RESISTO

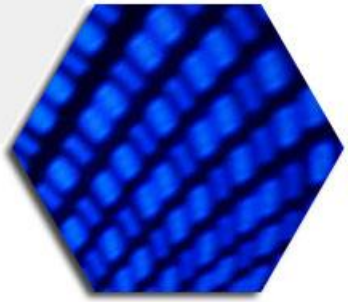
RESIlience enhancement and risk control platform for communication infraSTructure Operators

HORIZON 2020 #InvestEUresearch

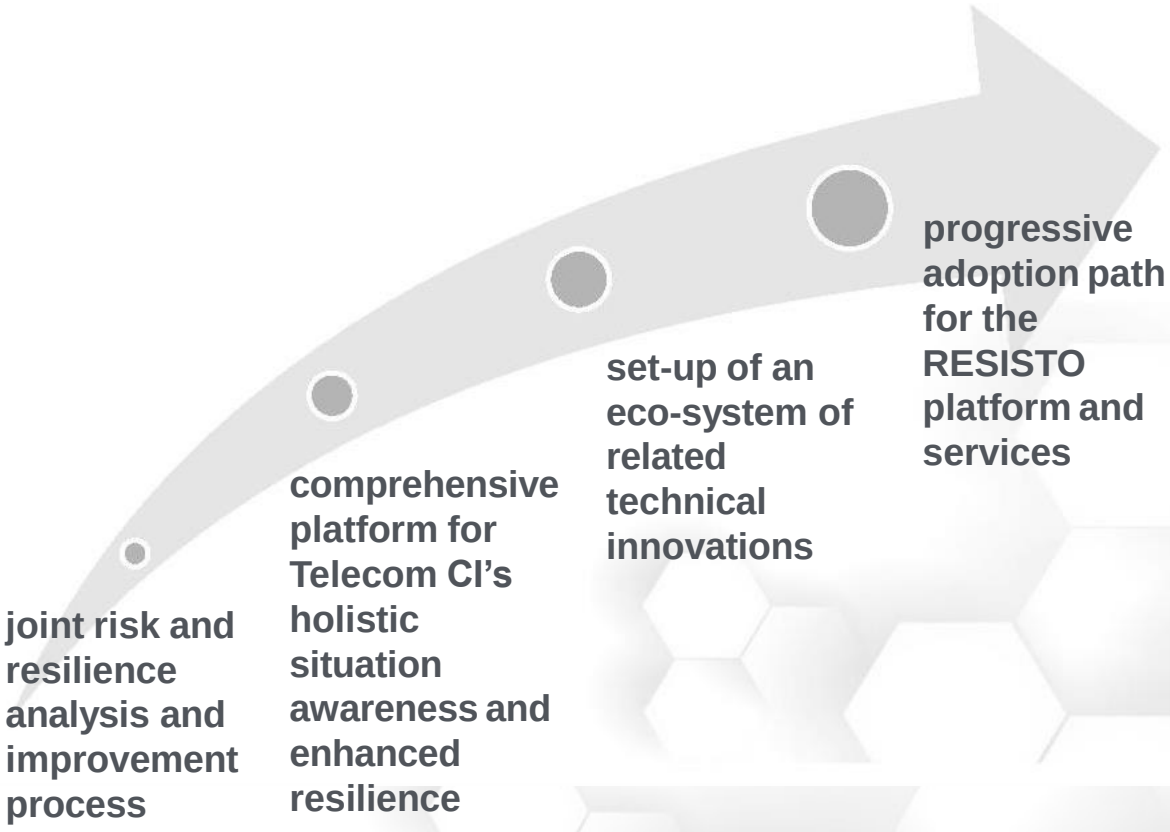
Risk and Resilience aspects in Telecommunication Infrastructures: the RESISTO approach

Nikolaos Uzunoglu

Institute of Communications and Computer Systems - ICCS



. *to **IMPROVE RISK CONTROL AND RESILIENCE** of modern Communication CIs, **against a wide variety** of Cyber-Physical Threats, being those natural disasters or even un-expected faults or malicious situations **to result in resilience improvement** and enhanced protection*



The project is at its early stages. However, a presentation of its overall risk and resilience framework will be attempted, being one of its major objectives

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 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 and Strategy of the European Union, providing suitable inputs

What is Critical Infrastructure?

Critical Infrastructure is a term used by governing bodies to describe assets that are essential for the functioning of a society and economy

TELCOs as C.I.s

Telecommunication Operators can be assets regarded as C.I. operators because they provide services necessary for coordination and basic inter-human communications

Specific VULNs & Threats

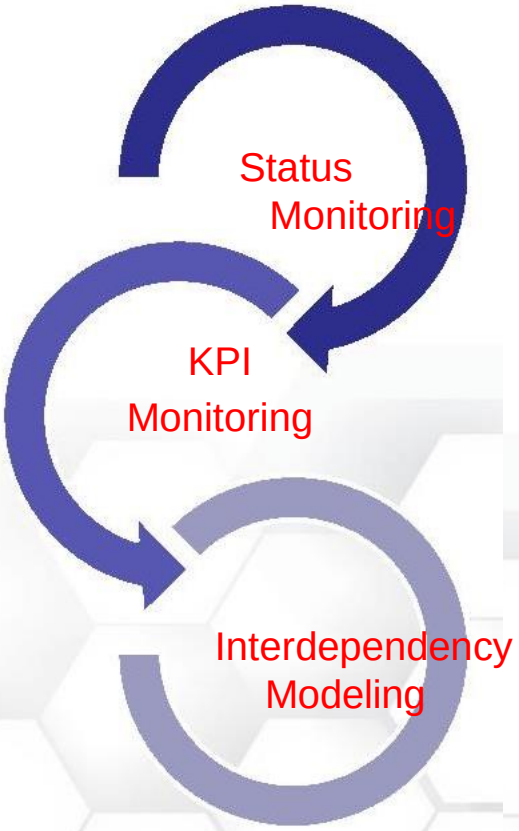
Large, complex technical infrastructure;	→ Cyber-Physical Threats
Provides services for current-gen and at least N-2 Gen devices (such as 2.5G / EDGE);	→ Specific vulnerabilities and threats (SS7)
Heavily reliant on human decisions	→ APTs relying on Social Engineering (SIM Hijacking)

RESILIENCE: The ability to provide and maintain an acceptable level of service in the face of threats, faults and challenges to normal operations.

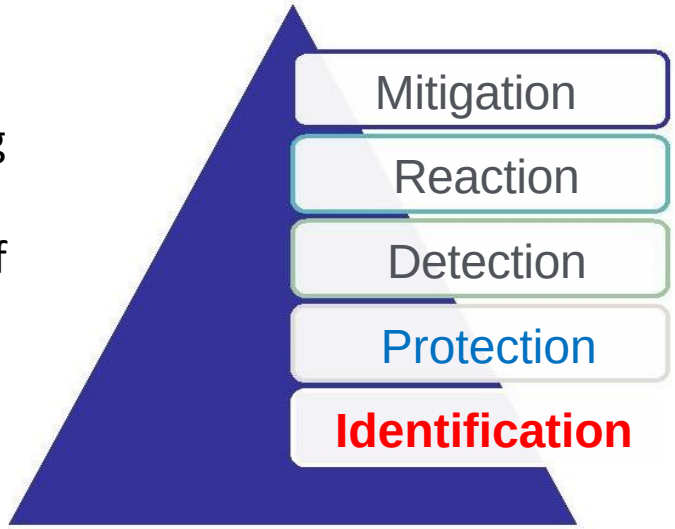
In order to increase resilience of a given system, the probable threats, challenges and risks have to be identified.

The RESISTO risk and resilience framework refers mainly to:

- Holistic Approach to Situation Awareness
- Innovative Risk & Resilience & Improvement Process Management
- Decision Support System
- Protection against cyber- physical threats
- Modeled on state-of-the art technologies (Machine Learning, IoT, Block chain)



- Introduces specific KPI monitoring
- And exploits interdependency modeling techniques
- To provide identification of system performance functions



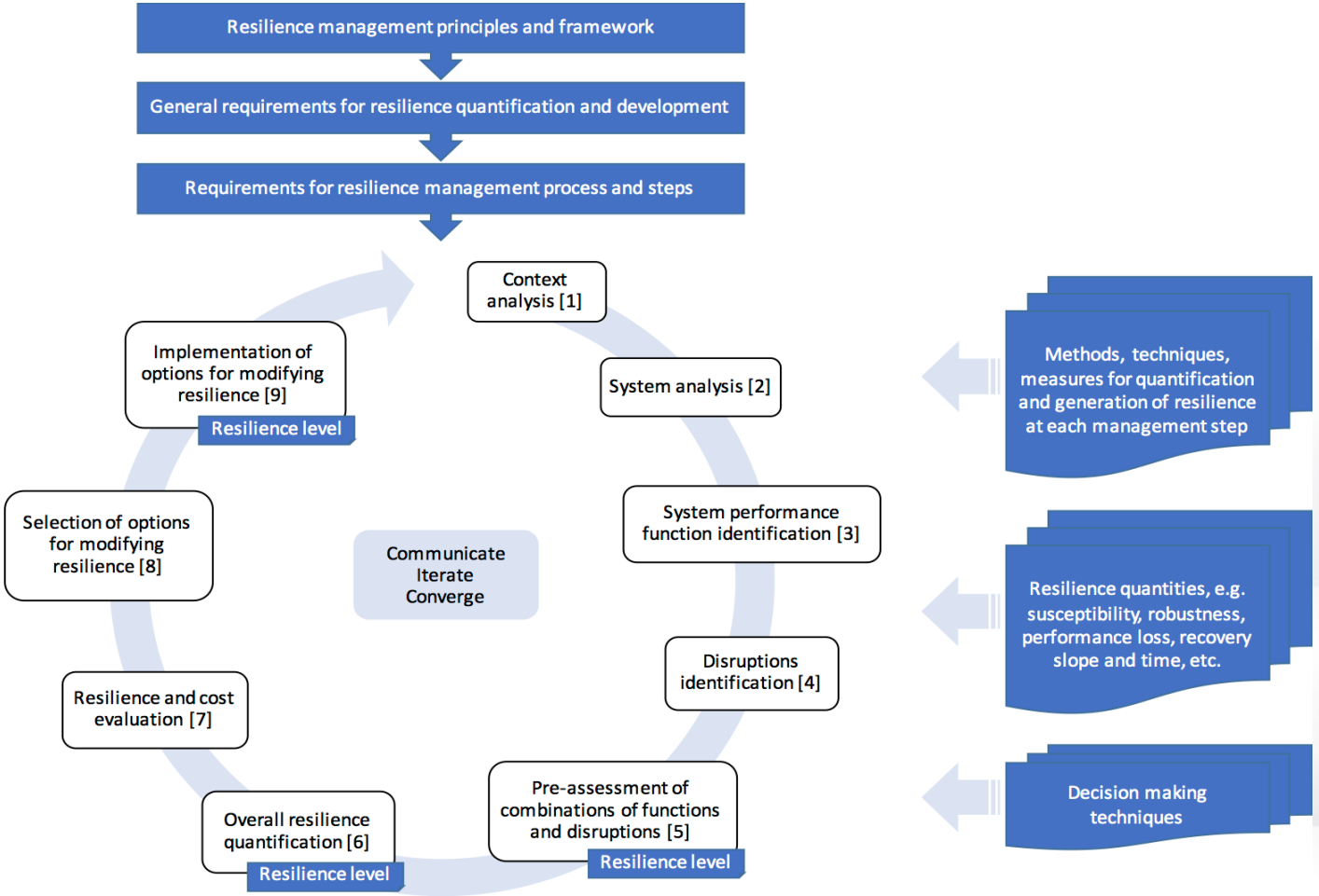
The risks and hazards list (Disruptions identification) consists of 7 ordered sub-steps:

- Threat/ Hazards/ Disruptions identification (possible root causes), classical risk events
- Identification of service function disruptions
- Elicitation of means to cover (as far as possible) unexampled events, e.g. in terms of their effects on system (service) functions
- Identification of loss of (technical) resilience capabilities
- Consideration of potentially affected system layers, e.g. physical, technical, cyber, organizational, etc.
- Summary/ Inventory of disruptions space relevant for resilience
- Assessment of uncertainty of disruptions identification

- Häring I. et al. (2017) *Towards a Generic Resilience Management, Quantification and Development Process: General Definitions, Requirements, Methods, Techniques and Measures, and Case Studies*. In: Linkov I., Palma-Oliveira J. (eds) Resilience and Risk. NATO Science for Peace and Security Series C: Environmental Security. Springer, Dordrecht

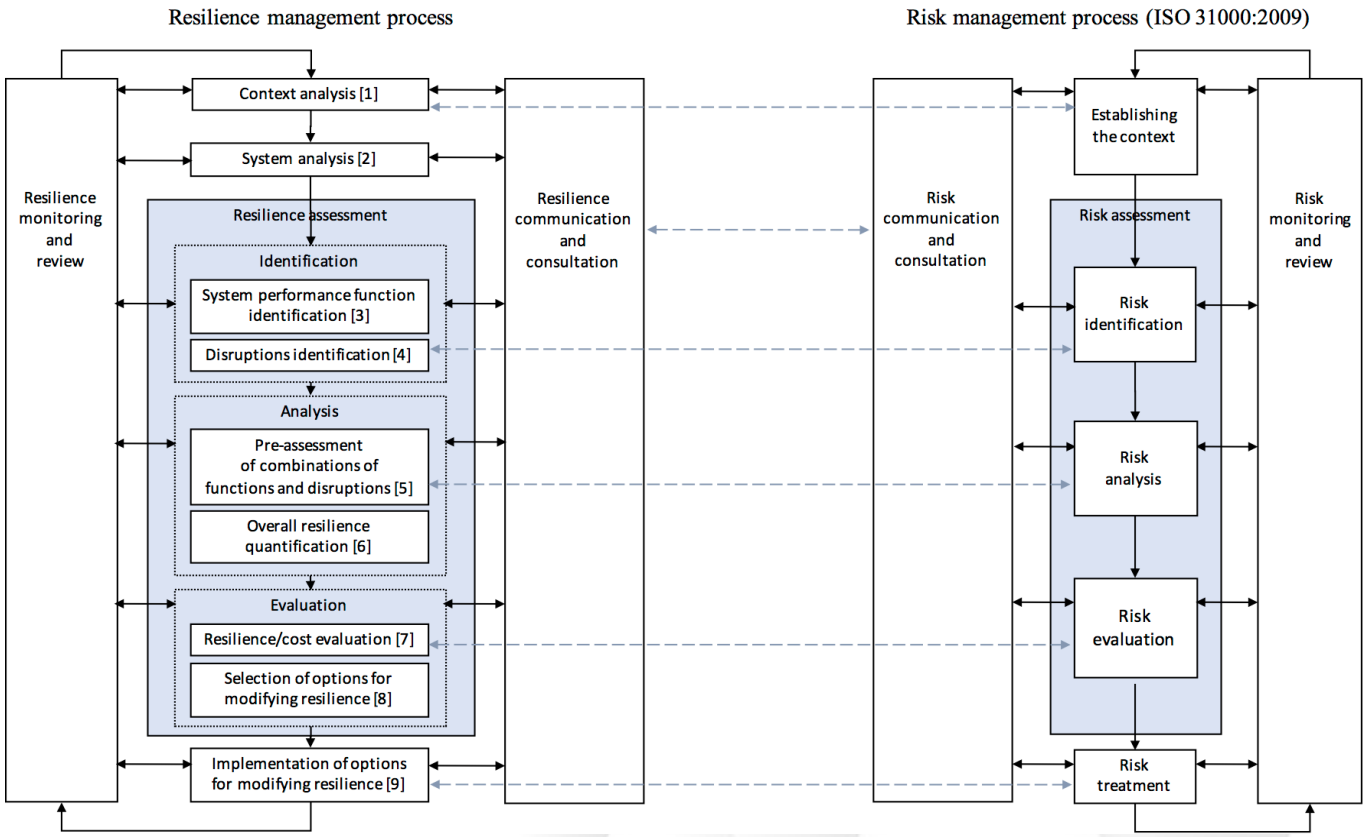
An iterative resilience management cycle, consisting of 9 sequential steps is defined

- That provides a Generic resilience management process covering resilience quantification and development



An extended resilience management process is introduced by RESISTO to define the long term analytical assessment and improvement process, in comparison to the ISO 31000 standard for risk management

- The RESISTO 9 steps risk and resilience framework are compared to the 5 steps of the ISO 31000 (2009) risk management process

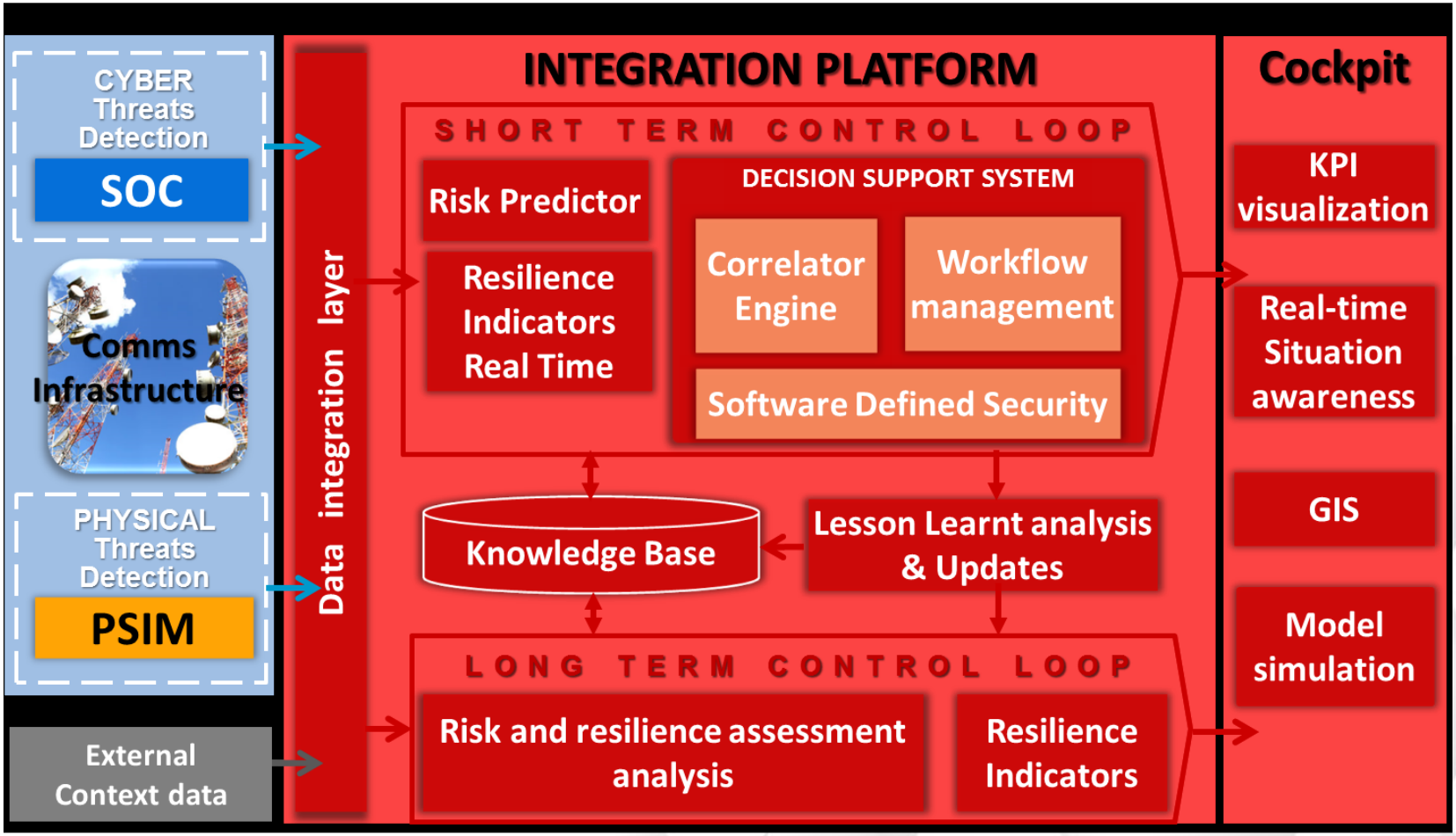


The RESISTO Logical Architecture is based on 2 control loops:

- ***The Long Term control loop:*** is in charge of defining configuration of the system.
- It mainly consists of the “Risk and resilience assessment analysis” that:
- identifies the context,
- analyzes the interdependencies (physical, cyber, logical and geographical) and the risks,
- evaluates semi-quantitatively and quantitatively those risks,
- suggests the risks treatment and “Resilience indicators” as summarizing measures of resilience of the communication CI in its operational phase;

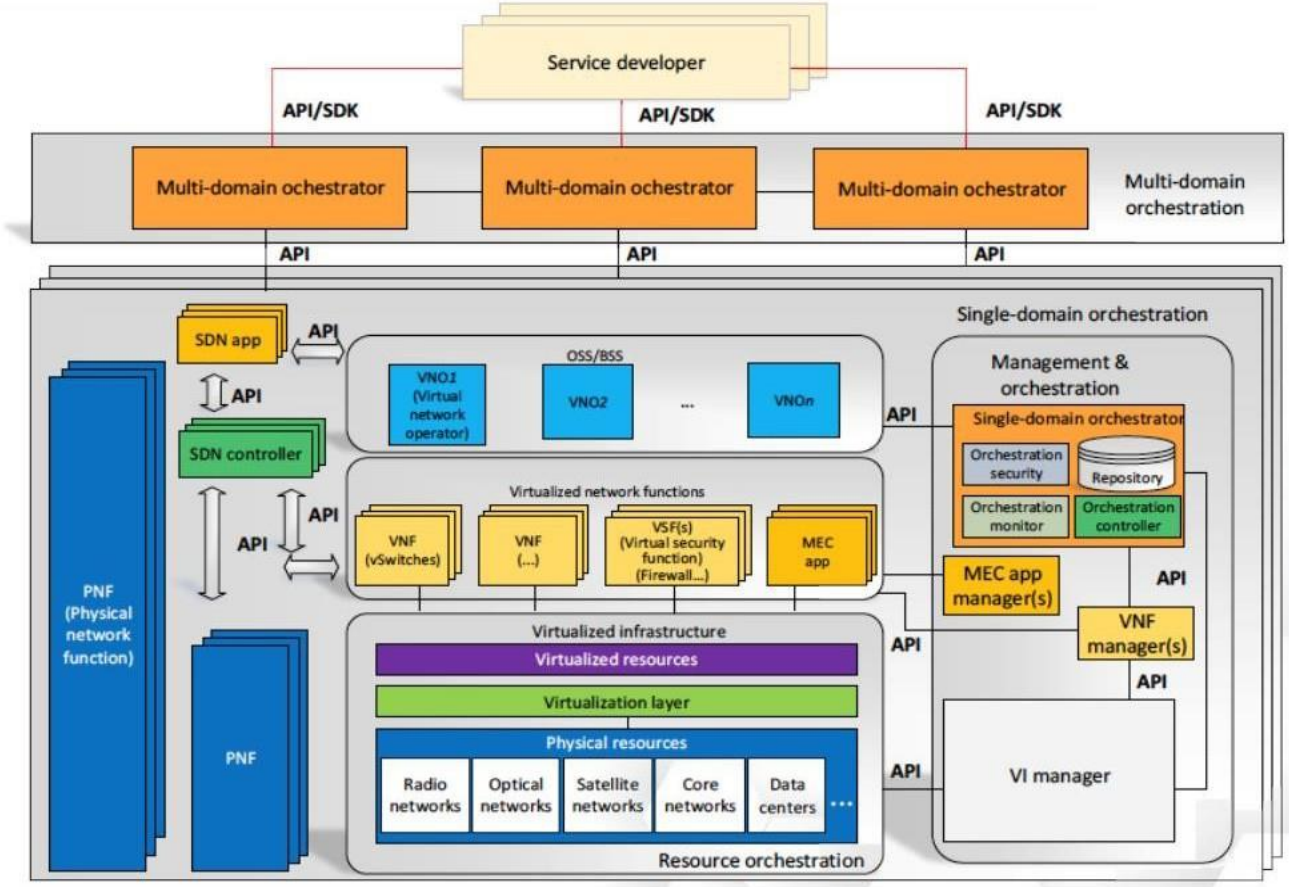
- ***The Short Term control loop:*** is in charge of promptly reacting to the impact of risks
- o Monitors the status of the infrastructures, according to the real time indicators identified by the Risk and Resilience assessment analysis,
- correlates the physical and cyber domain events in order to detect anomalies and provide early warnings.
- o Performs the “Interdependency analysis”, (**Risk Predictor**), by simulating the impact with respect to performance degradation based on possible cascading effects in other critical infrastructures in the vicinity or beyond
- orchestrates all the above to verify the resilience of the communication services

Schematic of the RESISTO Logical Architecture, where cyber and physical risks and threats are input to the system:



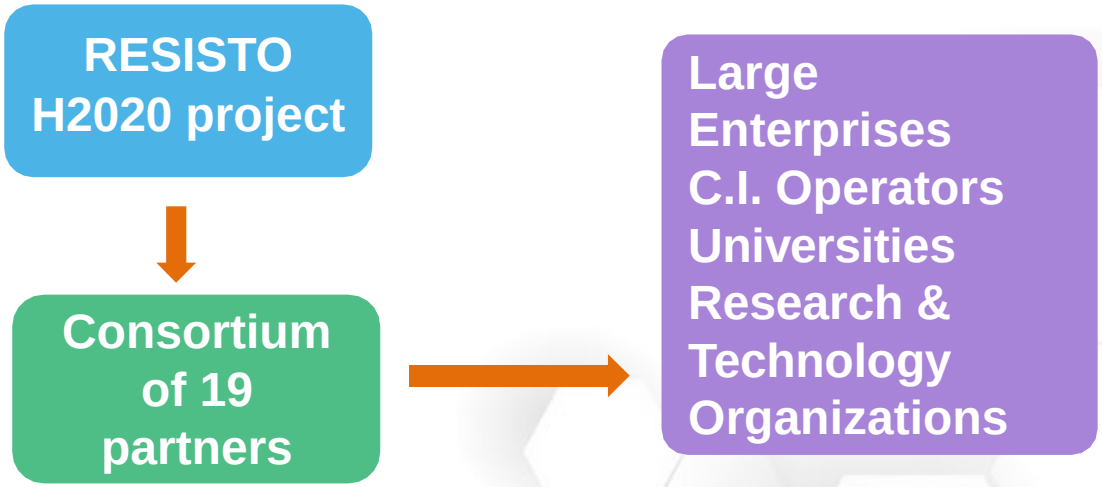
The RESISTO architecture could accommodate:

- 5G network slices, composed of configured network functions combined together for a specific use case and/or business model (e.g. 5G network functions and specific radio access technology settings)
- addressing the deployment of multiple logical networks as independent business operations on a common physical infrastructure to provide protection and management mechanisms

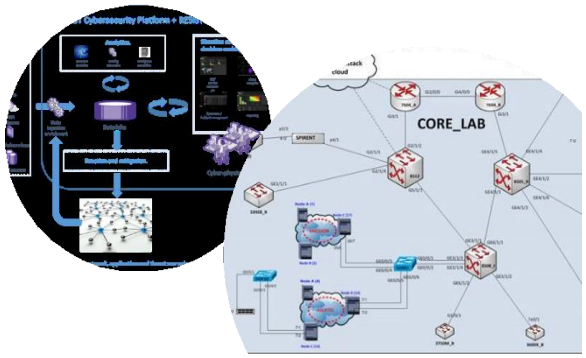


- All telecom Operators involved in the project as end users will cooperate:
- to implement on their infrastructures the Use Case pilots
- composing 3 main macro-scenaria
- and assess the results

- real joint developments activities among the involved RESISTO Telco Operators / End-Users will be demonstrated.

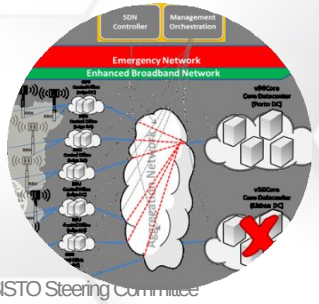


- **3 (Macro)-Scenarios, each one involving a set of related Use Cases for Improving of resilience of:**



- **Macro-Scenario 1 –Current telco Infrastructures**
  - EXCHANGE of resilience relevant information
  - i.e. real-time information sharing on a major disruption or attack between CIs
  - Protection of the existing Telecom CIs

- **Macro-Scenario 2 – Interconnected CIs**
  - Interconnected/Interdependent CIs and cascade effects
  - Their interdependencies as providers of essential communication services to other interlinked CIs
  - related cascade effects in the vicinity i.e. in power grid



- **Macro-Scenario 3 – Future telco Infrastructures (toward 5G)**
  - Their evolution towards the future 5G networks and the emerging IoT world.
  - i.e. distributed 5G study composed by direct interconnection of End Users' Test Beds

Thank you !!!