%). The slice subnet that had been instantiated in the previous step is now activated.

The third phase is triggered by a third service loss probability threshold (e.g. 65%). The SP decides to migrate the affected C-RAN and edge components from NSSP-A to NSSP-B; the service to end users is not supposed to be impacted.

For a more detailed description of the use case, refer to Deliverable D2.8 [3].

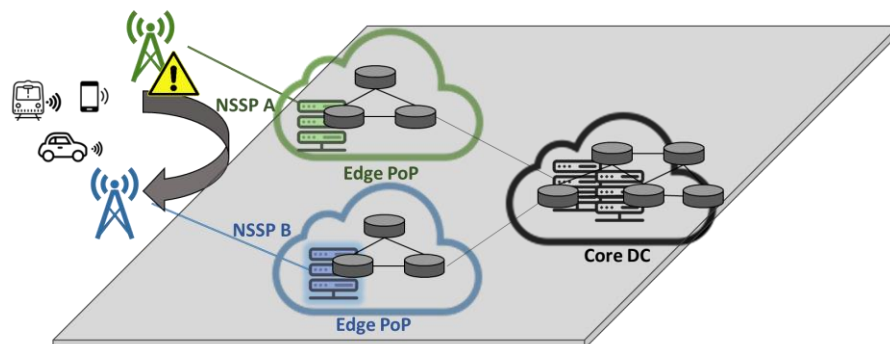


Figure 2 – Basic use case scenario

## 6.2. Test-bed setup

Figure 3 illustrates 5G Altice Labs testbed topology and the status of the main components as of March 2020. The infrastructure is currently hosted at the Institute of Telecommunications (IT), in Aveiro, in two different buildings, IT-1 and IT-2, as represented in the figure.

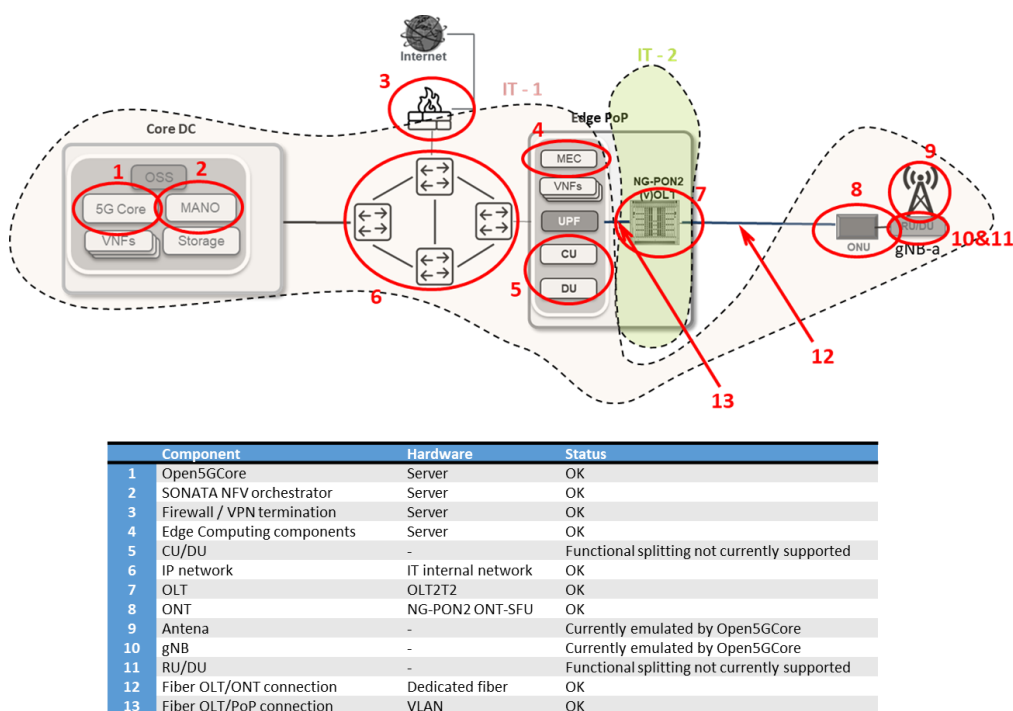


Figure 3 – Altice Labs 5G testbed (as of March 2020)

Figure 4 represents the 5G testbed topology planned to run the use case, which includes a third site hosted at the Altice Labs headquarters, in addition to IT-1 and IT-2. Both Altice Labs and IT will host edge PoPs, and the 5G core is planned to be moved to Altice Labs, as well as the MANO and OSS components. The RAN infrastructure represented in the figure is for experimental purposes only and is currently emulated by an Open5GCore component.

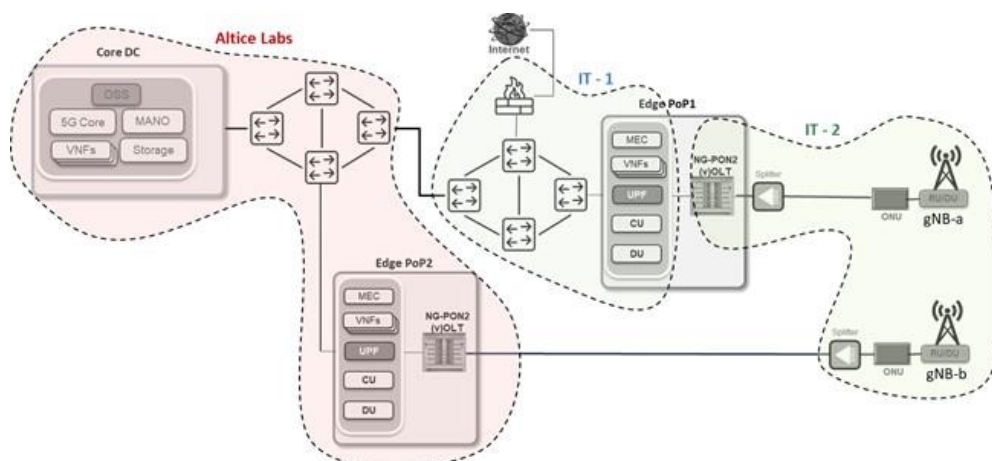


Figure 4 – Altice Labs 5G testbed: topology to run the use case

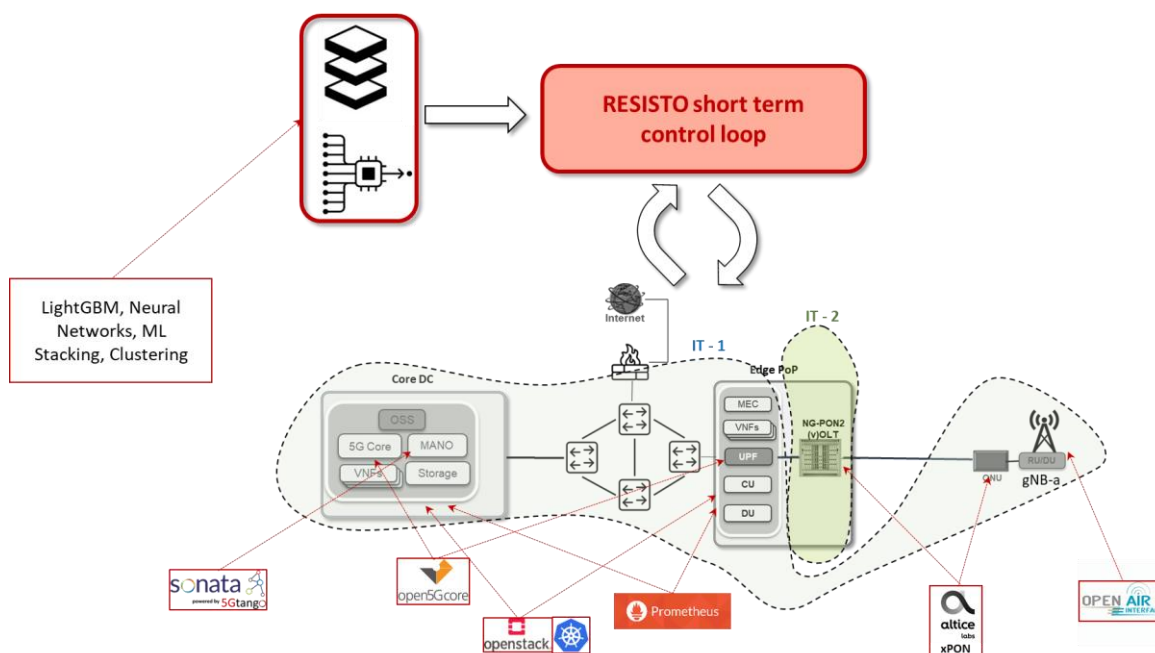
It should be noted that Figure 3 and Figure 4 only include 5G testbed components. The RESISTO platform, including the short term control loop, as well as machine learning components running locally, but out of the scope of the 5G testbed, are represented in

Figure 5.

### 6.2.1. Technologies involved

The main technological building blocks, including RAN, edge PoP, 5G core and NFV MANO are represented in

Figure 5, as well as the machine learning components, and the respective technologies deployed in each of these components.



**Figure 5 - Main technological building blocks**

The table below lists the main technological components, the respective roles and descriptions.



Technology	Role	Description
LightGBM, Neural Networks, ML Stacking, Clustering	ML-based event detection	Based on real dataset (e.g. alarms, trouble tickets) the ML/AI model (e.g. Neural Network) enables the transition from a reactive to a proactive approach, thus anticipating potential disruptive events and streamlining operational management systems. Applying ML techniques to available operational data enables the creation of a new pipeline of precocious diagnosis, followed by preventive actions.
SONATA	NFV Orchestrator	SONATA performs the lifecycle management of virtualized network resources.
RESISTO Platform	Monitoring, detection, response and mitigation	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.
Open5GCore	5G Core	Supports 5G Core components, including AMF, SMF, UPF, NRF, AUSF, UDM.
Edge PoP	Edge computing	Edge infrastructure located at the network edge; typically includes 3 <sup>rd</sup> party application or media.
Prometheus	Infrastructure monitoring	Open source, metrics-based infrastructure monitoring system.
NGPON-2 xHaul	5G transport network	Backhaul/Midhaul/Fronthaul network infrastructure.

Table 7 Technologies involved UC9

### 6.2.2. Preconditions

Preconditions include:

1. The network, including all components (e.g. RAN, 5G core, transport, edge components) is up and running
2. MANO components are up and running and able to perform orchestration
3. The RESISTO platform is up and running and interoperable with the MANO layer
4. Prometheus is collecting monitoring data
5. Network data set is available; ML/AI components are operational and able to interoperate with the RESISTO platform

### 6.2.3. Use case Work flows

The basic storyline is described below. The use case workflow can be divided in three basic phases, as described below and illustrated in

Figure 6.



1. The SP owns and operates the core network components and has a business relationship with two NSSPs in a specific geographical area, who provide C-RAN and edge components – NSSP-A (primary, active by default) and NSSP-B (backup, activated if/when needed).
2. The first phase of the use case (*preparation phase*) is triggered when the probability of service loss affecting resources run by NSSP-A goes above a certain threshold (e.g. 35%). The cause may be something like the temperature rising in Edge PoP. The event may be accidental, caused by a natural event, or by a malicious action.
3. The SP requests NSSP-B to instantiate an edge slice subnet, in case a relocation of resources from NSSP-A proves to be necessary.
4. The second phase (*activation phase*) is triggered when the service loss probability goes above a second threshold (e.g. 50%). The slice subnet that had been instantiated in the previous step is now activated.
5. The third phase (*service migration phase*) is triggered when a third service loss probability threshold (e.g. 65%) is reached. The SP decides to migrate the affected C-RAN and edge components from NSSP-A to NSSP-B; the service to end users is not supposed to be impacted.

It should be noted that this sequence of steps is based on the assumption of a continuously increasing service loss probability. Variations of this scenario can be defined, e.g. returning to initial state after reaching the 1st and 2nd phases. However, they are not considered in this slide and next slide for the sake of simplicity.

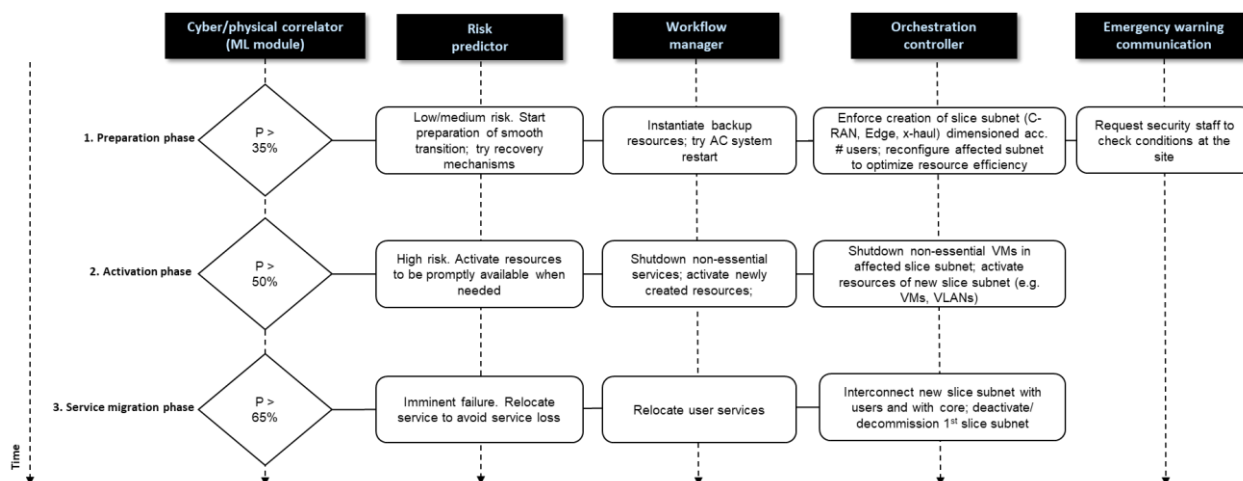


Figure 6 – Basic use case workflow

### 6.3. Key Performance Indicators to Evaluate the Pilot

KPI number	KPI title	D3.8 section
K1	Time to detection	3.1.8
K2	Decision-making time	3.2.2
K3	Mitigation time	3.2.3
K4	Downtime	3.2.6
K5	Financial impact	3.4.2

Table 8 KPI UC9

### 6.4. Pilot Execution Time plan

Activity	Number of Months necessary for each Task Implementation											
	1	2	3	4	5	6	7	8	9	10	11	12
Pilot Sites preparation, users training												
Pilot implementation and test first run												
Pilot implementation and second run												
Operation end-user validation												

Table 9 Work Plan Gantt

## 7. USERS INVOLVEMENT AND TRAINING

User involvement and training description at general level is the same in all the WP, 7,8 and 9. Here can be found the same description has may be found in other deliverables. In D9.2 and D9.3 we will detail more precisely the differences and peculiarities for each one of the use cases.

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

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

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

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

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

### 7.1. User involvement

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 artefact fits into a complex work or home environment”. Along this line, it is obvious that reports are inadequate as sources of information and direct contact with users is urgent to comprehend the various contexts of utilization. Also, in principle, user involvement is most efficient and powerful in the beginning stages of system framework development as the cost engaged with making changes increases during system advancement [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].

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:

- Early focus on the users and tasks
- Empirical measurement
- 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 **Errore. L'origine riferimento non è stata trovata.** 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].

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.  
Increased participation in decision-making within the organization.
5. The list is fairly participatory design focused, but it aptly represents the underlying assumptions regarding the benefits of user-centred design and usability engineering.

Training of the end clients is one of the most significant strides for an effective system usage. The end users can be included in parallel testing, and training needs to be carried out before that. At this point, having the end users involved is also a good way to get them excited about the proposed system because many of them may not been familiar with the project before training. A parallel research assistance will help them plan for the moment when the device goes online. End users in more of a “real world” environment are good at using the system and can determine when process flows are not working. When everyone interested in suing the program is included in the training, they will feel more comfortable about using it when they move into

production and the user community can see the implementation when positive. The system may have been checked for functionality and all customizations work properly, but if the end users don't know how to use it or feel confident with it, then the launch of the new system would be deemed ineffective. The scheduling of end-user training is therefore important and must be scheduled and executed prior to the beginning of the parallel test process to ensure an effective implementation.

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

In her excellent 2006 overview of end-user training, "Plan your end-user experience training strategy before software roll-out"<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, using a completely new software, such as the RESISTO platform, is very complex and needs time to allow operator to manage it. More important not all software is equal, neither are all operators.

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

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

- Individual hands-on instructor: a teacher will personally guide each user through the process of performing specific task with the RESISTO platform and answer questions. This is the costliest and possibly the most successful tool.
- Hands-on classroom style instructor-led training: a teacher demonstrates to the students how the RESISTO platform operates and how to execute specific tasks in a classroom with users performing the task themselves. Every user or pair of users has a copy of the RESISTO platform where they can practice on.
- Seminar style group demonstration: a teacher demonstrates to the users how the RESISTO platform functions in a live demonstration and how to execute specific tasks.

---

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

- 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 [38].

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.

## 7.2. Training Plan

The training will be performed using webinars, or eventually workshops. A webinar is a seminar on the web. Webinars are most commonly performed by encouraging key personnel to call into a toll-free phone number or to sign into a website so they can see and hear what is going on. A

webinar can also be registered and referenced at a later date. It enables new personnel to study the webinar as if they were already participating.

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

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

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

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

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

The webinars are demonstration of the RESISTO platform in the different case studies. They are based on the deliverables that are produced in WP6, especially D6.3. [ref 39]

## 8. CONCLUSION

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

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

The list of the actual tests that will be performed during the validation of the scenarios will be described analytically into the foreseen deliverables D9.2 and D9.3.of WP9.

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] KPI
[3] D2.8 RESULTS OF RESISTO ARCHITECTURE, SCENARIOS AND USE CASES
[4] 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 Namoida 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 projects there 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. Mantei, T.J. Teorey, Cost/benefit analysis for incorporating human factors in the software lifecycle, Commun. ACM. 31 (1988) 428–439. doi:10.1145/42404.42408
[26] 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] 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.

[39] D6.3