

# RESISTO: D10.12\_EXPLOITATION ACTIVITIES- THIRD



# RESISTO

## D10.12 – EXPLOITATION ACTIVITIES – THIRD

<b>Document Manager:</b>	Federico FROSALI	LDO	Editor
--------------------------	------------------	-----	--------

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

<b>Document ID N°:</b>	RESISTO_D10.12_200611_01	<b>Version:</b>	1.0
<b>Deliverable:</b>	D10.12	<b>Date:</b>	11/06/2020
		<b>Status:</b>	APPROVED

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

Approval Status	
<b>Prepared by:</b>	Federico FROSALI (LDO), Claudio BECCHETTI (LDO)
<b>Approved by: (WP Leader)</b>	Federico FROSALI (LDO)
<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>	NA

## CONTRIBUTING PARTNERS

Name	Company / Organization	Role / Title
Federico FROSALI Claudio BECCHETTI	LDO	Editor
Maria BELESIOTI	OTE	Contributor
Tuuli LOHMUS	GT	Contributor
Rodoula MAKRI	ICCS	Contributor
Mirjam FEHLING-KASCHEK	Fraunhofer	Contributor
Sylvia BACH	BUW	Contributor
Jorge CARAPINHA	ALB	Contributor

## 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
0.9	01/03/2020	All	All	Final draft
1.0	11/06/2020	All	All	Final release

## COPYRIGHT STATEMENT



© 2018-2021 This document and its content are the property of the RESISTO Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the RESISSO 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 (GE) – 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

**Market analysis Update** An update of the overall market value for security solutions is introduced. The updated value for CI protection market is estimated as part of the total market for security solutions. **Draft Business plan:** based on the latest available market data for the Critical Infrastructure protection and emerging drivers in the market a preliminary business plan is drafted linked to revenue and costs streams. **Exploitation strategy update** where consortium and individual exploitation activities are reviewed in light of the second year project results and envisioned business models. **Innovation strategy update** based on second year project results a review of the State of the art analysis is presented to show how RESISTO keeps up with technology innovation and market demand evolution. **IP protection Plan update:** The IPR plan updated to deal with the delay in the activity is presented.

## CONTENTS

<b>ABBREVIATIONS .....</b>	<b>8</b>
<b>1. INTRODUCTION .....</b>	<b>10</b>
<b>2. SECURITY MARKET ANALYSIS .....</b>	<b>11</b>
2.1 Business External Environment update .....	11
2.2 Security Market value update .....	13
<b>3. RESISTO BUSINESS PLANNING .....</b>	<b>18</b>
3.1 RESISTO Business Model .....	21
3.2 RESISTO Go-to-market strategy .....	22
<b>4. Exploitation Plan Update .....</b>	<b>23</b>
4.1 Exploitation – consortium .....	23
4.2 Exploitation – individual partner .....	26
<b>5. Innovation Management – update .....</b>	<b>31</b>
5.1 Cyber-physical Risk/Resilience assessment of Communication infrastructure .....	31
5.2 Holistic System Modelling and interdependency simulation analysis for Risk Predictor .....	31
5.3 Cyber-Physical correlation .....	33
5.4 Software Defined Security .....	34
5.5 Innovative secure IoT for physical security .....	35
5.6 Audio and visual analytics .....	36
5.7 Responsible Disclosure Framework – RDF (NEW) .....	36
<b>6. IP Management Plan update .....</b>	<b>38</b>
<b>7. REFERENCES .....</b>	<b>41</b>

## List of Figures

Figure 1 - Security Market Value – Total Market split by domain .....	13
Figure 2 - Security Market Value – split by domain .....	14
Figure 3 - Security Market Value – split by geographic areas (*) NATO and European Commission/ Agencies markets are included in Europe and Israel Region estimations .....	15
Figure 4 - Total Market Value (CIP segment details) .....	16
Figure 5 - Market Drivers and KSFs .....	18
Figure 6 - Real GDP rowth April 2020 Forecast .....	19
Figure 7 - RESISTO Draft Business plan .....	20
Figure 8 - RESISTO Service Offering .....	21
Figure 9 – Broadway project phases .....	23
Figure 10 - Ppdr4Europe consortium .....	24
Figure 11 - Broadway SpiceNET architecture .....	25
Figure 12 - IP management plan - original .....	38
Figure 13 - Innovation potential assessment per RESSITO technological element .....	39
Figure 14 - IP management plan update .....	40

## ABBREVIATIONS

<b>IP</b>	Intellectual Property
<b>CI</b>	Critical Infrastructure
<b>CIP</b>	Critical Infrastructure Protection
<b>LET</b>	Long Term Evolution
<b>B2B</b>	Business to Business
<b>B2G</b>	Business to Government
<b>PPDR</b>	Public Protection Disaster Relief
<b>CAGR</b>	Compound Average Growth Rate
<b>TETRA</b>	TErrestrial Trunked RAdio
<b>EU</b>	European Union
<b>MENA</b>	Middle East North Africa
<b>HSCI</b>	Homeland Security& Critical Infrastructures
<b>TLC</b>	Telecommunications
<b>HW</b>	HardWare
<b>ISI</b>	Inter System Interface
<b>GDP</b>	Gross Domestic Product
<b>PoC</b>	Point of Contact
<b>LE</b>	Large Enterprise
<b>SME</b>	Small Medium Enterprise
<b>RTO</b>	Research Organization
<b>PPDR</b>	Public Protection and Disaster Relief
<b>PTT</b>	Push To Talk
<b>QoS</b>	Quality of Service
<b>SW</b>	SoftWare
<b>IoT</b>	Internet of Things
<b>KPI</b>	Key Performance Indicator
<b>SoTA</b>	State of the Art
<b>HMI</b>	Human Machine Interface



SDN	Software Defined Network
5G-PPP	%G Private Partnership Project
NFV	Network Function Virtualization
WP	Work Package

## 1. INTRODUCTION

This deliverable addresses the following topics

- **Market analysis Update:** An update of the overall market value for security solutions is introduced. The updated value for CI protection market is estimated as part of the total market for security solutions
- **Draft Business plan:** based on the latest available market data for the Critical Infrastructure protection, the development of RESISTO framework after the second year a preliminary business plan is drafted linked to revenue and costs streams.
- **Exploitation strategy update** where consortium and individual exploitation activities are reviewed in light of the second year project results and the business models introduced in D10.10/D10.11.
- **Innovation strategy update** based on second year project results a review of the State of the art analysis is presented to show how RESISTO keeps up with technology innovation and market demand evolution.
- **IP protection Plan update:** The IPR plan for the RESISTO has been updated to deal with the delay in the activity. Despite the innovation potential of the project no formal IPR form has been submitted so far. The recovery plan extends the “collection of ideas” phase of 4 months during which two consortium focus meeting will be held in order to elicit and formalize the most innovative ideas developed within the RESISTO framework.

## 2. SECURITY MARKET ANALYSIS

In the following chapters the a market analysis is reviewed and updated in the light of the evolution of the context and of latest available market data, and the refinement of RESISTO framework in the second year.

Starting from a review of the main trends market of Security solutions, an updated focus on the Critical Infrastructure (CI) protection market, as part of the larger Security market, is presented in light of the last year updates, and the market size for RESISTO platform and the solutions developed in the project is re assessed.

### 2.1 Business External Environment update

The following table outlines the main megatrends and technologies influencing the CI protection market, the inhibitors that has to be properly taken into account and the main perceived customer needs. In red the changes compared to Ref.2

About the Mega Trends the main changes concern the “Pandemic threat”, with clear reference to the COVID-19 pandemic that has emerged as a major trend over the first half of 2020 and the “Need for cyber security and personal data protection” even more stressed by the increasing use of cyber resources/solutions driven by the social distancing and remotization of the workforce forced by the health emergency

About the Technology trends “AI” and “Blockchain” previously part of “Cognitive computing” and “Cyber security” are now listed in clear due to the increasing role as technologies that can impact across all the sectors of CI protection (being also part of RESISTO technological core ). The reference to networks evolution has been extended to broadband in general (previously was LTE) in light of the 5G progressive implementation across the world and the evolution of broadband local connectivity based on WiFi 6

About the Inhibitors “Government spending cuts” has been added in light of a shift of public spending towards public health services due to the need to manage the COVID-19 pandemic that may hinder investments in CI protection

About the Impacts On Customers Needs “Global harmonization of standards and solutions” has been added to outline the increasing importance of standard solutions.

SECURITY / CI protection	
MEGA TRENDS	
<ul style="list-style-type: none"> <li>▶ Massive migrations</li> <li>▶ Political tensions</li> <li>▶ Terrorism</li> <li>▶ Growth of cyber crime</li> <li>▶ <b>Pandemic Threat</b></li> <li>▶ <b>Need of cyber security and personal data protection (GDPR)</b></li> </ul>	<ul style="list-style-type: none"> <li>▶ Climate Change</li> <li>▶ Population growth</li> <li>▶ Urbanization</li> <li>▶ Hyper-connectivity and extended enterprise</li> <li>▶ Cyber as <i>Fifth Domain</i></li> </ul>
TECHNOLOGY TRENDS	

- ▶ “Walk through security”
- ▶ Cyber security & resilience
- ▶ Big Data & Analytics
- ▶ Cognitive Computing
- ▶ Mobile, IoT, M2M
- ▶ AI
- ▶ Blockchain

- ▶ Next Gen Managed Security Services
- ▶ Cloud & Edge Computing
- ▶ Media sources variety, Social
- ▶ Biometric solutions
- ▶ Evolution towards broadband networks
- ▶ Wearable devices
- ▶ UAV

### INHIBITORS

- ▶ Privacy rights/ Political and legislative Implications
- ▶ Cultural issues limit cross-agency info-sharing programs

- ▶ Uncertain return on investment
- ▶ Government spending cuts

### IMPACTS ON CUSTOMERS NEEDS

- ▶ Integration of structured and unstructured data
- ▶ Situational awareness and command and control
- ▶ Inter agency data sharing and collaboration

- ▶ Actionable intelligence
- ▶ Real-time decisions support and rapid response
- ▶ Global harmonization of standards and solutions

## 2.2 Security Market value update

Security & Safety Total market exhibits continuous growth up to 2023. The total market value is estimated to be **386B€**, compared to the **353B€** of the previous analysis. Over the five year period the CAGR is **8,1%**, slightly higher than the previous year (**7,9%**). Forecasts are probably **conservative** and not taking into account the recent COVID-19 pandemic whose effects have still to be clearly addressed.

Compared to Ref.2 the Security & Safety Total market has been split across 4 macro segments:

- ▶ **Critical Infrastructure Protection** (in particular Oil&Gas, Utilities and Telcos) addressing solutions for CIs operators and their security (cyber and physical) (
- ▶ **Counter Terror & Crime:** covering technologies and services for PPDR (Professional Comms, Control rooms, sensors, cyberdefence, etc.)
- ▶ **Emergency Management:** covering technologies and services for PA and agencies dealing with emergency management (including earth observation, command and control, fast deployable communication systems etc.)
- ▶ **Safe City:** a relatively new market, rapidly growing as cities/municipalities are increasingly investing in physical security

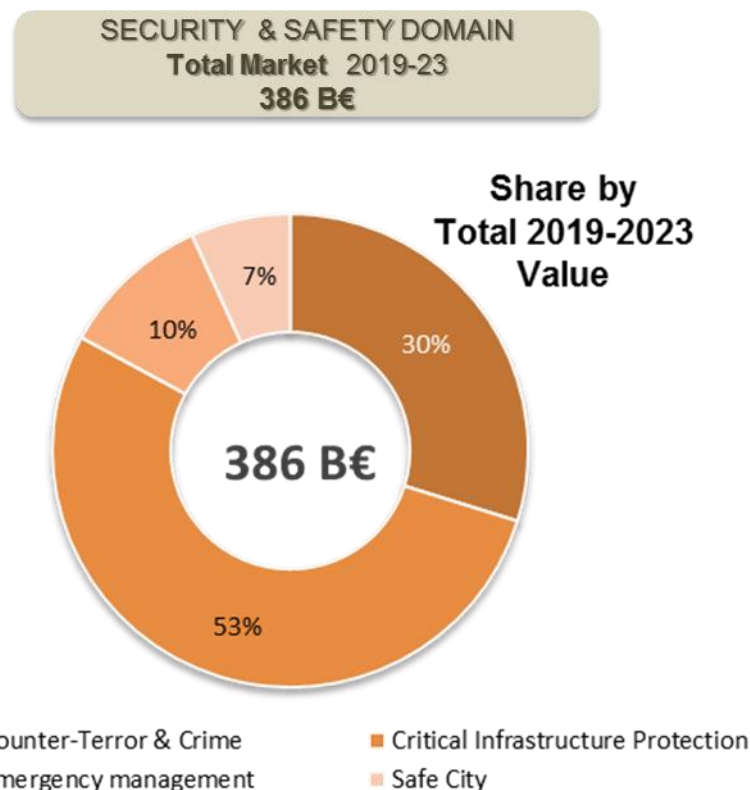
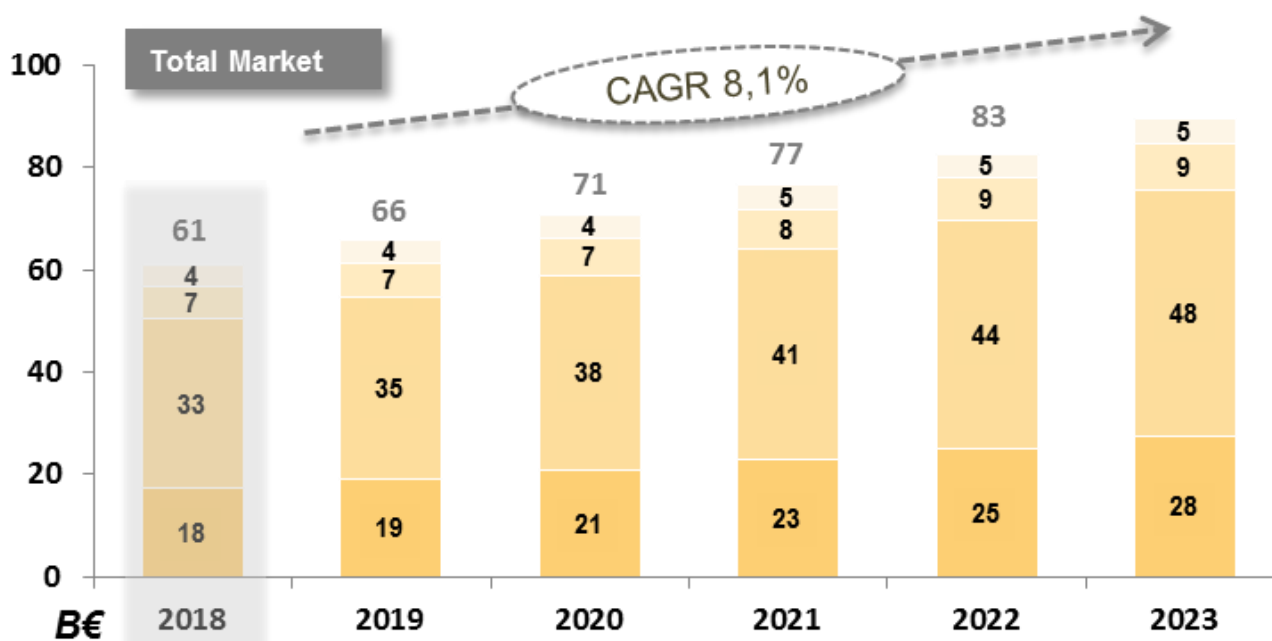


Figure 1 - Security Market Value – Total Market split by domain

The global CIP market exhibits a profitable growth potential for the next five years. In the past, the systems and networks of the infrastructure elements were logically and physically independent. They had little interaction or connection with each other or other sectors of the infrastructure. With advancement in technology, the structures within each division became automated, and interlinked through computers and infrastructures facilities.

All critical infrastructures are nowadays highly dependent on telecommunications such as public telephone network, the internet, or it may be wired or wireless networks. So, it is proven that the market is doing a huge investment on IT and smart grid technology, which is driving the growth in the CIP market.



	CAGR 2019-23	Total
<b>SECURITY</b>		<b>8,1%</b>
Safe City		3,2%
Emergency Mngt		7,1%
<b>Critical Infrastructure Protection</b>		<b>8,0%</b>
Count Terror & Crime		9,5%

Figure 2 - Security Market Value – split by domain

The overall Security and Safety solutions market is split across 4 main segments:

- **CIP** is the largest segment both in terms of total and target market. In this segment, in the medium to long term we will see as main trend the convergence between physical and cyber security solutions as addressed by RESISTO.
- **Counter Terror & Crime** Total Market is characterized by the growing demand for C3I solutions and the availability of interoperable solutions (Hybrid Tetra / LTE platform).
- **Emergency management** Total Market is growing also due to technologies not addressed by RESISTO (geo spatial, ...), while the target market is conditioned by the availability of *ad-hoc* command and control solutions and broadband comms
- **Safe City** is a relatively new market, rapidly growing as cities are just beyond deploying video surveillance infrastructure. It could offer good opportunities conditioned to the ability to provide situational awareness solutions, leveraging advance analytics and security concepts

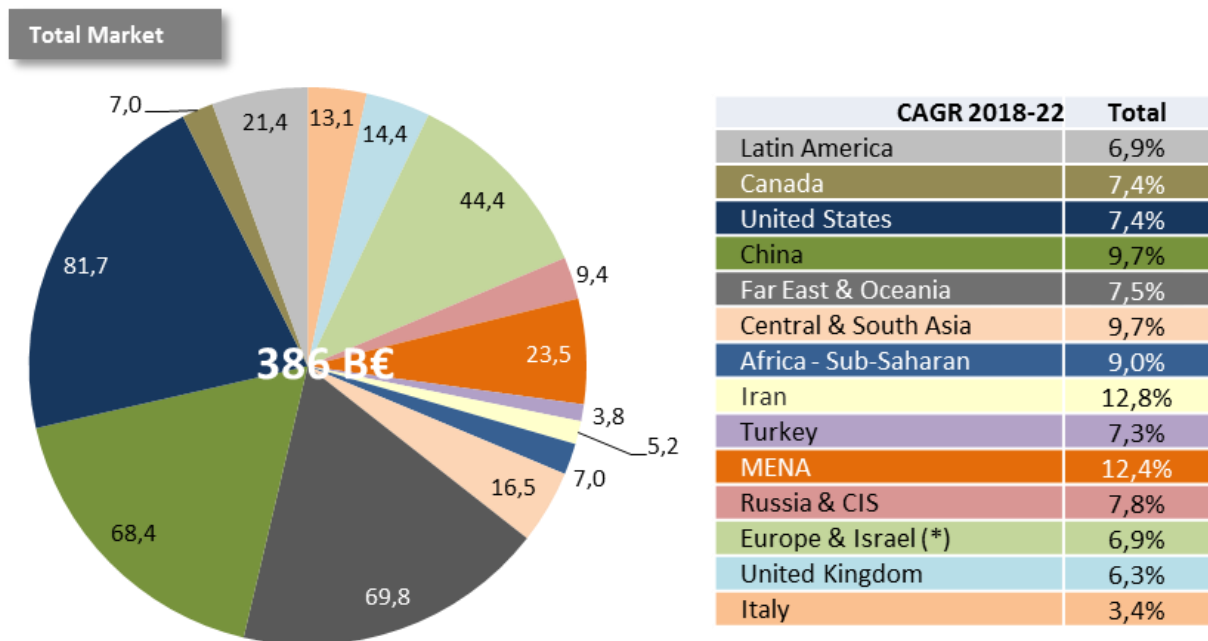


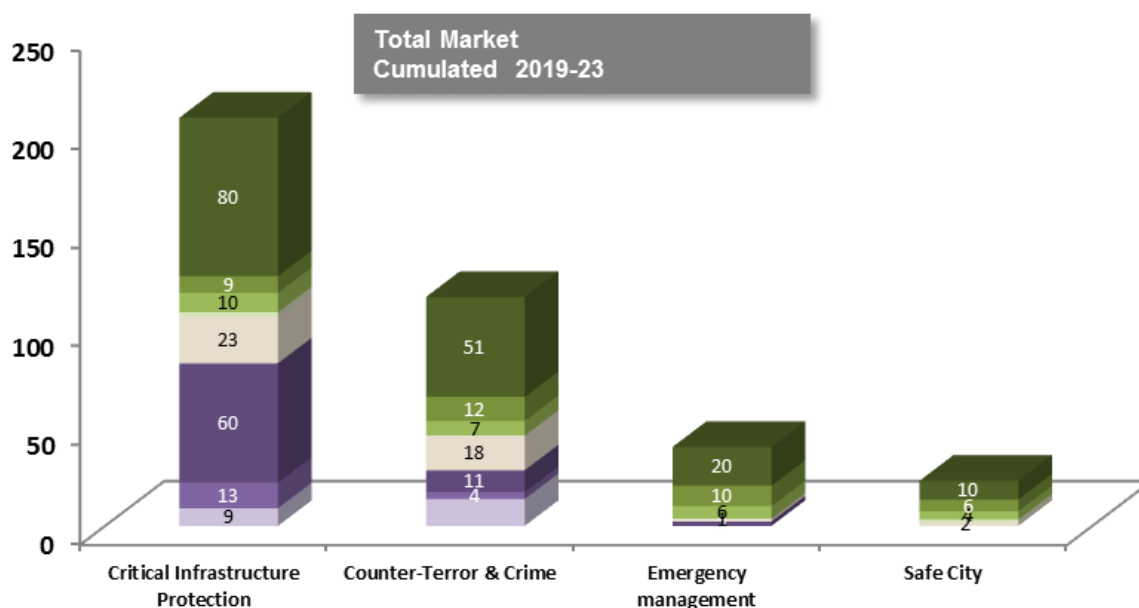
Figure 3 - Security Market Value – split by geographic areas (\*) NATO and European Commission/ Agencies markets are included in Europe and Israel Region estimations

The market split by geography sees the highest CAGR in the MENA Region, China, Central and South Asia as well as Africa. Europe (plus UK and Italy) accounts for almost 19% of the total market and sees a 7% CAGR in the period. Given the geographical footprint of the companies involved in RESISTO project we expect Europe to be the main market for the RESISTO solution at least in the first stage.

The following chart provides a split by technology for each Security and Safety solutions market segment:

- **Critical Information System** market is driven by the growing digitalization
- **Cyber security & Intelligence** Market will continue to grow focusing on diagnostics, mitigation and prediction, threat intelligence and the protection of critical infrastructures; target market can be further extended leveraging on deep learning and AI technologies

- **Transportation Technologies & Solutions** market is projected to grow due to an increasing demand for advanced vehicle-related IT systems, secure comms , automated fleet management, cloud-based data analytics and autonomous vehicle technologies
- **Control Room** Total Market is driven by technology integration and system interoperability, increasing value placed on "big data" and analytics, and C2 consolidation; Target mkt growth is linked to the availability of customizations addressing end users' SOPs
- **Professional Comms** Total Market is driven by digital LMR and, in the long term, by broadband networks, with a growing seamlessly interoperable networks' demand
- **Integrated Solutions** represent a significant share of the market and are addressed by system integrators who leverage on proprietary products and integrator of third parties' systems and components.
- **Services for Homeland Security&Critical Infrastructures (HSCI)** is expected to steadily to grow focusing mainly on managed security services and consultancy



CAGR 2018-23	Total
Critical Information System	7,0%
Intelligence	13,9%
Cyber Security	12,5%
Services for HSCI	9,7%
Transportation Technologies & Solutions	2,2%
Professional Comms	7,5%
Control Rooms	7,1%
Integrated Security Solutions (including sensors)	5,7%

Figure 4 - Total Market Value (CIP segment details)



Within the Critical Infrastructure Protection segment Cybersecurity and Integrated Security solutions represent the lion's share of the market, followed by Services. RESISTO technologies (in red in the table above) cover 89% of the CI protection market.

RESISTO as cyber-physical CI protection platform is well position to exploit this market segment.

### 3. RESISTO BUSINESS PLANNING

The CI protection market is mainly driven by the need for:

- 1) Increased Situational awareness and response capabilities
- 2) Ability to defence from physical and logical (and combination of) attacks
- 3) Operational efficiency flexibility
- 4) Communications for speed response

The main Key Success Factors for the market are:

- a) Unified security platform for a complete security picture and incident response management
- b) Integrated security governance solutions (incident management, workflow management...) for physical and cybersecurity
- c) Control room consolidation and integration with legacy systems, use of managed security services and use of data sharing and advance analytics fro increased situation awareness
- d) Communication for speed response: Interoperability (i.e Hybrid Tetra/LTE platform) - High speed connectivity (broadband solutions) - Common Operating Picture (wearable devices/IoT)



Figure 5 - Market Drivers and KSFs

All key success factors are addressed by the RESISTO platform that is aimed at providing a solution for Communication Infrastructure providing holistic (cyber/physical) situation awareness and enhanced resilience to minimize impacts from both physical and cyber-attacks. RESISTO an integrated governance solution leveraging on data sharing and advanced analytics to detect attacks/threats to take the best countermeasures and reactive actions. For this reason RESISTO is in a good position to exploit the CI Protection Market described in chapter 2.

But Recent world drivers, impacting the TLC operator market, confirm and add new reasons to market RESISTO solution: the speeded-up deployment of 5G commercial networks across Europe and the strong push toward digitalization even more reinforced by the COVID-19 pandemic emergency.

5G is expected to add significant revenues to commercial TLC operators enabling valuable benefits to users. Unfortunately, part of the population perceives a hidden risk on health from 5G. on April 2020 UK experienced something like 40 attacks from arsonists to mobile phone masts claiming even a link

between 5G technology and coronavirus<sup>1</sup>. The numerous base stations spread over even dispersed country areas are easy targets for any malicious protester. RESISTO platform may be usefully deployed to reduce frequency and impact of such attacks by providing a physical security and effective counteractions to device failures by automatically rerouting traffic.

Cyber security of 5G network is also an area where RESISTO can provide great value. TLC cyber-attacks remain a relevant issue worldwide that are going to grow in a 5G context taking into account the frequent attacks and associated economic impact for companies and states. This is confirmed in recent studies as for example the one from Harvard University<sup>2</sup> where IPR issues may cost in the range of \$180 billion to as high as \$540 billion per year to industry and governments.

Concerns about the cybersecurity of 5G have also been raised within the European Community. In the "EU Coordinated Risk Assessment of the CyberSecurity of 5G networks<sup>3</sup>" from NIS cooperation group the European Agency for Cybersecurity outlines that *"The security of 5G networks is and will be a top priority in the years to come as they will form the future backbone of our societies and economies, connecting billions of objects and systems, including in critical sectors such as energy, transport, banking, and health, as well as industrial control systems carrying sensitive information and supporting safety systems"*.

The recent COVID-19 pandemic is also expected to have an impact on the market. In macroeconomic terms initial impact globally is expected to be profound and produce a contraction on global GDP and economic recession comparable with the great Depression. The following table provides a preliminary estimation of the impact on GDP growth

#### *IHS Markit Global Economics Alert, April 2020*

##### *Real GDP Growth: Preliminary April Forecast*

	2018	2019	2020	2021	2022	2023
<b>World</b>	<b>3.2</b>	<b>2.6</b>	<b>-2.6</b>	<b>3.9</b>	<b>3.5</b>	<b>2.8</b>
United States	2.9	2.3	-5.4	6.3	4.0	1.6
Canada	2.0	1.6	-5.5	4.9	3.3	1.9
Eurozone	1.9	1.2	-4.5	1.2	1.7	1.4
United Kingdom	1.3	1.4	-4.3	0.8	1.5	1.5
China	6.7	6.1	2.0	6.3	5.6	5.4
Japan	0.3	0.7	-2.5	1.2	0.8	0.8
India*	6.2	4.9	2.1	5.7	6.9	7.6
Brazil	1.3	1.1	-4.5	3.5	3.2	2.2
Russia	2.2	1.1	-3.6	0.8	2.0	1.8

Figure 6 - Real GDP growth April 2020 Forecast

The timing of a decisive rebound in the economy, will come only with medical progress in identifying and containing the spread of the virus, treating illness more effectively, and increasing immunity. In the European zone (the main market for RESISTO) recession in 2020 will be significantly deeper than during the global financial crisis of 2008. This may represent a threat to the CI protection market due also to the high pressure on government budget that may divert resources and delay investments. But COVID-19 is also expected to act as strong booster for digitalization with acceleration of fundamental shift

<sup>1</sup> <https://www.businessinsider.com/attacks-cellphone-towers-coronavirus-5g-conspiracy-2020-4?r=US&IR=T>

<sup>2</sup> Harvard University, Confronting China's Efforts to Steal Defense Information, Jeffrey B. Jones, May 2020

<sup>3</sup> <https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security>

towards tele – service (first of all tele-medicine) an tele-work, increasing use of on line collaboration tools and moves towards cloud based control room technology. To this respect the potential market contraction of the 2020 that may also impact CI protection investments is expected to be counter balanced by increasing need of digitalization and resilience of communication infrastructures enabling those services.

In light of the overall market value for CI protection outlined in chapter 2.2 and the drivers outlined above, taking into consideration that geographical footprint of the project (Europe) the RESISTO Consortium has drafted a preliminary business plan. Under the Hypothesis to start to market the RESISTO solution in 2021, given an overall Market value of CI Protection around 44B\$ Worldwide, with average CAGR 8,1%, an addressable market (based on geographical foot print: Europe, Italy and UK and associated relevant technologies) around 3B\$, a 120M€ revenues over 5 years may be expected that accounts for approximatively 0.8% of the addressable market. Considering typical financial figures from RESISTO companies a 20% net profit is achievable corresponding to 24M€ cumulated over 5 years. Break even is expected by mid 2022.

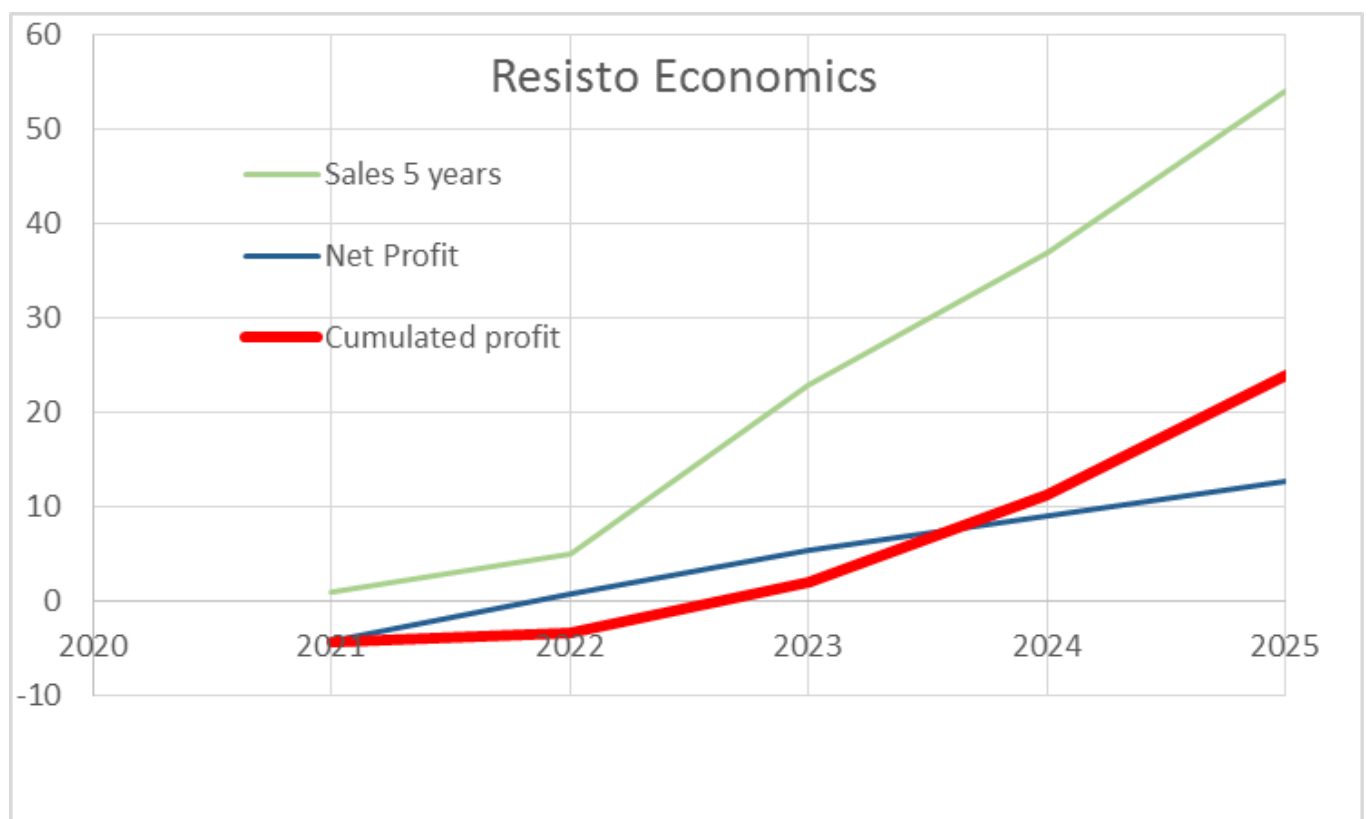


Figure 7 - RESISTO Draft Business plan

Such data have to be enforced by proper go to market strategy and implementation of appropriate business models.

### 3.1 RESISTO Business Model

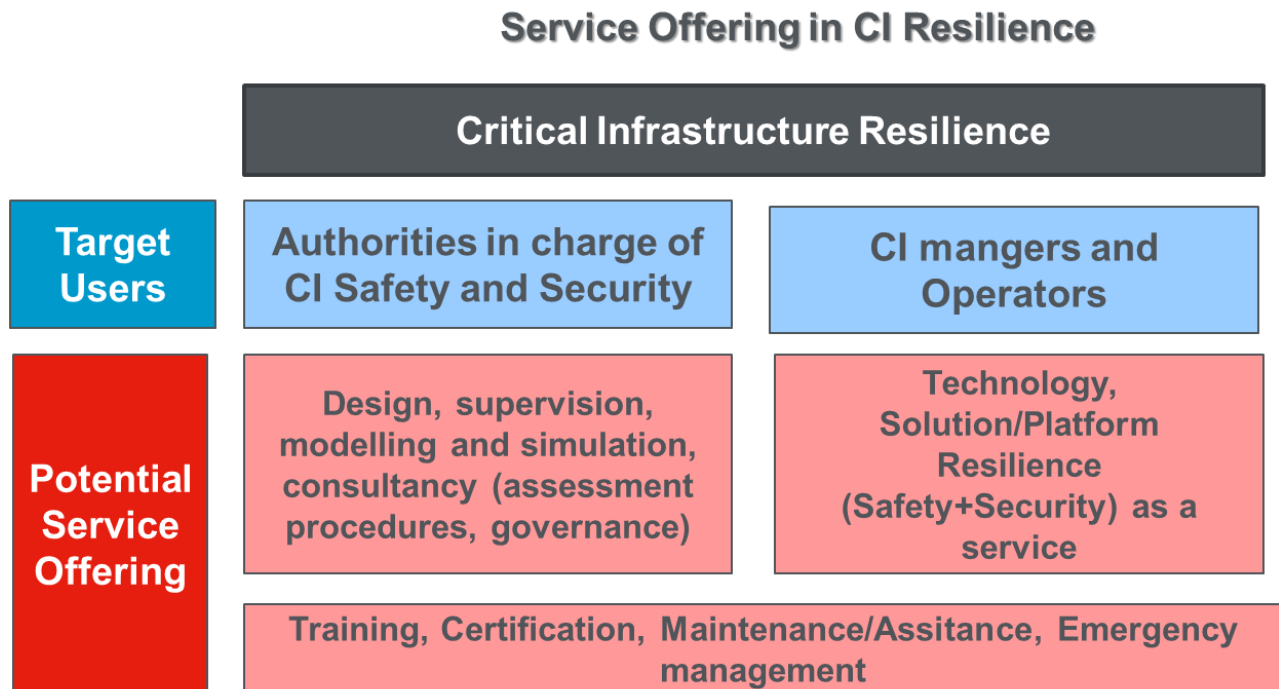


Figure 8 - RESISTO Service Offering

RESISTO Target Users can be split in two classes

- CI managers and operators (B2B) mainly Telco/Communication Operators but also other CI operators (managed security services)
- Authorities in charge of CI Safety and Security (B2G) since protection of CI sites involves also National Governments and local institutions

The potential service offering can be split in three areas:

- Pre sales services
- Technology, Platform and Resilience as service
- Post sales services

As already outlined in D10.10 The most appropriate business models for the RESISTO platform identified at this stage are:

- **The system integrator business model:** Under this kind of model Large Enterprises like LDO and TEI, can provide RESISTO platform as a scalable solution/system customized on the end-user. This kind of model requires a close cooperation between experts in risk modelling and resilience design (i.e. RM3, EMI, BSS) technology providers (GT, INT, ADI) and LE/system integrators (LDO and TEI) that have to take the lead to promote RESISTO Framework to potential customers starting from the end user in the consortium like TIM, BT, OTE ORO, RTV). The profit of this kind of model is high for high end (complex) solutions over large systems.

- **The resilience as a service business model.** Telco operators already provide managed security services to their customers. RESISTO platform may be adopted by Telco operators (like TIM, BT, OTE ORO, RTV) to extend or reinforce their offering targeting their CI customers and largely leveraging on their customer intimacy. Large Enterprises with expertise in managed services like TEI, and CI protection may embrace this business model as well.
- **The service business model.** This kind of business model includes consultancy service, design service, supervision service, training service, maintenance service. It is expected that consultancy, design and training services will be sold as part of the solution (to this regard the Cisia Pro tool and the modelling approach from EMI can be very powerful) while supervision and maintenance services can be sold long after the delivery of the system. The profit of this kind of business model is higher in % compared to the previous model due to reduced investment required (mainly opex cost). The partner in the best position to exploit this business model are the Large Enterprises with expertise in the field of CI protection security management, like LDO and TEI; and managed security services providers like the telco operators (TIM, BT, OTE ORO, RTV).

### 3.2 RESISTO Go-to-market strategy

**Go-to-market strategy** - Major drivers for selling the RESISTO platform to the market are

- the ability to improve detection reaction and mitigation capabilities of the communication operators
- In face of complex cyber-physical attacks the ability to improve decision making process, leading to a more efficient selection and use of countermeasure and mitigation
- the ability to increase overall infrastructure resilience

The main obstacle to RESISTO adoption relies in the need to integrate data from many different domains (cyber and physical), typically managed by different department in the same organization, implying the need to review also company processes and responsibilities.

In the third year, leveraging on the validation trials within the project and the adoption of the RESISTO framework within the EU PCP Broadway project (see chapter 3.1) as a reference, RESISTO platform will be proposed to a number of telco operators starting from the ones in the consortium and CI operators (leveraging on the customer base of the Les: LDO and TEI). In order to make the process more effective

- 1) each telco end user in the consortium has been requested to identify a PoC (i.e. Security dep. Responsible) in the company that can assess the platform in technical terms and has the power to allocate budget (or influence budget allocation) on RESISTO platform acquisition. The trials will be exploited as much as possible to support the technical assessment
- 2) all the partners have been requested to suggest potential customers, outside the consortium, both in the field of telco operators and from other Cis. Also in this case is considered key to identify a PoC in the company that can assess the platform in technical terms and has the power to allocate budget (or influence budget allocation) on RESISTO platform acquisition. Where applicable/feasible the potential customer will be invited to assist the trials. The possibility of an ad-hoc trial, currently outside the scope of Resisto project, will be in case evaluated by the consortium members

In order to facilitate the meetings a “marketing kit” composed of a whitepaper on RESISTO (value proposition, architecture, features and references) and an on-line demo of the platform will be made available. In the following the update Value proposition.



## 4. EXPLOITATION PLAN UPDATE

The exploitation has been performed twofold: within the partners through developing a joint proposition to the market promoting the RESISTO platform as a whole (or self-consistent parts of it), like in the case of the EU Broadway<sup>4</sup> project, and at individual partner level, exploiting RESISTO as a way to market specific components, networking with partners and potential customers

### 4.1 Exploitation – consortium

The PCP (Pre-Commercial Procurement) Broadway project<sup>4</sup>, started in May 2018, is a H2020 EU funded project (Grant Agreement No. 786912) with the aim to procure innovation activity to enable a pan-European broadband mobile system for use by our public safety responders.

The BroadWay project team consists of 11 procurers from 11 European countries comprised of national ministries and agencies responsible for communication services used by 1.4 Million public safety responders across Europe. ASTRID, the operator of the TETRA network used by the Belgian emergency and security services, is acting as the lead procurer

The pre-commercial procurement process consists of three phases: solution design, prototype development and field testing (see graphic below). Each stage is subject to a new tender for selection of the best proposals among the winners of the previous stage. The total procurement budget for BroadWay is approximately 9.1 Million Euros.

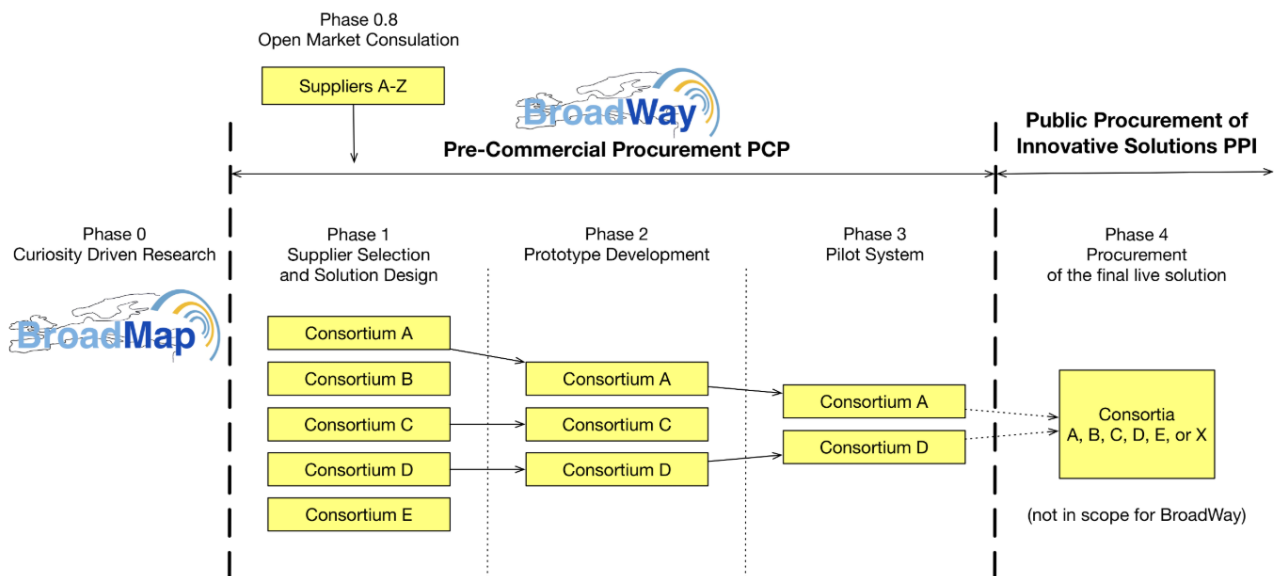


Figure 9 – Broadway project phases

Leonardo as leader of PPDR4Europe, one of the 4 consortia admitted to phase 1 (solution design), has successfully passed the stage and has submitted its proposal for phase 2 prototype development.

<sup>4</sup> <https://www.broadway-info.eu/>

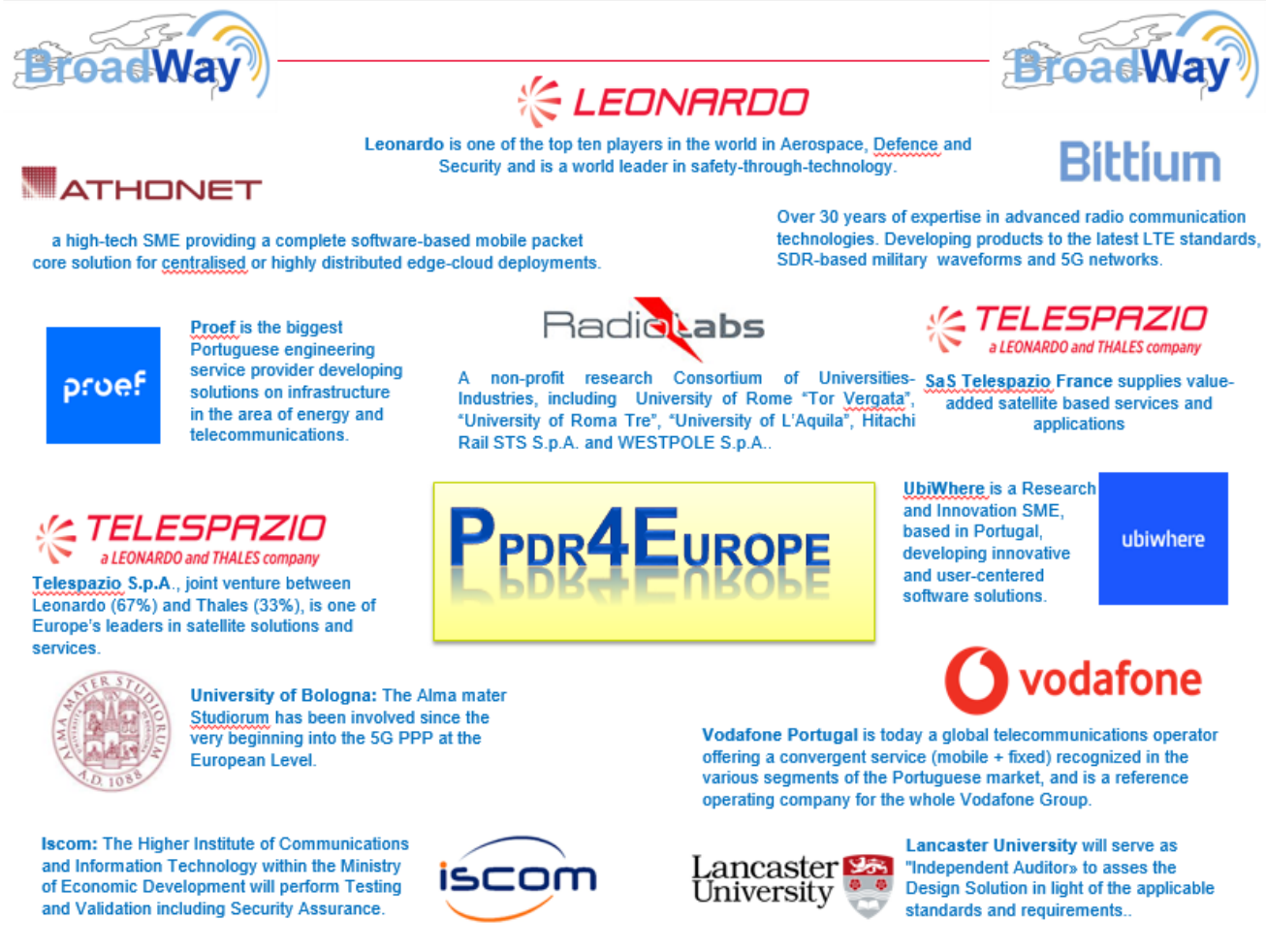


Figure 10 - Ppdr4Europe consortium

In PPDR4Europe proposal for stage 2 the security of Broadway architecture (SpiceNET) is addressed exploiting the RESISTO framework. If, at the end of June 2020, the PPDR4Europe proposal will be awarded the contract for the prototype development, RESISTO will be part of the prototype for SpiceNET and a demonstration if the framework will be performed within the following 12 months providing an important reference for RESISTO.



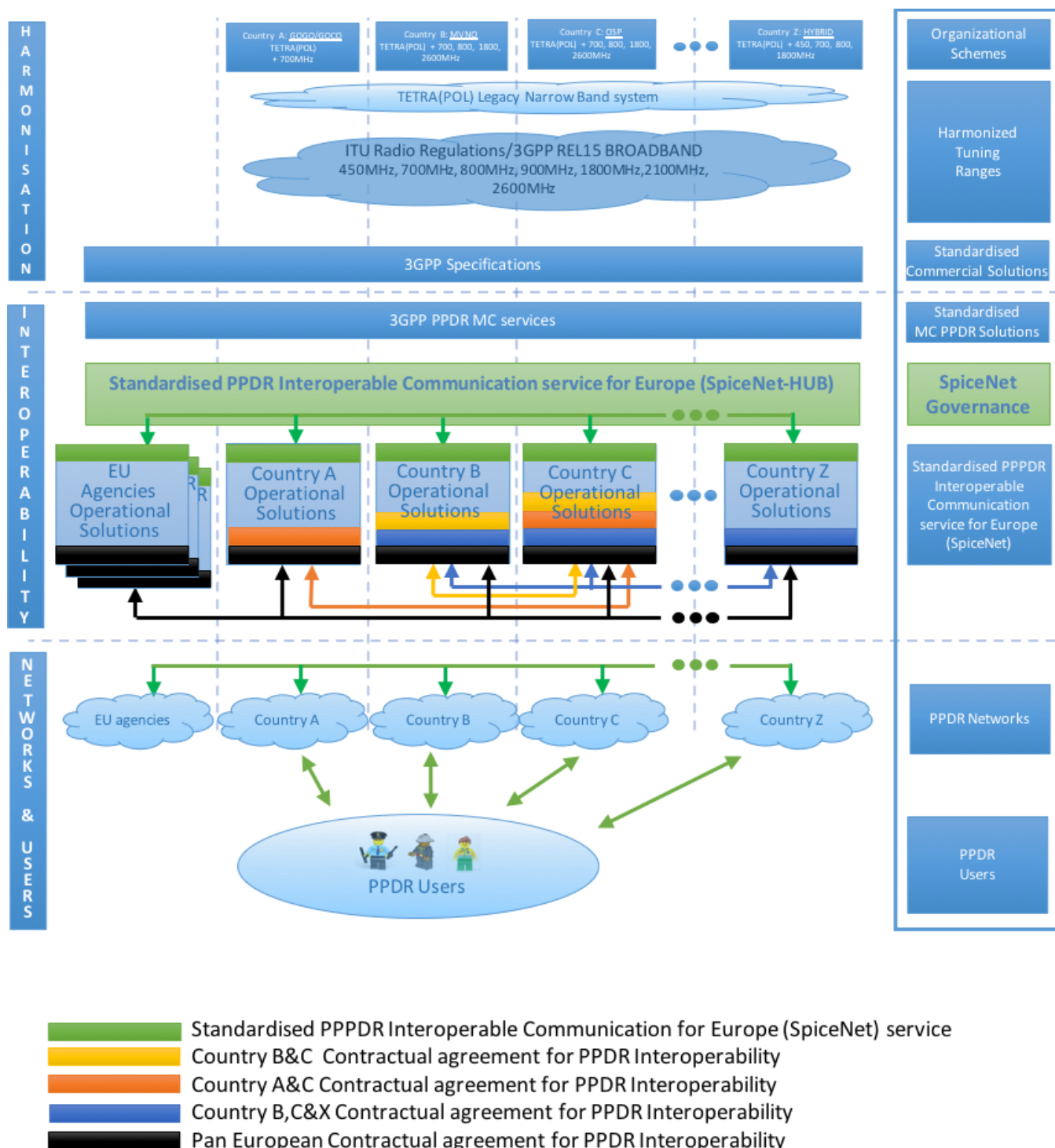


Figure 11 - Broadway SpiceNET architecture

## 4.2 Exploitation – individual partner

Exploitation of RESISTO at individual partner level is intended as a way to market specific components, networking with partners and potential customers

Individual exploitation plan are split in two groups: LEs/SMEs/RTOs whose main target is to leverage on RESISTO to develop technology, skills and capabilities, establish relations with potential commercial partners and customers, build reference in the field of CI protection, and Telco operators that to the above mentioned target add the opportunity to test RESISTO solutions in their existing and future platforms promoting their image of innovative and “resilient” companies.

In order monitor individual exploitation progress compared to original exploitation plans defined in D10.11 a set of KPIs (number of meetings with customers, number of follow-ups, average feedback, number of customers engaged) have been defined and monitored

The following table summarizes the results achieved in the second year. Due to the COVID-19 pandemic the activity has been slowed down this year (with postponement of physical meetings and the need to convert to on-line meetings where possible) and in order to ensure proper exploitation a

P.	Individual Exploitation Plan UPDATE for LEs/SMEs/RTOs	Action performed and KPIs
1 · L D O	<p>LDO exploitation plan aims reinforcing its position in the national and international CI market establishing links with a number of potential customers and partners. Thys strategy encompasses the following steps:</p> <ul style="list-style-type: none"> <li>- Propose the RESISTO solution (or a part of it) in other new funded and research projects</li> <li>- Leonardo is already involved in other projects financed on the subject of resilience, in these cases the objective is to pool the knowledge and needs of the various programs to face them with a unified strategy.</li> <li>- Involve the LDO commercial and marketing functions to acquire customers and propose the system both on the market and in the Leonardo environment which is large and complex.</li> <li>- The Business plan of the Cyber division of LDO cites the objective of integrating solutions for physical security with solutions for Cyber security; the RESISTO system represents a good starting point for this type of solutions.</li> <li>- For customers who already use Leonardo solutions for physical <b>or</b> cyber security, try offering the physical <b>and</b> cyber solution.</li> <li>- Leonardo is engaged on the 5G front. RESISTO, in particular with the part of Orchestrator and SVN, is able to manage the security of the 5G infrastructure, this feature can be proposed into LDO 5G project initiatives</li> </ul> <p>Leonardo is committed to coordinating the exploitation activity of the entire RESISTO consortium with the aim of pursuing a common, coordinated and efficient strategy to maximize the result</p>	<p>A number of meetings have been arranged with customers from the CI market to introduce RESISTO and Leonard technologies (SSC2 ad Cyber Securty platform)</p> <p>KPIS #Nbr of meeting: 6 #Nbr of follow ups: 3 #Average feedback from customers: 3/5 #Interest in experimenting the technology: 4/5</p>
2 · R M 3	<p>Over the last years, RM3 research group has been appointed as consultant for CIP and CIIP activities by several industrial and governmental entities thus acquiring a valuable knowledge about mechanisms and architectures of actual CIs both at national and European level. RM3 will exploit RESISTO results and contacts with end-users to further develop its consultancy services in the field of CIP and risk management. At this stage, RM3 also envisions the possibility to develop an industrial product based on CisiaPro, through the collaboration with Leonardo and other partners in the project. The Orchestrator tool might be improved, in cooperation with Leonardo and Ericsson. It might be made customizable and might become the basis of a product.</p>	<p>RM3 exploits the results of the RESISTO project, in its three main activities (i.e., training, research, and technology transfer). At training level, RM3 exploits both the outcomes and the methodologies adopted in the RESISTO project to improve and update the content of university courses. Topics related to RESISTO are also being exploited in the Roma TRE Ph.D program and in the several master and bachelor theses that have been carried out during the RESISTO project.</p> <p>At research level, RM3 exploits the results of RESISTO in scientific publications.</p> <p>Thanks to RESISTO, RM3 is investigating the</p>

		<p>potentiality of collaborations with industrial partners for further improvement of components and algorithms. CISIApro 2.0 has been improved during the RESISTO project and we are developing consultancy services in the field of CIP.</p> <p>KPIs:                      #nbr of courses: 2                      #nbr of PhD students: 2</p>
9 · T E I	<p>TEI is involved in developing Mobile Telecommunication infrastructure with a strong commitment on 5G evolution. RESISTO results in the field of security of telecom systems and of SDN and NFV in particular will be exploited in the development and extension of future TEI telecom infrastructure product portfolio. The Emergency Warning Communication Function validated in RESISTO will be exploited within the mission critical communication market. The collaboration with Leonard is seen as a great opportunity to this aim.</p>	<p>ETI activity has been delayed and further impacted by the pandemic crisis in 2020. A recovery plan is underway</p>
1 1 · E M I	<p>Fraunhofer EMI cooperates with leading industrial companies. The planning, supporting and disaster management tools developed and adapted by Fraunhofer EMI to the Communication CI domain will be exploited both to reinforce and extend cooperation with industrial companies in the field of CIP and to enhance its IP (Intellectual Property) knowledge portfolio.</p>	<p>Many efforts into improving Fraunhofer EMI's resilience tools have been completed. This tool will extend cooperation with industrial companies and partners. Currently, potential reuse of the tools in the context of new research proposals is planned. RESISTO and Fraunhofer EMI's contributions have been introduced through conference papers and presentations.</p> <p>KPIs:                      # of (web) meetings: 3                      #of papers (published and accepted): 4</p>
1 2 · I C C S	<p>RESISTO will give ICCS the opportunity to improve its position in scientific fields of anomaly detection, radio networks, 5G, sensors and signal processing. ICCS will exploit project results by pursuing patents applications, creating new research links, establishing further research collaborations within national and European projects, participating in exhibitions and related events, exploiting its connections with the Hellenic Public/Private Security Sector and Regulatory Bodies. It will give the opportunity to employ skilled researchers and PhD students contributing to further high-tech jobs creation on cutting-edge research topics.</p>	n.a.
1 3 · B U W	<p>Project results have been and will be included in the safety engineering curricula of the university, especially in the courses „Organization and Communication in Crisis Management“ and „Principles of Crisis Management“. It is assumed that the participation will strengthen the competencies of the institute in EU and international crisis management R&amp;D.</p>	n.a.
1 5 · I N T	<p>Through RESISTO, INT will have the opportunity to reinforce its leading position in the satellite spectrum monitoring market, offering commercial cellular spectrum protection tools and also addressing new business models from being a provider of complete packages towards offering pluggable RF simulation and measurement components. Another appealing opportunity generated in RESISTO for INT, will be the collaboration with industrial IoT sensor providers to offer a firmware reliability solution for use cases requiring secure sensors.</p>	<p>Several meetings have been held with cellular network operators to introduce the features and capabilities of the cellular spectrum protection tools developed by INT within RESISTO.</p> <p>KPIs                      #Nbr of meeting: 4                      #Nbr of follow ups: 2                      #Average feedback from customers: 3/5                      #Interest in experimenting the technology: 4/5</p>
1 6 · G T	<p>GT is the largest industrial blockchain platform provider, offering KSI technology that enables massive scale data authentication without reliance on centralized trust authorities. GT is KSI technology provider to TEI and other telecommunication providers and partner in industrial blockchain commercialization. Through developing a KSI-based solution and linking it with the RESISTO platform, GT expects to get in touch with a number of new potential customers in the Telco sector and to promote its solution in the CI cyber protection market exploiting new</p>	<p>Telecom sector analysis performed for the company.</p>

	commercialization opportunities.	
1 7 . A D I	<p>ADI has already began to exploit RESISTO results with reference to its solutions for video analysis and UAV detection with key stakeholders in Cypriot market and other areas where ADI operates (e.g. Balkans and Middle East): Cyprus Telecommunication Providers, in particular with Cyprus Telecommunications Authority (CYTA) with which ADI has a successful collaboration track; Office of Electronic Communications &amp; Postal Regulations (OCECPR), ENISA national contact point of ENISA. ADI is developing a plan in promoting RESISTO to the Cyprus Research Promotion Foundation, coordinator of the EEN Cyprus that is expected to offer collaboration and commercialization possibilities and potential joint ventures. These collaborations are expected after the finalization of the project.</p> <p>ADI is exploring a potential collaboration with META Group. META has already supported more than 800 research projects throughout Europe to do this, through EU-supported initiatives like the Common Exploitation Booster, the IP Booster and Support Services for Exploitation of Research Results (SSERR). Recently, META Group won the "Impact Booster" a 4-year European Commission contract worth €12 million to boost impact arising from EU research projects.</p>	<p>A number of meetings have been arranged with stakeholders within the domain of physical security in Cyprus: G4S, Cyprus Telecommunications Authority (CYTA), Marina Ayia Napa-Cyprus. Introduction to RESISTO with emphasis on video analytics has been given. Follow up discussion will be scheduled for demonstration of ADITESS RESISTO related test bed.</p> <p>KPIS #Nbr of meeting: 3</p>
1 9 . B S S	<p>BSS goal is to promote RESISTO platform to business customers that are operating Critical Infrastructures. BSS plans to use and engage its offensive, defensive and intelligence capabilities combining them with operations and innovative functionalities brought by integrating RESISTO ecosystem within its customers' CIs systems. In this way BSS will develop new services for customers until this point not accessible.</p>	<p>A number of meetings with potential end users for RESISTO have been arranged from Romania, in defense and energy sector. Moreover, some of the existing customers were contacted to propose using the Responsible Disclosure Framework (RDF) in a 12 months-POC.</p> <p>KPIS: #No. of meetings: 5 #No. of emails: 10 #No. of follow-ups: 5 #No. of potential companies to use RDF as a POC for 12 months: minimum 10</p>

Table 1 Individual Exploitation Plan for RESISTO LEs/SMEs/RTOS

P.	Individual Exploitations and/or Potential Adoption Plan (short description) for End Users	Action performed and KPIs
3 . T I M	<p>TIM, being an international infrastructure operator and TLC-ICT service provider, has an interest in exploiting RESISTO's results internally and in the market. RESISTO solutions will be proposed towards Network internal lines with the aim of improving security and with a clear positive impact on its image. TIM would like to exploit RESISTO also in the offer of 5G services (e.g. 5G for Italy) with consequent extension of its portfolio of managed security services, in this perspective TIM intends to test the services resisto, at some of its customers, during the development of the project, in order to identify with greater precision the market tags and consequent direction of the development.</p>	<p>TIM has organized, and is organizing, several meetings both with internal structures and with potential customers, to introduce TIM and Leonardo's RESISTO technologies.</p> <p>KPIS #Internal meeting #Nbr: 05 #Nbr of external meeting: 03 #Average customer feedback: 4/5 #Interested in experimenting technology: 4/5</p>
4 . O T E	<p>Based upon technical and market-led priorities, OTE aims to exploit RESISTO results into its existing and future network/service solutions, thus strengthening customers' confidence and enhancing its competence in the field of telecommunication networks security. OTE intends to promote a policy that will be beneficial for the company, also within the broader Deutsche Telekom Group. The RESISTO's results will also help to design and promote new business models</p>	<p>A number of meetings have been arranged within OTE group of companies. In the meeting experts mainly from cyber security domain participated. Also associates from corporate activities participated in one of the meetings. RESISTO concept was presented.</p> <p>KPIS #Nbr of meeting: 3/5 #Average feedback from customers: 2/5 #Interest in experimenting the technology: under discussion from security experts.</p>

		Waiting for the outcomes of the pilots
5 · B T C	BTC expects to incorporate the project results in evolved and extended versions of its unified Cyber Security Platform (CSP). CSP is used to implement its own cyber self-protection and as a basis for managed Cyber Security Operations Centre services for major public and private sector customers.	<p>BTC RESISTO researchers continued to share their knowledge and progress with other BT teams and brainstormed how and where RESISTO outcome could be tested and evaluated. Meetings held with BT security platform and SOC team architects and managers; with BT TV research teams and BT TV operation architects. Their requirements have been considered when BTC built RESISTO testbed/use case. Also worked with BTC research exploitation team on exploitation/dissemination plans including showcase RESISTO in next BT research innovation week (delayed to 2021 due to Covid-19). RESISTO is also in line with BTC self-healing system/network automation programme. A plan to incorporate RESISTO solutions for SDN/NFVs will be further developed in the coming months.</p> <p>KPIs:          6+ meetings          Two presentations to senior managers          Two evaluation/trials leads.</p>
6 · O R O	ORO will promote RESISTO platform as a service towards the business customers operating CIs such as utility (water, gas, energy) providers in line with ORO cyber security strategy and ORO cyber security solutions portfolio including the Security Operation Center (SOC) and security solutions for Industrial Control and Metering Systems. RESISTO innovative functionalities will be integrated in ORO SOC. ORO will also promote RESISTO at France Telecom group level	<p>During the first Quarter of the RESISTO Project timeline, in anticipation to the Requirements definition process, ORO has extended to several Critical Infrastructure Operators from Romania, an inquiry form on their perception of resilience as a holistic processes, their approach to physical and cyber security and their means, methods and technologies used for risk assessment and mitigations. The inquiries were sent to C.I. operators across the country, from various Infrastructure areas such as Water, Electricity and Gas distribution, Rail and Road Transport, Financial and Banking and Public Institutions. Their responses were normalized and aggregated and requirements for a C.I. Risk and Resilience enhancement platform were extrapolated, processed and further integrated in the Requirements Definition process of RESISTO, by ORO's Contribution. This process anticipates the specific needs of various C.I. verticals as regards to Risk and Resilience processes and paves the way for a more targeted approach on the exploitation of the RESISTO platform to other C.I. verticals, communications. Thanks to this inquires based initial step we also benchmarked the interest of other C.I. operators to engage in extensive validation of a relevant use case for C.I protection (TRL 7). Part of the exploitation plans ORO will focus on validating RESISTO components in a scenario with two C.I ecosystems (one belonging to ORO) where the effects will be cascaded. Following the validation, ORO will be able to Go To Market with a new managed security services capability, addressing in particular the business users that operates C.I. such as water, gas or energy utilities</p>

		<p>infrastructures, but also other private and public sector organizations, thus enabling a progressive adoption path for the RESISTO platform.</p> <p>KPIs</p> <ul style="list-style-type: none"> <li>• Number of inquiries sent to C.I. operators in Romania: 15</li> <li>• Number of collected and processed answers to inquiries sent to C.I. operators in Romania: 3</li> <li>• Number of C.I. operators accepting to engage into an extensive validation based on RESISTO platform: 1</li> <li>• Potential of improving the current managed security services offer for C.I. organizations: YES</li> </ul>
7 · R T V	RTV will exploit RESISTO to set up a platform to protect its internal infrastructures and RTV's Maritime critical infrastructure to enhance its resilience. Moreover in full synergy with 5G City project RTV will exploit RESISTO results to secure the LTE-PPDR virtual slicing system to provide to the Mission Critical market the most secure and performant broadband connectivity service.	n.a.
8 · A L B	ALB will exploit RESISTO results by assessing and eventually integrating the expected enhancements provided by RESISTO in services and products provided by Altice Labs, especially in cyber/physical security scenarios. Altice Labs will leverage on RESISTO results to prepare the transition to the next generation of the product portfolio, in particular those products with a potential to be deployed in a 5G environment (e.g. OSS/BSS, access & transport network solutions). In addition, RESISTO use cases to be developed by ALB will be incorporated in the Aveiro 5G experimentation facility, thus enriching the breadth of the 5G pilot and strengthening the competences of ALB in emerging technological domains, based on 5G and network virtualization	<p>The following target KPIs can be defined in relation to services potentially leveraging on innovations developed and demonstrated in the framework of the RESISTO pilot:</p> <ul style="list-style-type: none"> <li>- Number of ALB products candidate to be evolved or adapted to 5G &gt; 2</li> </ul> <p>Number of ALB services candidate to be evolved or adapted to 5G &gt; 2</p>

Table 2 **Individual Exploitation Plan and/or Potential Adoption Plan for End Users**



## 5. INNOVATION MANAGEMENT – UPDATE

As part of the the innovation management process we report here the current key potential innovation elements characterising the RESISTO platform, comparing them with the updated technological State of the Art [SoTA] and putting in evidence their more distinguishing features.

Among the key innovation elements the Responsible Disclosure Framework – RDF proposed by BSS has been added as it features an unique settlement process to provide guarantees about reports to identify and patch security vulnerabilities that looks very innovative and promising.

### 5.1 Cyber-physical Risk/Resilience assessment of Communication infrastructure

**State Of The Art:** Risk analysis and management according to ISO 31000 is best practice and applied in various variations and terminologies to critical infrastructure to improve critical infrastructure protection in Europe<sup>5</sup>. A step further is to distinguish basic event rates, conditional vulnerability given an event occurs and again damage, e.g. as propagated by FEMA<sup>6</sup>. This is a step forward, since it shows that there are several time-ordered and logically depending steps till the final damage manifests and hence also the risk. Currently, several EU-projects aim at deriving resilience management standards for critical infrastructure: DARWIN, IMPROVER, RESILENS, RESOLUTE, SmartResilience, and SMR. RESISTO's joint risk and resilience analytical approach starts out from efforts in the context of RESILIENS<sup>7</sup> and German national project on measuring technical resilience<sup>8</sup>. The approach draws on a rich experience of Fraunhofer EMI of implementing (quantitative) risk, resilience and safety management approaches to new domains, e.g.: countering terrorism<sup>9</sup>, urban security assessment and improvement supported with methods<sup>10</sup>, applied knowledge in the (functional) safety domain<sup>11</sup>.

**Progress Beyond State Of The Art:** RESISTO develops an analytical risk and resilience analysis approach and a related software tool covering cyber and physical integrated threats on (key) system performance function level to assess the overall risk taking into account all resilience dimensions. This goes beyond the segregated perspectives of existing standards. Within RESISTO modern best practices for a specific domain are collected as benchmark for effective and efficient risk control and resilience enhancement. **Progress update:** a nine-step risk and resilience management process has been developed for the communication infrastructure according to the plan. This included collecting necessary inputs from the end-users and adapting software tools to the needs of RESISTO. The progress is described in the reports of WP3, in particular see D3.2 “Risk and resilience management process for cyber-physical threats of telecom CI” for an introduction of the risk and resilience management process and D3.9 “Analytical security assessment application to use cases and their refinement” for a demonstration of first results based on the RESISTO use cases.

### 5.2 Holistic System Modelling and interdependency simulation analysis for Risk Predictor

**State Of The Art with respect to performance degradation modelling and simulation.** The approach followed covers the time-dependent analysis of interdependencies of different system layers and level such as Physics, Cyber, Logic and Geographic, modelling infrastructure on an abstract level. The CISI Apro simulator<sup>12</sup> (Critical Infrastructure Simulation by Interdependent Agents) analyzes the effects

<sup>5</sup> <http://publications.jrc.ec.europa.eu/repository/bitstream/JRC96623/lbna27332enn.pdf>

<sup>6</sup> <https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf>

<sup>7</sup> E. Bellini, N. Martyn, T. Kovalenko, M. Kitsak, G. Vogelbacher, K. Ross, U. Bergerhausen, K. Barker, I. Linkov, In: Resilience and Risk: Methods and Application in Environment, Cyber and Social Domains, Eds.: I. Linkov, J. M. Palma-Oliveira, 2017, pp. 21-80, <http://www.springer.com/de/book/9789402411225>; Quantification of resilience for resilience engineering of socio-technical systems, I. Häring, S. Ebenhöch, A. Stolz, European Journal for Security Research, Volume 1, Issue 1, pp. 21-58, <http://link.springer.com/article/10.1007/s41125-015-0001-x>

<sup>8</sup> I. Häring, J. Scheidereiter, S. Ebenhöch, D.J. Schott and L.M. Reindl, S. Köhler, J. Bordoy, C. Schindelhauer, H. Scheithauer, S. Kaufmann, ESREL 2017, Eds.: M. Cepin, R. Bris, pp. 1069-1079, 2017 <https://doi.org/10.1201/9781315210469-136>

<sup>9</sup> K. Fischer, I. Häring, W. Riedel, G. Vogelbacher, S. Hiermaier, International Journal of Protective Structures, Volume 7, Issue 1, pp. 45-76, 2016, <http://prs.sagepub.com/content/7/1/45.short?rss=1&source=mfr>

<sup>10</sup> C. A. Schoppe, I. Häring, U. Siebold, ESREL 2013, Eds.: R.D.J.M. Steenbergen, P.H.A.J.M. van Gelder, S. Miraglia, et al., pp. 1411-1418, <http://www.crcpress.com/product/isbn/9781138001237>

<sup>11</sup> U. Siebold, M. Larisch and I. Häring, 15. ITG/GMA-Fachtagung, Eds.: ITG, GMM, AMA., pp. 737-741, <http://www.vde-verlag.de/proceedings-de/453260131.html>

<sup>12</sup> <http://cisiapro.dia.uniroma3.it/>

of failure both in terms of faults propagation and with respect to performance degradation and effects of mitigation, in particular response and recovery. Currently such abstract models are not directly linked with models with higher resolution that allow to predictively assess the effect of natural and man-made physical but also cyber threats. Existing physical damage models or investigations for telecommunications subsystems cover, e.g., seismic<sup>13</sup>, heavy storm<sup>14</sup>, ice rain<sup>15</sup> but also (terroristic) explosive loading<sup>16</sup>, impact<sup>17</sup> and flooding. Possible effects of drones are known<sup>18</sup>, also shelling occurred in similar cases<sup>19</sup> but are respectively much less investigated. By now tools with drag and drop capability exist that allow for the assessment regarding, e.g. explosive and seismic threats. The CAESAR simulator analyses cascading effects in interconnected networks (e.g. water, power, communication) and provides resilience quantification methods for the evaluated networks.

Several works reviewed the proposed approaches for modeling interdependencies among critical infrastructures.<sup>2021</sup> In literature, there are three main methodologies for the modeling approaches of critical infrastructures: agent-based simulation, input-output analysis, and network modeling. In literature, it is also possible to find heterogeneous and/or unclassified approaches.<sup>22</sup>

The agent-based simulations consider each infrastructure as complex adaptive systems, composed of agents representing single aspects in the infrastructure itself. The main advantage of agent-based simulation is the ability to arise synergistic behaviors when agents are starting to interact together.<sup>23</sup>

The second approach is based on the Input-Output economic analysis introduced by Leontief but then adapted to study the effect of interdependencies on the inoperability of interconnected networked systems by Haines and Jiang. The main advantage of their approach (called Input-Output Inoperability Model – IIM) and its improvements is related to the simplicity and flexibility of the proposed approach. Usually, IIM is limited to the economic costs of interdependencies.<sup>24</sup>

In the last years, researchers explored new approaches for modeling infrastructure interdependencies. The most promising approach is based on graph and network theory. The main advantage is to exploit closed-form expressions and numerical simulations to characterize their topology, performance, and uncertainty.

**Progress Beyond State Of The Art:** RESISTO will use models and engineering-simulations to refine and develop telecommunication subsystem damage and resilience behaviour models sufficient for predictive assessment regarding critical risks as put forward by the sample cases, in particular out of the set (terroristic) explosions, effects of drones, impact, cyber induced effects, and seismic. It starts out with existing structural model inventories adding typical nodes and edges of Telecommunication CI, e.g. sending masts, ground stations, backbone-components.

**Progress update:** CISIApro 2.0 has several innovative features respect to other Interdependency simulators:

1. CISIApro 2.0 can operate in a distributed model, with only minimal sharing of information, retaining a shared vision of the overall system.
2. CISIApro 2.0 can manage cyber threats details and can more precisely assess the impact of cyber-attacks on physical infrastructures.

<sup>13</sup> K. K. Sharma, S.K. Duggal, D. K. Singh, A.K. Sachan, Civil Engineering and Urban Planning: An International Journal (CIVEJ) vol.2, no.3 (2015), pp. 13-31.

<sup>14</sup> G. Ghodrati Amiri, Computers and Structures, vol. 80, no. 03, (2002), pp. 349-364, <http://www.sciencedirect.com/science/article/pii/S0045794901001754>

<sup>15</sup> N.D. Mulherin, Cold Regions Science and Technology, vol. 27, no. 2 (1998), pp. 91-104, <http://www.sciencedirect.com/science/article/pii/S0165232X97000256>

<sup>16</sup> Mark G. Stewart, Michael D. Netherton, David V. Rosowsky, Natural Hazards Review, vol. 7, no. 3 (2006), pp. 114-122, [http://ascelibrary.org/doi/abs/10.1061/\(ASCE\)1527-6988\(2006\)7:3\(114\)](http://ascelibrary.org/doi/abs/10.1061/(ASCE)1527-6988(2006)7:3(114))

<sup>17</sup> C. U. Penalba, New Orleans Structures Congress (1999), <https://ind.tn.org/view.aspx?id=511641>

<sup>18</sup> See e.g.: [http://www.business-standard.com/article/news-ians/interpol-warns-of-drone-attacks-by-terrorists-on-critical-infrastructures-117021400178\\_1.html](http://www.business-standard.com/article/news-ians/interpol-warns-of-drone-attacks-by-terrorists-on-critical-infrastructures-117021400178_1.html)

<sup>19</sup> Eusgeld, I., D. Henzi, and W. Kröger. 2008. "Comparative evaluation of modeling and simulation techniques for interdependent critical infrastructures". Scientific Report, Laboratory for Safety Analysis, ETH Zurich: 6-8.

<sup>20</sup> Ouyang, M. 2014. "Review on modeling and simulation of interdependent critical infrastructure systems". Reliability engineering & Systems safety. 121: 43-60

<sup>21</sup> Gopalakrishnan, K. and S. Peeta. 2010. Sustainable and resilient critical infrastructure systems: simulation, modeling, and intelligent engineering. Springer.

<sup>22</sup> Rinaldi, S. M., J. P. Peerenboom, and T. K. Kelly. 2001. "Identifying, understanding, and analyzing critical infrastructure interdependencies". IEEE control systems magazine. 21(6): 11-25

<sup>24</sup> Haines, Y. Y. and P. Jiang. 2001. "Leontief-based model of risk in complex interconnected infrastructures". Journal of Infrastructure systems. 7(1): 1-12



3. CISIApro 2.0 is fast enough to work on nearly real time connected to SCADA control centres to gather the actual situation on the physical components of the infrastructure.
4. CISIApro 2.0 evaluates services, as key metrics to be displayed to operators. Services are aggregated value for vital components, metrics already used by operators such as the number of supplied customers or related to Service Level Agreement with other infrastructures.
5. CISIApro 2.0 can implement detailed telecommunication networks, in terms of routing and services.

### 5.3 Cyber-Physical correlation

**State Of The Art:** Most TLC enterprises have a SOC (Security Operation Centre) for the logical protection of the infrastructure and different systems (CCTV, Access control, Intrusion detection, biometrics etc.) for the physical security management and, in some cases, a PSIM (Physical Security Information Management) the integration platform for a single monitoring and control centre. So, risk and threat scenarios as well as solutions for the protection of two domains are well known and implemented. In each domains the systems or platforms for the protection include specific modules for the correlation of information: cyber security uses this approach to improve significantly the detection of anomalies and attacks; one of main characteristics of PSIM systems is the correlation capability to integrate data from various systems in order to automatically identify situations and then gradually update those situations<sup>25</sup>.

**Progress Beyond State Of The Art:** The RESISTO platform adopts the approach of information correlation to data coming from two fields traditionally separated; besides the correlator will apply the deterministic pattern-matching algorithm to detect a specific threat situation and the not deterministic techniques (Artificial Neural Networks e.g.) to update incrementally the rules and thresholds on the basis of data collected from the ICT systems and the sensors/systems for its physical security. This allows for early detection of a new class of threats (i.e. an employee entering a room with restricted access – physical- and then logging into a high security system with non-personal credentials – logical) combining physical and logical means so far largely underestimated and normally seen as disjoined. **Progress Update:** An important objective of the RESISTO project is the unification of physical security management and cyber security management. For the event correlation part, a normalization of all events (field events, sub-system events, etc.) has been provided in a common format. This made it possible to unify their type of processing. Consequently, it was possible to make correlations regardless of the source and the type of event triggered (both physical and cyber).

The correlation of events was carried out using a suitably configured CEP (Complex Event processor).

The configuration of the CEP required a study concerning the detection of anomalous and dangerous situations for the system, starting from events (physical and cyber) that taken individually would not have given rise to concern, but if detected in anomalous numbers or in correspondence with other significant events, can generate suspicion of danger and therefore are notified to the operator in the form of alarms. In addition to the CEP which is based on deterministic rules, RESISTO makes extensive use of Deep Learning which uses appropriately trained artificial neural networks to detect events of particular interest that would not be detectable by correlation rules. In particular, this technique was used to detect anomalous traffic situations on communication networks by exploiting operating information through SNMP. Events detected through neural networks can in turn be correlated with other events through the correlator. The unification between the vision of Cyber and physical security has also required the use of a common operator interface (HMI), both at the application level and at the level of schematization of resources and event sources., Alarm management allows to independently manage cyber, physical and combined alarms (cyber + physical).

25 Frost&Sullivan "Analysis of the Worldwide Physical Security Information Management Market" M683-11 November 2010

Also countermeasures applicable through workflows follow this concept. The innovative approach consists precisely in considering the problems with a single paradigm so as to be able to better manage border situations and those that involve a double countermeasure that is managed by a single person (or team) who takes care of all aspects in an integrated and contemporary approach.

## 5.4 Software Defined Security

**State Of The Art:** The SDN architecture with its separation of data and control plane from network devices drastically simplifies configuration and management of security policies, with significant reduction of security risks associated to policy inconsistency. On the other hand, the main SDN benefits pave the road to new attacks exploiting the vulnerabilities associate to softwarization and centralized control. Since OpenFlow is the most diffuse protocol for SDN implementation and deployment, research on SDN security mostly addressed OpenFlow based solutions. Recently, based on the softwarization trend that is pervading every element of a communication network, as witnessed by the reference documents published by 5G-PPP and NGMN Alliance, the Software Defined Security (SDS) paradigm has been introduced. Among the SDS solution we cite Catbird<sup>26</sup>, OneControl<sup>27</sup> and OpenSec<sup>28</sup>. Solution proposed in literature have been focus on cybersecurity. The SDS paradigm is being successfully experimented by RM3 and LDO in the H2020 Atena project (www.atena-h2020.eu).

**Progress Beyond State Of The Art:** One major progress beyond the state of the art proposed by RESISTO is the extension of the SDS architNecture in order to manage virtualization of both cyber and physical security. Concerning physical security virtualization it essentially applies to the logical controllers of physical security mechanisms involving programmable devices (e.g. video surveillance, electronic access control). The major difference between the ATENA and the RESISTO consists in the number of nodes and in the variety of security functions to be virtualized being ATENA simpler in terms of both nodes and functions. Thus the progress beyond the state of art will concern scalability of the solution, policy management, inclusion in the virtualized functions of those related to physical security as well as of those security functions related to wireless channels, with emphasis to functions pertaining to Physical and Logical Link layers, Radio Resource management and Mobility Management. In addition, the SDS architecture will be extended in order to fully support 5G communications, slicing and multi-tenant solutions included. **Progress Update** The SDS approach, that is exploited nowadays in literature, has been improved and may be adapted to different communication scenarios. The analysis performed during the design of the SDS component of RESISTO lead us to conclude that the use of SDS may increase the possibility to effectively cope with the security challenges of a complex attack scenario. It will lead to further improvements in the upcoming telecommunication systems with the progressive use of SDN / NFV based systems which will allow faster and more effective reaction on systems, automatically or by even non-specialized operator through high-level orchestrator interfaces that hide the complexity of the underlying network.

The resilient routing algorithm proposed in RESISTO represents a meaningful improvement of the SDS framework. As a matter of fact, the SDS orchestrator will be able to perform intelligent re-routing based on the traffic requirements and constraints, accounting for modern threats to virtualization that cannot be addressed otherwise. It is worth to note that the proposed algorithm represents an approach to routing that can be used to address the problem of NFV placing and NS prototyping, a challenge for which no well accepted, automated solution is to this date available. This represent a strategic function for 5G slicing, that could otherwise be reliant on static NS prototypes, with all the associated lack of flexibility and resiliency to network conditions. Furthermore, the nature of multi-objective optimization allows for upgradability thorough the inclusion of novel constraints and that could arise in the future.

<sup>26</sup> "Private cloud security, a catbird white paper," Catbird Networks, Inc, white paper, 2014.

<sup>27</sup> "Netcitadels onecontrol platform the key to intelligent, adaptive network security," NetCitadel, Inc, white paper, 2012.

<sup>28</sup> A. Lara, B. Ramamurthy, "OpenSec: Policy-Based Security Using Software-Defined Networking", IEEE Trans. On Network And Service Management, Vol.13, No.1, March 2016

## 5.5 Innovative secure IoT for physical security

**State Of The Art:** Industrial IoT nodes today present varying and sparse security functions not fully integrated with datalinks and are not widely used in telecom infrastructure protection<sup>29</sup>. Some IoT-specific networks such as those of LPWAN class enjoy inherent security characteristics (e.g. transmit-receive decoupling in SIGFOX), but a complete security solution still does not exist due to interoperability, cost or complexity-avoidance reasons. Several recent attacks have raised concerns about the overall security of IoT and its adequacy for industrial contexts<sup>30</sup>. There exist solutions such as Pelion IoT Platform for secure device management but for firmware provisioning they rely on PKI infrastructure where certificate validation can be compromised.

When it comes to cellular IMSI-catcher and smart jamming detection, no permanent smart spectrum surveillance capability is commonly deployed at telecom radio sites today. For smart jamming detection, there are available solutions such as Spectrum-NET, VMWare Uhana and VIAVI monitoring solutions but they are generally based on spectrum analysers and also require integration with the network equipment. Apart from these solutions, only specialised radio surveillance missions are activated when significant interference is (indirectly) detected through network equipment monitoring. Specialised companies contracted ad-hoc perform radio surveys using normally expensive portable instruments, which is both expensive and useless in case of purposely planned, elusive radio threats which can be executed with extremely low cost hardware and limited knowledge thanks to today SDR equipment and related software frameworks<sup>31</sup>. In order to detect IMSI-catcher threats, the solutions whether business (e.g.:FirstPoint Mobile Guard) or consumer-grade (e.g.:Android IMSI Catcher Detector) are only focused on the device protection but not taking into account the RAN network perspective.

Lastly, regarding the protection of the telecom node physical assets, a WIDS (Wireless Intrusion Detection System) - Bastille Networks, Extreme AirDefense,...- can improve physical security by detecting unauthorized devices and threats. However, it is essential that the solution is not excessively complex and can be integrated with the rest of the operator's network to be protected.

**Progress Beyond State Of The Art (updated):** INT will develop a solution for secure IoT sensors firmware provisioning and management. The IoT node features that will be secured will include a full lifecycle handling of security functions: firmware/keys provisioning, protection of data (at-rest and in-transfer), firmware integrity and updates check; authenticating in every step the peer interacting nodes. The key technological components of the sensor are a crypto-chip providing a secure execution and storage environment and a dual-link capability (LPWAN + BLE) able to operate in harsh environments and including a secure execution environment for crypto-key and software integrity protection. The key innovative feature of the solution for secure IoT sensors firmware, will be the use of KSI (Keyless Signature Infrastructure) on top of PKI to provide signing time reference for certificate verification, thus highly increasing the reliability of the IoT sensor firmware.

Moreover, within RESISTO two Smart Spectrum Surveillance innovative solutions will be developed by INT and integrated with the platform for telecom infrastructure protection. The first one, RANMONITOR, will be designed to offer detection and reporting of threats and attacks to 4G (LTE) Radio Access Network (RAN). These events include: Full band or partial band interference, Protocol-aware jamming and Rogue Base Stations (e.g. IMSI-catchers). RANMONITOR will bring an innovative approach by allowing to permanently monitor smart jamming or IMSI-catcher threats as it will be able to be easily integrated with the RAN node equipment or co-located. The other tool, RADIOFILTER, will offer passive detection, location and reporting of 802.11 WLAN (Wi-Fi) based threats and attacks events to Critical Infrastructures protected assets. These events include: Rogue Access Point (AP), Unauthorized device location, Unauthorized connections or Denial of Service (DoS). They key

<sup>29</sup> Strategic Principles for Securing the IOT; U.S. Department of Homeland Security

<sup>30</sup> Protecting operational technology from cyber-attacks <https://www.cgi.com/sites/default/files/white-papers/convergence-security.pdf>, last accessed 08/ 2017

<sup>31</sup> Shaik, A.; Seifert, J.; Borgonkar, R.; Asokan, N.; Niemi, V. Practical Attacks against Privacy and Availability in 4G/LTE Mobile Communication Systems. In Proceedings of the 23rd Annual Network and Distributed System Security Symposium (NDSS 2016), San Diego, CA, USA, 21–24 February 2016

innovative aspect to RADIOFILTER will be its modular and distributed nature based on secure sensors, along with the capability to integrate with an external platform (RESISTO) for physical/cyber threat correlation.

## 5.6 Audio and visual analytics

**State Of The Art:** Critical infrastructures are attractive targets for attacks by intruders with different hostile aims. Modern information and sensor technology provides abilities to detect such attacks. Video and Audio sensors are widely used in surveillance operations and protection of critical infrastructures. Intelligence algorithms are applied in audio and video streams with the focus on early threat detection at the perimeter of critical infrastructures.

Pattern recognition and machine learning techniques are used to extract acoustic events (i.e. gunshot, screaming, glass breaking) or to classify persons, vehicles and other objects that are moved within the controlled by the infrastructure area. Upon an event detection by analytics algorithms, a video clip is generated and delivered to the security operator. Security operator is notified with an alert about the suspicious activity and with important information about the event (location, etc.). This intelligent process reduces the effort of the operator by monitoring in a 24/7 base a huge number of sensors. Additionally, the early detection of events (real-time) and the ability to extract semantic information (i.e. type of event, illegal access in restricted area, location of the event) can provide useful data to event processing and correlation platforms for further analysis.

**Progress Beyond State Of The Art (updated):** In RESISTO, beyond the acoustic event detection, audio analytics are enhanced with techniques capable for localization of the source of the detected event. This feature can be used as an input to the video sources (CCTV) cameras in order to adjust the position to the source of the acoustic event. The surveillance systems with embedded audio and visual sensors, will be able to support the security staff at the facility to detect and respond to attacks from intruders at an early stage and thus the protection and surveillance of the perimeter of the facilities will be in focus to make it possible to give early warnings. The system will alert the operators (through cross-correlations of audio and video analysis) of threats carried out by different types of objects, (persons, vehicles, etc.). Eventually, these capabilities of warnings should be realized by state-of-the-art sensor solutions.

## 5.7 Responsible Disclosure Framework – RDF (NEW)

**State Of The Art:** Current Vulnerability Disclosure Frameworks focuses on large enterprises which has a tradition in Responsible Disclosure initiatives in order to identify and patch security vulnerabilities with the help of security specialists & researchers. Most frameworks provide a centralized environment in order to escrow relationships between security researchers and hackers and companies employees. Some of these frameworks also provide ways to track the security reports during their life cycles, starting from the first interaction up to the last, when the beneficiary of the report must decide what would be the reward for security specialist who reported the bug with limited ways to reward the specialist - hall of fame, swags or money.

**Progress Beyond State Of The Art:** In RESISTO, BSS is developing a fully-functional framework for Vulnerability Disclosure that has an unique settlement process to provide guarantees about reports, by using blockchain technology to confirm the report existence, vulnerability reported previously, report settlement status.

At the end, the RDF will embed a feature-rich Vulnerability Disclosure Framework within the main RESISTO framework combining innovative functionalities such as: the ability of the system to alert operators and to allow teams assignments to individual reports. Moreover, we will use cutting edge ML algorithms to group similar reports, which in return will ease the work of operators. Last, the RDF will feature a triage functionality that allows end-users to set a team which pre-check all the reports which will reduce the workload for production teams



## 6. IP MANAGEMENT PLAN UPDATE

The figure below describes the planning of the IP actions to perform during the project and the responsibility of each partner.

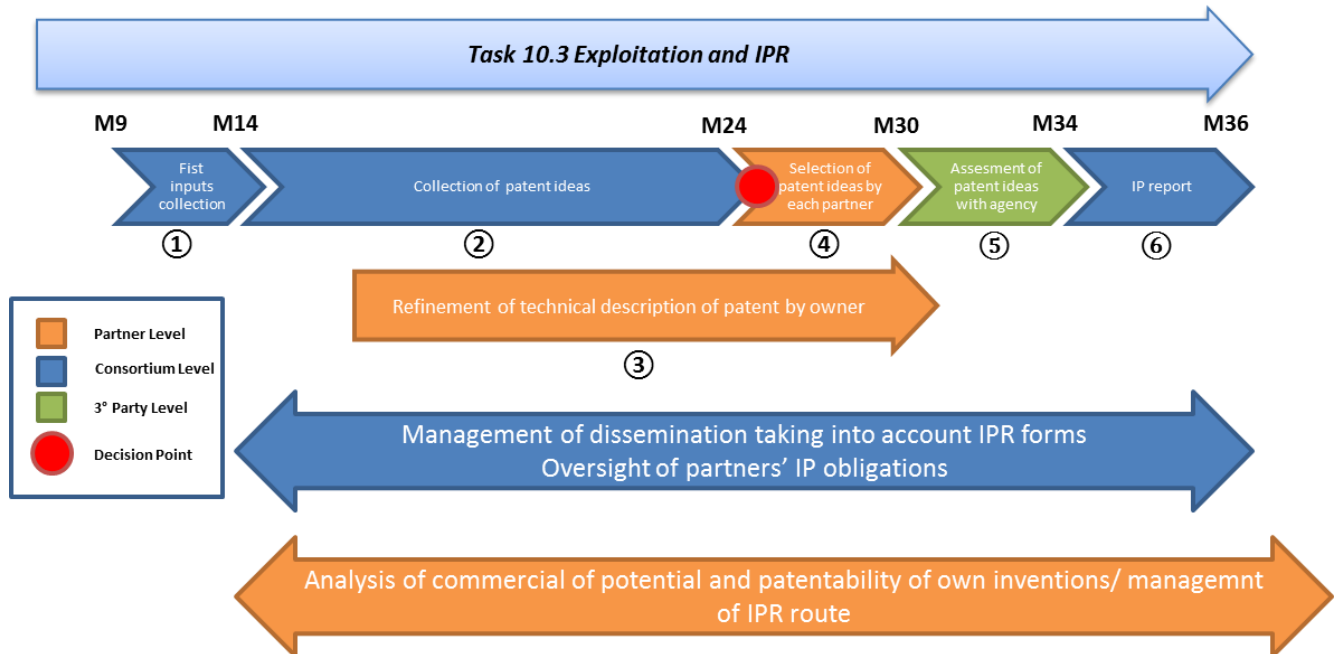


Figure 12 - IP management plan - original

According to the IP management plan at the end of the second year the project is expected to have provided a number of patent ideas for their following selection and review.

Despite the innovation potential of the project and its technological components, as discussed and acknowledged by the partner during the PMT in Sevilla in December 2019 (see Innovation Potential matrix below) when another innovation Area (Responsible Disclosure Framework – RDF) was introduced by BSS, no formal IPR form has been submitted so far.

#	Innovation Area	Innovation Potential
1	Cyber-physical Risk/Resilience assessment of Communication infrastructure	+++
2	Holistic System Modelling and interdependency simulation analysis for Risk Predictor	+++
3	Cyber-Physical correlation	+++
4	Software Defined Security	++
5	Blockchain for Data integrity	++
6	Machine Learning for Threat Intelligence	++
7	Airborne Threats (UAVs, drones) detection and tracking	+
8	Innovative secure IoT for physical security	+
9	Audio and video analytics	++
10	Emergency communications – Emergency Warning Communication Function	+
11	Responsible Disclosure Framework – RDF	++

Figure 13 - Innovation potential assessment per RESISTO technological element

In order to deal with the delay a recovery plan has been defined within WP10.

The recovery plan can be described as following:

2. M24-M28: Collections of patent ideas (IPR forms) phase will be extended by 4months (M28). In this period two meeting (end of third and fourth month) will be held involving all the partners and soliciting definition of innovative ideas both individually and at consortium level
3. M24-M28: Refinement by each innovation owner of technical description of innovation regarding innovation qualifiable to patent,.
4. M28-M34 Selection by innovation owner of IP agencies to assess the patentability of innovation according to worldwide innovation and patent panorama and Assessment of partners' innovations by IP agencies. Each IP agencies should provide a report which will be shared (entirely or partially) with the consortium.
5. M34-M36 Reporting by consortium of a consolidated report regarding the patentability of project innovations according to IP agency's reports.

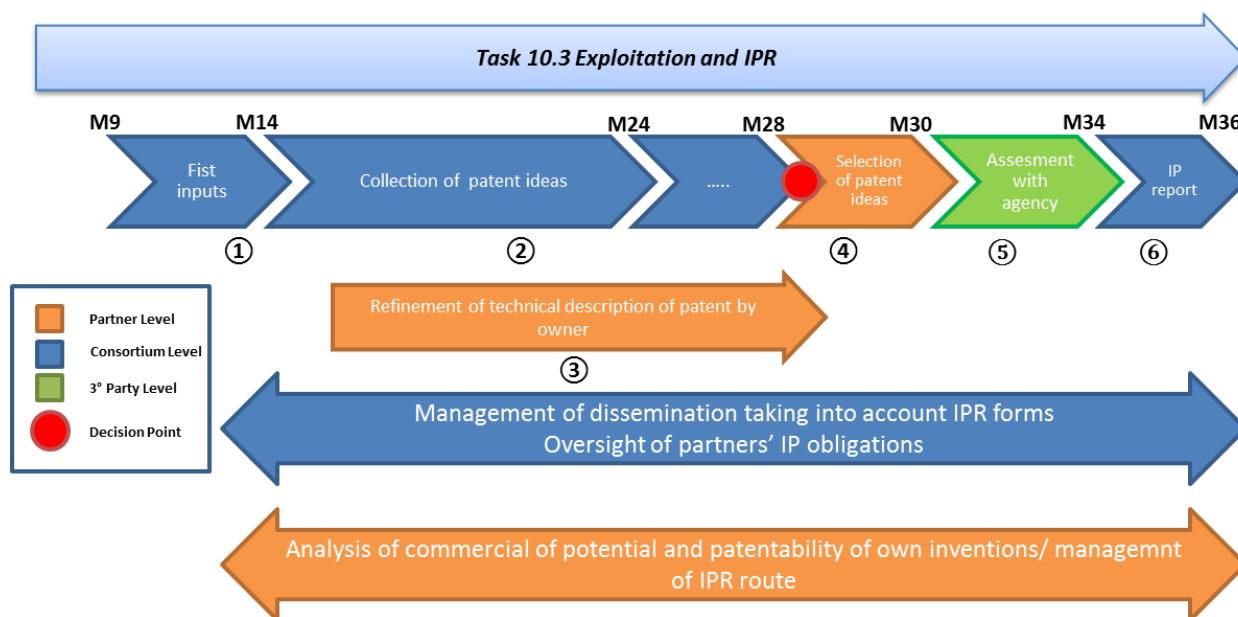


Figure 14 - IP management plan update



## 7. REFERENCES

INDEX	REFERENCE
[Ref1]	RESISTO – Grant Agreement. Project Starting Date: May, 1 <sup>st</sup> 2018
[Ref2]	RESISTO – D10.11 Exploitation Activities – second
[Ref3]	RESISTO – Consortium Agreement – V8.0
[Ref4]	RESISTO – D10.10 Exploitation Activities – first