

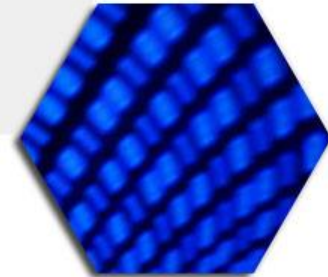
RESISTO: Improving the Resilience of a Telecommunication Infrastructure

ECSCI (European Cluster for Securing Critical Infrastructures) Workshop

Venue: Google Meet

24th June 2020

Bruno Saccomanno (Leonardo)



RESISTO – This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 786409

- RESISTO: numbers and consortium
- Objectives and implementation status
- Basic idea
- RESISTO platform
- Validation
- Benefits

RESISTO: RESilience enhancement and risk control platform for communication infraSTructure Operators

- European Horizon 2020 project
- GA number: 786409 (IA - Innovation Action)
- 3 years (May 2018 - April 2021)
- EU Topic: CIP-01-2016-2017 - Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe
- Budget Info: ~10M€ eligible cost (funding ~8M€)
- Partners: 16 (and 1 Third Party)

RESISTO Coordinator

Scientific-Technical Coordinator



RESISTO COSORTIUM:



LEs:
Technology Providers



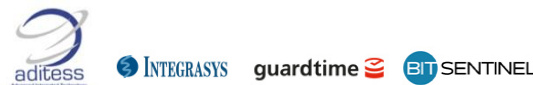
LEs:
TELCO Operators



RTOs:
Research and Technical Organizations



(ROMA3 Third Party)

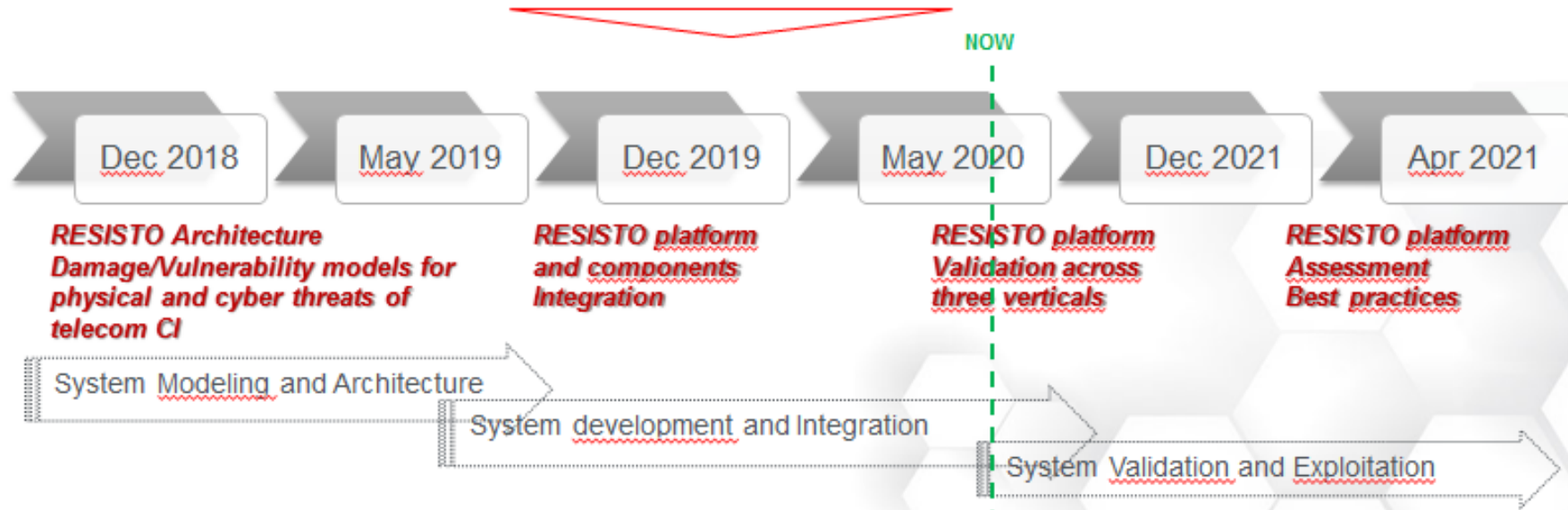


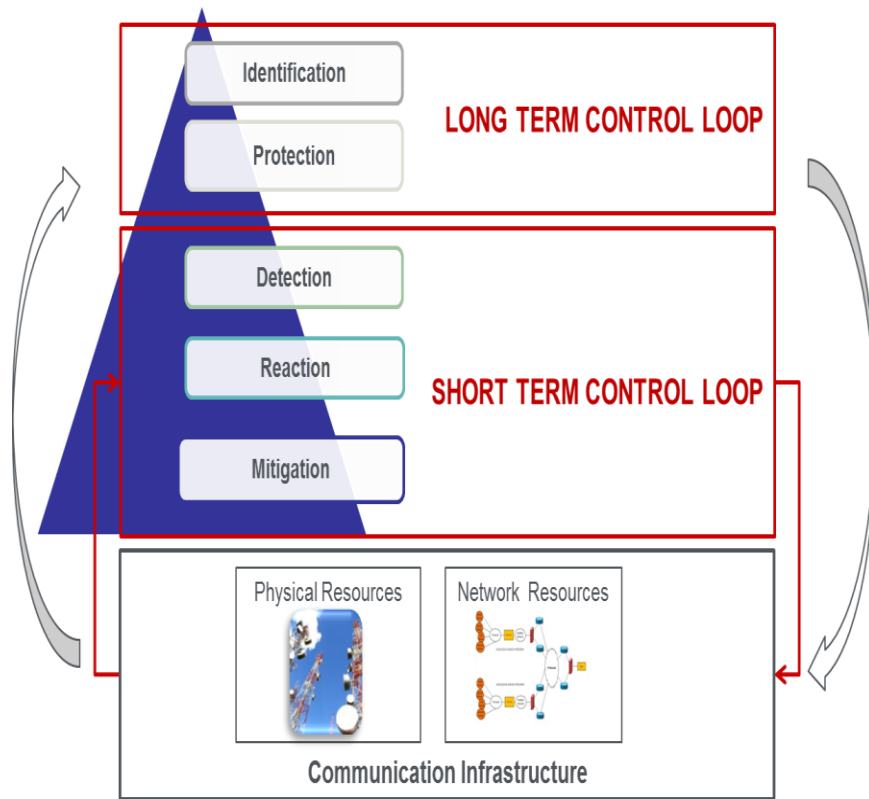
SMEs:
Technology Providers

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 unexpected faults.*

- Deliver an innovative platform for optimized decision support in the face of physical, cyber and **combined cyber-physical** threats
- Develop an Integrated **Risk and Resilience analysis and management framework**
- Provide, experiment and assess a suite of **innovative cyber/physical security solutions** for prevention, protection, detection and reaction

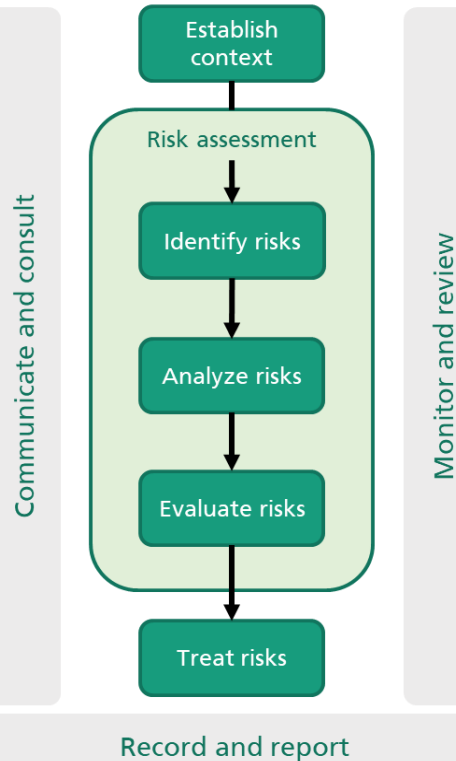




- LCTL (Long Term Control Loop) is an **offline** activity
- The loop is performed on a periodic basis (i.e. quarterly or annually) or even monthly or when particular events take place
- The STCL (Short Term Control Loop) is **the platform runtime component**, for the operative security management of the Critical infrastructure

Resilience management process

Risk management process

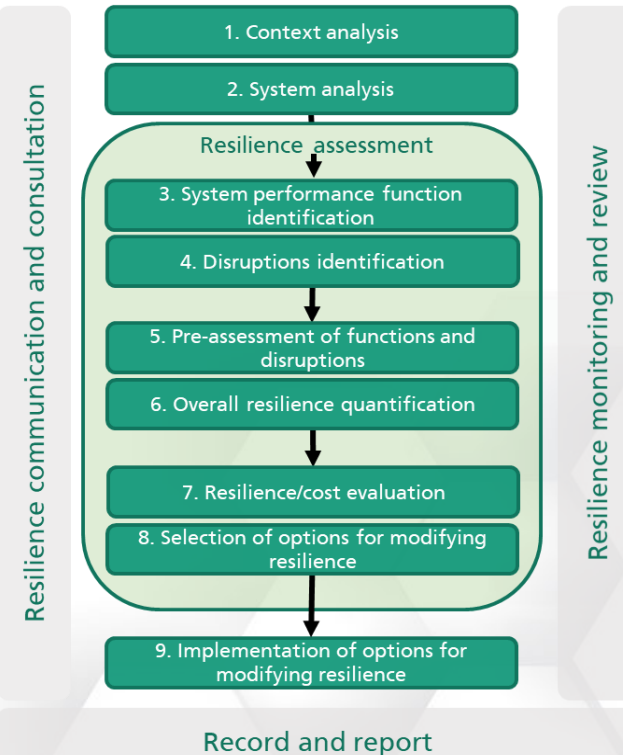


The resilience management process used in RESISTO is extension of the ISO 31000 standard [1] developed in [2].

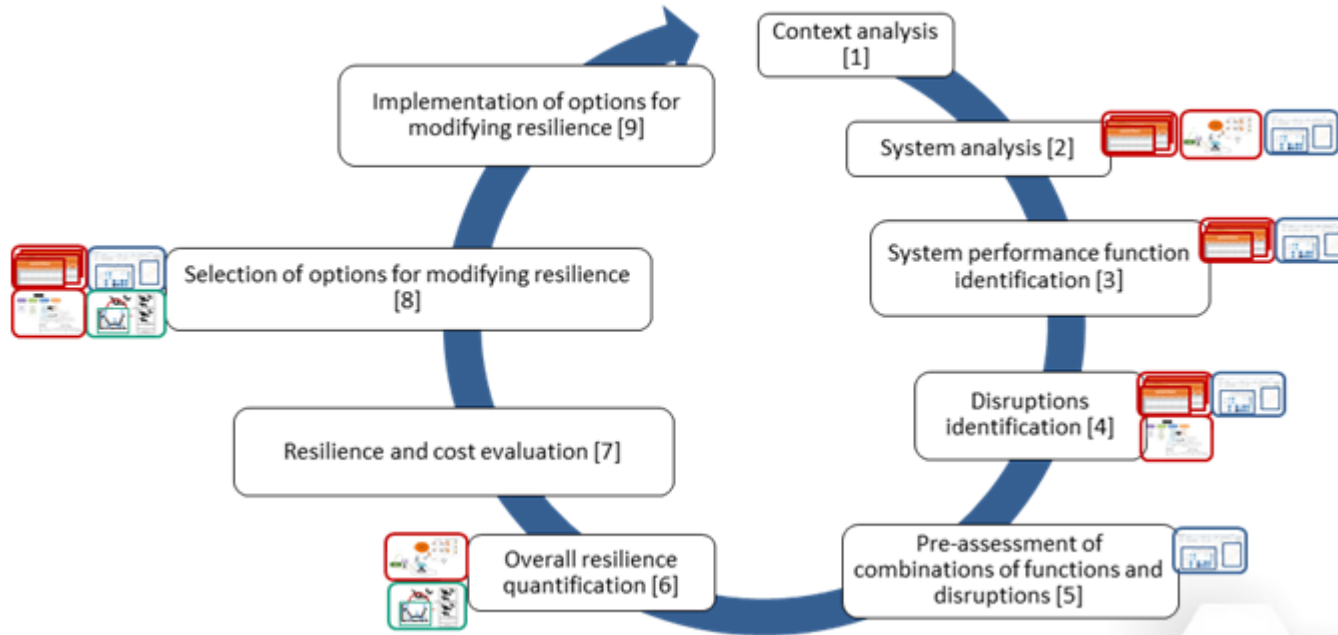


An iterative process that investigates resilience that requires certain inputs from end users and software tools at each step.

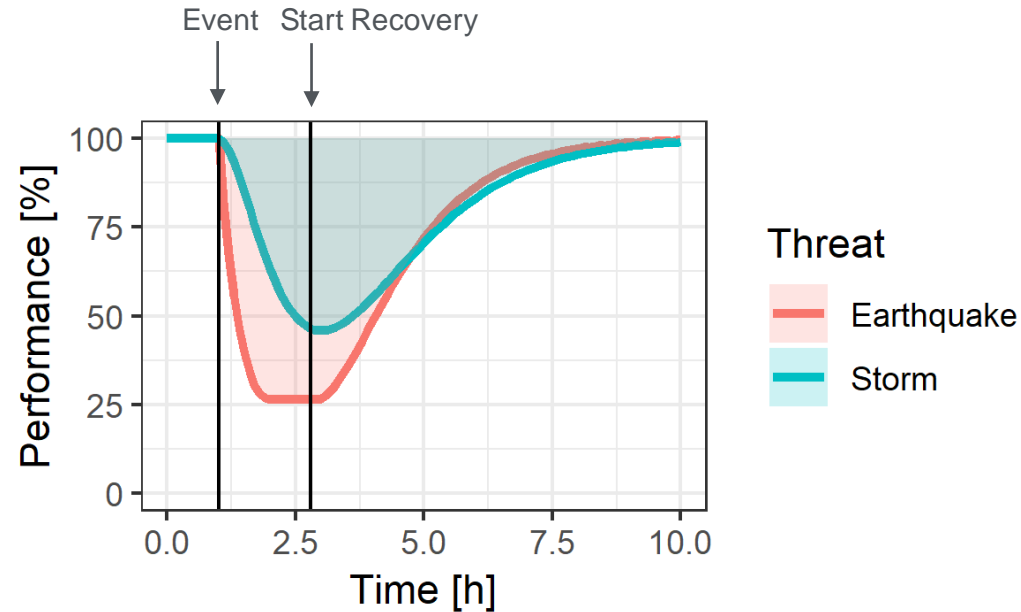
Resilience management process



LTCL is based on **Risk and Resilience Management Framework**



RIs - Resilience Indicators

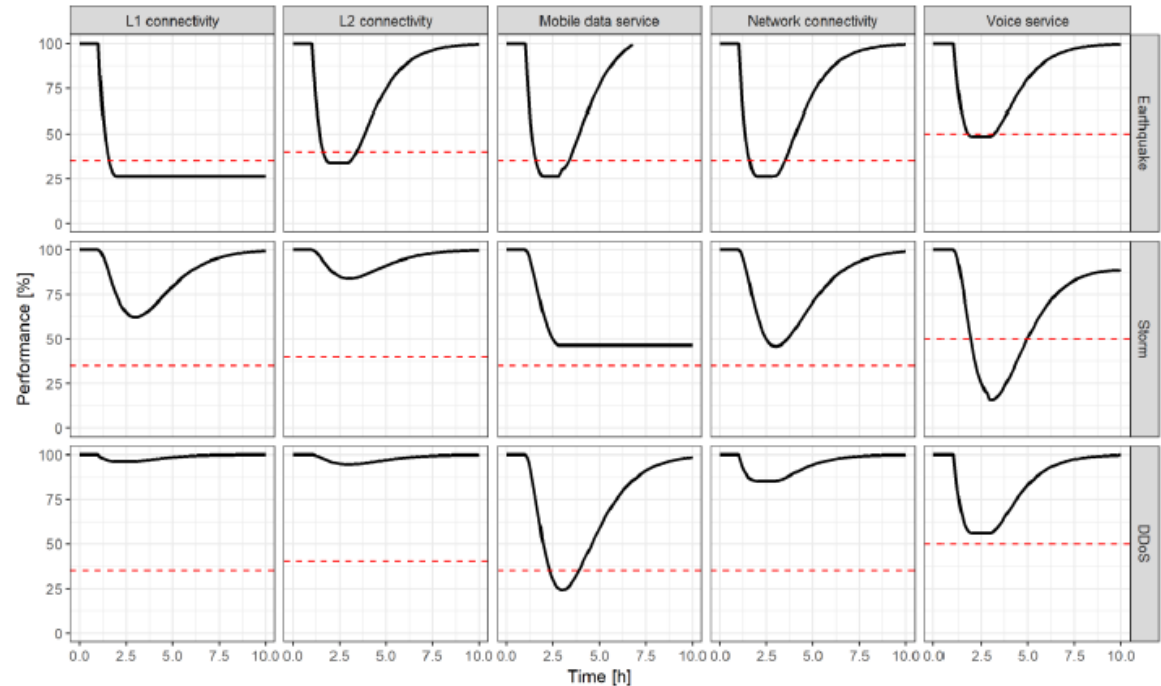


RIs - Resilience Indicators

Resilience indicators (RI) for each couple of threat/performance will be computed and stored in the knowledge base

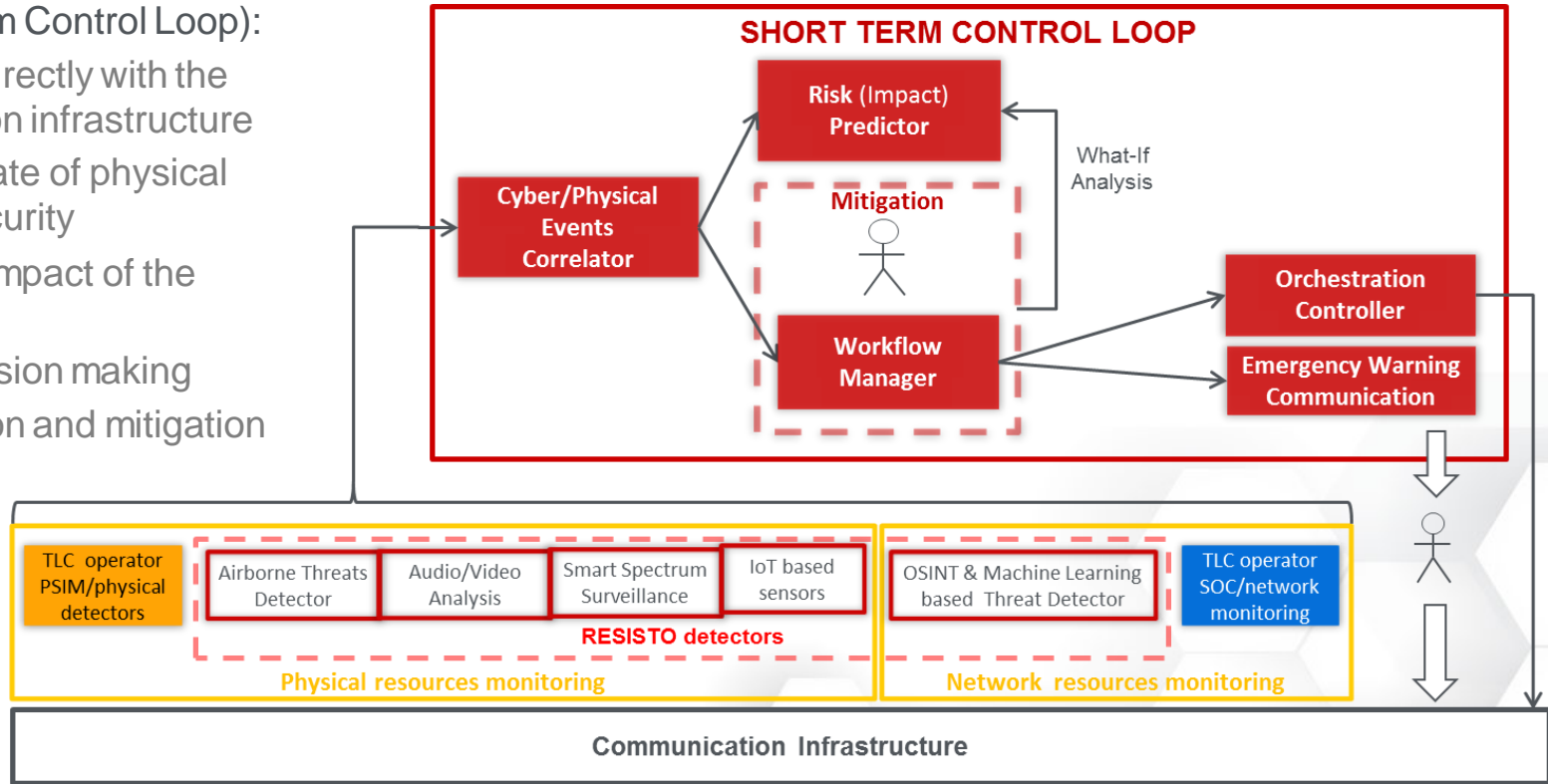
CaESAR (the simulator used in RESISTO) outputs performance time curves for different threats and performance functions.

Improvement measures can be implemented and tested to see their effectiveness.



STCL (Short Term Control Loop):

- it interfaces directly with the communication infrastructure
- checks the state of physical and cyber security
- evaluate the impact of the events
- supports decision making
- guides reaction and mitigation

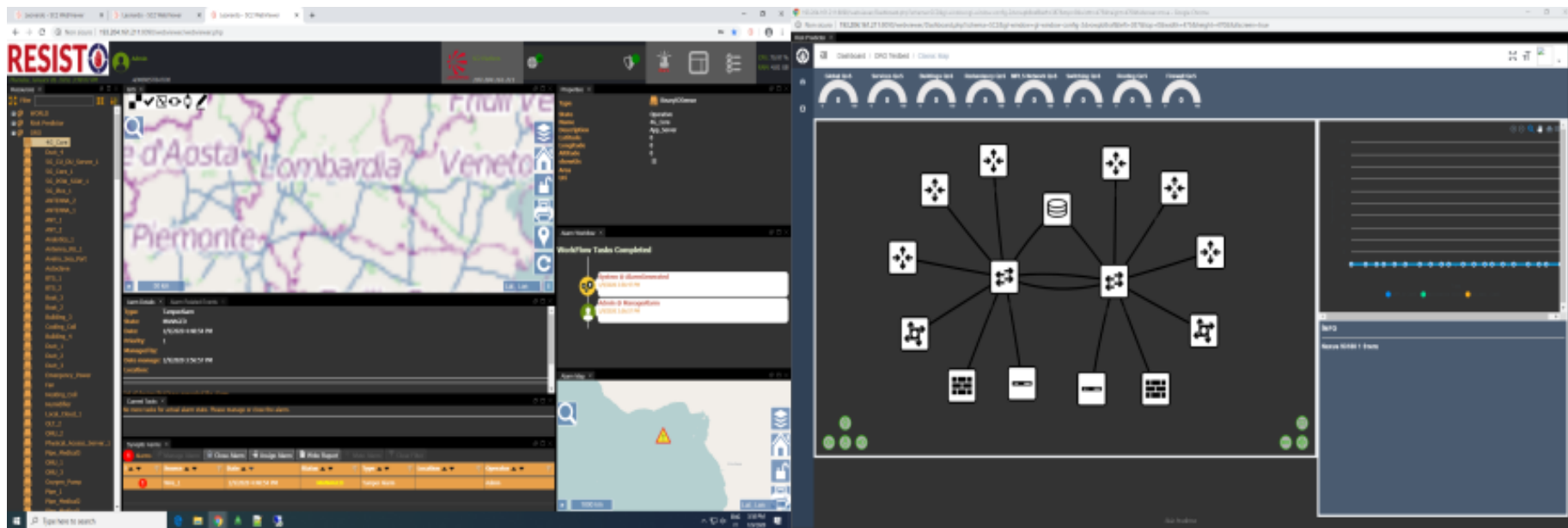


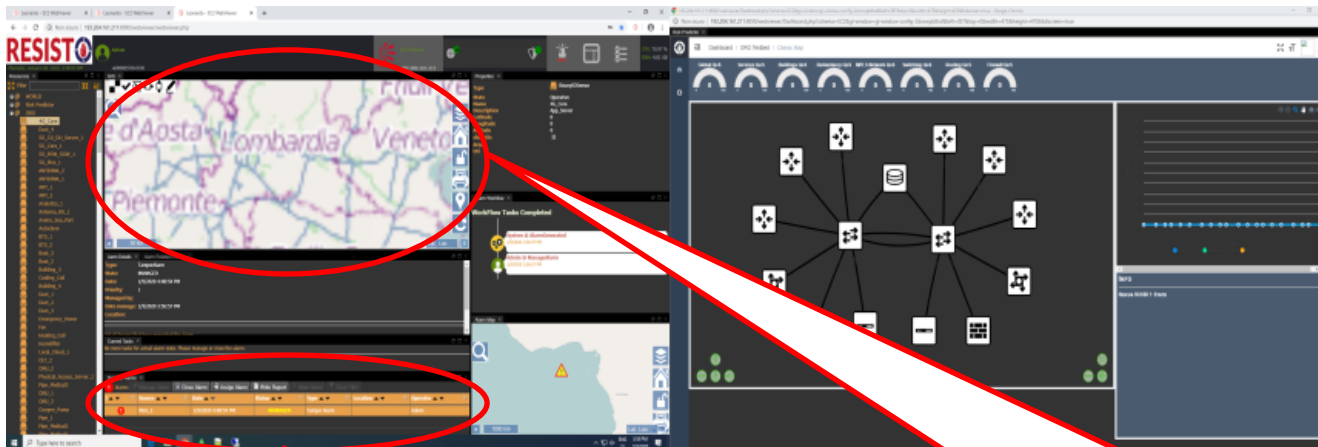
“A Decision Support System (DSS) is an information system that supports business or organizational decision-making activities. DSSs serve the management, operations and planning levels of and help people make decisions about problems that may be rapidly changing and not easily specified in advance.”

The RESISTO *Decision Support System* is composed by:

- Alarm Management dashboard
- Workflow manager
- Risk predictor

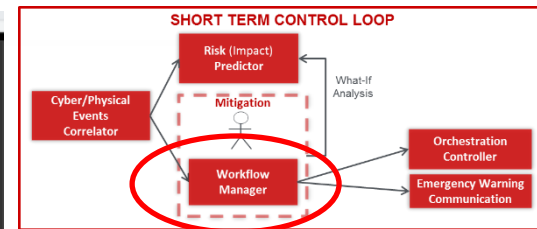
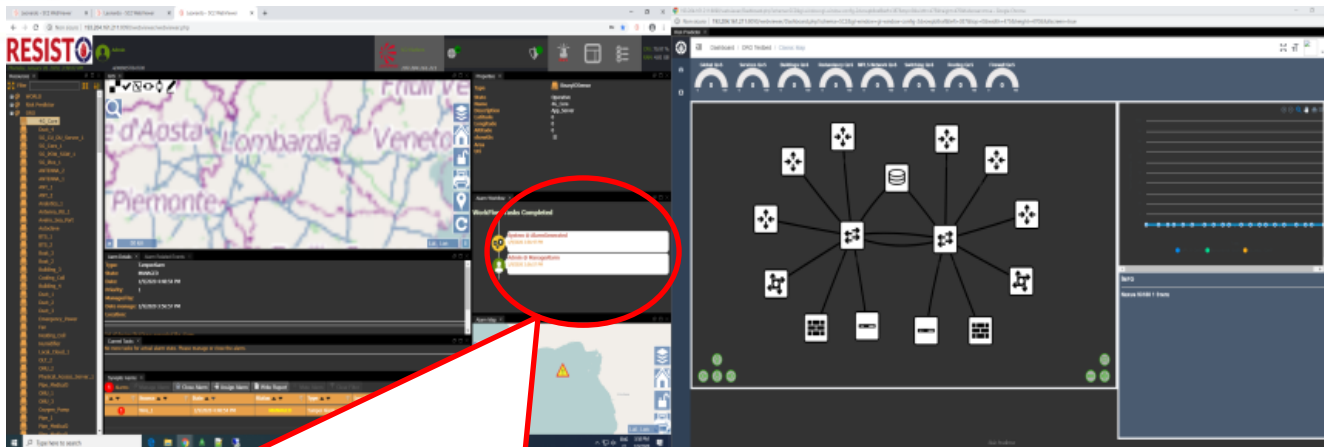
RESISTO DSS cockpit is built on the base of Leonardo SC2 platform and it is hosted on a 2 screens layout to provide to the operators a complete situation awareness along each alarm life cycle.





Alarm Management area collects all active alarms tracing the alarms progress

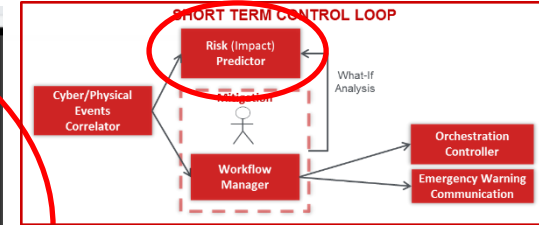
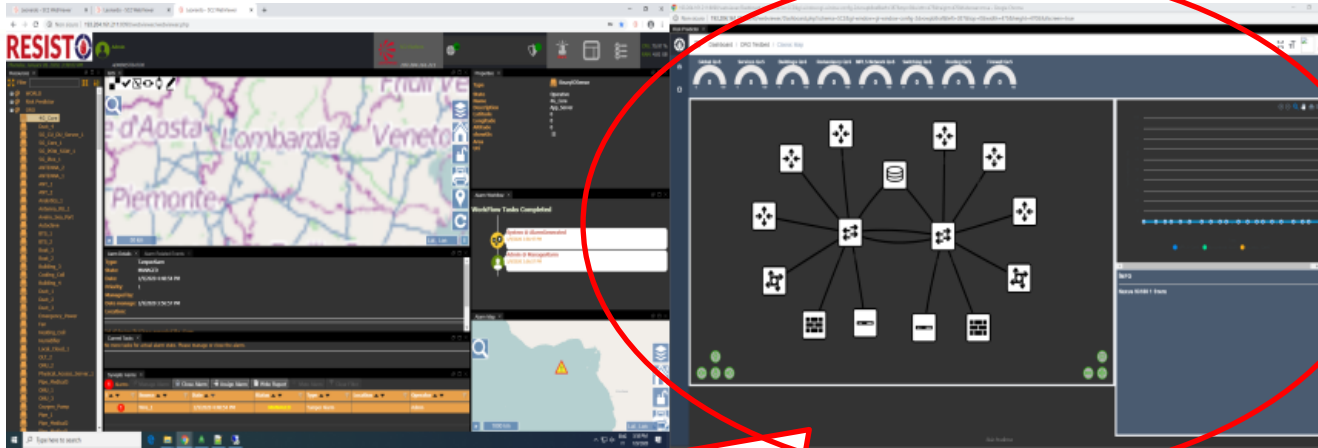
A **workspace** is available to display alarm specific contents (i.e. geographic views)



Workflow manager section lists all the tasks already completed for the workflow associated to the currently managed alarm. A color code helps to trace operations types and state:

- User Task: operations performed by the operator
- Service Task: automated tasks
- Current Task: current operation
- Completed Task: completed operations





Risk Predictor HMI is hosted in the 2nd screen, it provides:

- A synoptic view of infrastructure components status
- Alarm impact evaluation in terms of cascade effects and services provision
- Services provision vs. time view

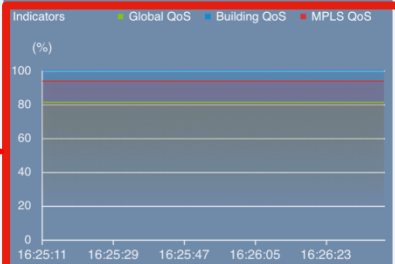
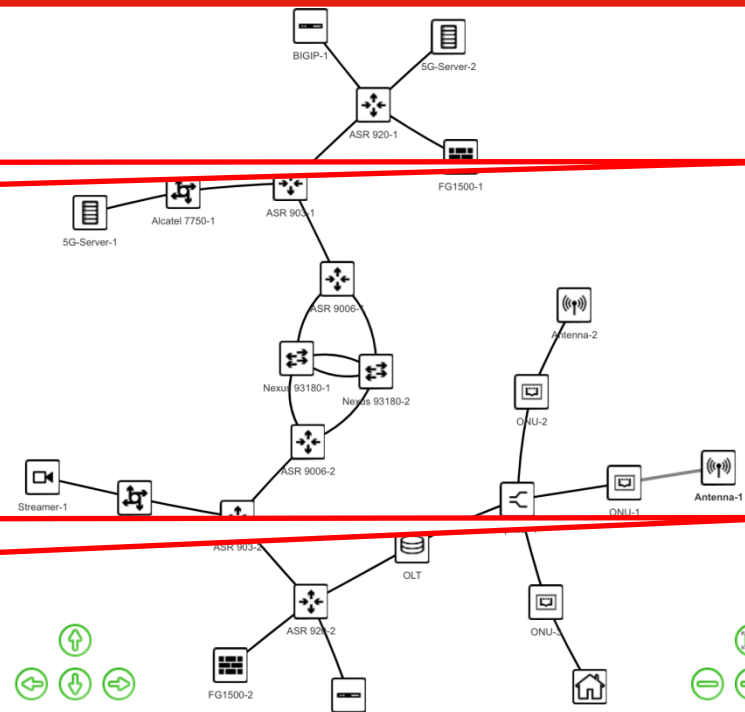
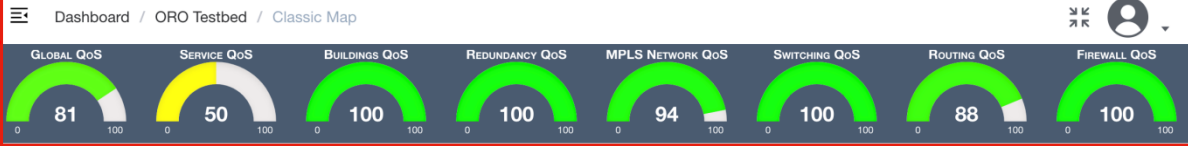
Indicators

Real-time chart

Details on the clicked object

RESISTO Risk Predictor

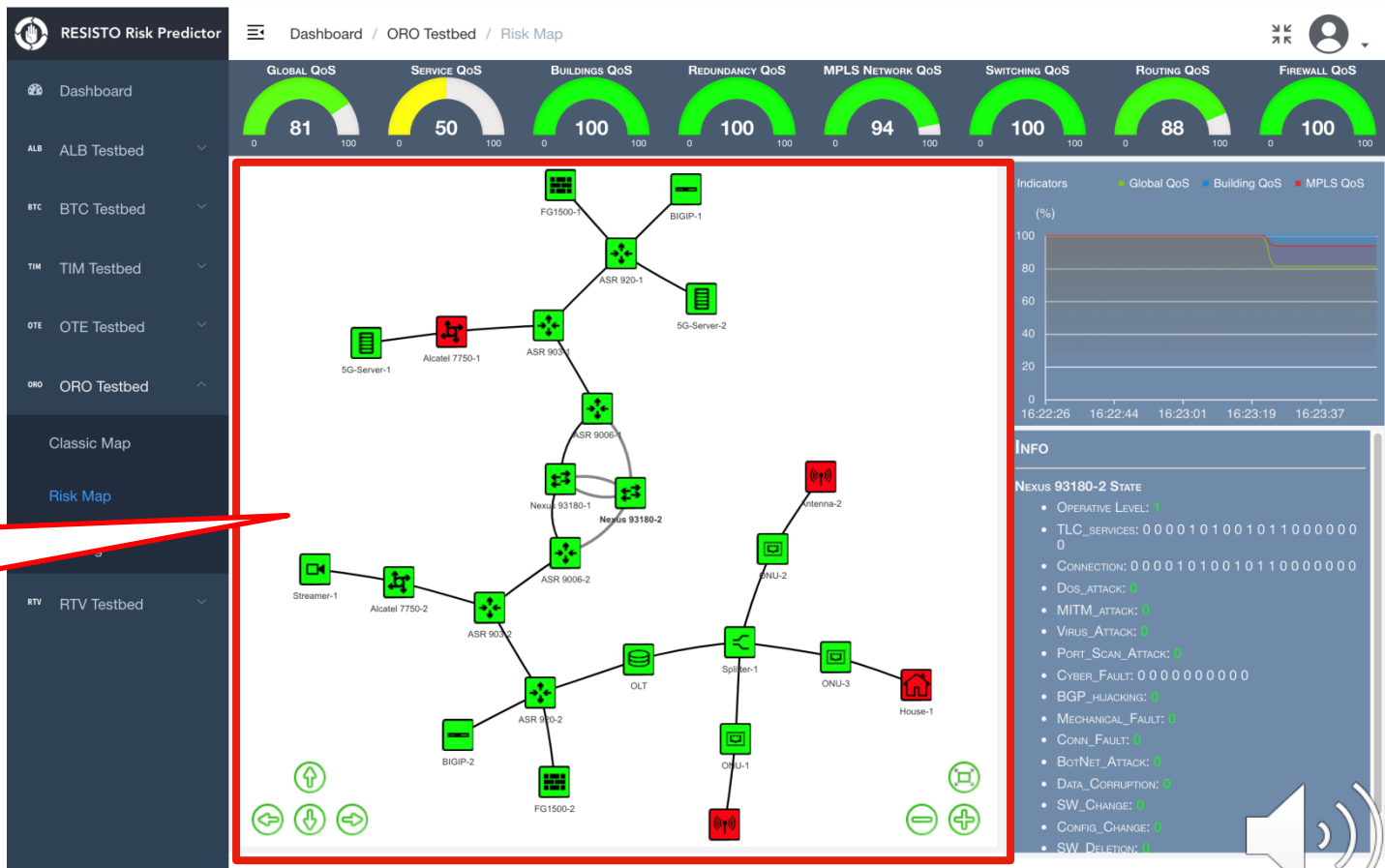
- Dashboard
- ALB ALB Testbed
- BTC BTC Testbed
- TIM TIM Testbed
- ORO ORO Testbed
- Classic Map
- Risk Map
- Building
- RTV RTV Testbed



INFO

ANTENNA-1 STATE

- OPERATIVE LEVEL: 0
- TLC_SERVICES: 00000000000000000000
- CONNECTION: 00000000000110000000
- DOS_ATTACK: 0
- MITM_ATTACK: 0
- VIRUS_ATTACK: 0
- PORT_SCAN_ATTACK: 0
- CYBER_FAULT: 0000000000
- MYCONN: 000000000000000000000000
- BGP_HIJACKING: 0
- MECHANICAL_FAULT: 0
- CONN_FAULT: 0
- CONSUMED_SERVICES: 00001010000000000000
- SERVICE_FAULT: 1
- BotNET_ATTACK: 0



Step 1

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



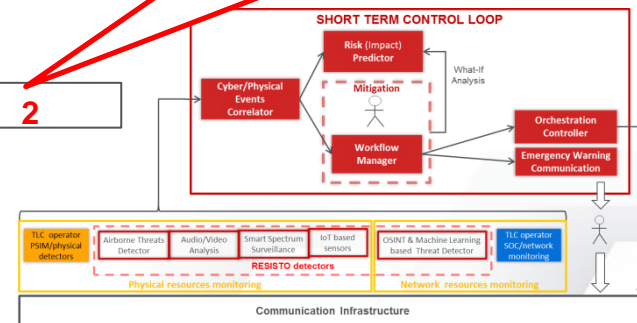
1

3

Knowledge Base

Step 2

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



2

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.

Validation performed through use cases defined in agreement with the manager of the critical infrastructure:

- **Macro-Scenario 1**
The protection of the Current existing Telecommunication Critical Infrastructures (OTE - Greece / RTV - Spain / British Telecom)
- **Macro-Scenario 2**
Their interdependencies as providers of essential communication services to other interlinked CIs and related cascade effects in the vicinity (TIM / Orange Romania / RTV)
- **Macro-Scenario 3**
Their evolution towards the future 5G networks and the emerging IoT world (Altice Labs - Portugal / RTV)

9 use cases have been developed

- Story telling
- Testbed setup
- Assets affected
- Impact of threats
- Actors and detection tools involved
- RESISTO response and added value
- Short term and long-term responses
- KPIs
- Innovation addressed

Use Cases
Use Case 1-2: Core Network Failure caused by Physical & Cyber Attacks or Natural Disasters to Telecommunication sites (OTE testbed)
Use Case 4: Disruption of major sporting event by combined physical & cyber-attack by a terrorist organization (BTC Testbed)
Use Case 5.1: Protection of Cloud Storage Services - Healthcare system (TIM Testbed)
Use Case 5.2: Protection of Cloud Storage Services - 5G Smart Manufacturing (TIM Testbed)
Use Case 6: Cyber and physical protection of network and network elements mechanisms used by critical services that impact users (ORO testbed)
Use Case 7: Maritime Safety and Emergency Case (RTV Testbed)
Use Case 8: Future Network (RTV Testbed)
Use Case 9: 5G network response to a security breach (ALB Testbed)

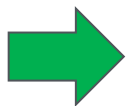
- Innovative cycle that combines integrated cyber/physical real time monitoring with a periodic resilience assessment:
 - interruption of service prevention, reduction of operating costs
 - applicable to wired, wireless 4 and 5G telecommunications networks, to cloud systems

KPIs examples

N. detected threats **Detection probability** **Time to detection**
Average decision-making time **Average mitigation time** **Human/Automated response**

- Contribution to the Product and Solution Roadmaps of the partners and development of skills leading to National / European sovereign solutions

- Collaboration between national champions and academia, and alignment with international peers in other use cases
- Advancement beyond state of the art:
 - “Combined Risk-Resilience Cyber & Physical Approach Framework”, applied to communications
 - Interdependence models adapted to the case of telecommunications networks
 - Automatic construction of dynamic workflows for more precise mitigation and
 - Automatic reconfiguration of flows on the network



This will foster credible **certification** of the resilience of Communication Critical Infrastructure

Bruno Saccomanno (LEONARDO) – RESISTO Project Coordinator

bruno.saccomanno@leonardocompany.com



www.resistoproject.eu



@RESISTO_project



@RESISTO.eu.project



@ RESISTO-project