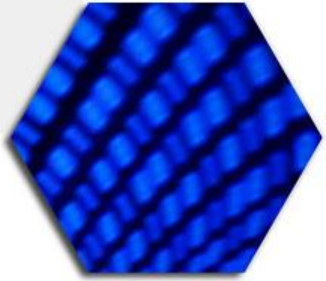
RESISTO

RESIlience enhancement and risk control platform
for communication infraSTructure Operators

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 No786409

Index

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

RESISTO

Numbers and consortium

RESISTO: RESIlience enhancement and risk control platform for communication infraSTtructure 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

LEONARDO

Scientific-Technical Coordinator

ROMA TRE UNIVERSITÀ DEGLI STUDI

RESISTO COSORTIUM:

LEONARDO ERICSSON

LEs: Technology Providers

TIM BT OTE GROUP OF COMPANIES orange retevisión altice labs

LEs: TELCO Operators

ROMA TRE UNIVERSITÀ DEGLI STUDI Fraunhofer EMI ICCS APRE Agenzia per la Promozione della Ricerca Europea BERGISCHE UNIVERSITÄT WUPPERTAL

(ROMA3 Third Party)

RTOs: Research and Technical Organizations

aditess INTEGRASYS guardtime BIT SENTINEL

SMEs: Technology Providers

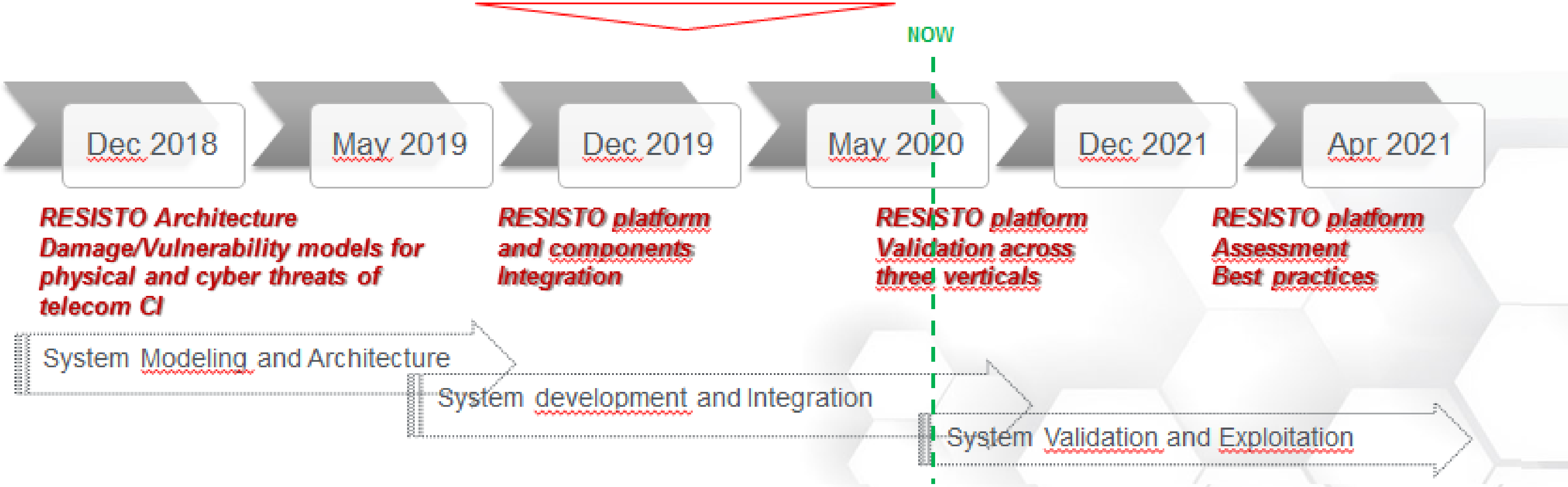
RESISTO

Objectives and implementation status

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



NOW

Dec 2018

May 2019

Dec 2019

May 2020

Dec 2021

Apr 2021

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

RESISTO platform and components Integration

RESISTO platform Validation across three verticals

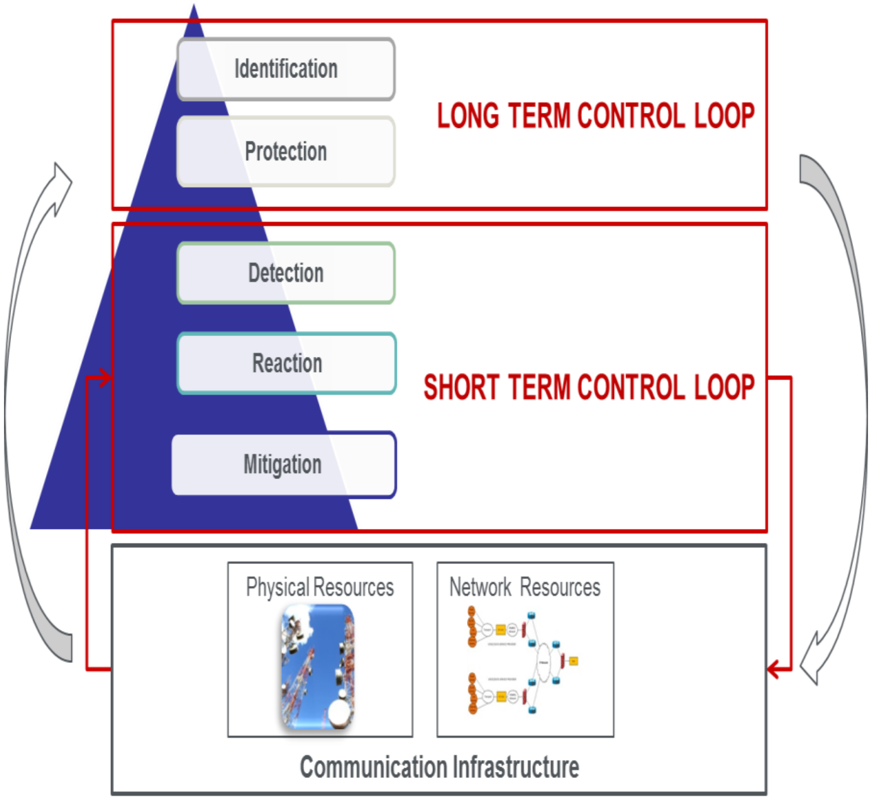
RESISTO platform Assessment Best practices

System Modeling and Architecture

System development and Integration

System Validation and Exploitation

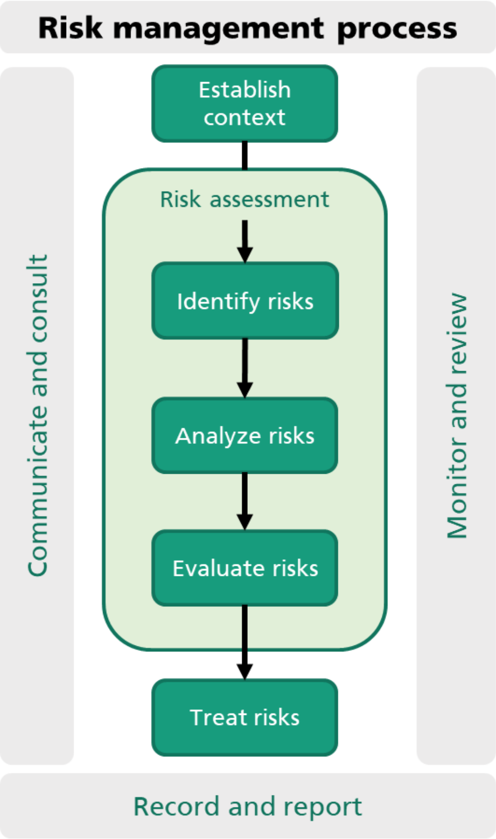
Basic idea



- 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

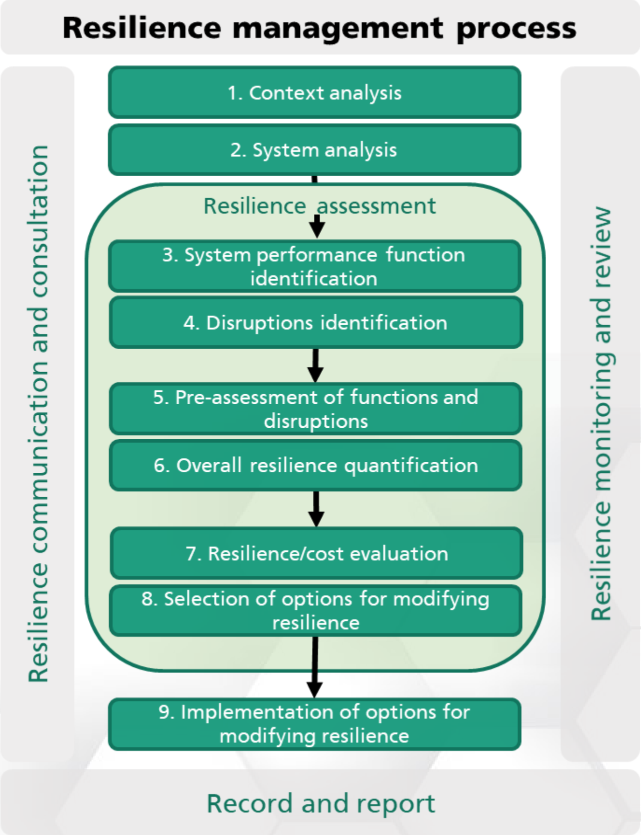
- The STCL (Short Term Control Loop) is **the platform runtime component**, for the operative security management of the Critical infrastructure

Resilience management process



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

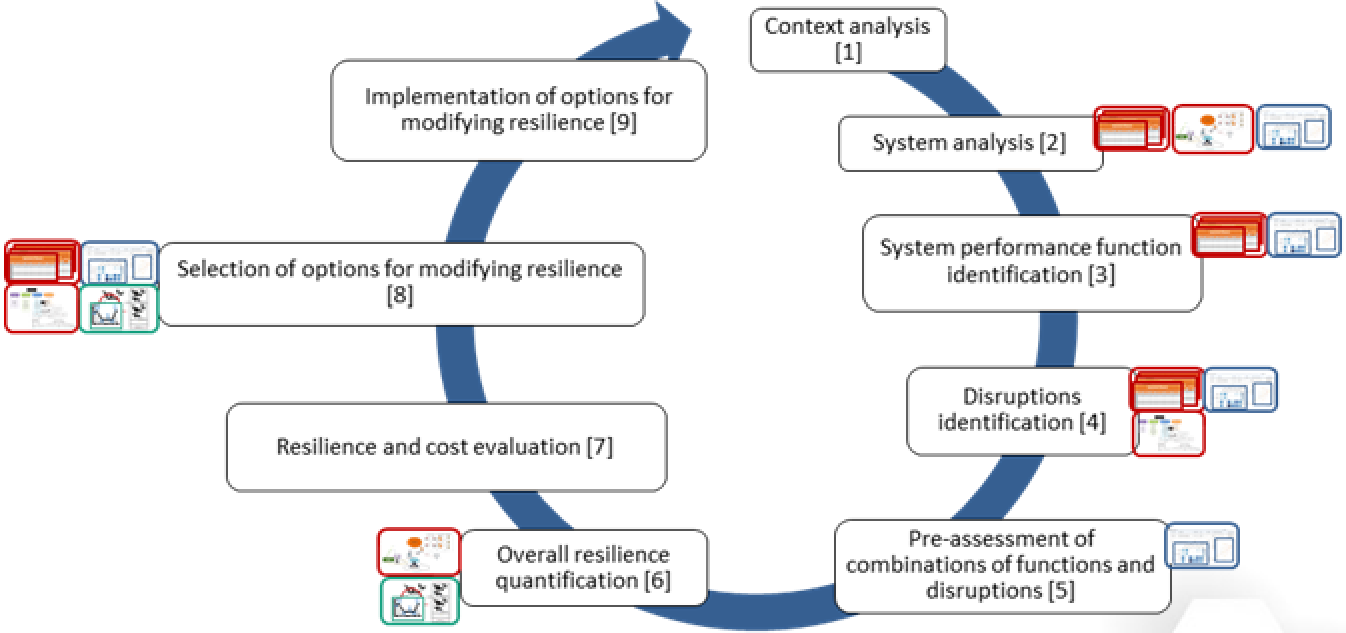
An iterative process that investigates resilience that requires certain inputs from end users and software tools at each step.


Resilience management process
1. Context analysis
2. System analysis
Resilience assessment
3. System performance function identification
4. Disruptions identification
5. Pre-assessment of functions and disruptions
6. Overall resilience quantification
7. Resilience/cost evaluation
8. Selection of options for modifying resilience
9. Implementation of options for modifying resilience
Resilience communication and consultation
Resilience monitoring and review
Record and report

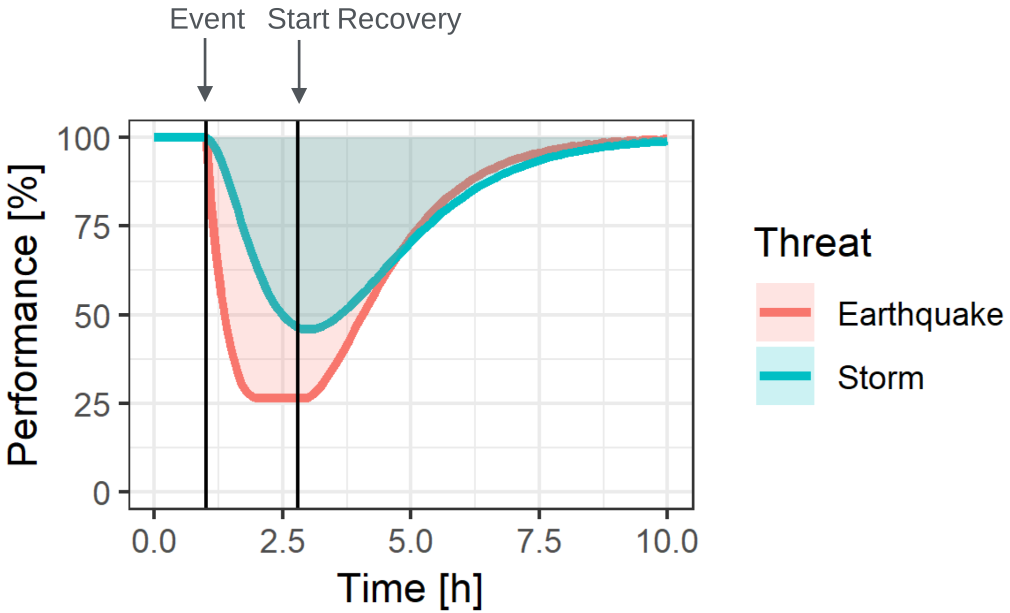
Long Term Control Loop (LTCL)

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

Fraunhofer EMI


Context analysis [1]
System analysis [2]
System performance function identification [3]
Disruptions identification [4]
Pre-assessment of combinations of functions and disruptions [5]
Overall resilience quantification [6]
Resilience and cost evaluation [7]
Selection of options for modifying resilience [8]
Implementation of options for modifying resilience [9]

RIs - Resilience Indicators

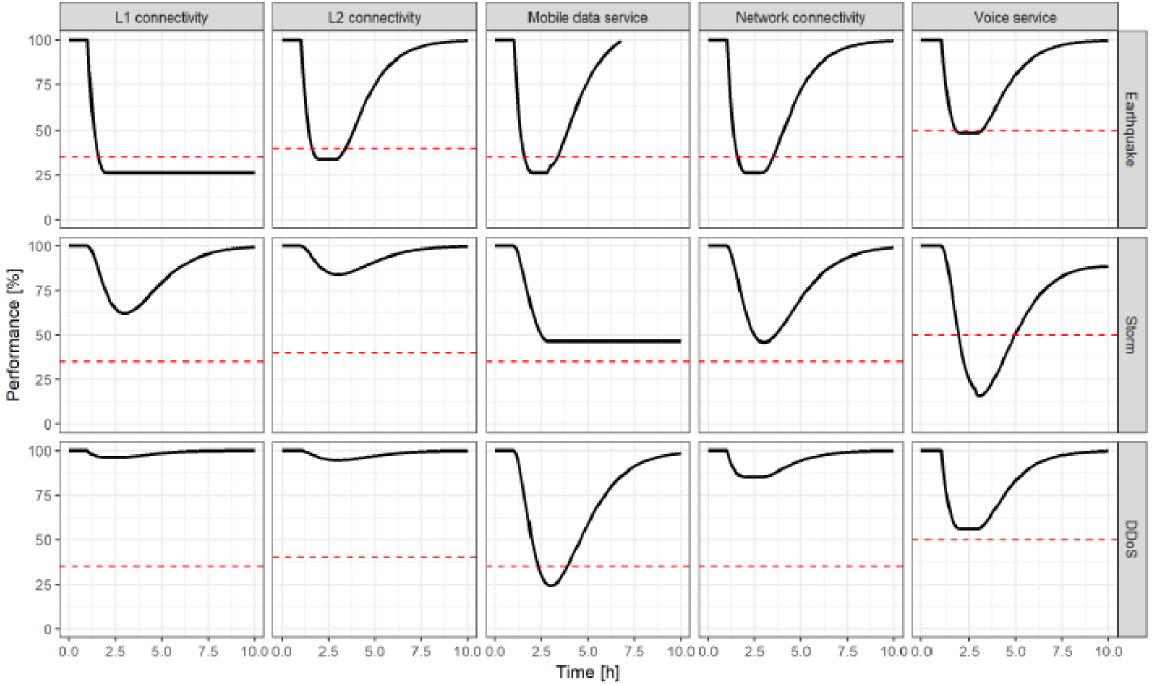


RIs - Resilience Indicators

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.

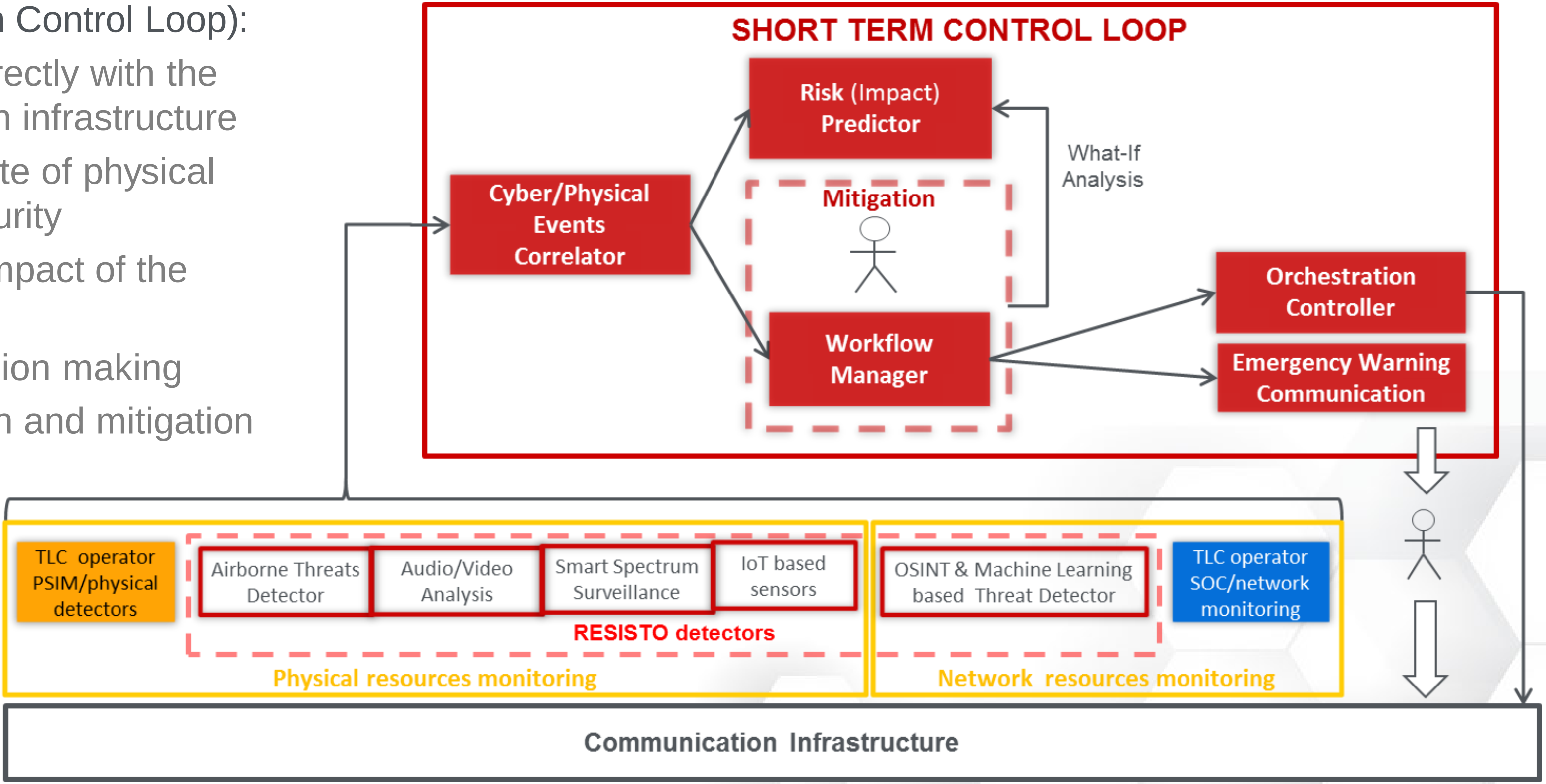
Improvement measures can be implemented and tested to see their effectiveness.



RESISTO Platform (Short Term Control Loop)

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


SHORT TERM CONTROL LOOP
Risk (Impact) Predictor
What-If Analysis
Mitigation
Cyber/Physical Events Correlator
Orchestration Controller
Workflow Manager
Emergency Warning Communication
TLC operator PSIM/physical detectors
Airborne Threats Detector
Audio/Video Analysis
Smart Spectrum Surveillance
IoT based sensors
RESISTO detectors
OSINT & Machine Learning based Threat Detector
TLC operator SOC/network monitoring
Physical resources monitoring
Network resources monitoring
Communication Infrastructure

DSS - Decision Support System

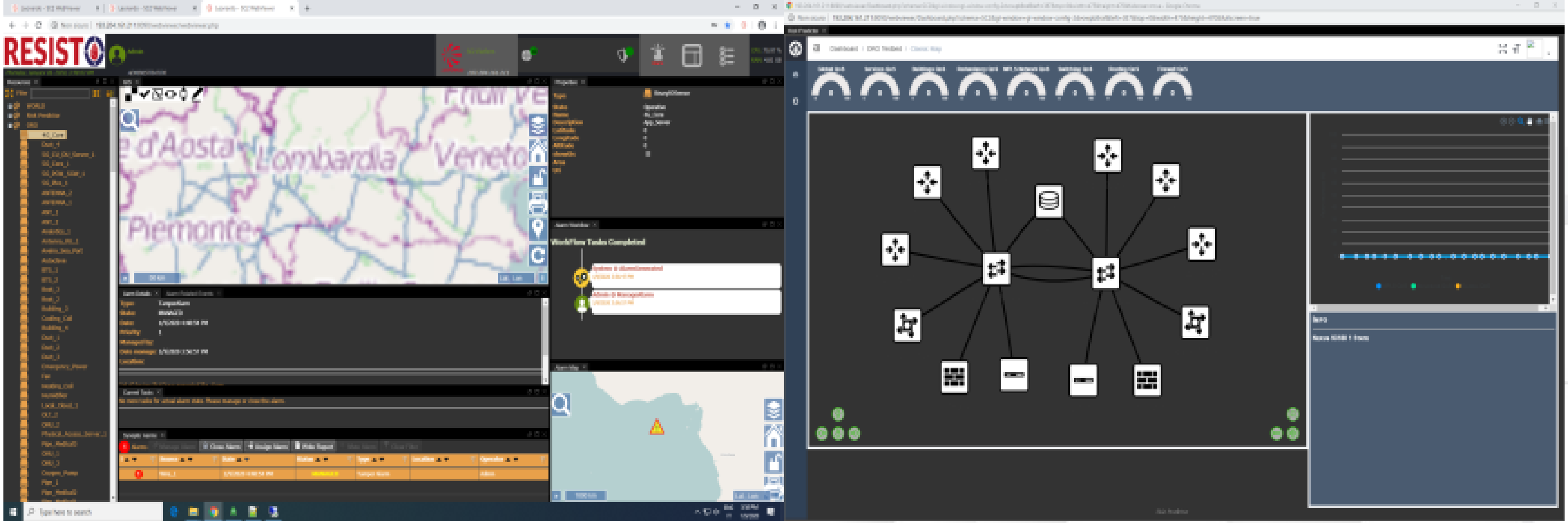
“A Decision Support System (DSS) is an information system that supports business or organizational decision-making activities. DSSs serve the management, operations and planning levels of and help people make decisions about problems that may be rapidly changing and not easily specified in advance.”

The RESISTO *Decision Support System* is composed by:

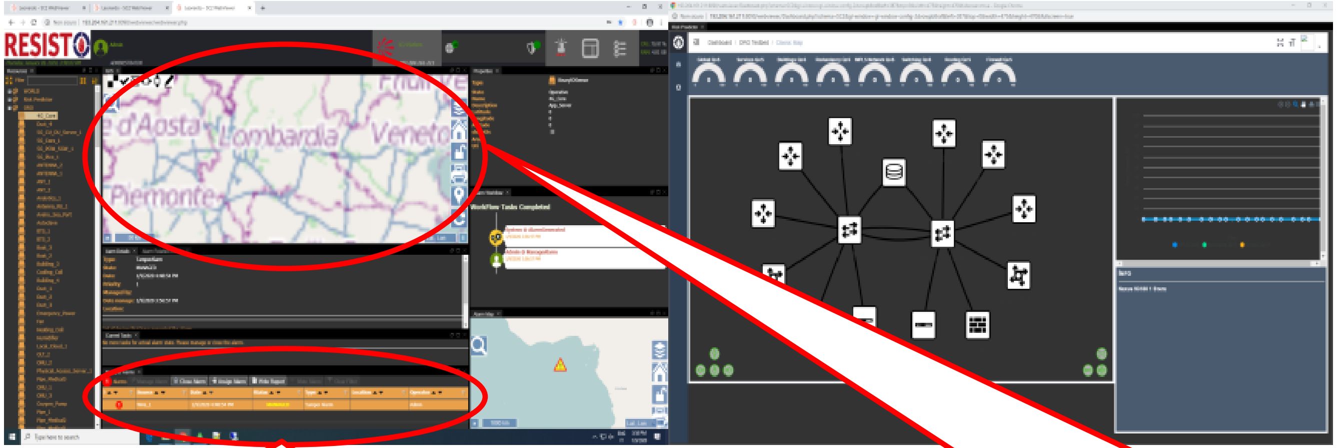
- Alarm Management dashboard
- Workflow manager
- Risk predictor

RESISTO DSS Cockpit

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.



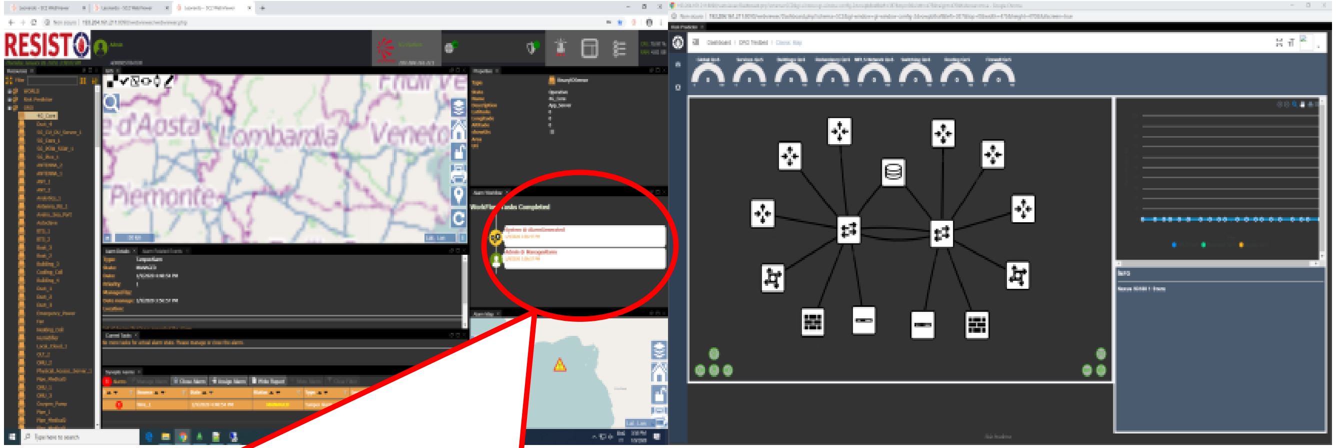
RESISTO DSS Cockpit

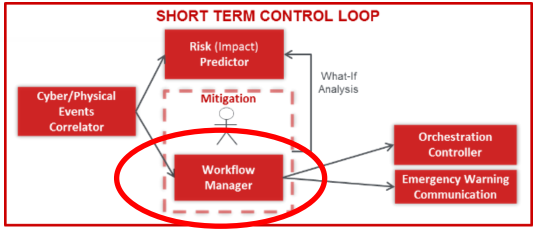


Alarm Management area collects all active alarms tracing the alarms progress

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

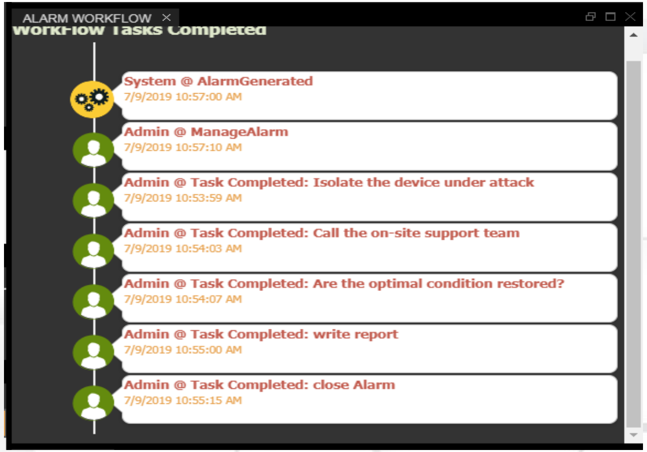
RESISTO DSS Cockpit





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



Workflow Tasks Completed

System @ AlarmGenerated
7/9/2019 10:57:00 AM

Admin @ ManageAlarm
7/9/2019 10:57:10 AM

Admin @ Task Completed: Isolate the device under attack
7/9/2019 10:53:59 AM

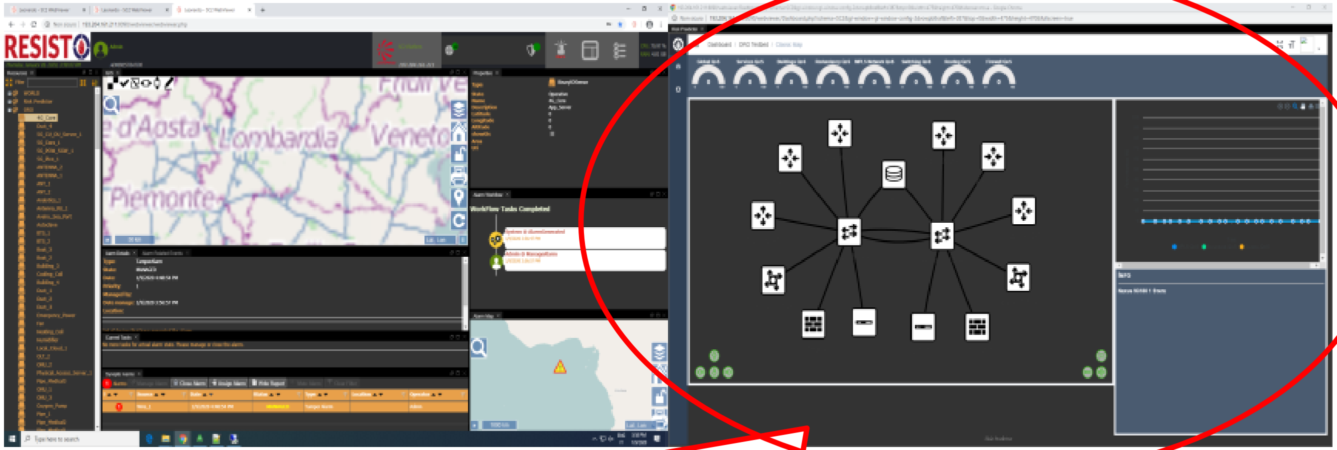
Admin @ Task Completed: Call the on-site support team
7/9/2019 10:54:03 AM

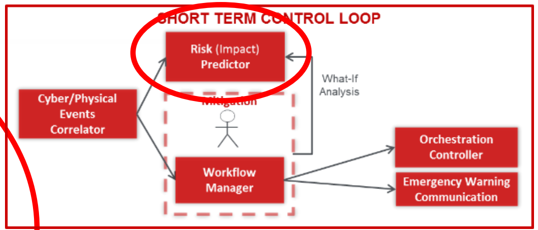
Admin @ Task Completed: Are the optimal condition restored?
7/9/2019 10:54:07 AM

Admin @ Task Completed: write report
7/9/2019 10:55:00 AM

Admin @ Task Completed: close Alarm
7/9/2019 10:55:15 AM

RESISTO DSS Cockpit





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

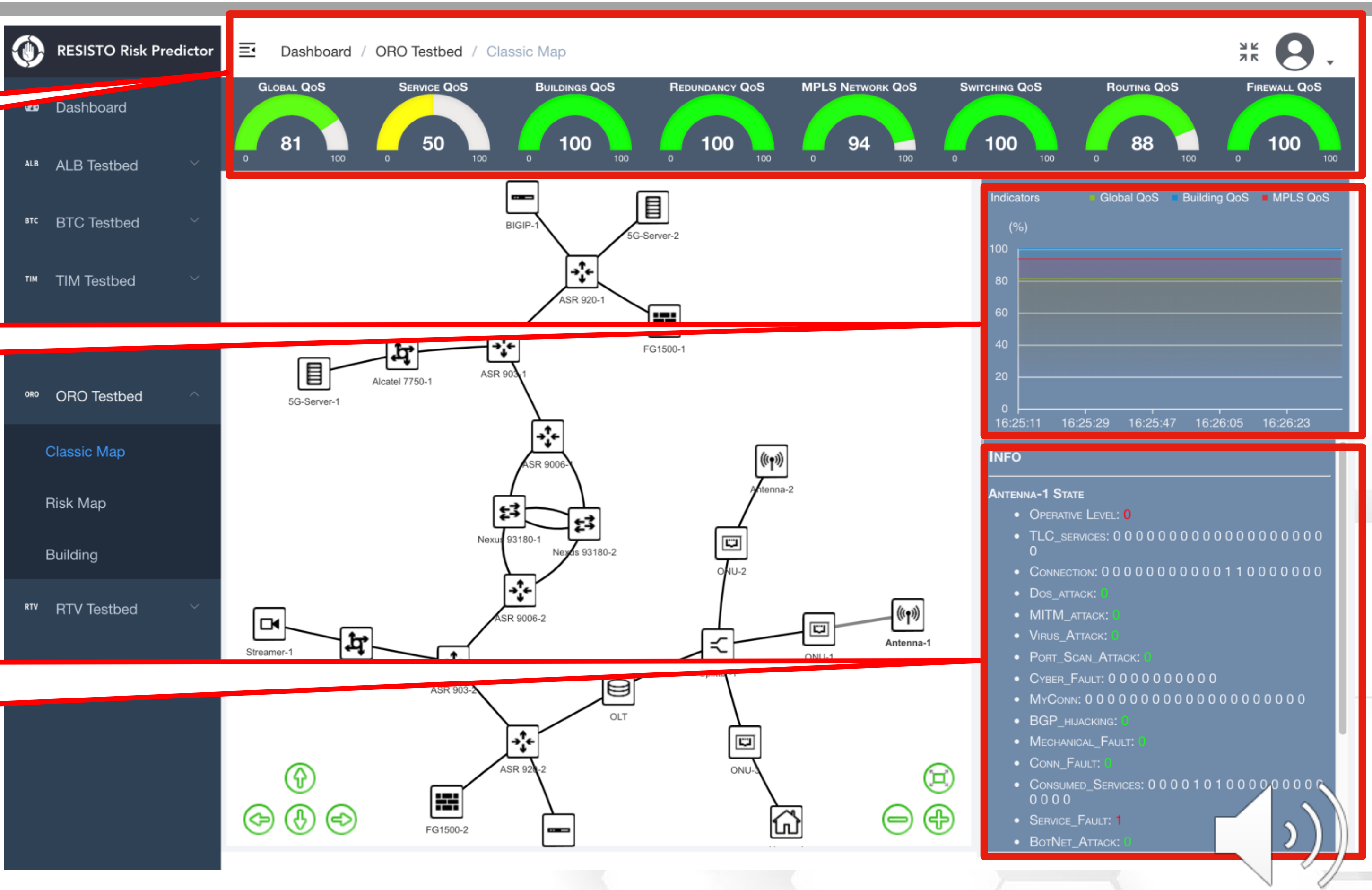
- A synoptic view of infrastructure components status
- Alarm impact evaluation in terms of cascade effects and services provision
- Services provision vs. time view

Risk Predictor UI

Indicators

Real-time chart

Details on the clicked object

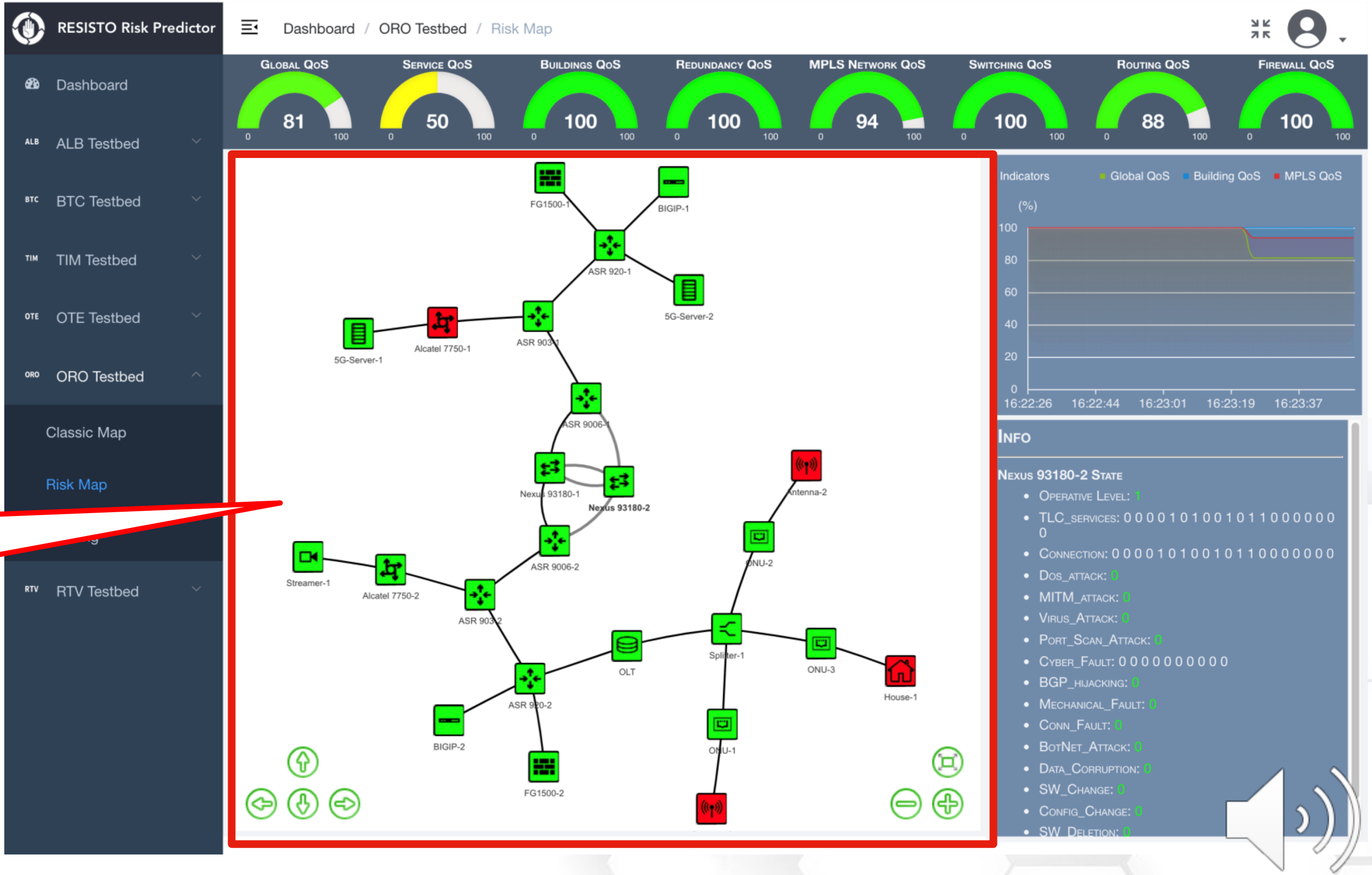


INFO

ANTENNA-1 STATE

- OPERATIVE LEVEL: 0
- TLC_SERVICES: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
- CONNECTION: 0 0 0 0 0 0 0 0 0 0 0 1 1 0 0 0 0 0 0 0
- DOS_ATTACK: 0
- MITM_ATTACK: 0
- VIRUS_ATTACK: 0
- PORT_SCAN_ATTACK: 0
- CYBER_FAULT: 0 0 0 0 0 0 0 0 0 0
- MYCONN: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
- BGP_HIJACKING: 0
- MECHANICAL_FAULT: 0
- CONN_FAULT: 0
- CONSUMED_SERVICES: 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0
- SERVICE_FAULT: 1
- BOTNET_ATTACK: 0

Risk Predictor UI



Info

Nexus 93180-2 State

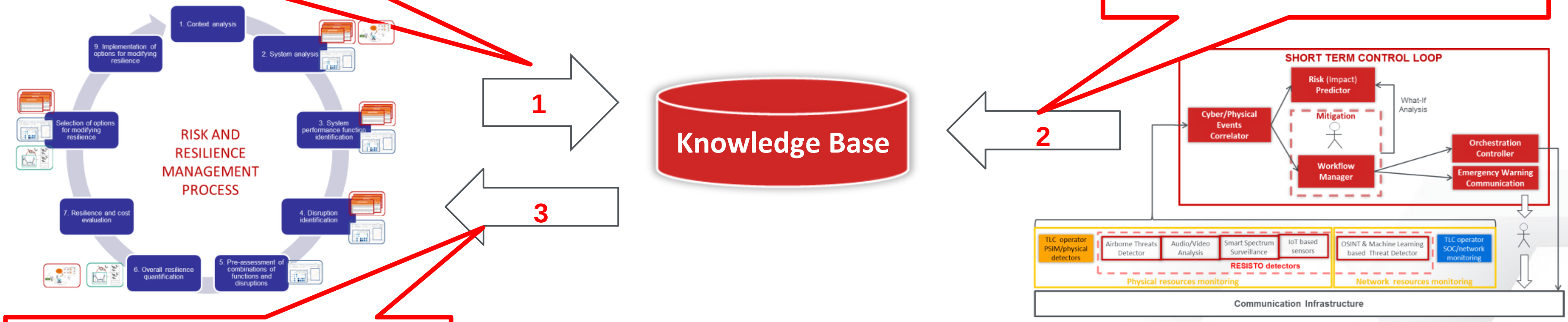
- Operative Level: 1
- TLC_services: 0 0 0 0 1 0 1 0 0 1 0 1 1 0 0 0 0 0 0 0
- Connection: 0 0 0 0 1 0 1 0 0 1 0 1 1 0 0 0 0 0 0 0
- Dos_attack: 0
- MITM_attack: 0
- Virus_Attack: 0
- Port_Scan_Attack: 0
- Cyber_Fault: 0 0 0 0 0 0 0 0 0 0
- BGP_hijacking: 0
- Mechanical_Fault: 0
- Conn_Fault: 0
- BotNet_Attack: 0
- Data_Corruption: 0
- SW_Change: 0
- Config_Change: 0
- SW_Deletion: 0

risk view of the ORO case study

Resilience Indicators flow: the High level control loop

Step 1
at the end of a LTCL cycle **Estimated** Resilience Indicators (**RIs**) s are stored in the Knowledge Base

Step 2
STCL, facing an Event<i>, measures **Actual RIs** and store them in the Knowledge Base


1. Context analysis
2. System analysis
3. System performance function identification
4. Disruption identification
5. Pre-assessment of combinations of functions and disruptions
6. Overall resilience quantification
7. Resilience and cost evaluation
Selection of options for modifying resilience
9. Implementation of options for modifying resilience
RISK AND RESILIENCE MANAGEMENT PROCESS
1
3
Knowledge Base
2
SHORT TERM CONTROL LOOP
Risk (Impact) Predictor
What-If Analysis
Cyber/Physical Events Correlator
Mitigation
Workflow Manager
Orchestration Controller
Emergency Warning Communication
TLC operator PSIM/physical detectors
Airborne Threats Detector
Audio/Video Analysis
Smart Spectrum Surveillance
IoT based sensors
RESISTO detectors
OSINT & Machine Learning based Threat Detector
TLC operator SOC/network monitoring
Physical resources monitoring
Network resources monitoring
Communication Infrastructure

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

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)

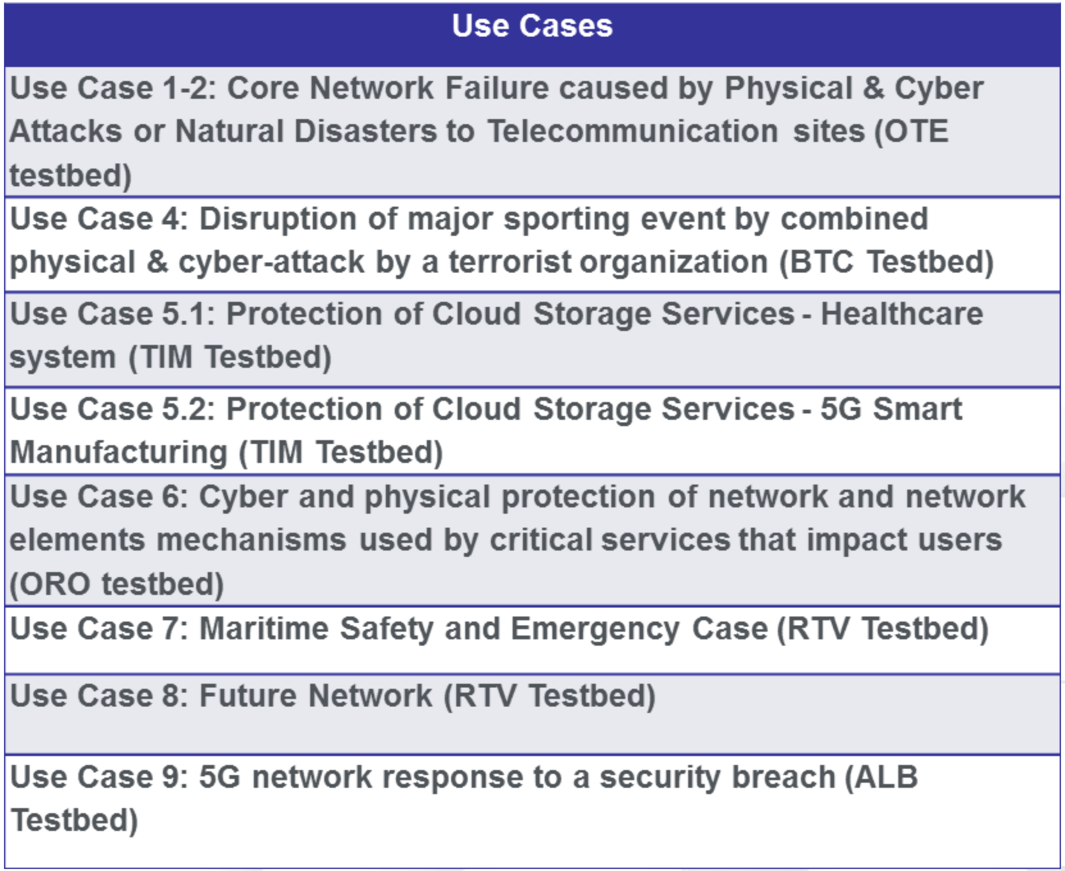
- Macro-Scenario 2
  Their interdependencies as providers of essential communication services to other interlinked CIs and related cascade effects in the vicinity
  (TIM / Orange Romania / RTV)

- Macro-Scenario 3
  Their evolution towards the future 5G networks and the emerging IoT world
  (Altice Labs - Portugal / RTV)

Use Cases

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)

Benefits

- 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

Benefits

- 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