RESIST🖐O

RESIlience enhancement and risk control platform
for communication infra**ST**ructure **O**perators
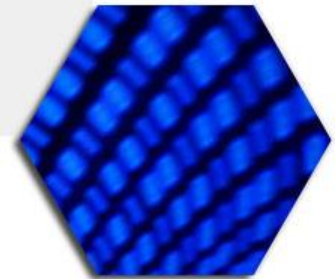
Cybersecurity risk management – how to strengthen resilience and adapt in 2021

23rd November 2020, web-conference

Dr. Mirjam Fehling-Kaschek, Natalie Miller

Fraunhofer
EMI

RESISTO

- Improve risk control and resilience of European current and future critical telecommunication infrastructures against physical, cyber and combined cyber-physical threats

2 Large Enterprises

5 RTOs / Universities

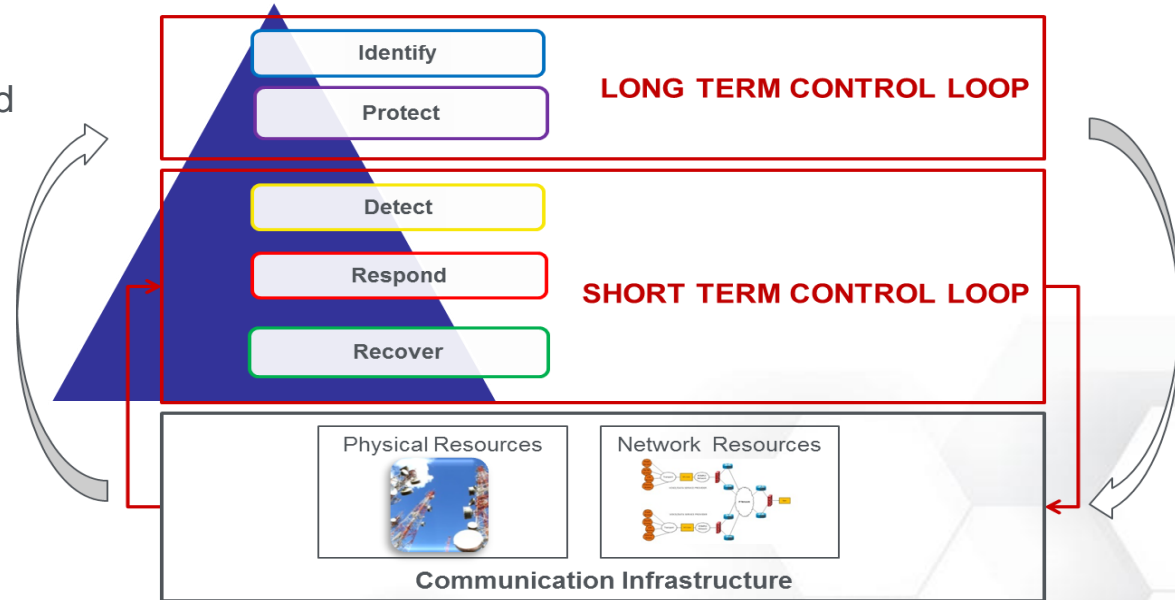(ROMA3 third party)

4 Small Medium Enterprises

6 Telco Operators

- Long term control loop
  - Periodic offline analysis
 - Determination of criticalities and long term strategies

- Short term control loop
  - Runtime component
  - Decision support system

- Knowledge base
  - Storage of data for both loops
  - Connection between the loops

Identify

Protect

LONG TERM CONTROL LOOP

Detect

Respond

SHORT TERM CONTROL LOOP

Recover

Physical Resources

Network Resources

Communication Infrastructure

Risk and resilience management process:

- Extension of ISO-31000 for risk management
- Addition of steps relevant for resilience assessment
- RESISTO specifications for all steps
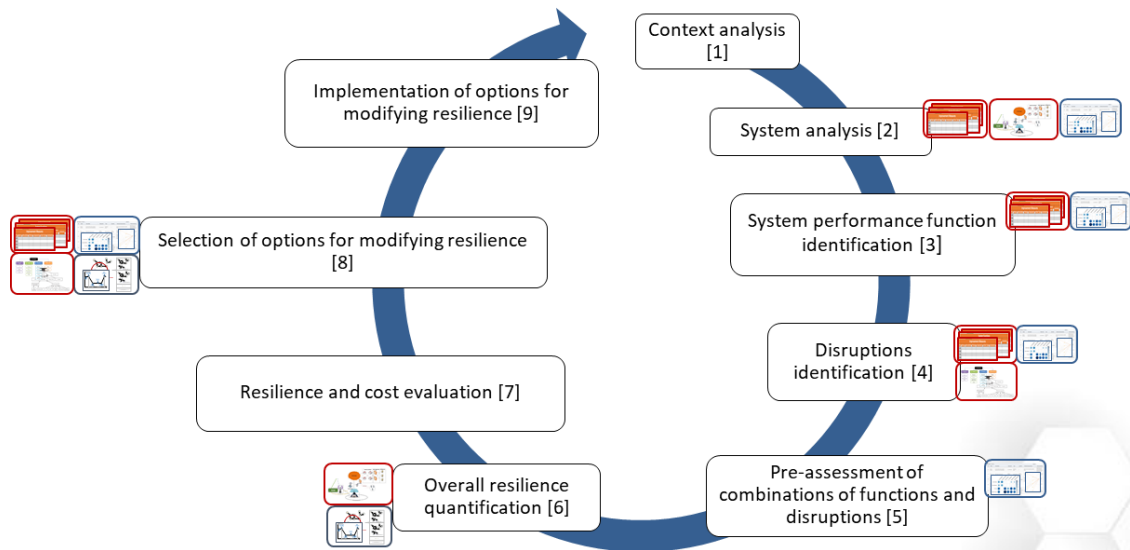
Input collection:

Extended threat list
- System components
- System functions
- Threats
- Mitigation options

Network representation
- Scheme of the testbed network for simulation
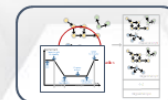
Testbed tools
- Results provided by operators (e.g. penetration tests, honey pots)
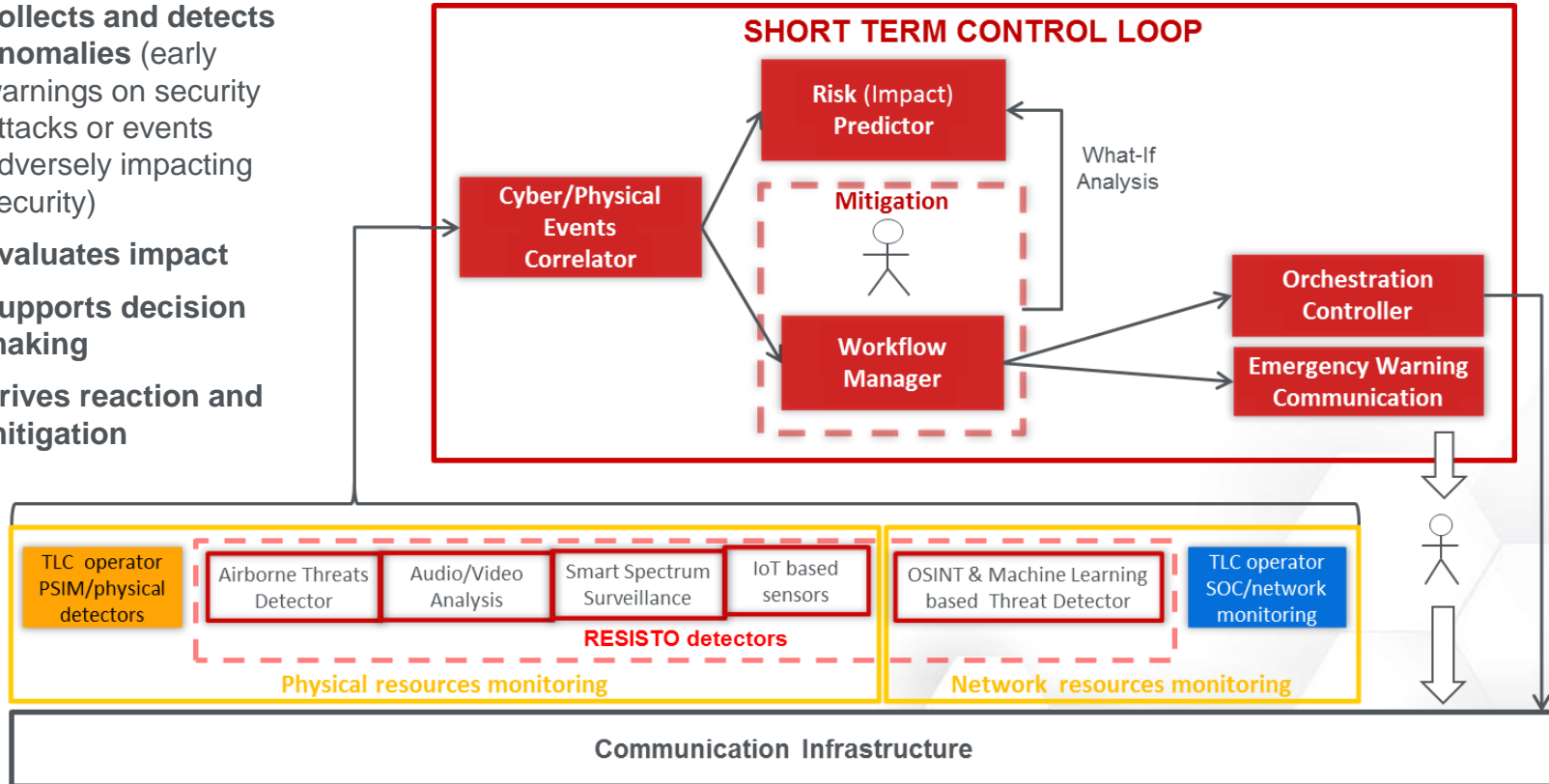
Supporting tools:

Shiny app
- Browse tables
- View correlations, e.g. critical combinations
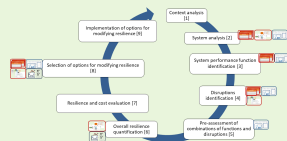- Threat ranking

Network simulators
- Resilience quantification
- Evaluate mitigation options

- **collects and detects anomalies** (early warnings on security attacks or events adversely impacting security)
- **evaluates impact**
- **supports decision making**
- **drives reaction and mitigation**

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

RESISTO detectors
- Airborne Threats Detector
- Audio/Video Analysis
- Smart Spectrum Surveillance
- IoT based sensors

OSINT & Machine Learning based Threat Detector

TLC operator SOC/network monitoring

Physical resources monitoring

Network resources monitoring
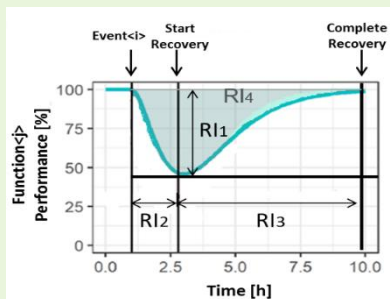
Communication Infrastructure
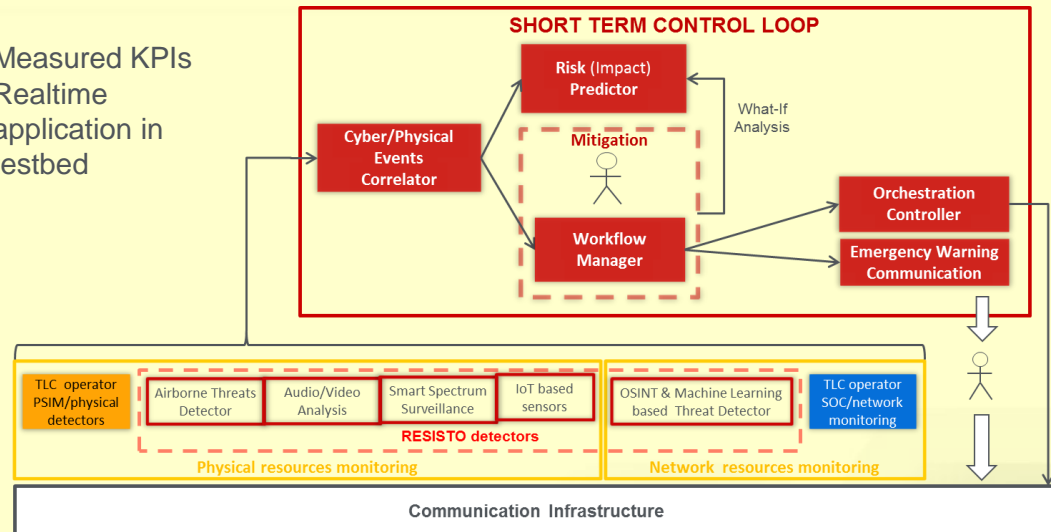
Long Term Control Loop

Risk and resilience management process

- **Resilience quantification**
  - Performance loss
  - Resilience indicators

- **Measured KPIs**
- Realtime application in testbed

SHORT TERM CONTROL LOOP

Cyber/Physical Events Correlator

Risk (Impact) Predictor

What-If Analysis

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

OSINT & Machine Learning based Threat Detector

TLC operator SOC/network monitoring

RESISTO detectors

Physical resources monitoring

Network resources monitoring

Communication Infrastructure

Knowledge Base

End of Presentation