

N. 1 NEWSLETTER

December 2019



RESilience enhancement and risk control platform
for communication infraSTructure Operators



IN THIS ISSUE

- Insight from the RESISTO project Coordinator
- Technical highlights
- Opinion about the project from an Advisory Board's member

... and MORE



THE RESISTO PROJECT HAS RECEIVED FUNDING FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME UNDER GRANT AGREEMENT NO. 786409.

SUMMARY

- pag. 3 **Insight from the RESISTO project Coordinator**
by Bruno Saccomanno, Leonardo S.p.A
- pag. 4 **Technical highlights**
by Marco Carli, Università degli Studi RomaTre
- pag. 5 **Opinion about the project from an Advisory Board's member**
by Luisa Franchina, AIIC
- pag. 6 **Resisto project online**
by Marco Ferraro, Arianna Magni, APRE - Agency of the Promotion of European Research
- pag. 7 **Resisto: we have been there!**



RESISTO newsletter is the official, semi-annual newsletter from Horizon 2020 RESISTO project. Each RESISTO newsletter issue aims to disseminate project updates as well as news. It is developed and compiled with the contributions from the RESISTO Consortium Partners and relevant Stakeholders.

INSIGHT FROM THE RESISTO PROJECT COORDINATOR



Dear RESISTO follower,

We are pleased to present to you our first RESISTO Newsletter!

On May 2018, RESISTO project was successfully launched to provide holistic (cyber/physical) situation awareness and enhanced resilience for Communication Critical Infrastructures (CI), that play a fundamental role in the economic and social well-being of the citizens and on operations of most Critical Infrastructures. RESISTO is a three-year EU research project led by LEONARDO (key player in Aerospace, Defence and Security) and co-funded by EU H2020 Research and Innovation Programme. It brings together end users, practitioners, research centres and industries from Cyprus, Estonia, Germany, Greece, Italy, Portugal, Romania, Spain and United Kingdom.

Until now the project has made significant progress both in the use cases definition and user requirements specification - thanks to the significant presence of TELCO Operators - and in all the RESISTO technical solutions, to deliver an innovative platform for optimized decision support in the face of physical, cyber and combined cyber-physical threats, taking account of critical schemes of infrastructures, functions and services and possible (cascading) event trajectories.

We are on the right path to help Communications Infrastructures Operators to take the best countermeasures and reactive actions, exploiting the combined use of risk and resilience preparatory analyses, detection and reaction technologies, applications and processes in the physical and cyber domains... **by RESISTO the physical security operators and the cyber security experts will finally work together!**

Stay tuned with the project progress by following our newsletters, social network accounts and web site (www.resistoproject.eu), to be informed about future developments towards a faster and more efficient critical infrastructures protection.



Bruno Saccomanno,
Leonardo S.p.A,

TECHNICAL HIGHLIGHTS

by Marco Carli, Università degli Studi RomaTre

During the first year of RESISTO project, the work has been performed following the scheduled time-plan towards the definition of an architecture able to jointly cope with cyber and/or physical security of telecommunication infrastructures. In more details, the user requirements have been collected, the main cyber-physical threats have been analyzed and, correspondingly, the possible countermeasures identified. At the same time, an in-deep assessment of existing key performance indicators has been carried out in order to select the most suitable ones. The mitigation/reaction engines have been designed and their ability to adapt to the different scenarios analyzed.

Some advancements with respect to the Description of Actions have been obtained from different points of view.

RESISTO architecture has been better designed to cope with the emerging 5G scenario and to the new communication standards. The architecture modeling has been improved for considering the dynamic aspect of virtual networks. The resilience concept has been evaluated in more details, by improving and adopting awareness tools (i.e., penetration test) specialized for the communication scenario by also taking into account, since the initial assessment phase, the available resources. At the same time, current efforts are devoted to measuring the resilience of systems.



Read our public access **DELIVERABLES*** from the project:

> www.resistoproject.eu/resources/

* These documents and its content are the property of the RESISTO Consortium. The content of all or parts of these documents can be used and distributed provided that the RESISTO project and the document are properly referenced.

OPINION ABOUT THE PROJECT FROM AN ADVISORY BOARD'S MEMBER

by Luisa Franchina, AIIC

The RESISTO proposal for Communication CIs holistic situation awareness and enhanced resilience is a strong valid solution based on an Integrated Risk and Resilience analysis management and improvement process, availing all resilience cycle phases and technical resilience capabilities.

The alignment with ECSO (European Cyber Security Organisation) objectives is significant and inclusive. RESISTO implements an innovative Decision Support System to protect communication infrastructures from combined cyber-physical threats exploiting the Software Defined Security model on a suite of state of the art cyber/physical security components and services, for detection and reaction in presence of attacks or natural disasters.

RESISTO will provide the Communications Operators with tools to implement a set of mitigation actions and countermeasures to significantly reduce the impact of threatening events. This contribution is relevant to deal with the vulnerabilities of the Communication CIs, especially nowadays with the advent of the 5G network.

The two control loops, the short term and the long-term control loop, are a strong solution for the objective of the RESISTO project to improve the resilience in communication infrastructures. In addition, the modelling approaches were selected with a view on scientific and operator acceptance.

Through the holistic approach of the RESISTO project, that includes the current theme about the 5G evolution, the landscape of the threat is enlarged, the Risk and Resilience management is integrated and the PSIM and Cyber Protection technology converge; finally, are also considered new and actual technology for detection/protection/response, such as blockchain, drones, machine learning algorithms, and software defined security. About the threat landscape, is significant the special emphasis given to the review of existing threat classification schemes and available threat lists and databases, adding the possibility and allowing the correlation of threats to additional information. Moreover, the collection of testbeds has the added value to considering realistic environments.

The results can be considered comprehensive and of high value.

RESISTO PROJECT ONLINE

by Marco Ferraro, Arianna Magni, APRE - Agency of the Promotion of European Research

RESISTO communication and dissemination activities have been launched from the very beginning of the project and are constantly ongoing to ensure wide visibility of the project and its results on timely basis. In this context, RESISTO social media accounts have been established:

Twitter: @RESISTO_project

Facebook: @RESISTO.eu.project

Linkedin: RESISTO project



RESISTO has a professional website with a smart graphic and a bold and lively layout: www.resistoproject.eu. The overall RESISTO concept is depicted in the About section while the Partners section offers a clear picture of the consortium. Moreover, during the whole lifetime of the project, the website will constantly collect news, interesting contents, information about upcoming Events. The Resources section will have public deliverables, informative and scientific resources of interest as well as the RESISTO Newsletters available for download.

Visit the RESISTO project website: www.resistoproject.eu

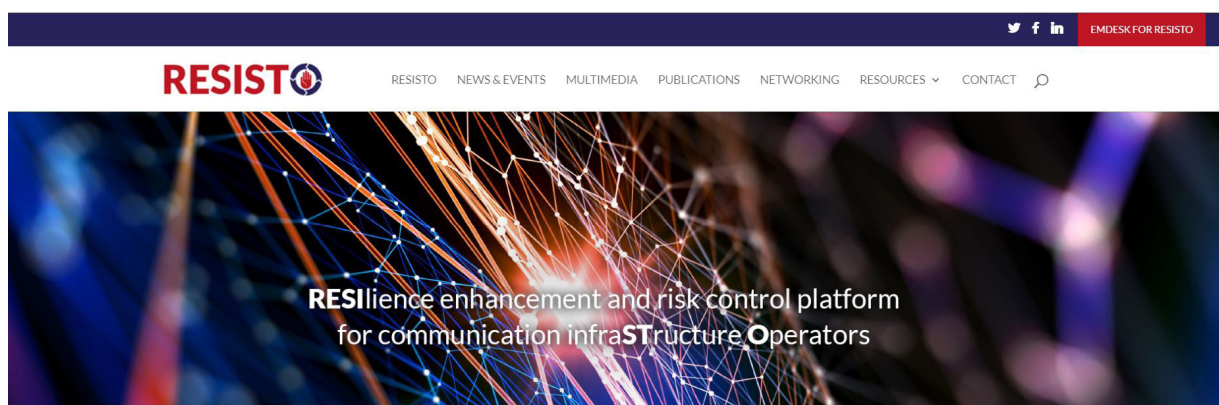


Fig. 1 - RESISTO homepage

RESISTO: WE HAVE BEEN THERE!



International Security Expo - ISE19

3 - 4 December 2019 | London

> MORE INFO [HERE](#)



MILIPOL 2019

19 - 22 November 2019 | Paris

> MORE INFO [HERE](#)



Mediterranean Security Event 2019

29 - 31 October 2019 | Crete, Greece

> MORE INFO [HERE](#)



14th CoU Thematic Workshop

16 - 20 September 2019 | Brussels

> MORE INFO [HERE](#)



ISCRAM 2019 | 1st RESISTO workshop

19 May 2019 | Valencia, Spain

> MORE INFO [HERE](#)

These events represented an important opportunities to diffuse the knowledge about the project at European level and to promote its achievements and objectives.

... to discover the other events visit the **RESISTO website!**



RESilience enhancement and risk control platform
for communication infra**ST**ructure **O**perators

PROJECT COORDINATOR



Bruno Saccomanno
bruno.saccomanno@leonardocompany.com

RESISTO PARTNERS



(RM3 third party) is responsible of
Dissemination, Communication and
awareness raising activities

www.resistoproject.eu

Follow us

