RESISTO

RESIlience enhancement and risk control platform
for communication infraSTructure Operators

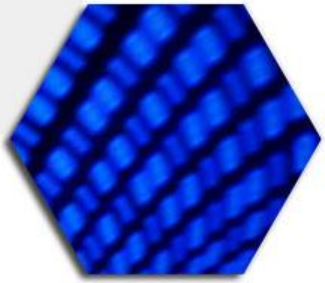
HORIZON 2020
#InvestEUresearch

Resilience in Critical Infrastructures

Maria Belesioti

Fixed Network R&D Programs Section
Research & Development Department, Fixed & Mobile

ΟΤΕ
ΟΜΙΛΟΣ ΕΤΑΙΡΕΙΩΝ



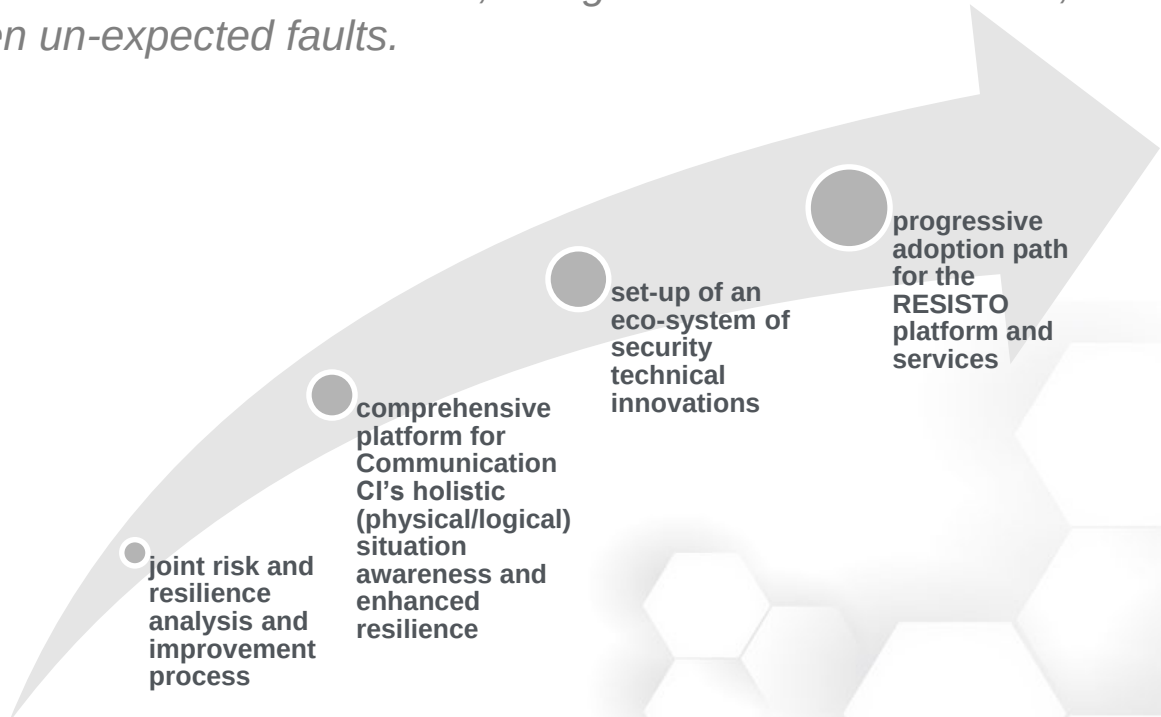
22nd Infocom World Conference – *Athens, Greece, November 06, 2020*

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

Main Objective

Core aim:

- ***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.*



Definitions

Resilience *is the* ***ability*** *to "****provide and maintain*** *an acceptable level of service in face of faults and challenges to normal operation".*

Resilience *can be perceived as* ***the polar opposite of vulnerability*** *or, in other words,*

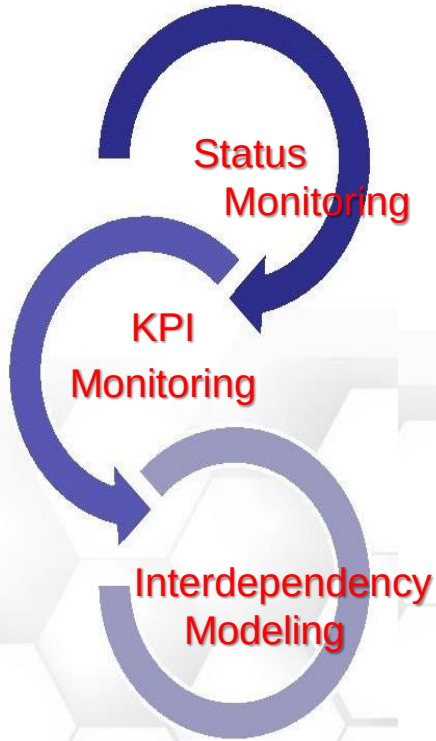
resilience and vulnerability have an inverse character with respect to each other.

Overall Concept

Risk and Resilience framework

The RESISTO risk and resilience framework refers mainly to:

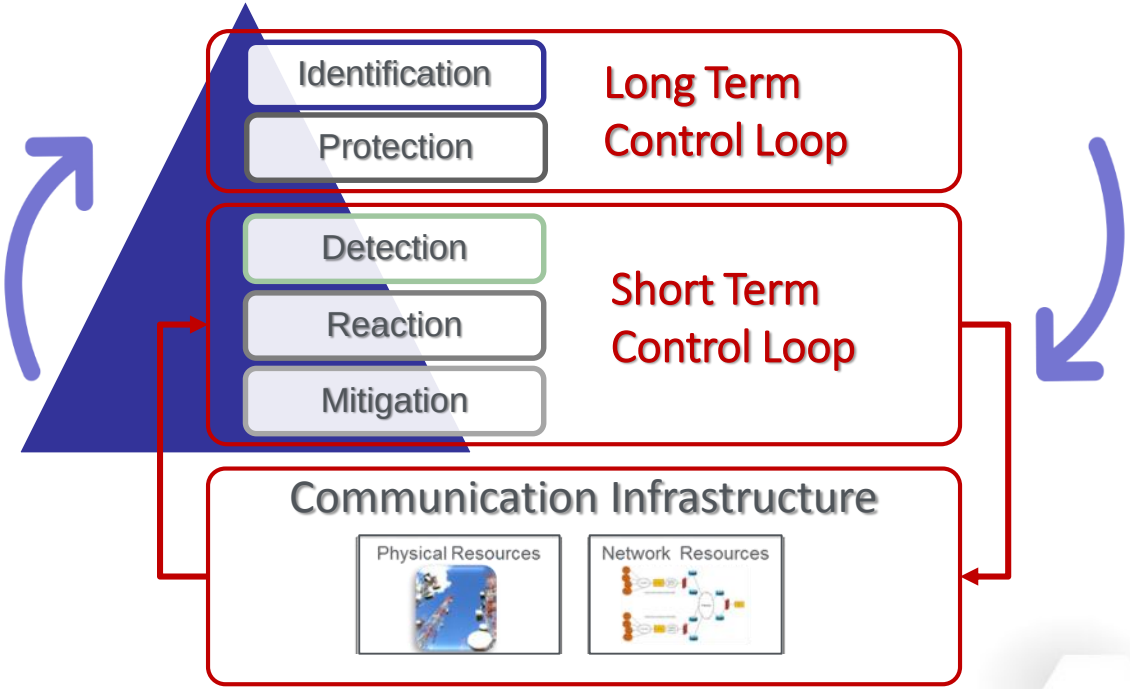
- *Holistic Approach to Situation Awareness*
- *Innovative Risk & Resilience & Improvement Process Management*
- *Decision Support System*
- *Protection against cyber-physical threats*
- *Modelisation on state-of-the art technologies (Machine Learning, IoT, Blockchain)*



The RESISTO context:

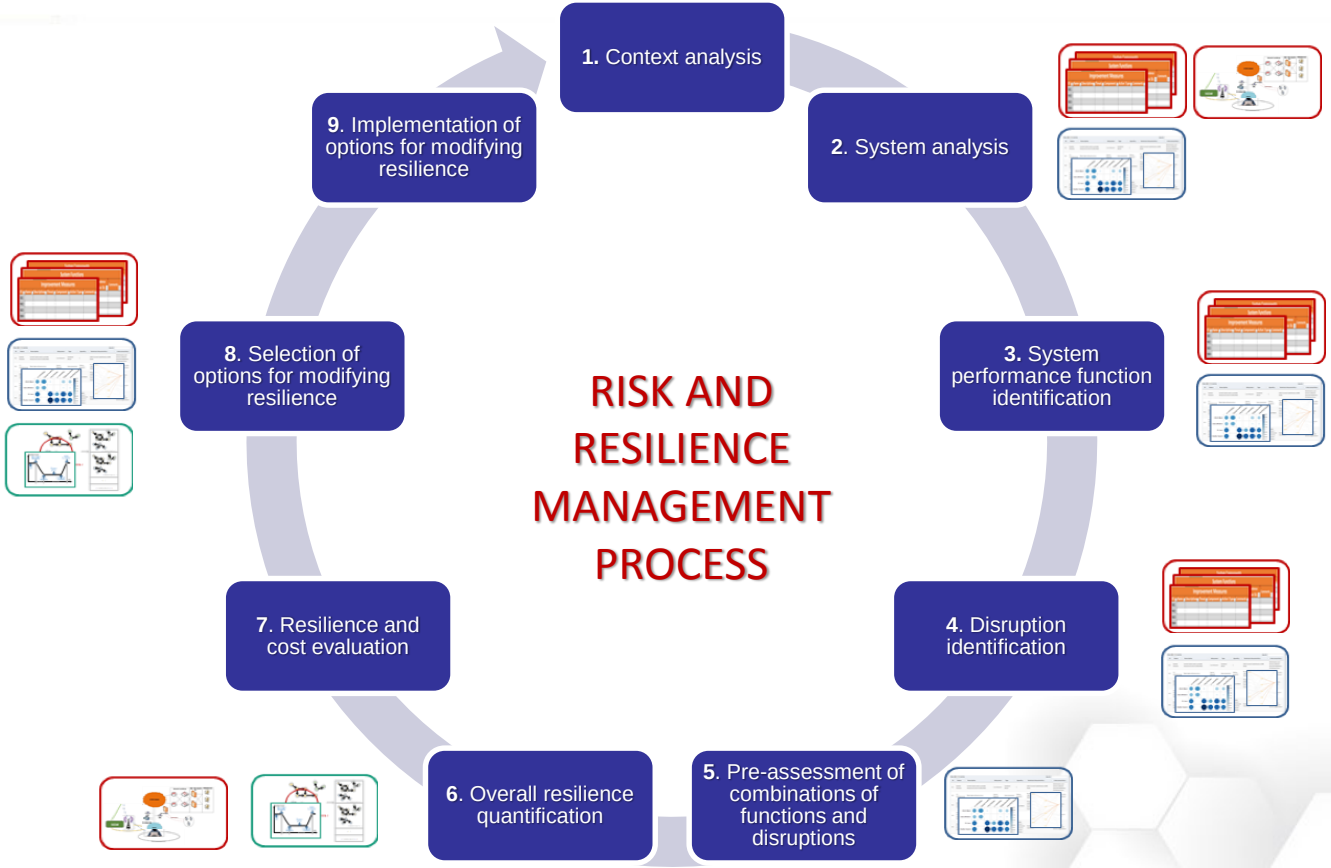
- *Introduces specific KPI monitoring*
- *Exploits interdependency modeling techniques*
- *Provides identification of system performance functions*

Main functional concepts



- 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

Long Term Control Loop



Input Collection

Extended Threat List

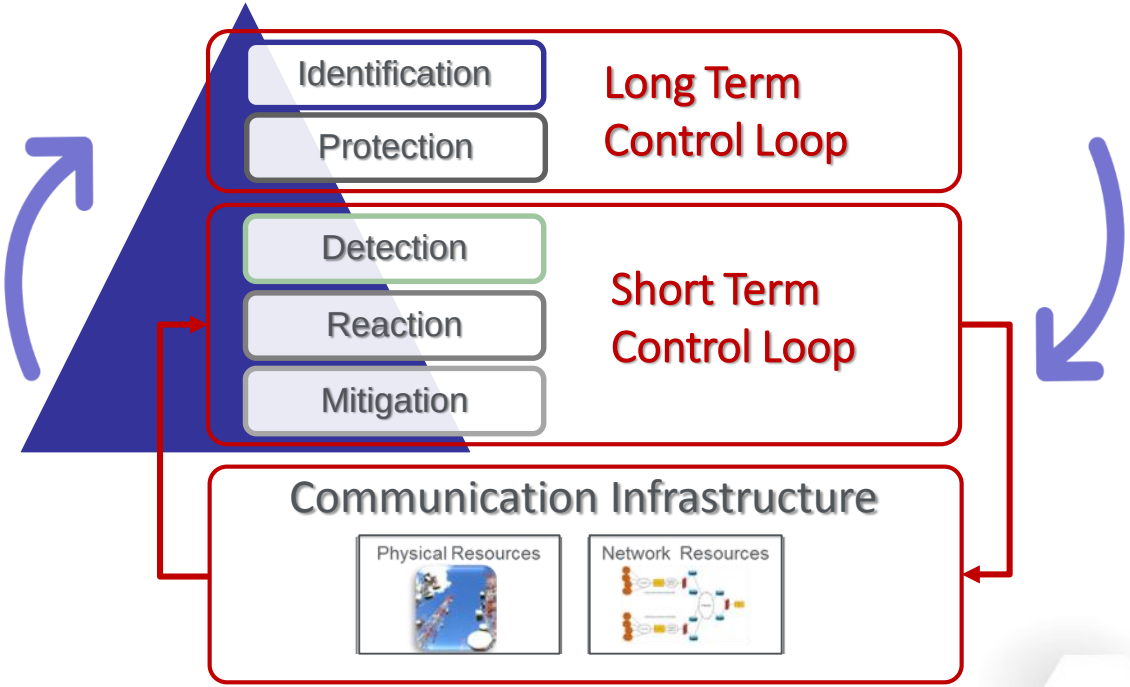
Network representation

Supporting Tool

Shiny App

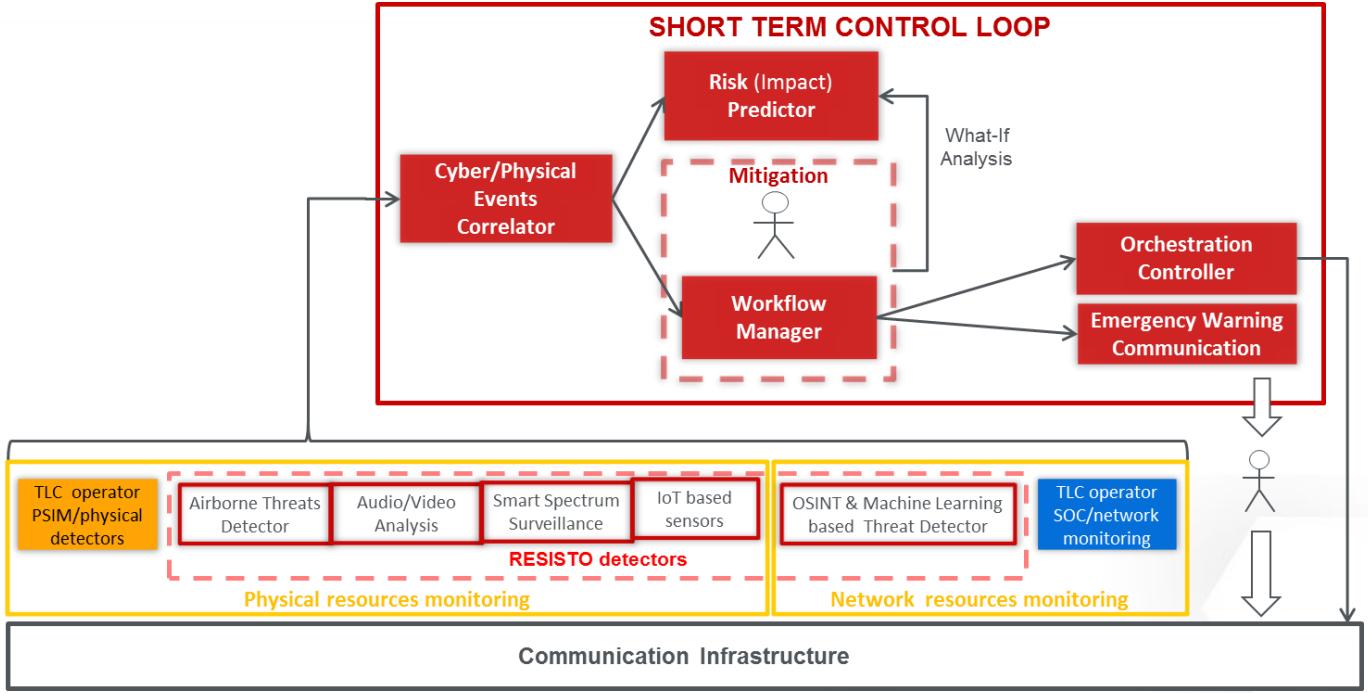
Network Simulator

Main functional concepts

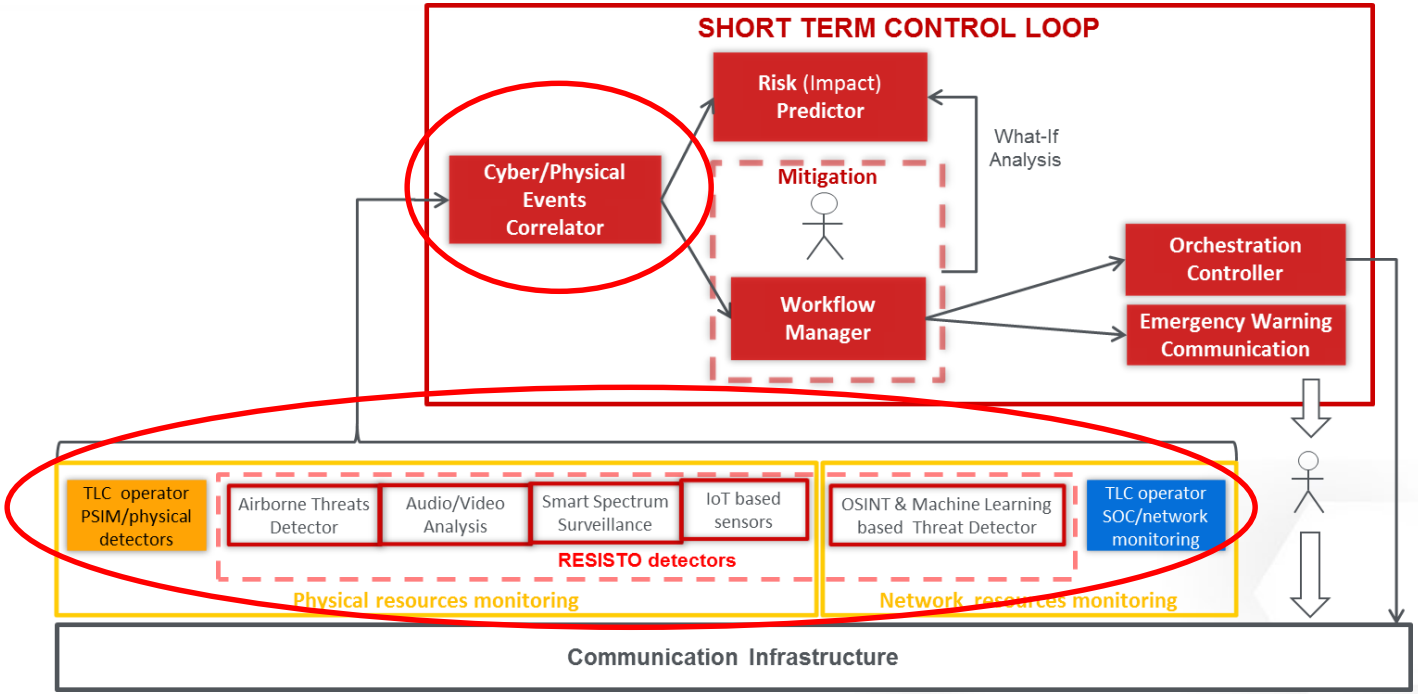


- The **Short Term Control Loop (STCL) reacts in real time** to detected cyber/physical attacks and events that may impact the operational life of the system.
- It **enhances situation awareness** and provides operators with a Decision Support System cockpit able to implement the best reactions.

Short Term Control Loop



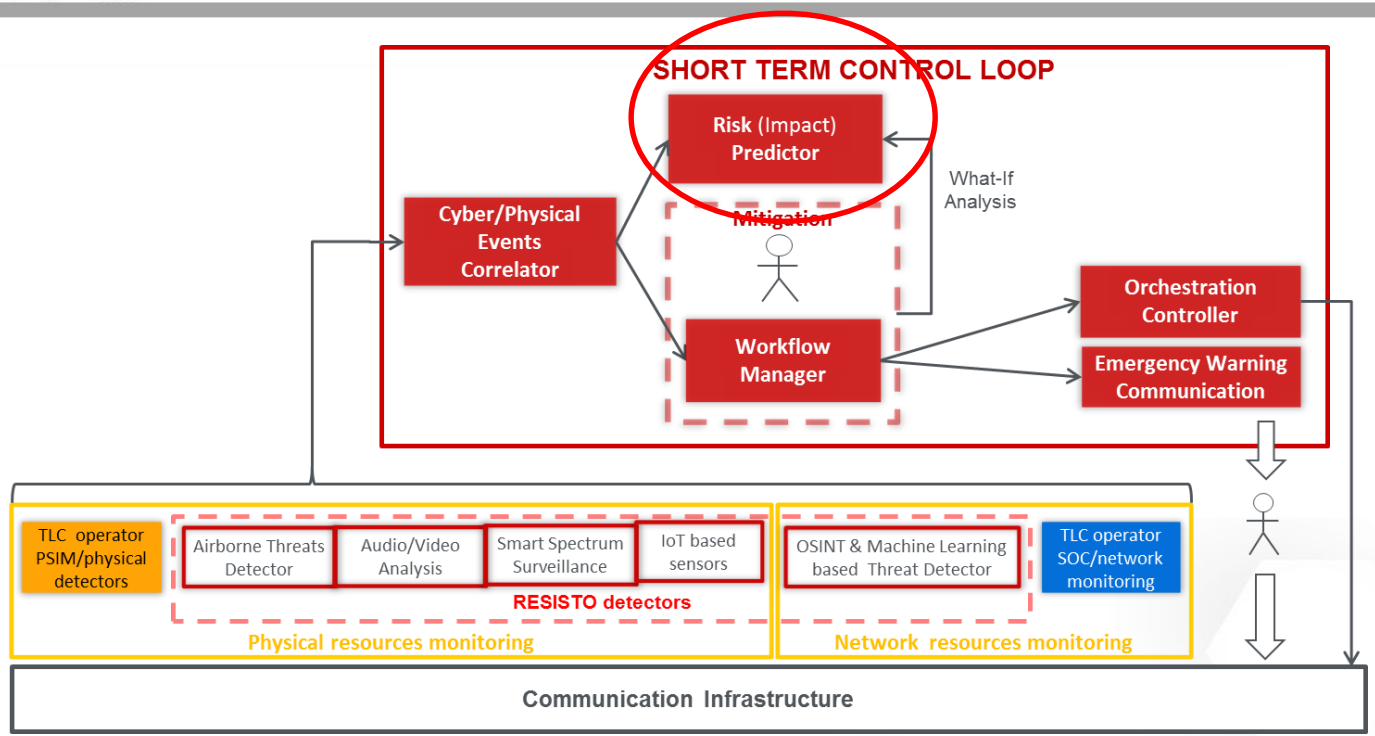
Short Term Control Loop



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.*

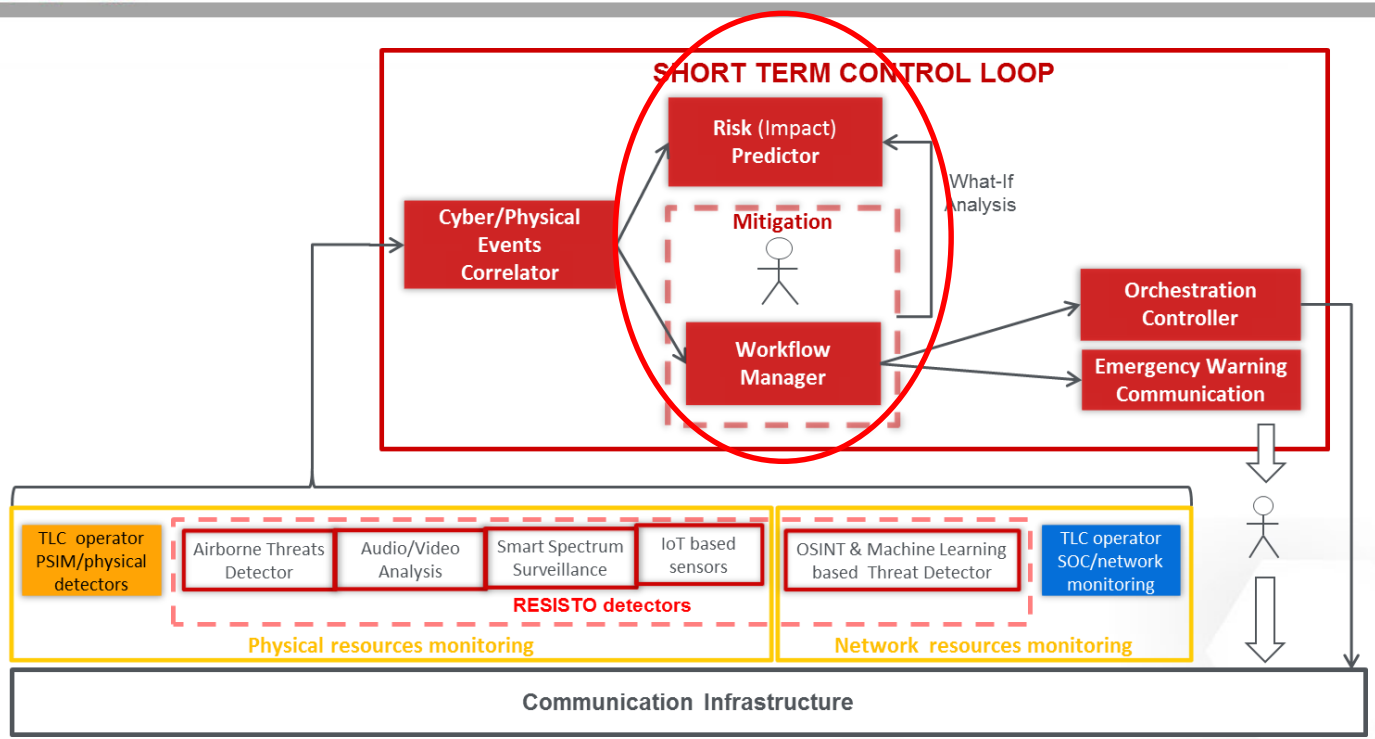
Short Term Control Loop



*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.*

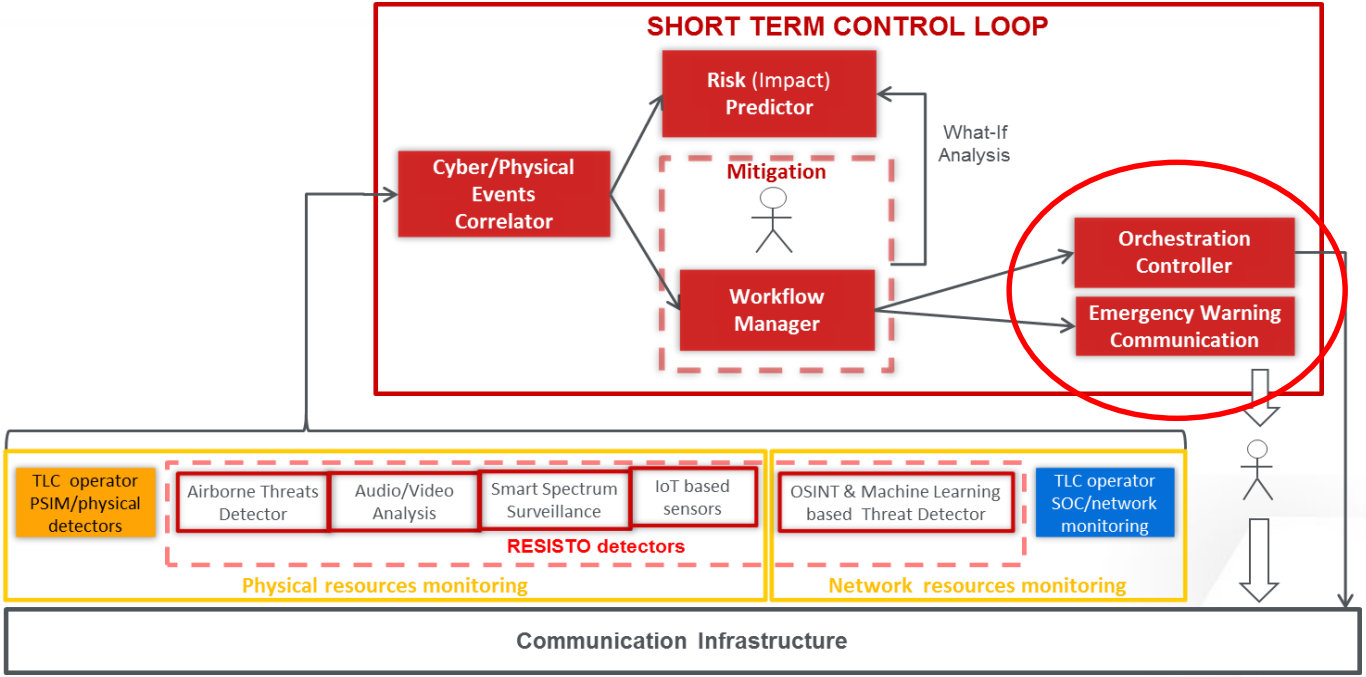
Short Term Control Loop



*The **Short Term Control Loop**:*

- ***Supports decision making,** by providing a qualitative and quantitative "What-If" analysis tool in order to evaluate the most resilient communication CI reconfiguration.*

Short Term Control Loop



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.*

Anomaly Detection

- The **RESISTO Cyber-Physical Event Correlator** is a ***Rule-Based engine*** + *a* ***Deep Learning engine*** customized to detect threats, alarms, critical events defined by the "Risk and resilience assessment analysis" and the "**Interdependency analysis**" able to detect critical situations to manage.

identifies threats and dangerous situations through the analysis of ***heterogeneous*** *data sources in real-time using several event correlation techniques. Events satisfying the correlation criteria are collected in event windows.*

analyses the behavior of the RESISTO platform and the phenomena affecting the system in order to make decisions accordingly

EVENT STREAM PROCESSING

MACHINE LEARNING

intelligent ***DEFENCE MODELS*** *to prevent damages created by cyber-attacks*

Thank You !!!