

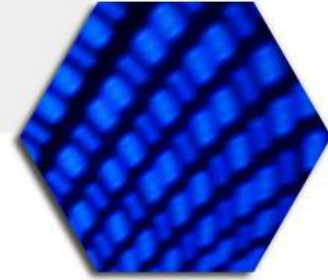


RESilience enhancement and risk control platform for communication infraSTructure Operators

RESISTO Kick off Meeting

RESISTO Project: WP, WP relations, Gantt, expected results

F. Frosali



RESISTO

- *3 years*
- *10M€ cost (8M€ funding)*
- *Validation across 3 Verticals: current, future and interdependent comms infrastructures*
- *Ambitious exploitation plan*

**RESilience enhancement and risk
control platform for
communication infraSTructure
Operators**



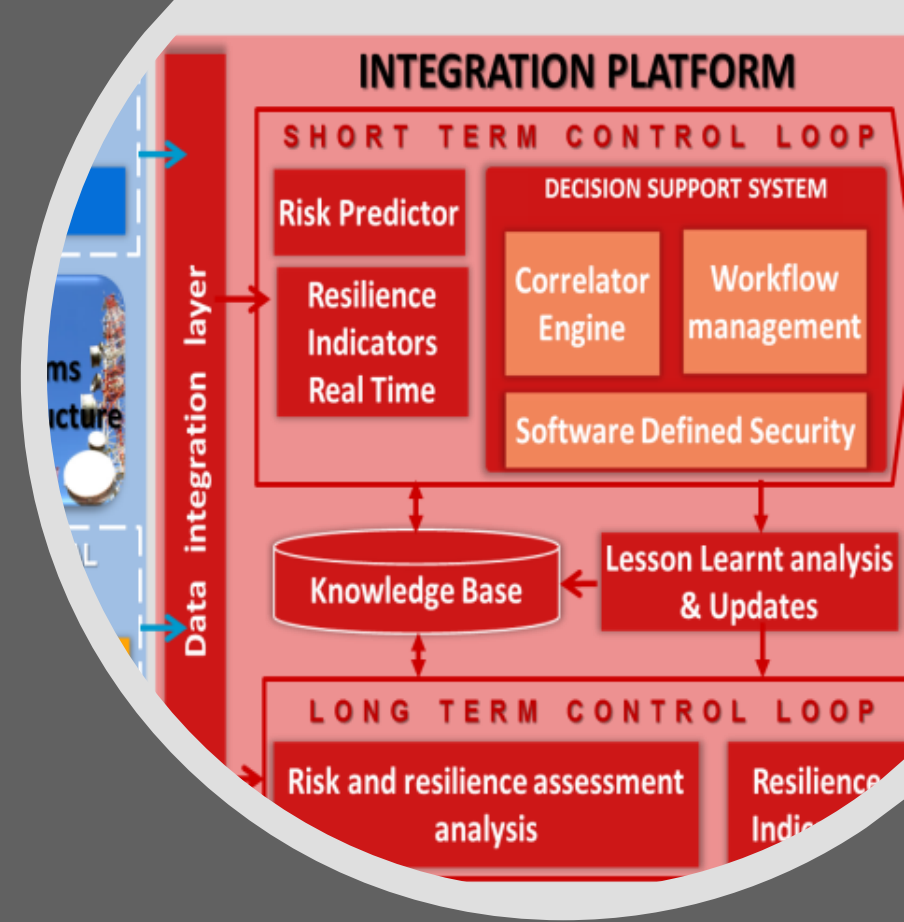
The Project

- **RESISTO aims to improve risk control and resilience of modern Communication CIs, against a wide variety of cyber-physical threats, being those malicious attacks, natural disasters or even unexpected faults**



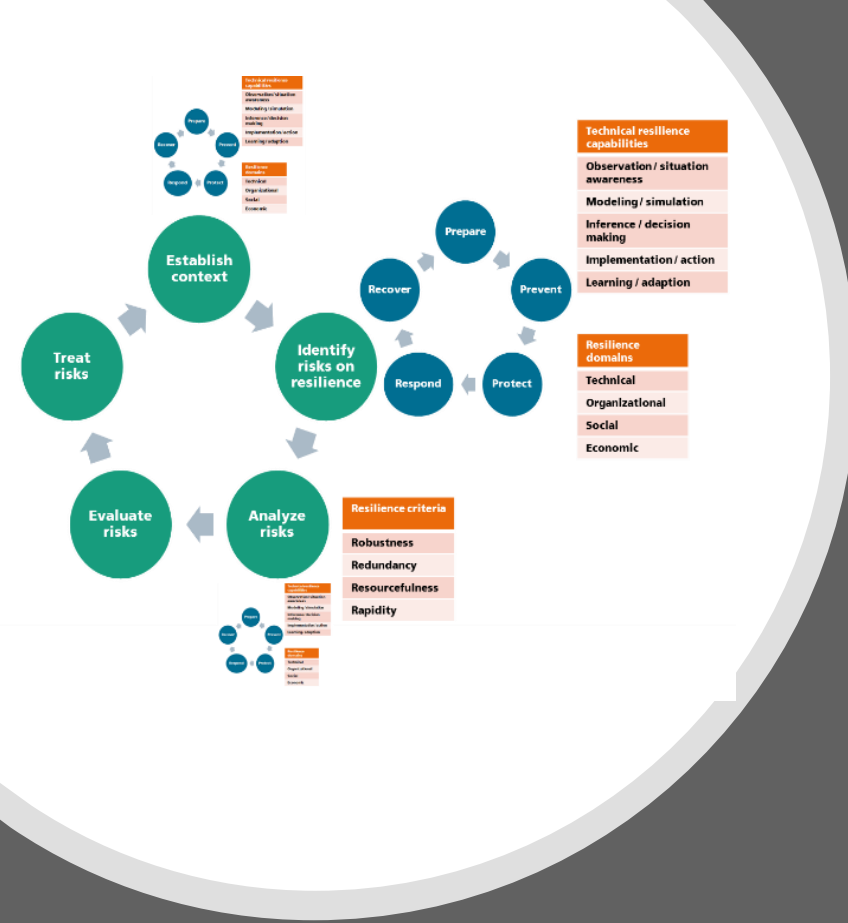
Objective #1

- Help managers of Communication CIs to guarantee improved business and asset continuity, delivering an innovative platform for optimized decision support in the face of physical, cyber and combined cyber-physical
- *All the Partners*



Objective #2

- Develop an Integrated Risk and Resilience analysis and management tool, that takes account of cyber and/or physical threats and disruptions jointly at the level of telecommunication service functions and performance functions
- *LDO, Fraunhofer, RM3*

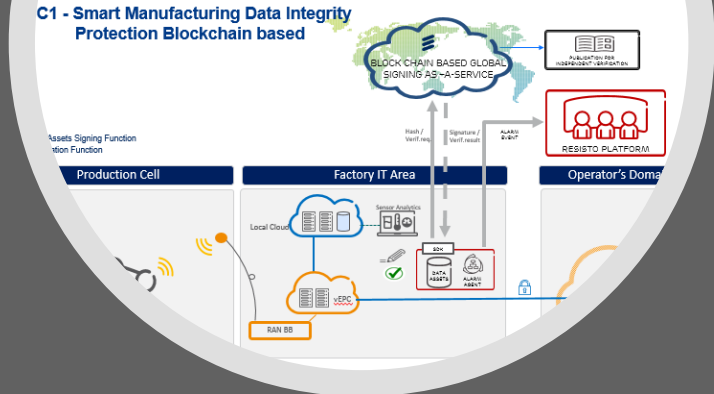


Objective #3

- Provide, experiment and assess a suite of innovative cyber/physical security solutions for prevention, protection, detection and reaction that can deliver unprecedented cost-effective performances in a holistic technology framework
- *LDO, TRE, GT, RM3, INT, ICCS, ADI*

Objective #4

- Support a progressive adoption path for the RESISTO platform and services through extensive validation in relevant use cases for Communication Infrastructure protection (TRL 7) directly involving relevant Communication CI operators, arising awareness and promoting a joint approach to resilience
- *All the Partners*

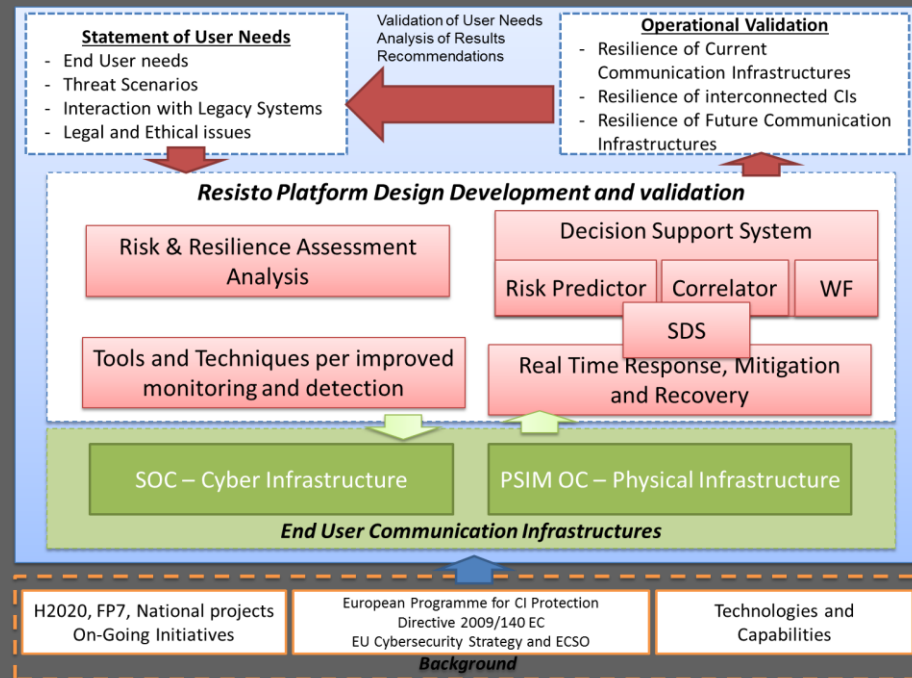


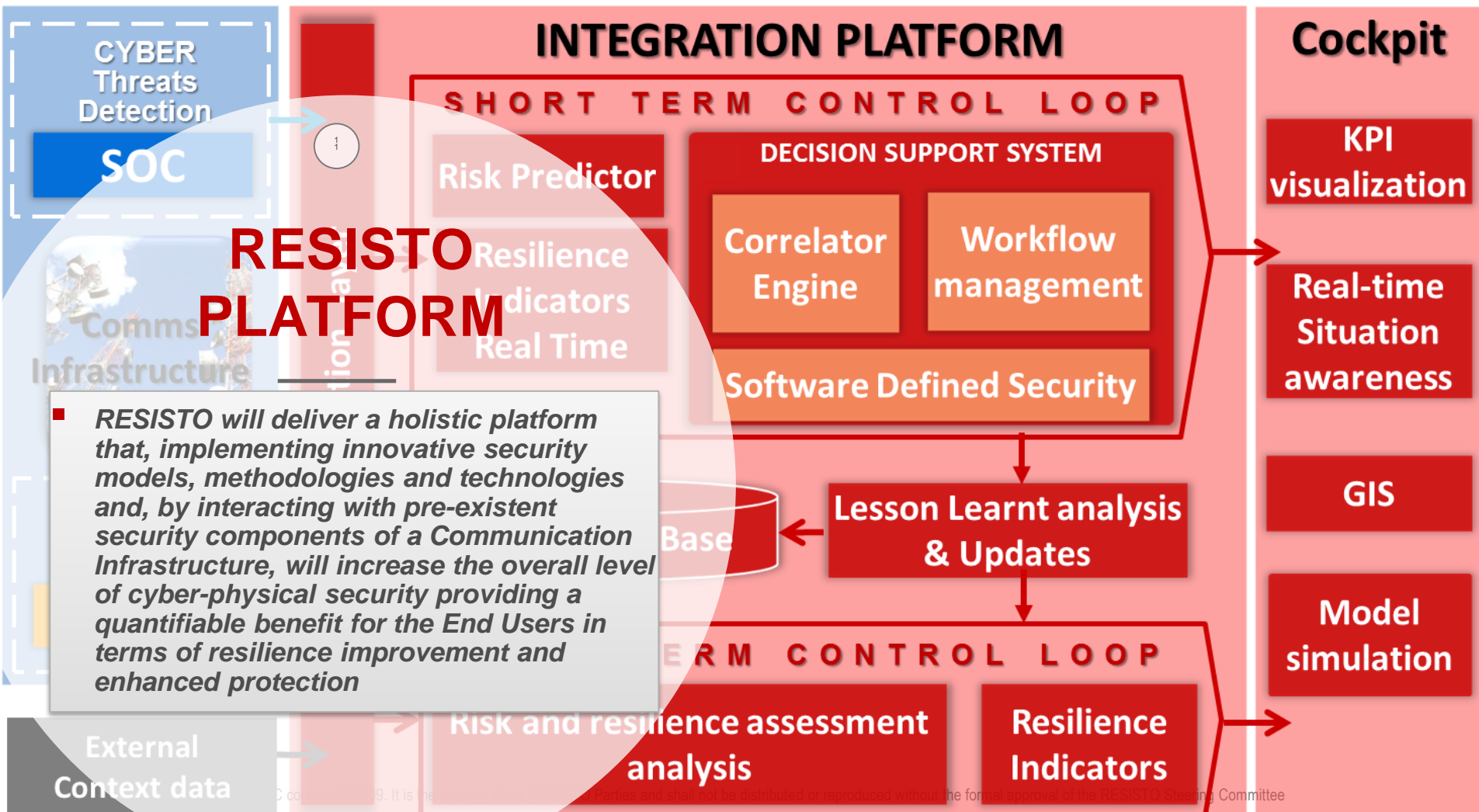
Objective #5

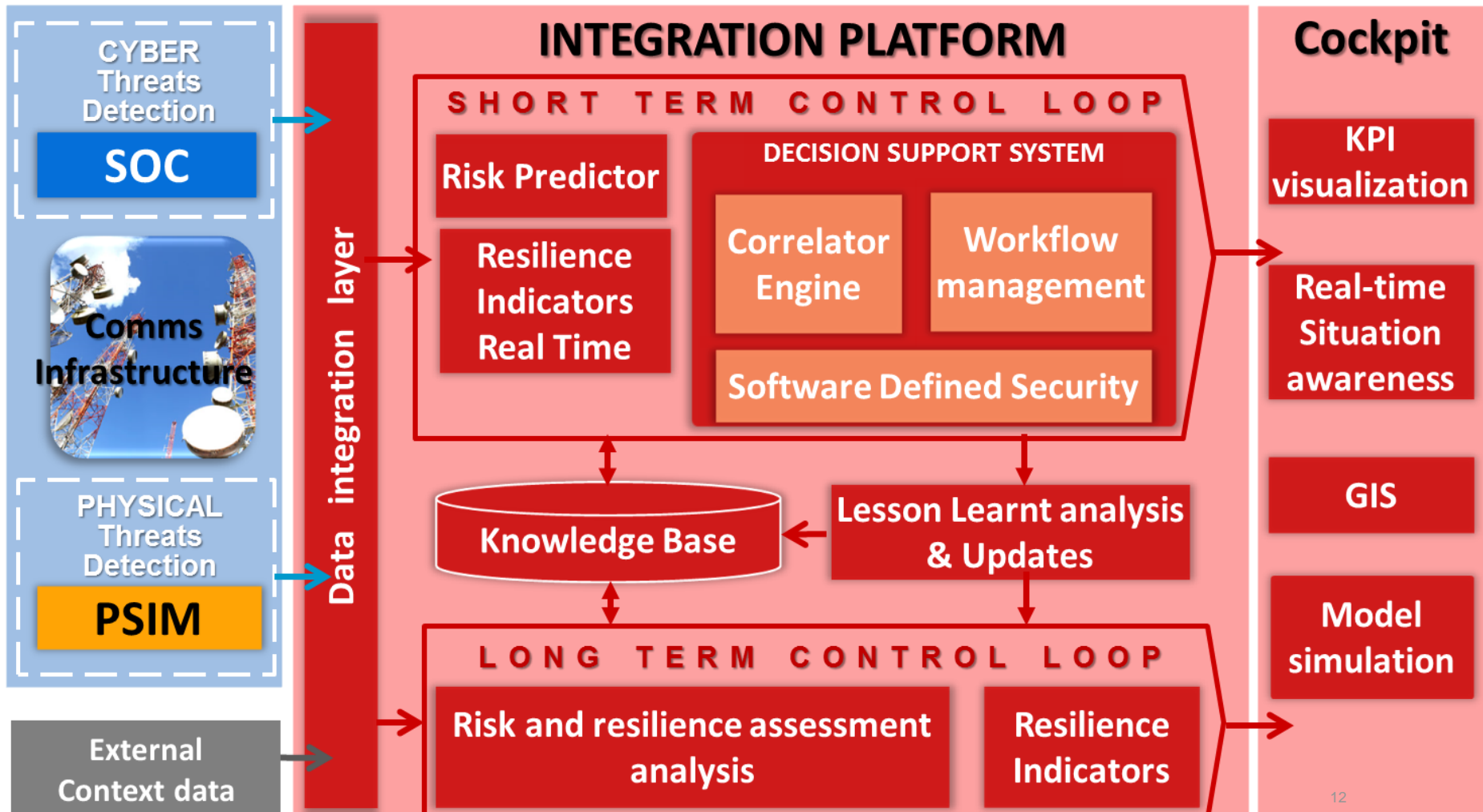
- Contribute to the European Programme for Critical Infrastructure Protection and to the objectives of the Cybersecurity Strategy of the European Union (as well as convergence of *of safety and security standards and Directive 2009/140 EC regulatory framework for electronic communications networks and services*)
- LDO, BTC, GT, AB (Orange FR, Telefonica, EOS)



Approach and methodology



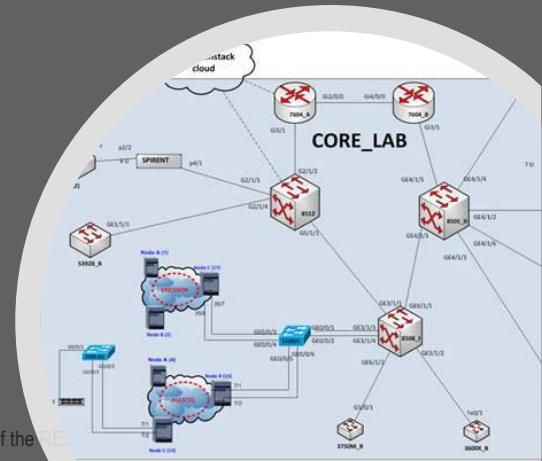
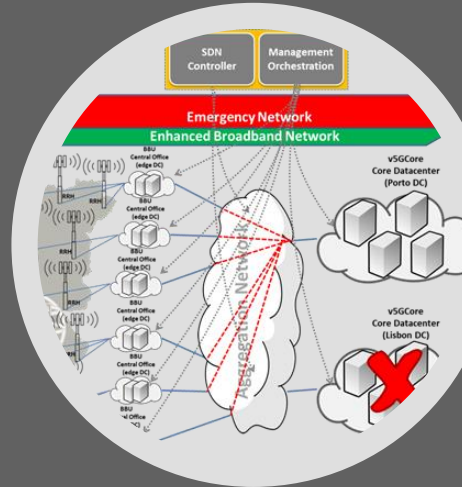
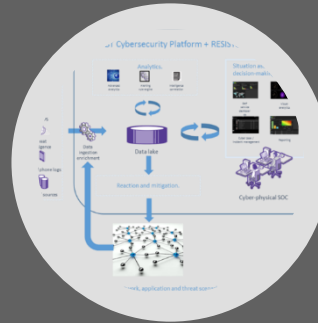




Functionalities	The RESISTO modules: Key elements and Capabilities	Responsible Partners
Security Analyses and Modelling Based Methods	Combined Risk / Resilience assessment of Communications Infrastructure	FRAUNHOFER, RM3
	Holistic System Modelling Interdependency analysis (Model and simulation analysis) and Risk Predictor	FRAUNHOFER, RM3
	Software Defined Security	RM3
	Decision Support System – Cyber-Physical Correlator	LDO, RM3, FRAUNHOFER
Technologies for cyber threats	Machine Learning for Threat Intelligence	TRE, LDO
	Blockchain for Data integrity	GT
Technologies for physical threats	Airborne Threats (UAVs, drones) detection and tracking	ICCS
	Telecom sites protection using IoT and Smart Spectrum Surveillance	INT
	Audio and visual analytics for Telecom assets protection	ADI
Emergency Communications	Emergency Warning Communication Function	TEI

Validation

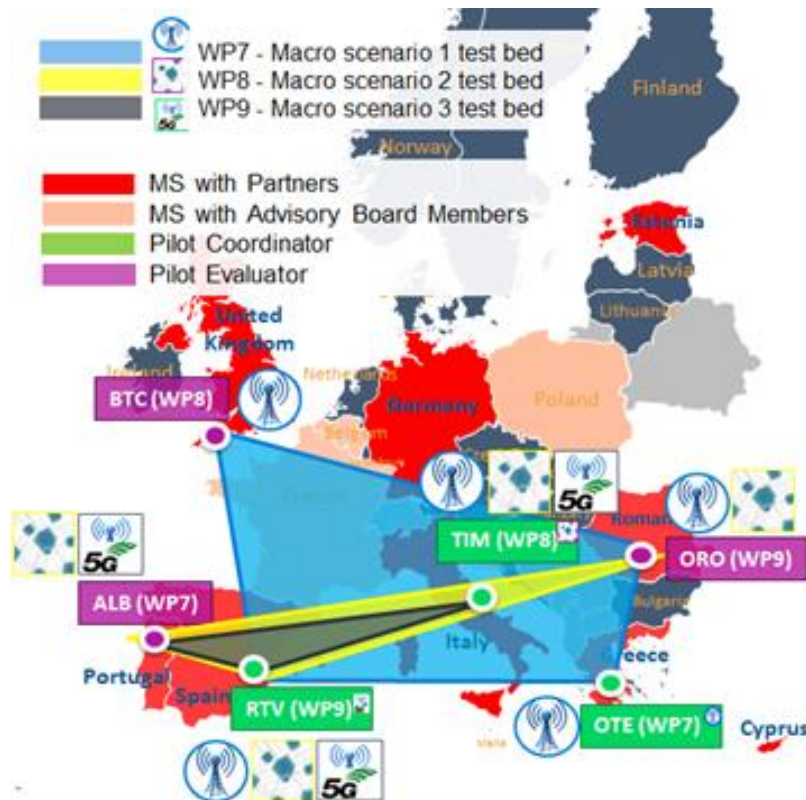
- **Macro-Scenario 1 - The protection of the Current existing Telecommunication Critical Infrastructures**
- **Macro-Scenario 2 - Their interdependencies as providers of essential communication services to other interlinked CIs and related cascade effects in the vicinity**
- **Macro-Scenario 3 - Their evolution towards the future 5G networks and the emerging IoT world**



Part #	Use case
OTE	1 Core Network Failure caused by Physical & Cyber Attacks
	2 Telecommunications congestion caused by natural (Earthquake)
TIM	3 Protection of (IT Sparkle's) ISP Backbone Nodes
	4 Protection of Cloud Storage Services.
	5 Smart Manufacturing Data Integrity (5G for Italy IoT Use Cases)
ORO	6 Cyber and physical protection of network and network elements
RTV	7 Maritime Safety and Emergency
	8 Telecommunication Sites
	9 PPDR Virtual Operator
ALB	10 5G network response to a large scale natural disaster in Italy
BTC	11 Disruption of major sporting event by combined physical and cyber attacks

Macro Scenario 1: "Current communication infrastructures"		
Candidate Pilot	1.Core Network Failure caused by mainly physical & cyber attacks	2.Cyber-attacks at the core network
Involved End Users	OTE, RTV, ORO, BTC	OTE, RTV, TIM
Involved partners	ICCS, ADI, LDO	ICCS, ADI, TRE, LDO
Scenario description	Physical and cyber-attacks in critical telecommunication sites affecting the core network. This is the case of deliberate terrorist attacks in telecom physical infrastructure (i.e. antenna towers parks or main telecom buildings) with both physical and cyber combined attacks aimed at maximizing disruption and confusion or a natural hazard (i.e. earthquake, flood etc.).	Deliberate cyber-attack targeting the core network, sensitive data and ICT systems. An attacker could violate security (integrity, confidentiality, availability) of backbone nodes with malicious hacking or taking advantage of security vulnerabilities and many points of weakness.
Focus of the use case	Focus of this use case is enhancing the resilience of current communication infrastructures correlating the domains of physical security systems and cyber protection. Taking advantage of interdependencies between the two domains it is possible to detect in advance threats and attacks and to use joint counter-measures.	Cyber threats to the vast amount of data stored on cloud servers of telecom providers are dangerous for the operation of communication networks. These attacks may have impact to the overall performance of the network or they may target specific applications causing a disruption of communication services.
Assets affected	<ul style="list-style-type: none"> Selected nodes serving core network traffic; Telecom sites for backhaul links, 3G/4G towers, antennas, sites for broadcast and radio transmissions; Wi-Fi networks; Buildings with network operation and management infrastructure; 	<ul style="list-style-type: none"> Core network or slices of core network; Inter-network-based communications (core routers); Hypervisor; Backbone nodes.
New countermeasure /solution implementation	1. OTE: OTE test bed (models validation, simulations / emulations of connection / traffic loss etc.) and selected buildings (with antenna towers/base stations/antenna parks/core network infrastructure) for visualization and representation of the area of interest; 2. ICCS: DJI Phantom 3 Advanced Drone with camera, Doppler radars in various frequencies, acoustic sensors and related control / DSP software, tools for radio links security against jamming; 3. ADI: 3 types of UAV platforms with payload (gyro, detector, camera), intelligent audio & video analytics; 4. LDO: integration platform for physical and cyber security.	1. OTE: test bed emulating core network 2. ICCS: software tools for network security 3. ADI: Network Simulator ns-2 and ns-3, Versatile Media Content Management System; 4. TIM: TI SPARKLE transmit alerts related to logical events that can occur on backbone nodes; 5. TRE: real time data processing, data mining and automated and deep learning strategies (artificial intelligence); 6. LDO: integration platform for physical and cyber security

Scenario 3 "Future communication infrastructures (toward 5G)"
WP9 (RTV)
EV



Use Cases Federation

- **Federation scheme of the pilot Use Cases within each Macro-Scenario**
 - sharing of design (logical interconnection of pilots) shared modelling approach and KPI selection
 - sharing of resilience relevant data (functional interconnection of pilots): exchange of data among the pilots to be better prepared and react jointly
 - sharing of the infrastructure (physical interconnection of pilots): pilot sites are physically interconnected as. in the 5G one in WP9

■ Internal benefits

- Cost savings, protecting themselves from potential damages to infrastructure and services coming from cyber and physical threats
- Enhanced Resilience, reducing the risk of service interruption toward their customers during terrorist attack and/or stress over the infrastructure due to natural disasters
- Better informed decision making and achievement of holistic understanding of a situation across the cyber and physical domain and interlinked CIs

■ External benefits

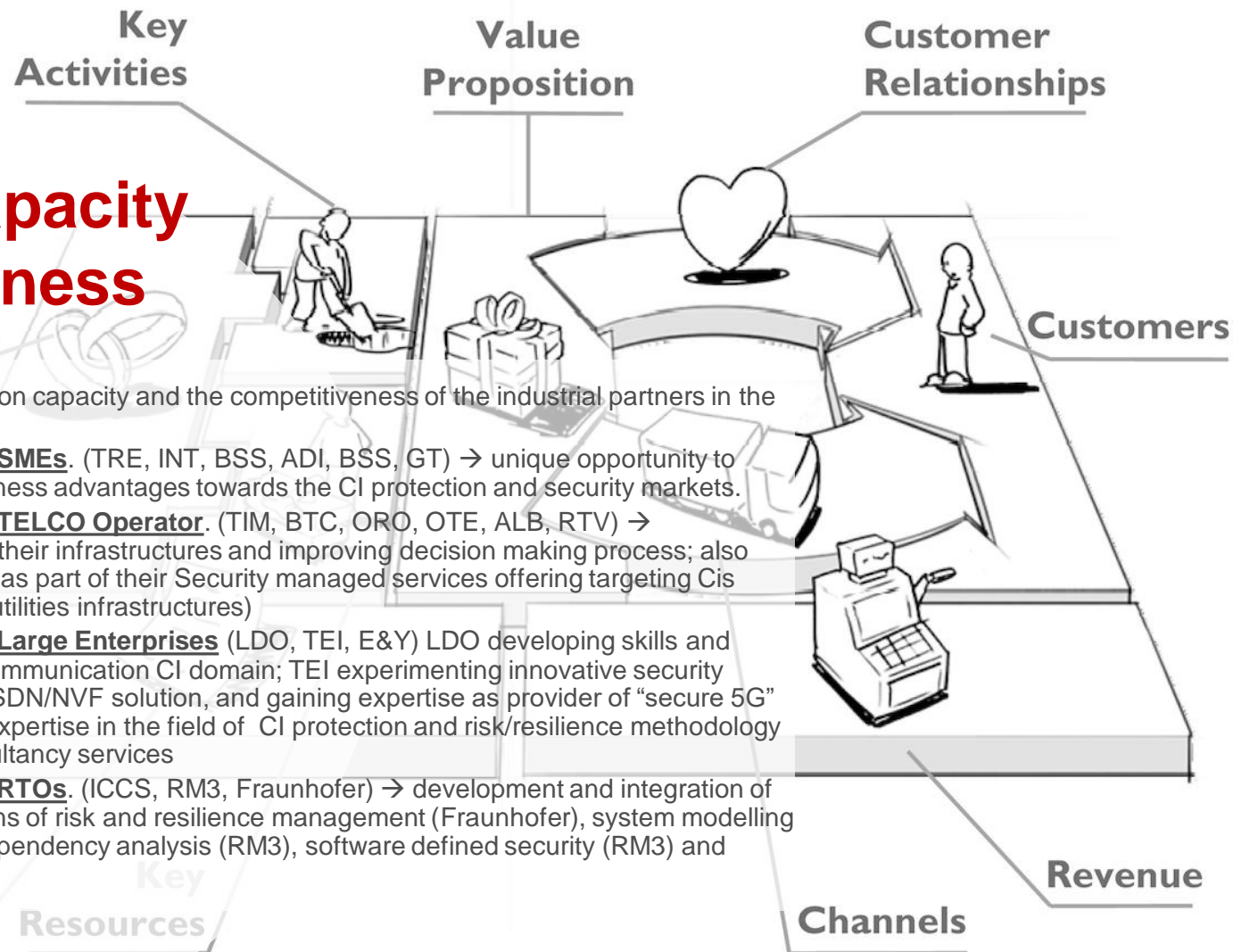
- Increasing incentives for cyber security, adopting standard certification and being compliant with European regulation;
- Develop Pilots and Bring to Market solutions maintaining competitive advantage of EU in the field of CI protection
- Increased Innovation capacity and Competitiveness (reduced time to market)
- Increasing awareness among Private and Public CI sectors, and citizen → promoting the development of Skills

RESISTO Value Proposition

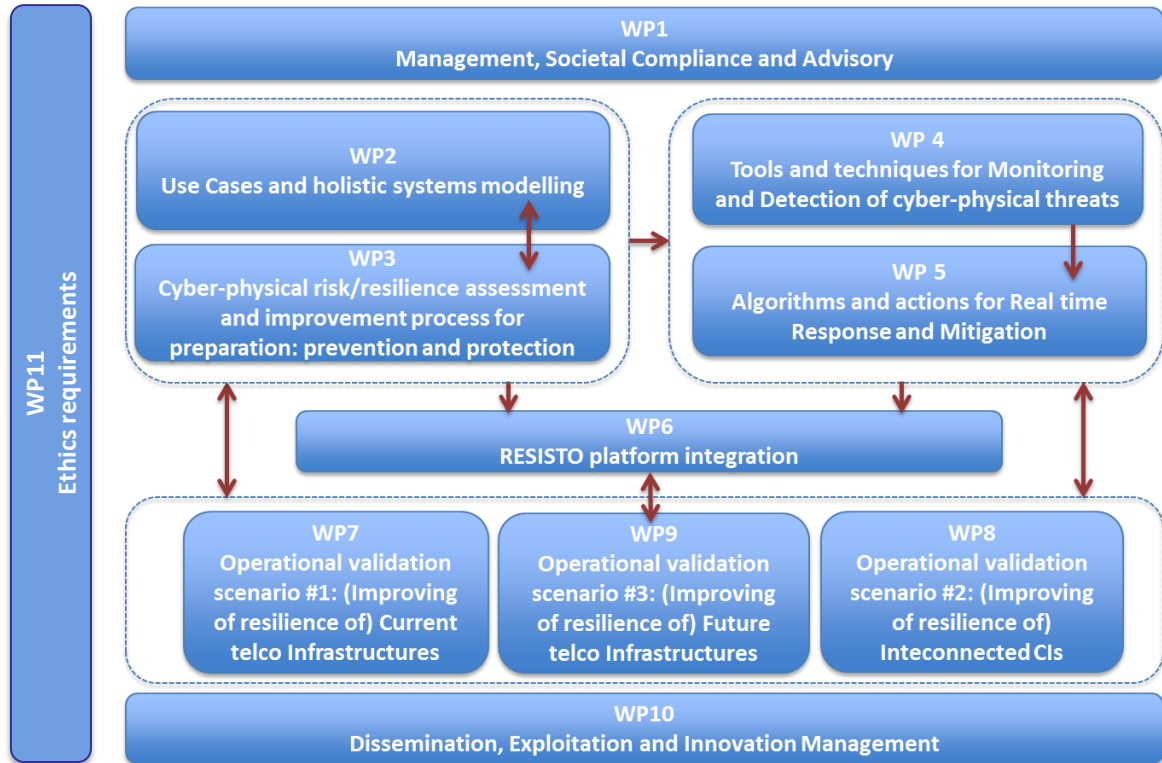
Innovation capacity Competitiveness

- The RESISTO will improve innovation capacity and the competitiveness of the industrial partners in the field of CI protection.

- **Competitive Advantages for SMEs.** (TRE, INT, BSS, ADI, BSS, GT) → unique opportunity to extend their offerings and business advantages towards the CI protection and security markets.
- **Competitive Advantages for TELCO Operator.** (TIM, BTC, ORO, OTE, ALB, RTV) → strengthening the resilience of their infrastructures and improving decision making process; also introducing RESISTO platform as part of their Security managed services offering targeting Cis operators (water, gas, energy utilities infrastructures)
- **Competitive Advantages for Large Enterprises** (LDO, TEI, E&Y) LDO developing skills and solutions customized for the communication CI domain; TEI experimenting innovative security solution like SDS on top of its SDN/NVF solution, and gaining expertise as provider of “secure 5G” networks; E&Y deepening its expertise in the field of CI protection and risk/resilience methodology as a means to extend its consultancy services
- **Competitive Advantages for RTOs.** (ICCS, RM3, Fraunhofer) → development and integration of new knowledge in R&D domains of risk and resilience management (Fraunhofer), system modelling (Fraunhofer, RM3) and interdependency analysis (RM3), software defined security (RM3) and signal processing (ICCS)



WBS and relations





***RESISTO Architecture
Damage/ Vulnerability models
for physical and cyber threats
of telecom CI***

***RESISTO platform
and components
Integration***

***RESISTO platform
validation across
three verticals***

***RESISTO platform
Assessment
Best practices***





RESilience enhancement and risk control platform
for communication infra**ST**ructure **O**perators

Expected Results

- State-of-the-art analysis of physical/cyber detection technologies and risk scenarios of Communication CIs
- Innovative tools, concepts, and technologies for combatting combined physical/cyber threats to Communication CIs (RESISTO framework).
- Security risk management plans integrating systemic and both physical and cyber aspects
- Extended validation of the RESISTO framework against physical/cyber threats across three verticals: current, future (towards 5G) and interconnected Communication infrastructures
- Convergence of safety and security standards, establishment and dissemination throughout the relevant user communities of specific models for information sharing on incidents, threats and vulnerabilities. Support to ECSO



RESilience enhancement and risk control platform for communication infraSTructure Operators



Thank you for your attention!

