

RESISTO: Resilience Enhancement and Risk Control Platform for Communication Infrastructure Operators

E. Aonzo, A. Neri

Leonardo – Cyber Security Division

The RESISTO platform is a Critical Infrastructure Protection solution designed to ensure drastic improvement in business continuity and management in case of physical, cyber and cyber-physical threats. The platform operates through two components: a Long Term and a Short Term Control Loop. The off-line Long Term Control Loop identifies the threats to which the Critical Infrastructure is most vulnerable; it is based on quantitative assessment of the resilience, and designs the necessary measures so that the Critical Infrastructure can deal with threats while guaranteeing the required levels of service. The Short Term Control Loop is mainly based on the Leonardo SC2 platform, which provides run-time operators with a system capable of detecting and collecting events and alarms; it promptly assesses cascading effects on the Critical Infrastructure and services provided, supports the Decision Making and guides the reaction to alarms until their complete recovery. The use of RESISTO ensures increase in the resilience of the Critical Infrastructure, better choice of countermeasures and reactions to be implemented and reduction in terms of time and its associated costs.

Communications play a fundamental role in the economic and social well-being of the citizens and on operations of most of the Critical Infrastructures (CIs). Thus, they are a primary target for criminals, as well as extreme weather events and natural disasters represent a challenge. Communication CIs are extremely vulnerable due to ever-increasing complexity of the architecture - also in light of the evolution towards 5G - and to the extensive use of programmable platforms and exponential growth of connected devices. The fact that most enterprises still manage physical and cyber security independently represents a further challenge. RESISTO is an innovative solution for Communications Infrastructures, which provides awareness and enhanced resilience. RESISTO will help operators of Communications Infrastructures, but also of other kinds of CIs, to take the best countermeasures and reactive actions by exploiting the combined use of risk and resilience preparatory analyses, detection and reaction technologies, applications and processes in the physical and cyber domains

PROJECT DESCRIPTION

The solution is an ICT platform composed by two macro elements (Figure 1):

1. Long Term Control Loop (LTCL);
2. Short Term Control Loop (STCL).

Long Term Control Loop

The long-term control cycle (LTCL) is an offline activity to be performed on a periodic basis. The LTCL is based on the

risk and resilience management process resulting from ISO31000 (see ref. [3]). It aims to assess the risks and vulnerabilities of the configuration elements, identify threats to cyber and physical security, evaluate how the CI could potentially react to the most critical and potentially threatening potential events, evaluate the impact of threats on the resilience of the system. In the event that this impact is beyond the acceptability threshold, the LTCL allows evaluating the opportunity to introduce changes to the system configuration and interventions to be carried out on the IC in order to improve its resilience.

The process is structured in 9 stages (Figure 2). For a detailed description of the procedure, see the RESISTO project documentation available at reference [1], section: Resources.

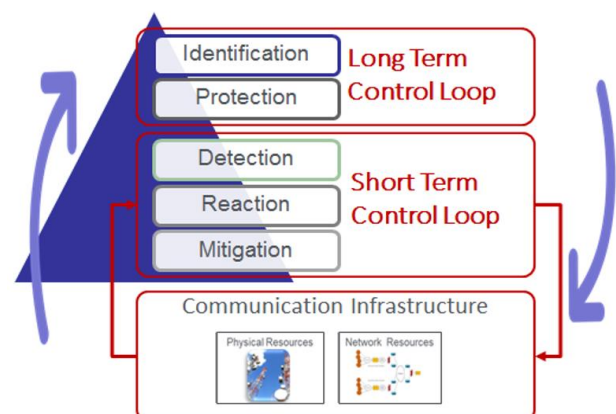


Figure 1 – RESISTO global schema

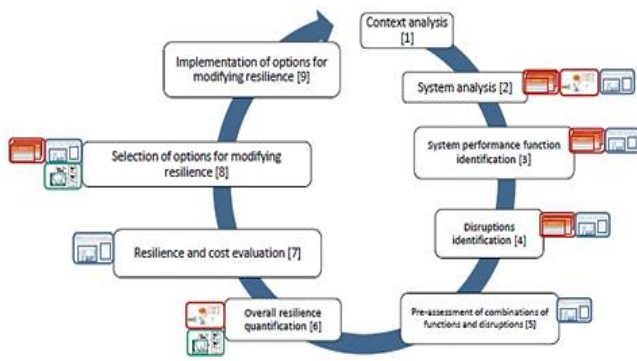


Figure 2 – Risk and Resilience management process

Short Term Control Loop

The Short Term Control Loop (STCL) is the run-time component of the platform. It is in charge of detecting potential physical/cyber threatening events that may impact the operational life of the system and enables it to react promptly, by:

- monitoring the physical and cyber security status of the infrastructures, correlating the physical and cyber domain events and monitoring communication infrastructure data, in order to collect and/or detect anomalies and provide early warnings on security attacks or events adversely impacting security;
- evaluating the event impact with respect to performance degradation of the detected anomalies and security attacks on the communication CI and interlinked CIs, if known, based on the cascading effect;
- supporting the decision making, providing a qualitative and quantitative What-If analysis tool in order to evaluate the best communication CI reconfiguration;
- driving reaction and mitigation by means of action workflows (consisting of directives to intervention teams, physical protection devices activation) and, mainly, of orchestrated Communication Network reconfiguration and activation of protection functions.

The STCL functional control flow is reported in Figure 3.

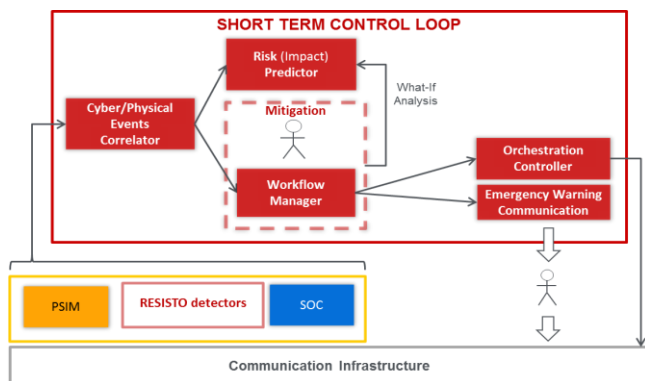


Figure 3 – STCL functional architecture

STCL is mainly based on Leonardo's SC2 platform.

The sources of such data and information could be:

- legacy Physical Security Information Management system(s) or other detectors made available by CI operator;
- legacy Security Operating Centers or other cyber-attack detectors made available by CI operator;

- RESISTO additional physical threat detectors (e.g., airborne threats detection systems, smart spectrum surveillance);
- RESISTO additional cyber threat detectors such as OSINT (Open-Source Intelligence)-based detectors.

From a functional point of view, input data are collected by the **Cyber/Physical Events Correlator**, a rule-based engine that applies customized rules to generate alarms from the managed events. The Correlator not only propagates externally detected and collected attack/anomaly events but it also generates alarms on its own from apparently harmless events and monitoring data. This latter action is performed by using several event correlation techniques, such as logical, causal and temporal correlation based on event time. The Correlator is also equipped with a Machine Learning (ML) based module that allows the detection of anomalous communication traffic situations if compared with the statistically detected traffic density. Historical data of such control flow retrieved from the past are used as the first baseline for the elaboration of the statistical procedure. The historical data repository can be increased continuously in order to tune the machine learning based detector with respect to the evolving curves of the data traffic.

The anomalies detected by the Correlator trigger the **Risk (Impact) Predictor**. The Risk Predictor evaluates and highlights the impacts of the detected anomaly on the communication infrastructure and, mainly, on the services provided by the infrastructure. The Risk Predictor Engine acts at run-time on a model of the CI.

The CI is modelled according to different interlacing points of view:

- physical elementary entities
- logical entities
- provided services

Moreover, the Risk Predictor supports the decision making process in allowing a “What-If analysis” by simulating the application of countermeasures, their reconfiguration and their impact on resilience of the system.

In parallel with the Risk Predictor, the Correlator also triggers the **Workflow Manager** in charge to guide the operator during the reaction phase. On the basis of the alarm type, the most appropriate workflow is selected and executed. As any workflow is a conditional sequence of steps, each step specifies a procedural action e.g., alerting a reaction team with an emergency message sent through the **Emergency Warning Communication (EWC)** function, drives a physical actuator (e.g., lock a physical gate), carries out a complex action on the Communication Network.

Complex actions on the Communication Infrastructure are performed by the **Orchestration Controller**. It is built around the concept of Software Defined Security (SDS) taking advantage of the Network Function Virtualization (NFV) and Software Defined Networking (SDN) paradigms of the underlying communication network. It implements security functions and services composing security mechanisms acting on physical resources (i.e. network physical equipment), as well as on Virtual Network Functions in a NFV/5G perspective. The Orchestration Controller operates on a communication infrastructure

already controlled by a telecommunication operator, so it works on top of a SDN Controller or on top of a network Operational Support System (OSS).

The EWC function is activated when it is needed to send instant messages, targeted alerts and operating instructions to specific categories of users who are located in a given area where events like natural disasters, physical or cyber-attacks are occurring. In particular, rescue teams called to execute actions on the infrastructure can leverage on the received information.

LTCL and STCL interact with each other by means of Resilience Indicators (RIs).

During the last steps of a LTCL cycle:

- CI «as it is» resilience is characterized and quantified for the most critical couples (function; threatening event)
- couples (function; event) showing RIs not in line with due SLA are identified
- interventions on CI are selected in order to improve resilience for most critical couples (function; event) estimating RIs in the new «to be» configuration
- interventions are implemented

So, at the end of each LTCL cycle some Estimated RIs for specific couples (function; event) are stored in a Knowledge Base (KB). During the operation system life, STCL operators could face real events for which RIs were previously estimated.

In those cases, the actual RIs can be measured and values can be stored in the KB. So the comparison between Estimated and Measured RIs is taken into account in the next LTCL cycle to improve CI resilience and/or resilience estimation methods if needed. This process triggers a continuous resilience improvement for the CI.

INNOVATION AREAS

The RESISTO project will promote the following key areas of innovation:

- Combined approach for cyber and physical threats;
- Advanced system modelling and monitoring to allow an accurate risk impact prediction to enhance operators awareness and support decision making;
- Integrated risk and resilience management;
- Convergence of PSIM (Physical Security Information System) and Cyber Protection technologies;
- 5G Network Orchestration to manage 5G Network function as virtualization of network services, slicing of the network, orientation to the cloud, etc.
- Advanced detection, protection and response technologies: drones detection, Machine Learning algorithms, Software-Defined Security.

CONCLUSIONS

RESISTO provides an innovative solution to the complex issue of CI protection as it proposes a global and integrated approach to the physical and cyber security of complex systems, by applying the best state-of-the-art technologies.

RESISTO combines a structured process to identify and protect the CI, as well as a Command & Control platform to promptly detect threatening events, support decision making and drive the reaction until complete recovery. The CI continuous improvement in resilience is addressed by the analytical and quantitative approach adopted.

Emanuele Aonzo: emanuele.aonzo@leonardocompany.com

REFERENCES

- [1] <http://www.resistoproject.eu/> : web site of RESISTO project.
- [2] A. Nadjaran Toosi, R. Mahmud, Qinghua Chi, R. Buyya, “*Management and Orchestration of Network Slices in 5G*”, Fog, Edge and Clouds.
- [3] International Organization for Standardization, “*ISO 31000: Risk management — Principles and guidelines*”, (<https://www.iso.org/iso-31000-risk-management.html>)
- [4] L. Carlson, B. Haffenden, G. Bassett, W. Buehring, M. Collins, S. Folga, F. Petit, J. Phillips, D. Verner and R. Whitfield, 2012, “*Resilience: Theory and Application*”, Argonne National Lab (ANL), Argonne, IL (United States).
- [5] I. Häring et al., “*Towards a Generic Resilience Management, Quantification and Development Process: General Definitions, Requirements, Methods, Techniques and Measures, and Case Studies Resilience and Risk*”, in *Resilience and Risk*, Bd. 6, I. Linkov und J. M. Palma-Oliveira, Hrsg., Dordrecht, Springer Netherlands, 2017, pp. 21-80.
- [6] C. Foglietta, C. Palazzo, R. Santini, S. Panzieri, “*Assessing Cyber Risk Using the CISIApro Simulator*”, in *Critical Infrastructure Protection IX: 9th IFIP 11.10 International Conference, ICCIP 2015, Arlington, VA, USA, March 16-18, 2015* (pp.315-331).