

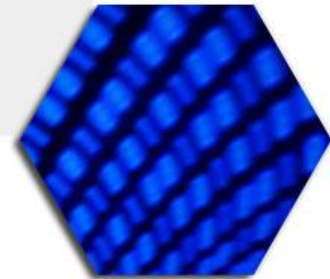


RESISTO Project and Architecture

Alessandro NERI (University of ROMA TRE) - Alberto NERI (Leonardo SpA)

Brussels, 17th September 2019

14TH MEETING OF THE
COMMUNITY OF USERS ON
SECURE, SAFE AND RESILIENT
SOCIETIES THEMATIC GROUP –
CRITICAL INFRASTRUCTURE
PROTECTION (CIP)



RESISTO – This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No786409

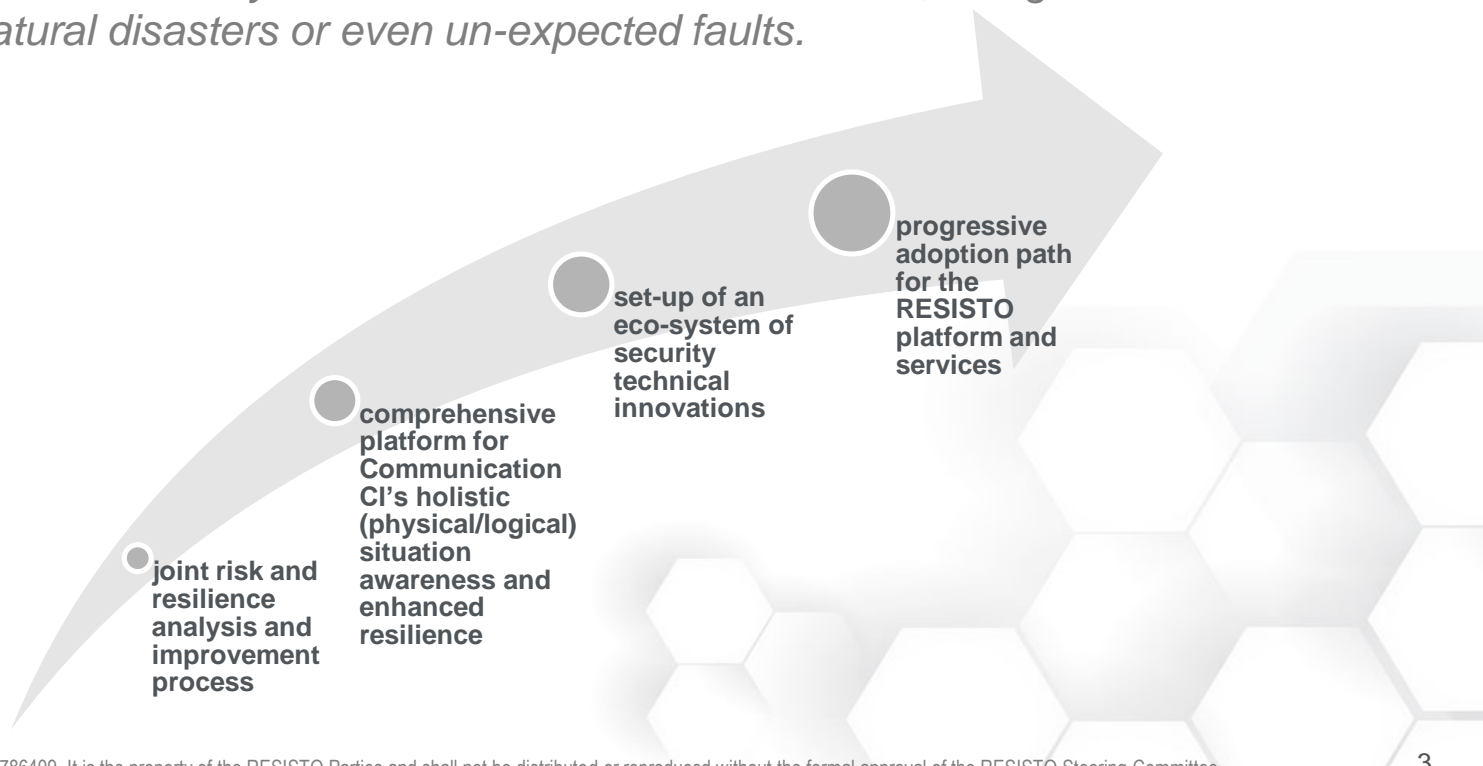


RESilience enhancement and risk control platform for communication infraSTructure Operators

- **3 years** (*to May 2018*)
- **Topic(s): CIP-01-2016-2017 – Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe**
- **10M€ cost (8M€ funding)**
- **17 partners** (*2 Large Enterprises, 6 Telco operators, 5 RTOs/Universities, 4 SMEs*)
- **Validation across 3 Verticals:**
 - **current,**
 - **future and**
 - **interdependent comms infrastructures**
- **Ambitious exploitation plan**

■ MAIN RESISTO's OBJECTIVE

- 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 un-expected faults.



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 threats** taking account of critical schemes of infrastructure, functions and services and possible (cascading) event trajectories

2

Develop an INTEGRATED RISK AND RESILIENCE ANALYSIS AND MANAGEMENT TOOL for improved preparedness and prevention in the communication domain that takes account of cyber and/or physical threats and disruptions jointly at the level of telecommunication service functions and performance functions, including systemic security management

3

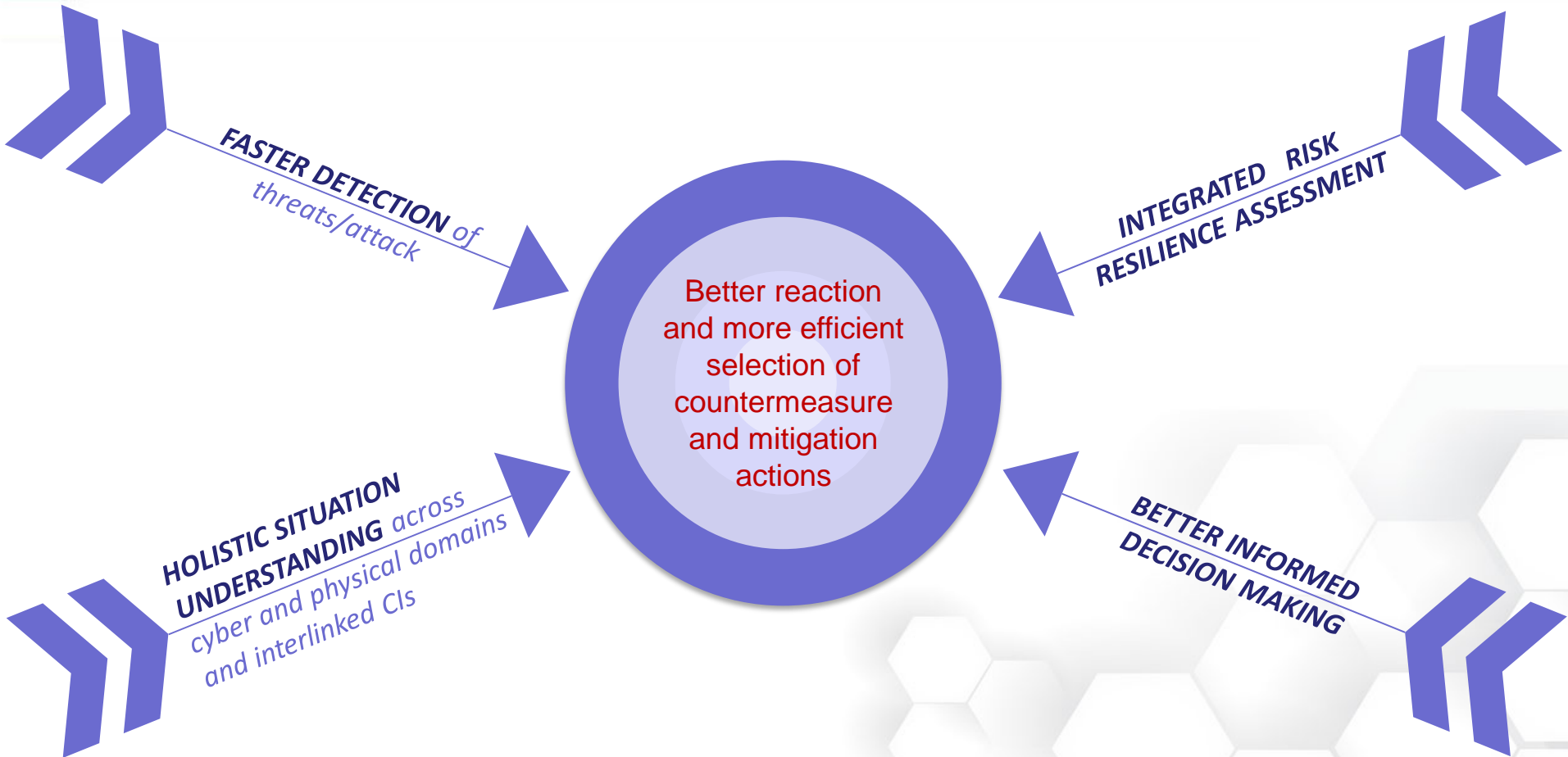
Provide, experiment and assess **a suite of innovative cyber/physical security solutions** for prevention/protection, detection and reaction that can deliver unprecedented cost-effective performances in a holistic technology framework

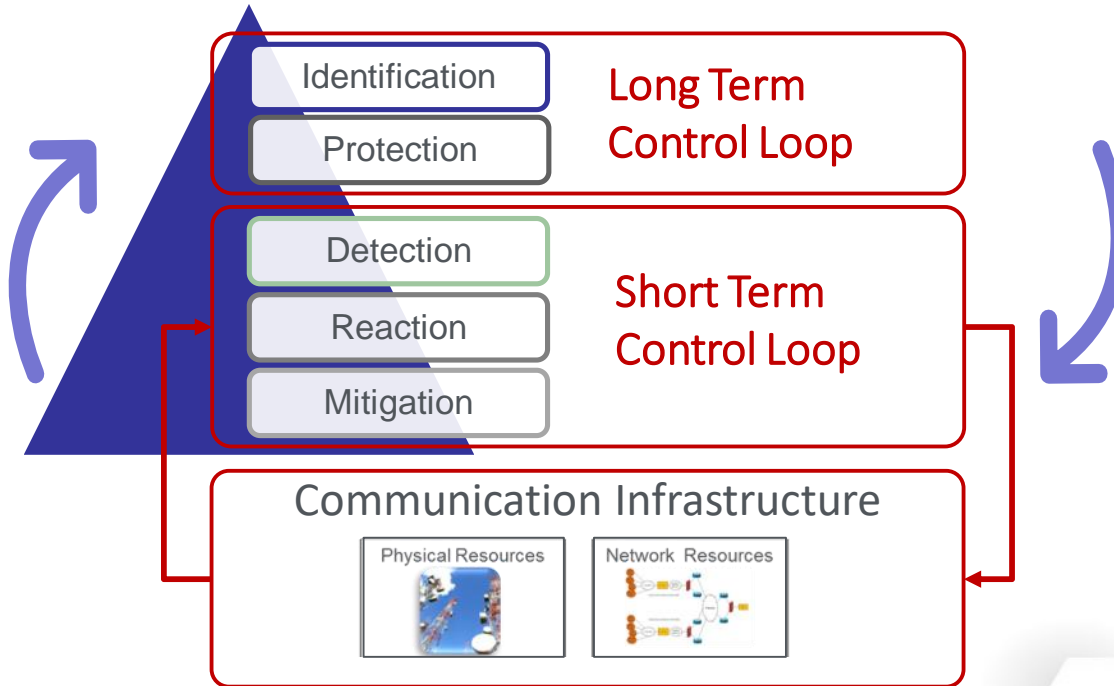
4

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

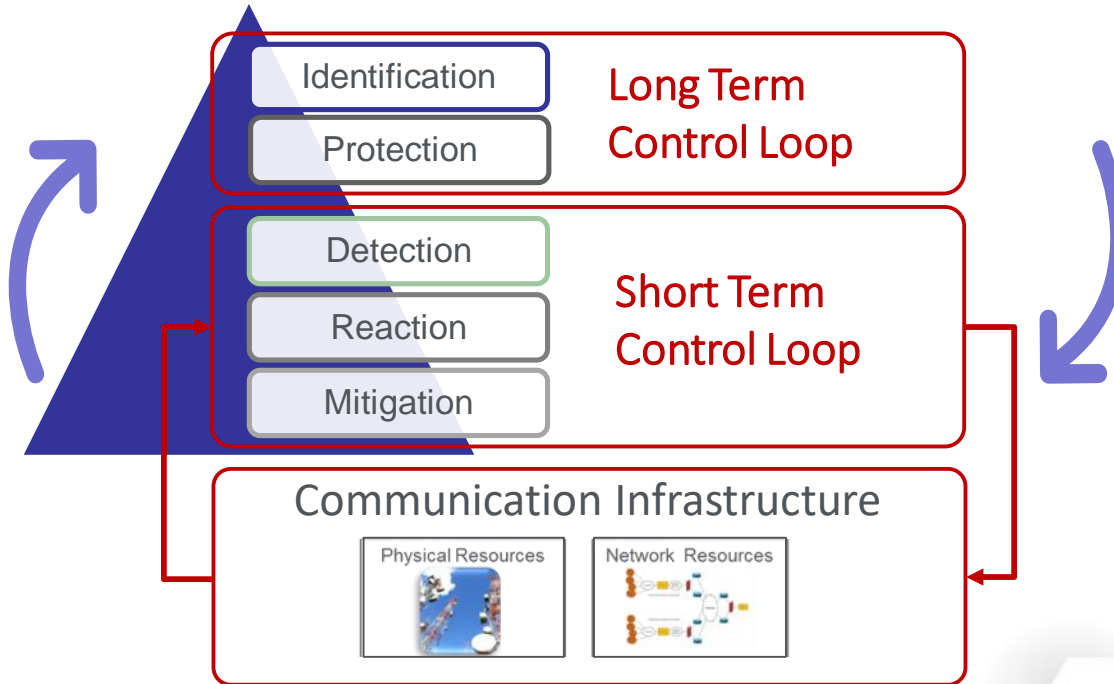
5

To contribute to the European Programme for Critical Infrastructure Protection and in particular to the objectives of the Cybersecurity Strategy of the European Union, providing suitable inputs also to the Cybersecurity PPP

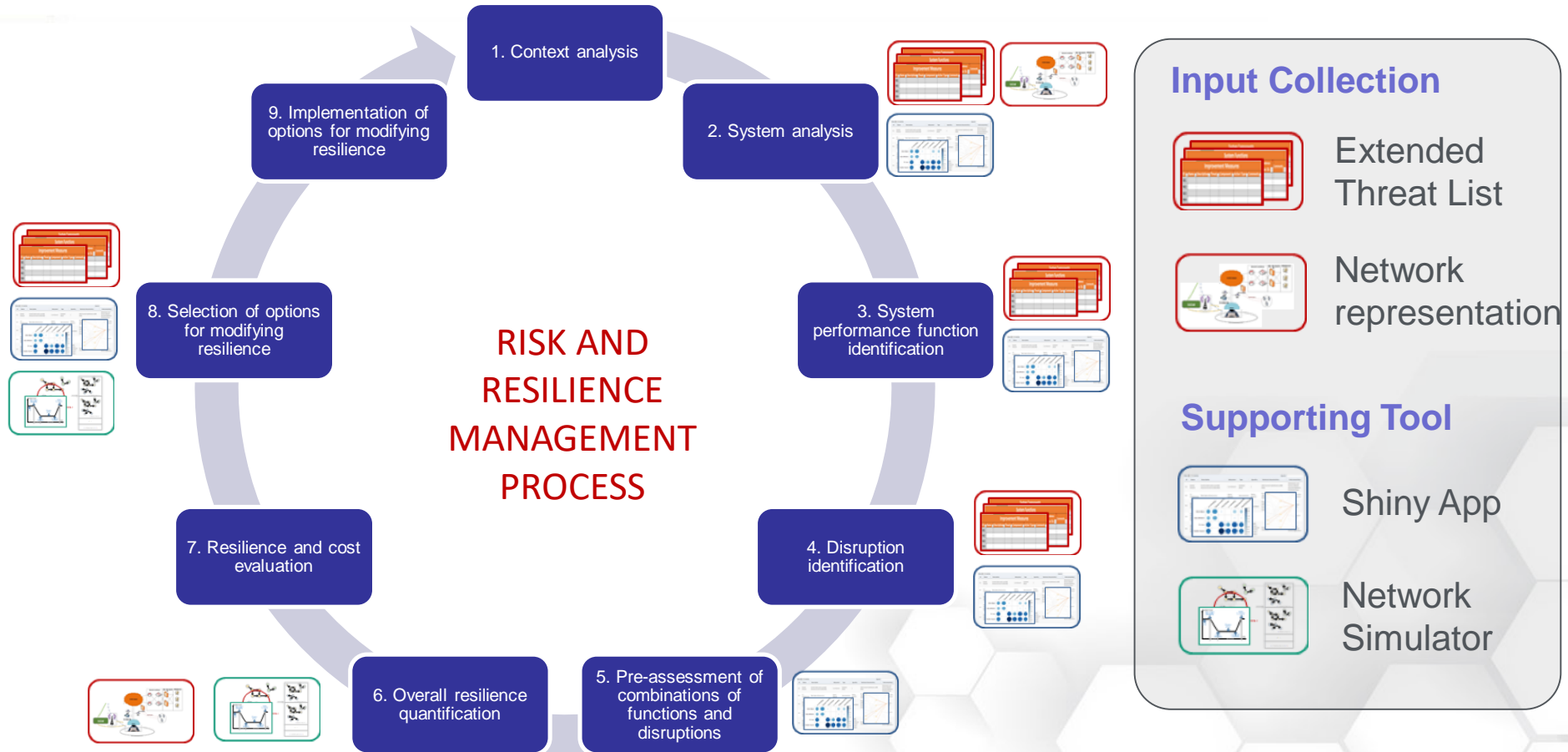


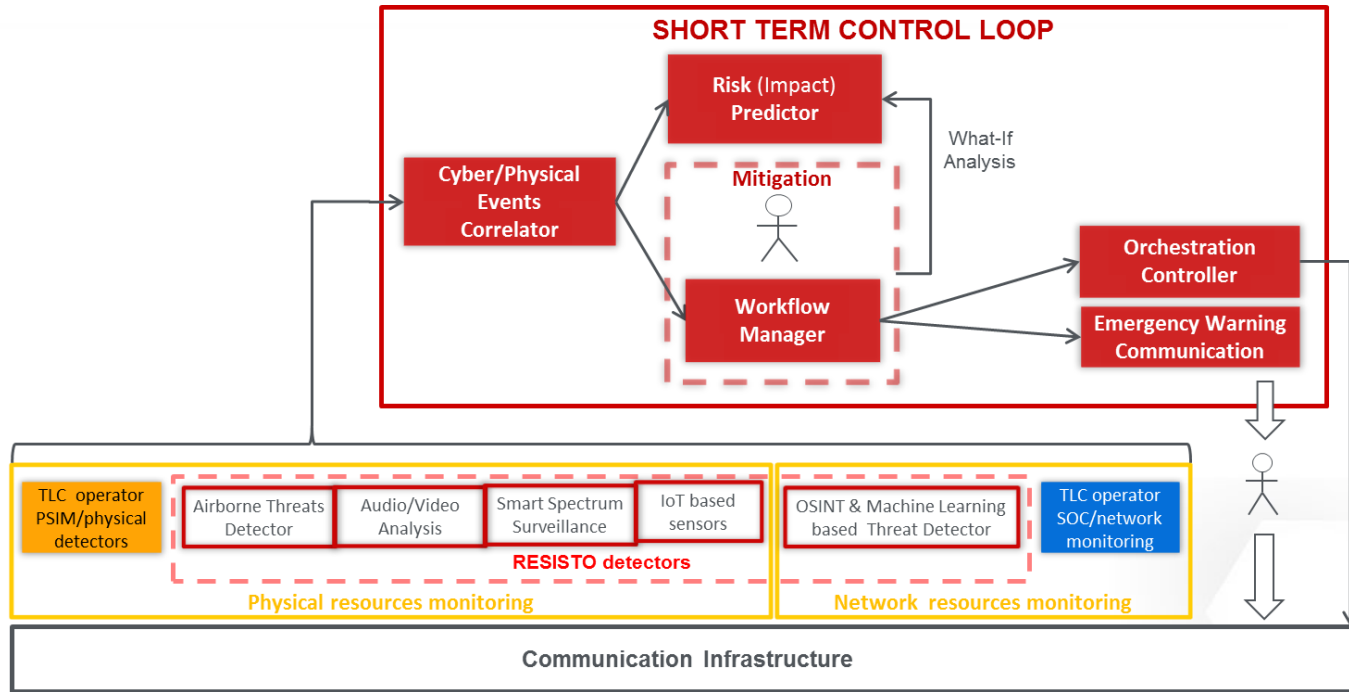


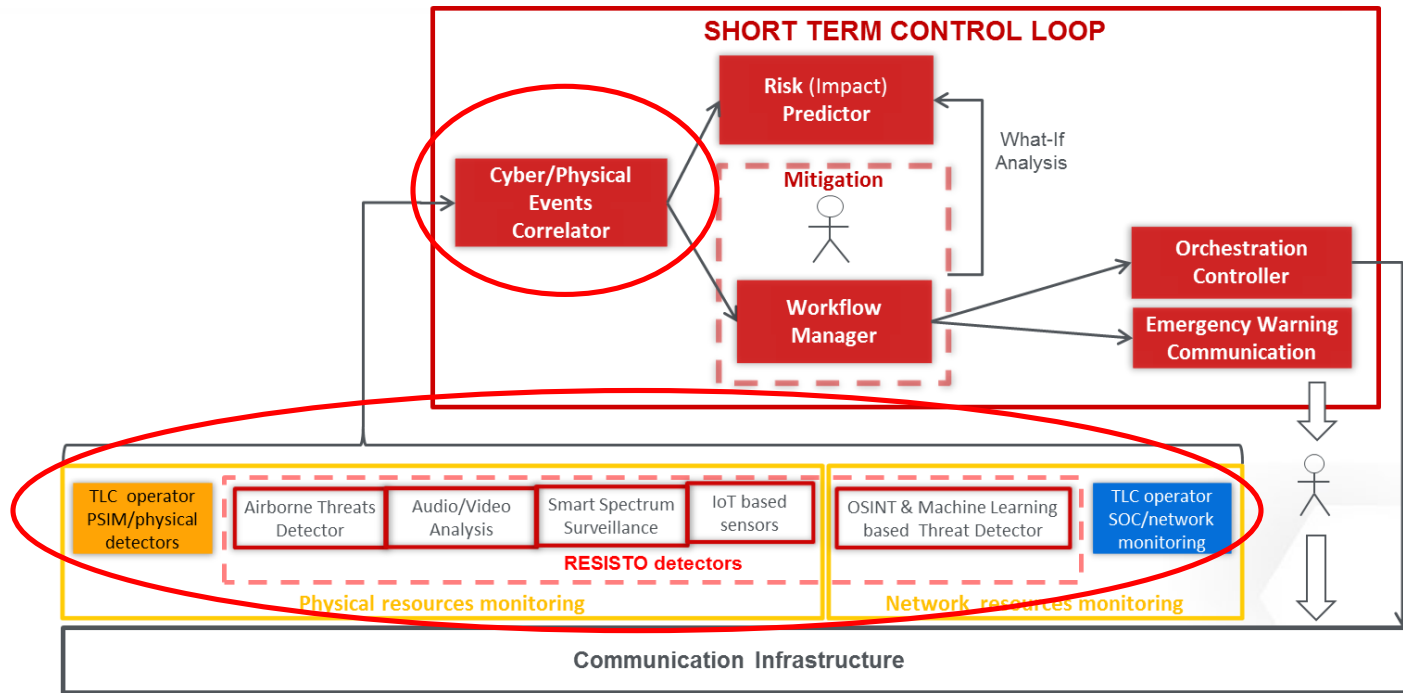
- The **Long Term Control Loop (LTCL)** is based on the ***Risk and resilience assessment analysis***.
- For each loop cycle a set of **Resilience Indicators (RIs)**, relevant to critical threat event typologies, are estimated and stored in a Knowledge Base (KB).
- Performed on a periodic basis (annually, quarterly or even monthly) or when particular events take place



- The **Short Term Control Loop (STCL)** **reacts** in **real time** to detected cyber/physical attacks and events that may impact the operational life of the system.
- It **enhances** situation **awareness** and provides operators with a Decision Support System cockpit able to implement the best reactions.

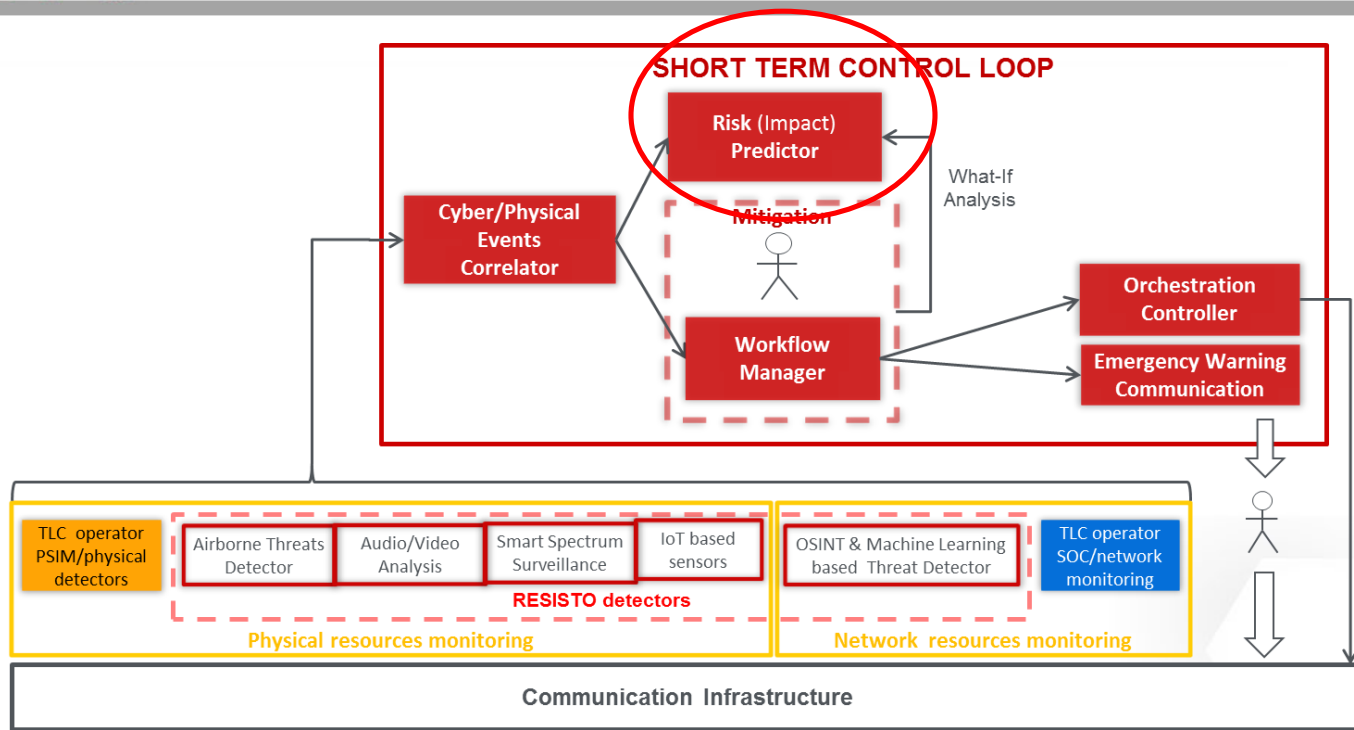






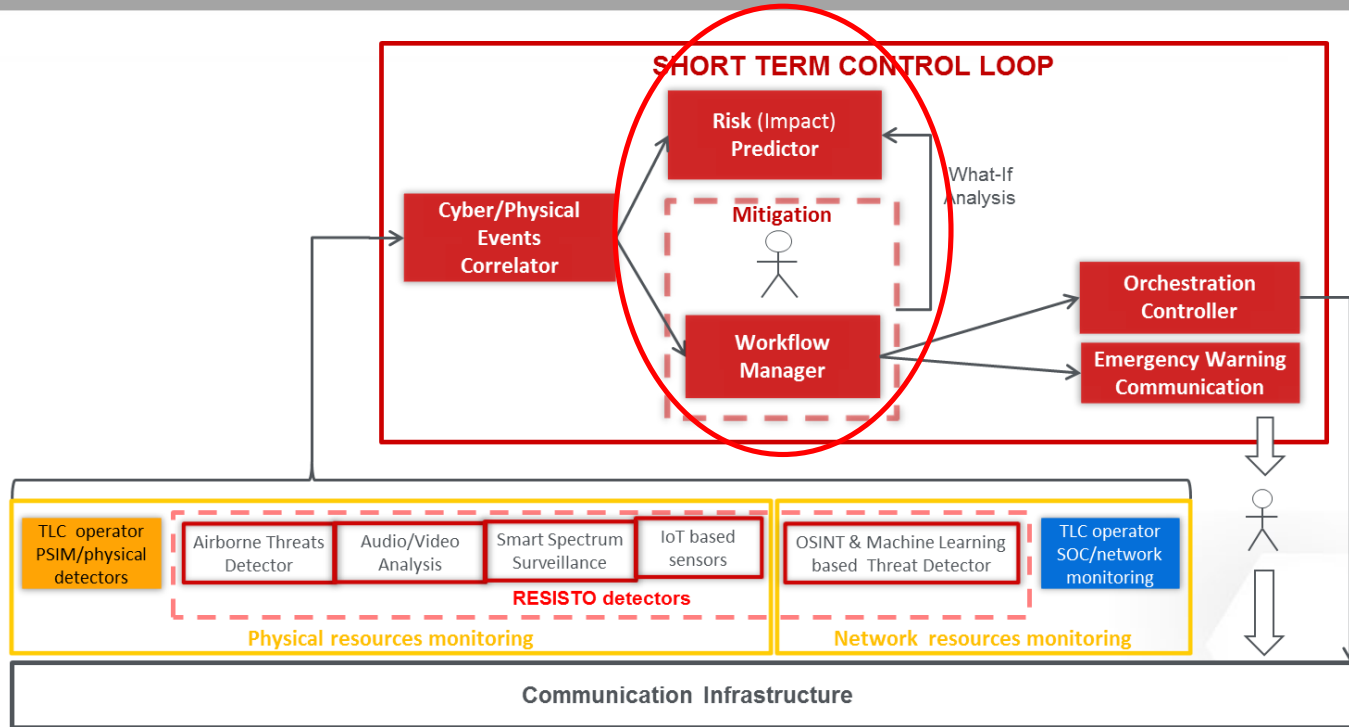
The Short Term Control Loop:

- **monitors the physical and cyber security status of the infrastructures**, correlating the physical and cyber domain events and network monitoring data to detect anomalies and provide early warnings on security attacks by detecting threats in advance;



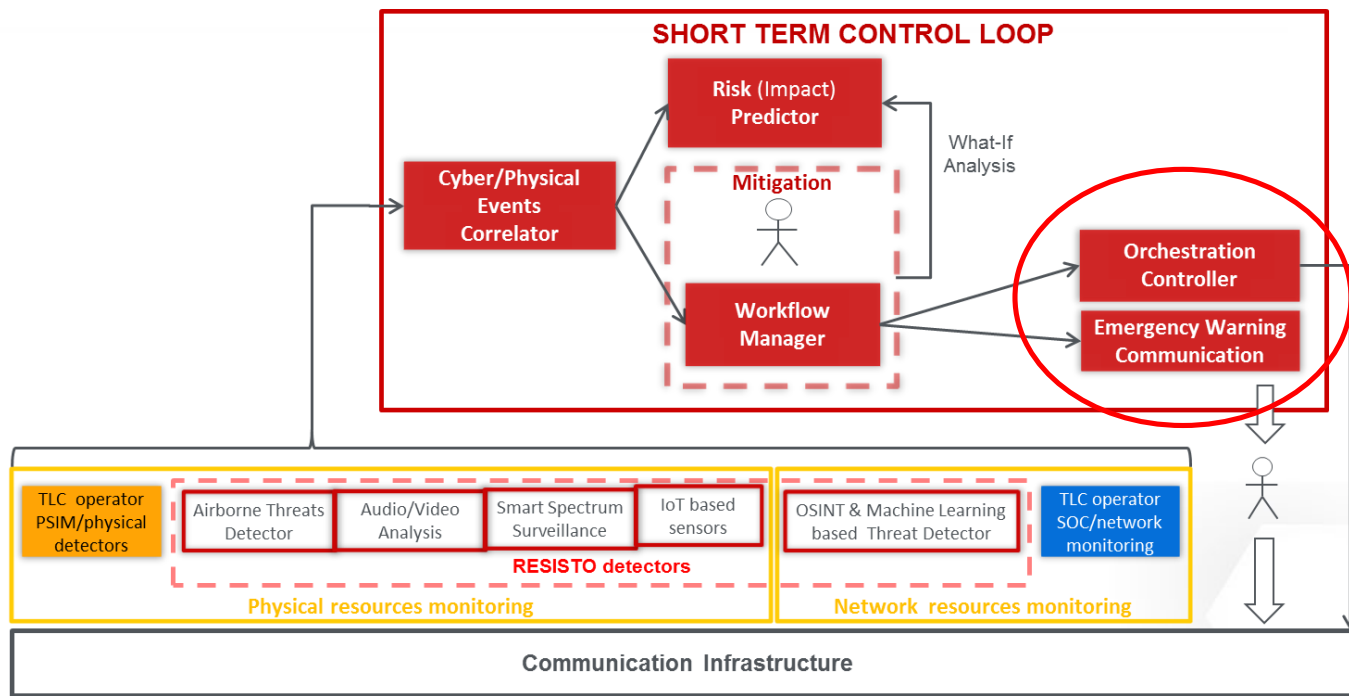
The Short Term Control Loop:

- **evaluates the attack impact** with respect to performance degradation of detected anomalies and security attacks on the communication CI, and interlinked CIs if known, based on the cascading effect;



The Short Term Control Loop:

- **supports decision making** providing a qualitative and quantitative What-If analysis tool in order to evaluate the most resilient communication CI reconfiguration;



The Short Term Control Loop:

- **drives reaction and mitigation** by means of action workflows (composed of directives to intervention teams, physical protection devices activation) and, mainly, of orchestrated Communication Network reconfiguration and protection function activation.

Step 1

at the end of a LTCL cycle
Estimated Resilience Indicators
(RIs) s are stored in the
Knowledge Base



1

3

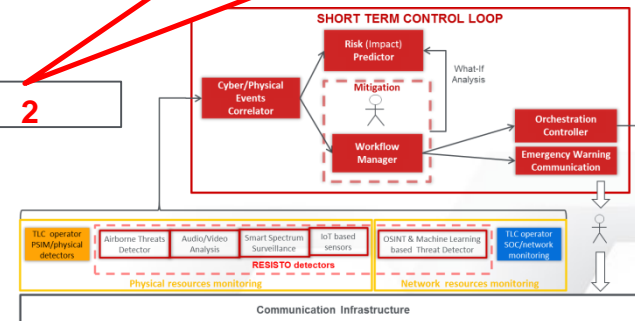
Step 3

Comparison between Estimated and Measured RIs are taken into account in the next LTCL cycle to improve resilience or estimation methods if needed.

Knowledge Base

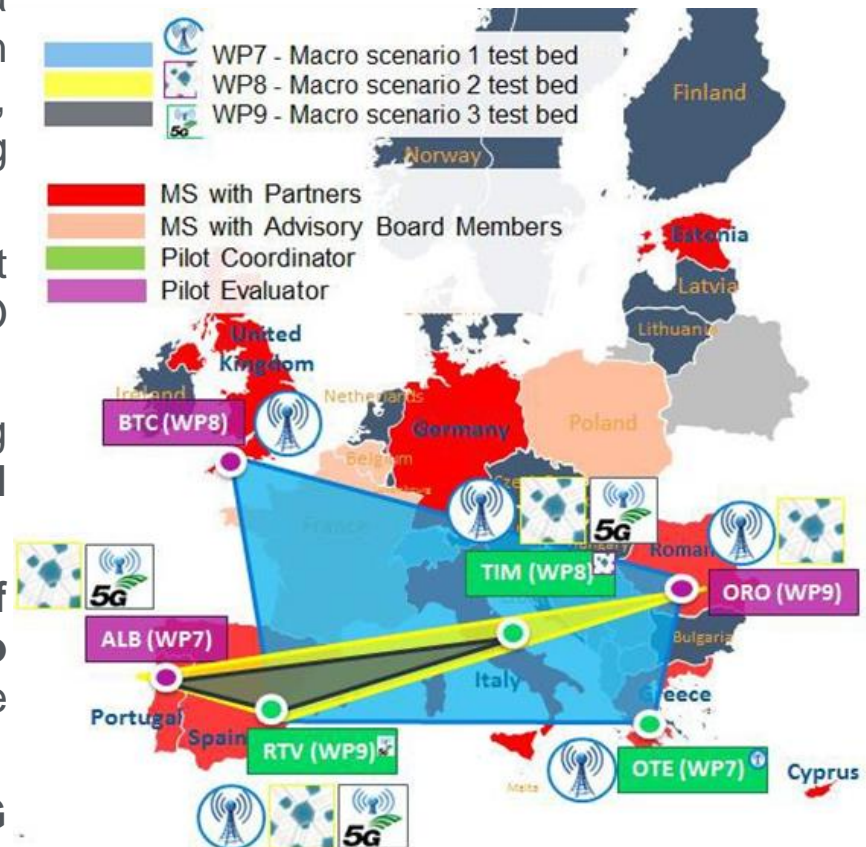
Step 2

STCL, facing an Event<i>, measures **Actual RIs** and store them in the Knowledge Base



2

- An extended validation is envisioned through a variety of operational Use Case pilots formed in sets configurations in terms of context, organization and impact, altogether consisting the RESISTO overall Validation Framework.
- **3 (Macro)-Scenarios**, each one involving a set of related Use Cases to prove the RESISTO concept :
 1. Protection of the **Current existing Telecommunication Critical Infrastructures**
 2. Their **interdependencies as providers of essential communication services to other interlinked CIs** and related cascade effects in the vicinity
 3. Their **evolution towards the future 5G networks** and the emerging IoT world.



- More degrees of freedom in mitigation
- Virtual Resources Vulnerabilities

Network
Function
Virtualization

Software
Defined
Network

- Unified Security Policy
- New Vulnerabilities

THREAT
EVOLUTION

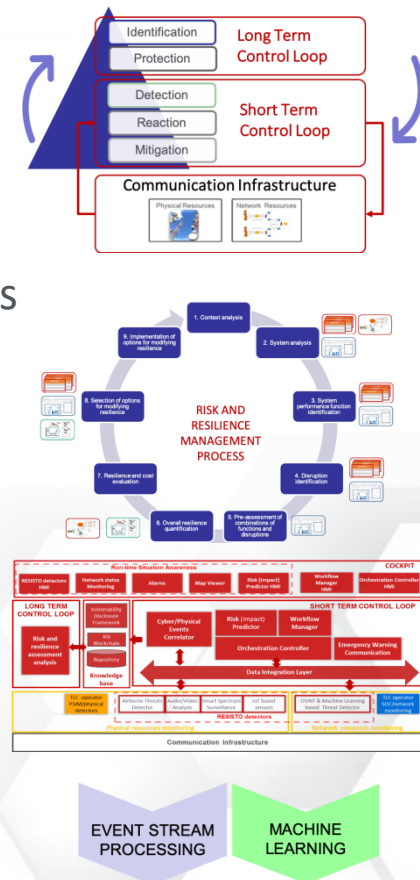
- Massive IoT
- User Equipment
- Access Network
- Core Network
- Mobile Edge Computing

RESISTO

5G

- Slicing
- Massive use of NFV+SDN
- Softwarization
- Integrate Communication and Computation

- A complete and **integrated framework** to cover off-line Identification and Prevention activities as well as Detection, Reaction and Mitigation on-line activities.
- Innovative tools, concepts, and technologies to face, in a **UNIFIED APPROACH**, **physical, cyber** as well as combined **physical/cyber** threats to Communication CIs.
- Security **RISK & RESILIENCE** management plans integrating systemic and both physical and cyber aspects.
- RESISTO framework approach scalability and grow capability
- **MODULAR FRAMEWORK** based on versatile technologies easily adaptable to face physical and cyber threats in continuous evolution.
- **Innovative** physical and cyber threatening events **DETECTORS**.



Contacts

- **Bruno SACCOMANNO** - RESISTO project Coordinator
Leonardo Spa – Cyber Security Division
bruno.saccomanno@leonardocompany.com
- **Prof. Alessandro NERI** - RESISTO project Scientific Coordinator
University of ROMA TRE – Engineering Department
alessandro.neri@uniroma3.it
- **Alberto NERI** - RESISTO project Technical Coordinator
Leonardo Spa – Electronics Division
alberto.neri@leonardocompany.com