

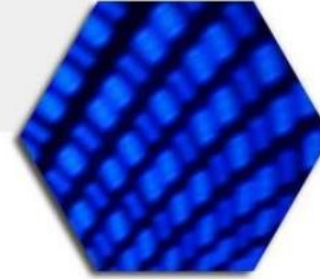


RESilience enhancement and risk control platform for communication infraSTructure Operators

ATENA Workshop, Luxembourg, October 18th

RESISTO TECHNICAL OBJECTIVES

STEFANO PANZIERI



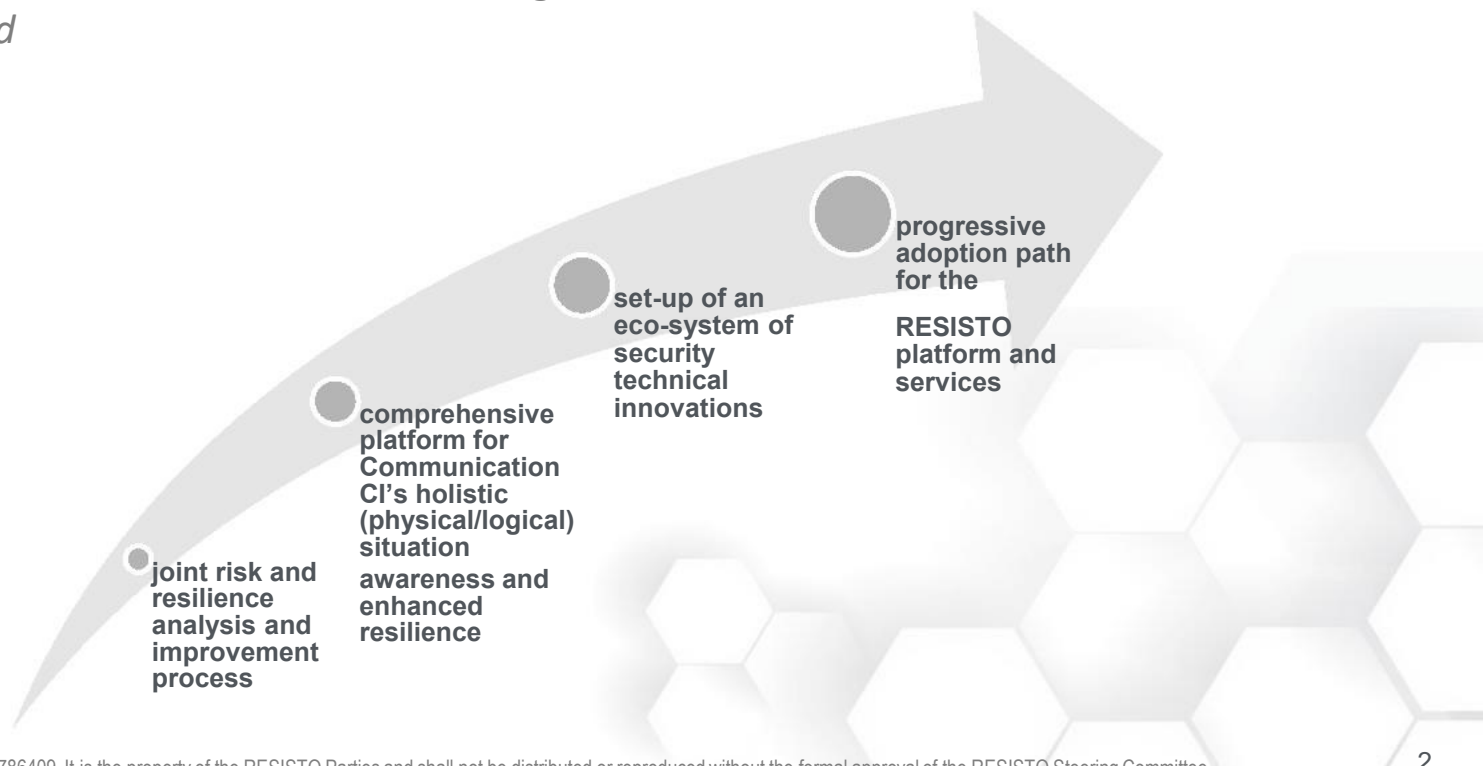
- ***3 years***
- ***10M€ cost (8M€ funding)***
- ***18 partners: 6 End Users (Telco operators) + AB***
- ***Validation across 3 Verticals: current, future and interdependent comms infrastructures***

<http://www.resistoproject.eu/>

Project Coordinator and Technical Coordinator			
1(coo.)	Leonardo S.p.A.	LDO	IT
2	Dipartimento di Ingegneria Università degli Studi Roma Tre	RM3	IT
Communication Infrastructure Operators - Practitioners			
3	Telecom Italia Mobile - TELECOM ITALIA SPA	TIM	IT
4	Hellenic Telecommunications Organization S.A. - (Organismos Tilepikoinonion tis Ellados)	OTE	GR
5	British Telecom – British Telecommunications Public Limited Company	BTC	UK
6	Orange Romania SA	ORO	RO
7	Retevision I, S.A. - Cellnex Telecom, S.A	RTV	ES
8	Altice Labs SA – Telecom Portugal	ALB	PT
Large Enterprises			
9	Ericsson Telecomunicazioni SpA	TEI	IT
RTOs/Universities			
11	Ernst-Mach-Institut - Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V.	EMI	D
12	Institute of Communication & Computer Systems - National Technological University of Athens	ICCS	GR
13	Bergische Univesitaet Wuppertal - University of Wuppertal, Institute for PS and EM	BUW	D
14	Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione – IT-CERT	CER	IT
Small Medium Enterprises - SMEs			
15	INTEGRASYS S.A	INT	ES
16	GUARDTIME AS	GT	EE
17	ADITESS Advanced Integrated Technology Solutions & Services LTD	ADI	CY
18	TREELOGIC Telematica Y Logica Racional Para La Empresa Europea SL	TRE	ES
19	BIT SENTINEL SECURITY	BSS	RO

. 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



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

Identification – Define and maintain a knowledge base on physical and cyber security risks to systems, assets, data, and capabilities characterizing Telecommunication CIs.

Protection – Develop and implement the appropriate safeguards to ensure delivery of CI services.

*The **high degree of redundancy** that usually characterizes telecommunication networks will be further emphasized in order to implement solutions with high resilience, with respect to both physical and cyber-attacks.*

*Graceful degradation of performance, when under attack, will take advantage of Communication or **NFV** and **SDN** paradigms.*



Mitigation

Reaction

Detection

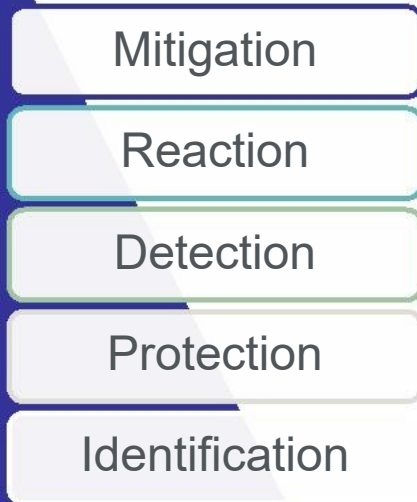
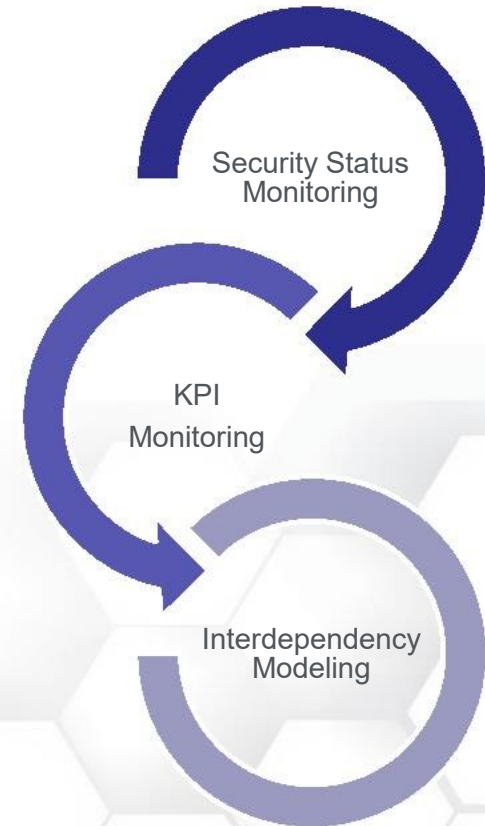
Protection

Identification

Detection – Early and timely discover the occurrence of physical and cyber security events.

Based on evaluation of impacts, recurrent patterns, and the occurrence of complex events.

To provide a timely detection of a cyber/physical attack, the project will leverage on use of innovative technologies delivered by partner SMEs and RTOs, properly integrated with security solutions/components already available in the communication CI.



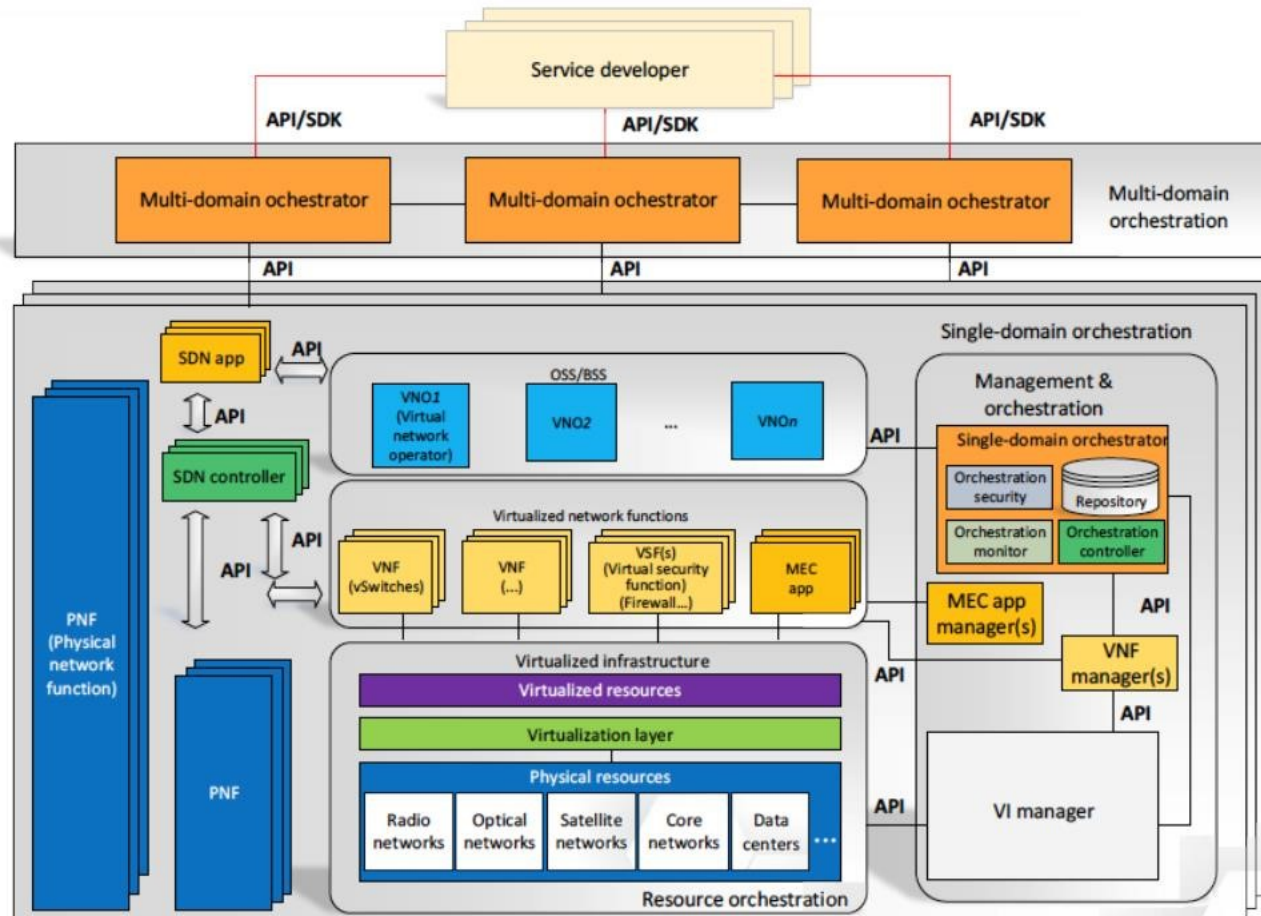


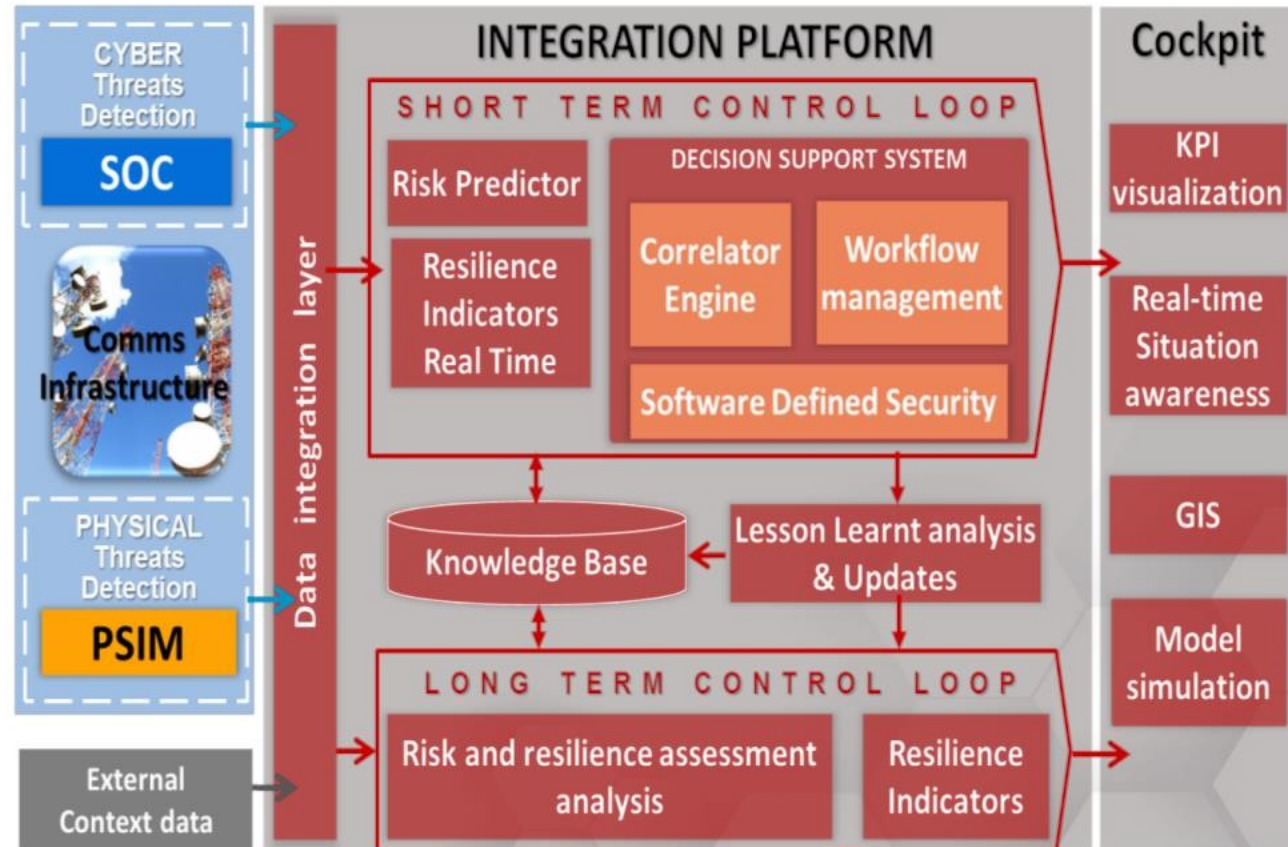
Reaction – Orchestrate and implement effective response to a detected security event.

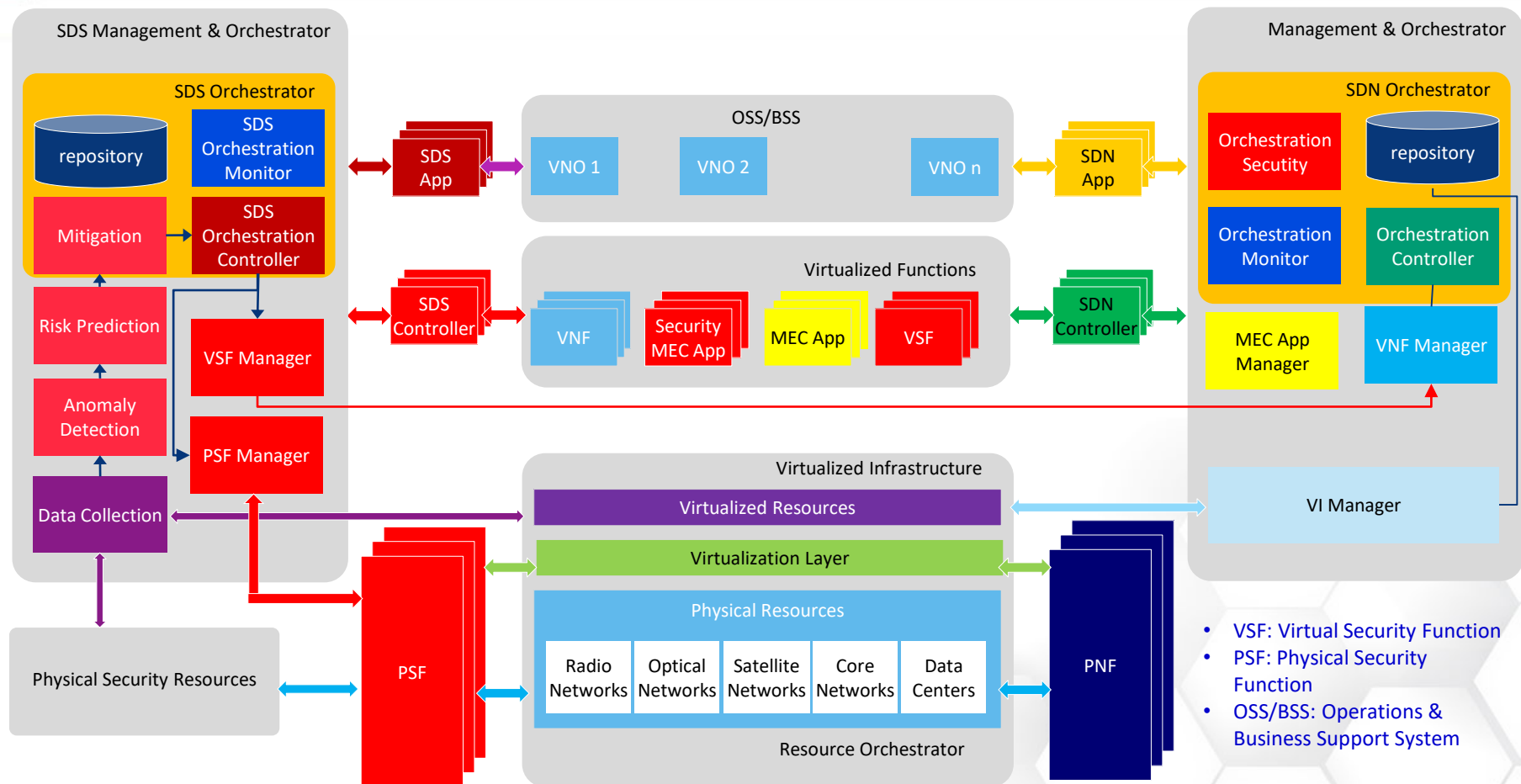
- *RESISTO will investigate the joint use of Security Function Virtualization and Software Defined Security.*
- *Moreover, identifying the best response requires significant advancements in the state of the art such as tools for the automatic impact assessment of the security risks and performance and effectiveness of potential countermeasures.*

Mitigation – Develop and implement the appropriate activities to mitigate the impacts of the threat and to restore as much as possible capabilities or services that were impaired due to a security event.

- **E2E (end to end) network slicing** addresses the deployment of multiple logical networks as **independent business operations** on a common physical infrastructure.
- The Network slice is a composition of adequately configured **network functions**. Network applications, and the underlying cloud infrastructure that are bundled together to meet the requirements of a specific use case.
- a “**5G SLICE**” could be composed of a collection of
 - **5G network functions (NF)** and
 - a specific **radio access technology (RAT)** settings combined together for a specific use case and/or business model.
- **network slices** must fulfill a set of requirements such as
 - the need for sharing and efficiently reusing resources
 - differentiation of traffic per slice;
 - visibility of slices;
 - protection mechanisms among slices (a.k.a. slice isolation);
 - and support for slice-specific management







- VSF: Virtual Security Function
- PSF: Physical Security Function
- OSS/BSS: Operations & Business Support System

- The **DSS SDS** is a **reaction/resilience mechanism** that integrates mitigation and resiliency functionalities into a unique framework able to dynamically and proactively react to the evolving threats by enforcing the most appropriate security policies in each CI node.
- SDS components:
 - **MITIGATION MODULE** selects the countermeasures, performing the updating of the security policies, on the basis of a multi objective analysis aimed at: increasing the resilience of infrastructure and services to customers, minimizing the risk of cascading effects, minimizing the impact on system performance.
 - **ORCHESTRATION MODULE:** manages the cyber physical resources needed to apply the security policies stated by the Mitigation Module.

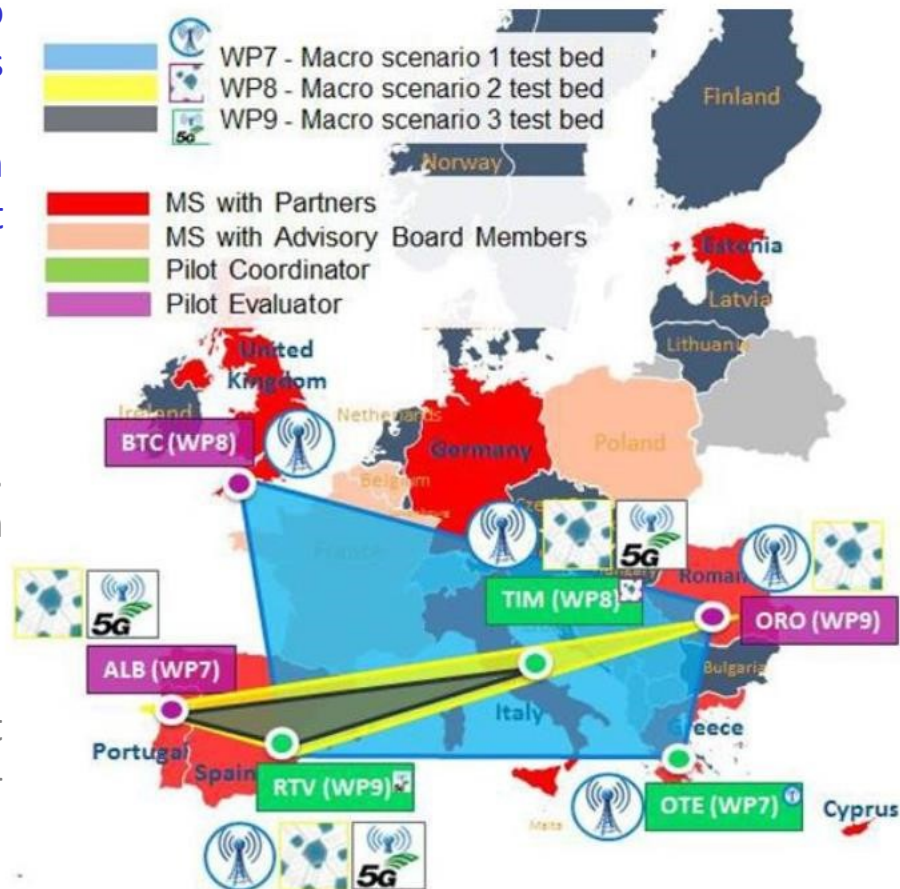
Its role is to build complex security functions and services from less complex/primitive security mechanisms/functions.

In this process, the orchestrator has to consider service specific requirements, in terms of Authenticity, Integrity, Confidentiality, etc.

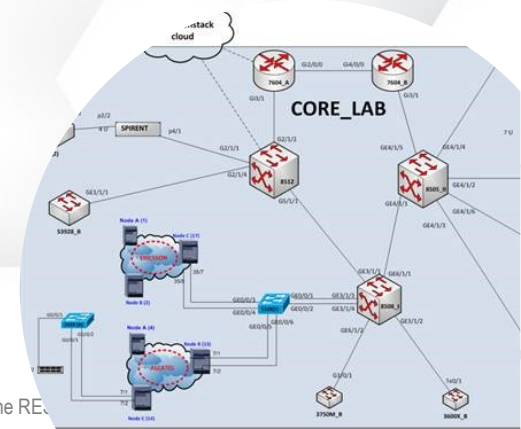
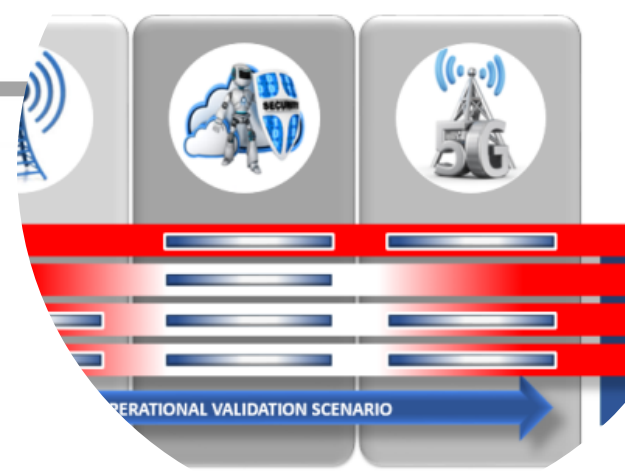
This is done through the entire lifecycle of a function/service, i.e. deployment, operation, monitoring and termination. In addition, it analyses the network situations in real time, diagnoses and predicts existing or emerging network issues, and determines and coordinates reactive or proactive actions to resolve issues.

All end users involved in the project will cooperate to implement on their infrastructures the Use Case pilots composing each macro scenario and assess the results. A Federation scheme of the pilot Use Cases within each Macro-Scenario is envisioned, to demonstrate real joint developments activities among the involved RESISTO Telco Operators / End-Users. This federation will be achieved through the exchange of:

- EXCHANGE of resilience relevant information (i.e. real-time information sharing on a major disruption or attack between three CIs: TIM, OTE and ORO in Scenario 1)
- direct interconnection of the Test-Beds (i.e. distributed 5G study composed by direct interconnection of Cellenext and AlticeLabs test-beds in Scenario 3).



-
- The diagram illustrates a 5G network architecture. At the top, two boxes represent 'SDN Controller' and 'Management Orchestration'. Below these are two horizontal bands: a red band for 'Emergency Network' and a green band for 'Enhanced Broadband Network'. The central part of the diagram shows a cloud labeled 'Aggregation Network'. To the left, a vertical stack of components includes '5G Core Network (Edge)' and '5G Core Network (Core)'. To the right, there are three 'Core Data Center (CDC)' blocks. The top CDC is labeled 'v4GCore Core Datacenter (Polaris DC)' and is connected to the Aggregation Network. The middle CDC is labeled 'v4GCore Core Datacenter (Atlas DC)' and is also connected. The bottom CDC is labeled 'v4GCore Core Datacenter (Atlas DC)' and is marked with a large red 'X', indicating it is not part of the current configuration or is deprecated.



Thank you for your Attention

