Panacea

People-centric cybersecurity in healthcare

Innovative cyber security solutions in healthcare

Matteo Merialdo, Technical Project Manager
RHEA System S.A.

Webinar
18 April 2019

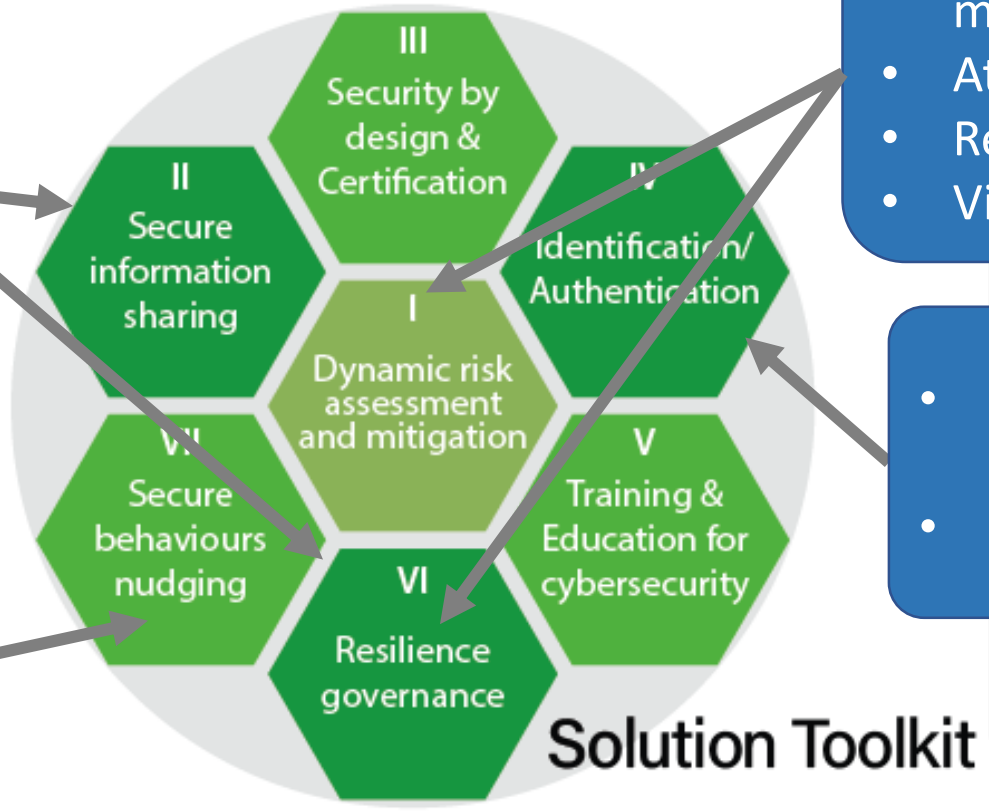
Funded by the European Union's Horizon 2020
Research and Innovation Programme, under Grant Agreement no 826293

PANACEA Solution Toolkit

- The toolkit will benefit from **nine main PANACEA research goals**

- Models for healthcare data secure information sharing
- Blockchain for secure information sharing

- Multi dimensional threat modelling
- Attack modelling
- Response management
- Visual analytics



- Biometric recognition/digital identity
- IoMT identification

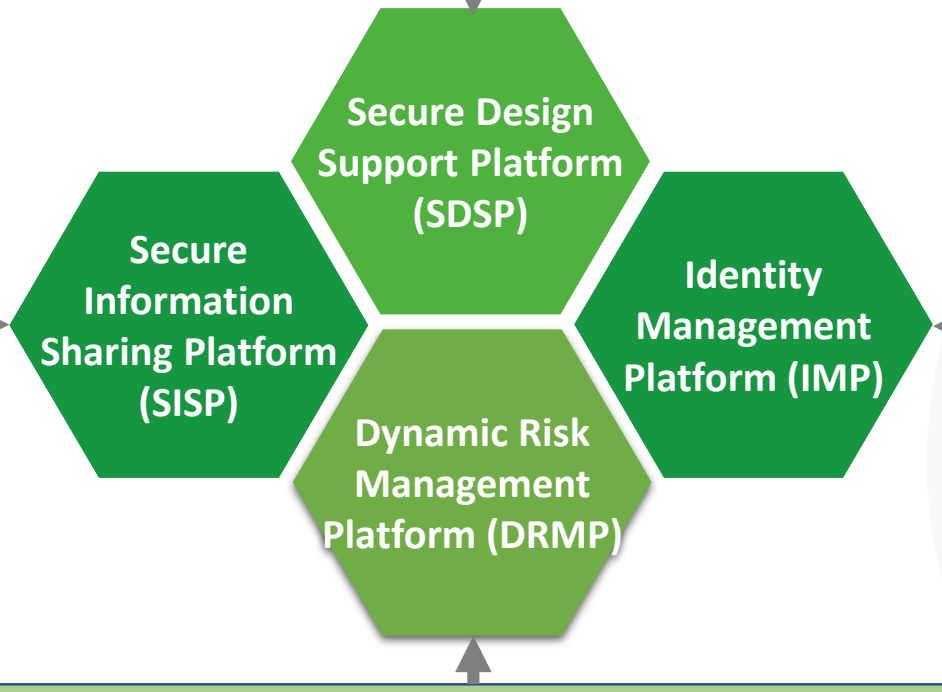
- Secure behaviours decision models and influencers

Panacea
People-centric cybersecurity in healthcare

PANACEA Technical Tools – TRL 6

Risk assessment over system/software in development in order to embed security from the beginning of system/medical device engineering life-cycle

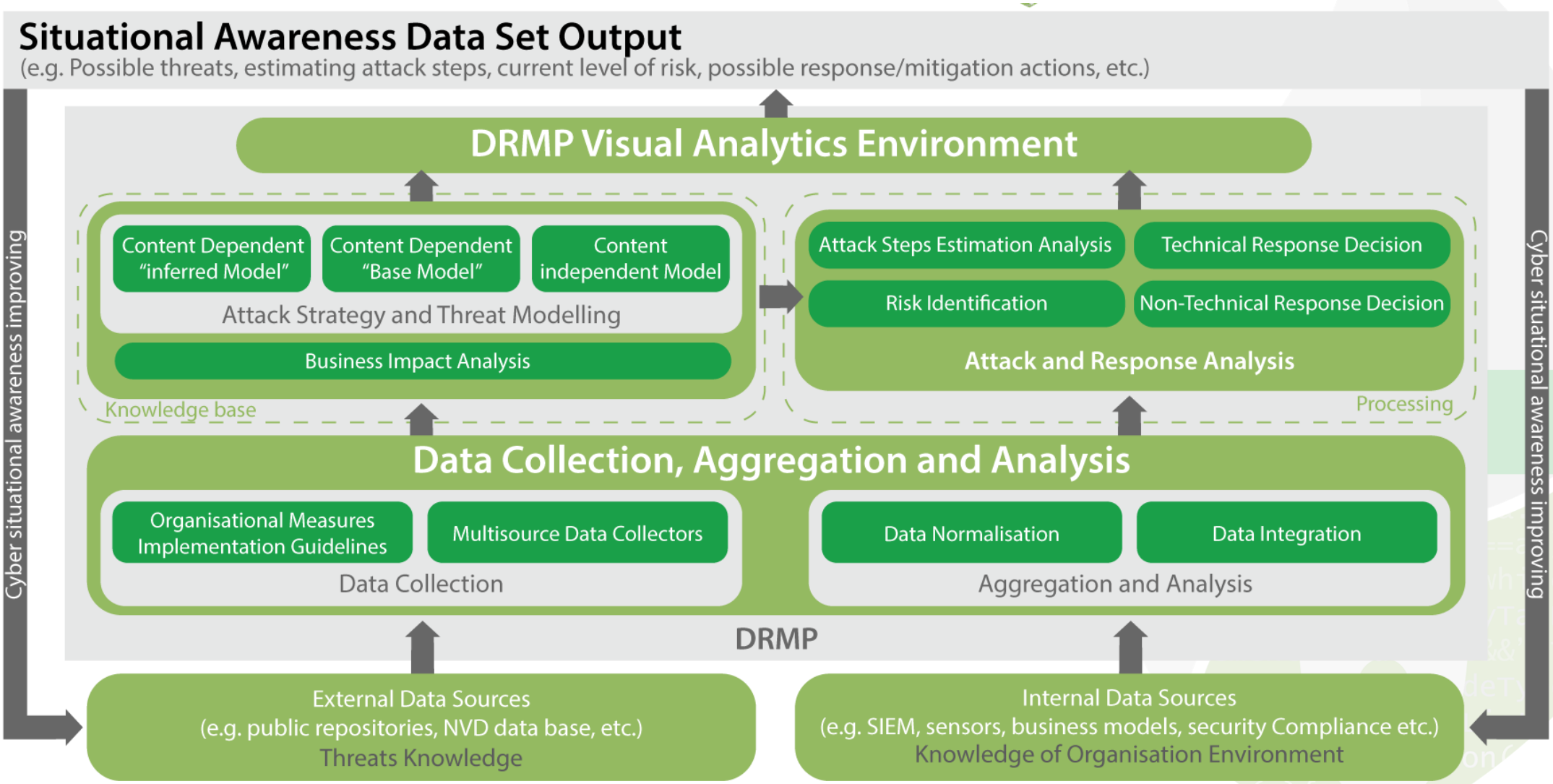
Healthcare information secure sharing, cross-border and multitenant. Shared persistency possibly based on private blockchain



A digital signature technique leveraging on digital IDs, enabling non-repudiation capabilities and integrated within the other technical tools

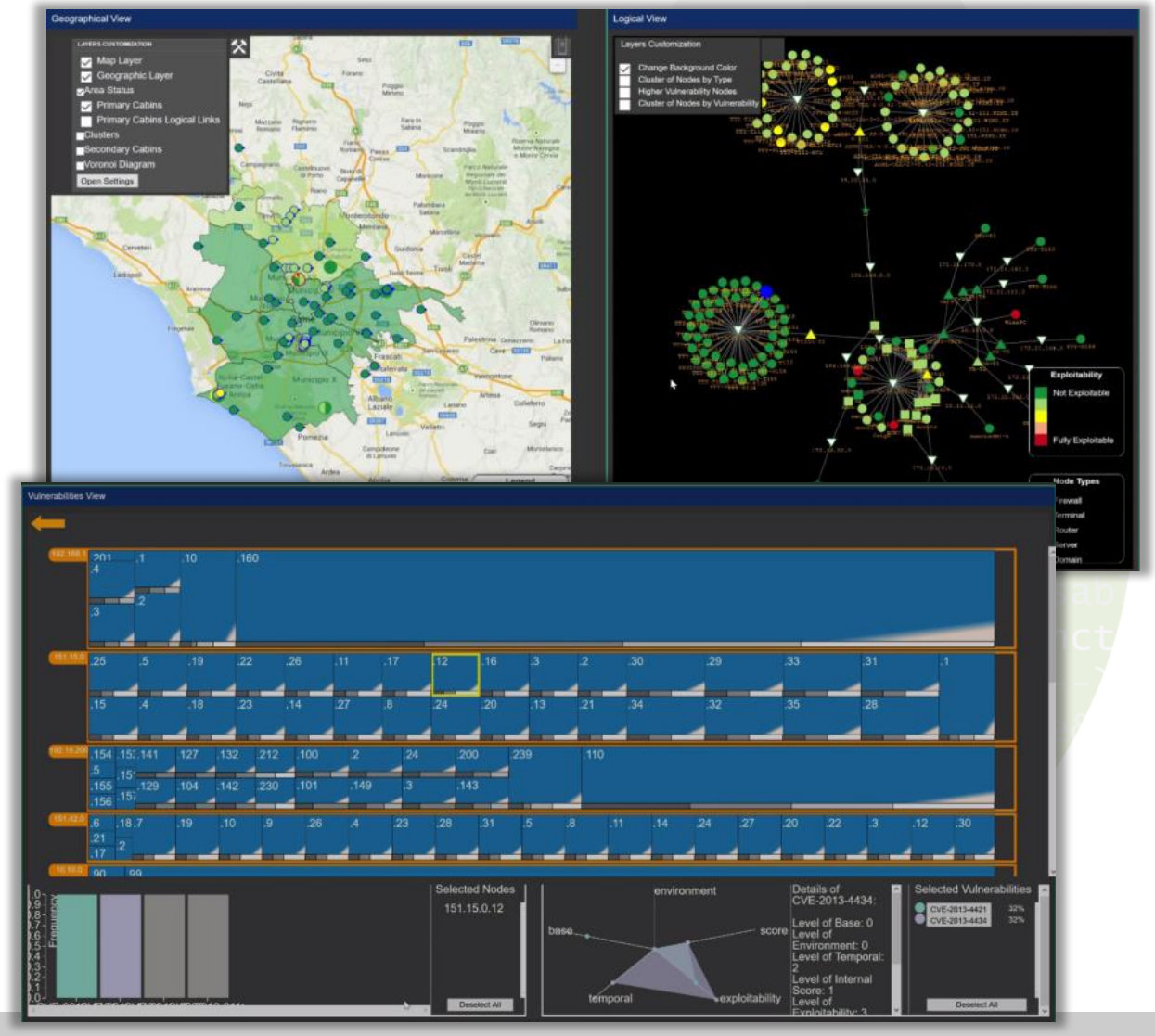
Multidimensional threat modelling, dynamic risk assessment with business impact dynamic computation, technical and organisational response for complex infrastructure

Dynamic Risk Management Platform (DRMP)



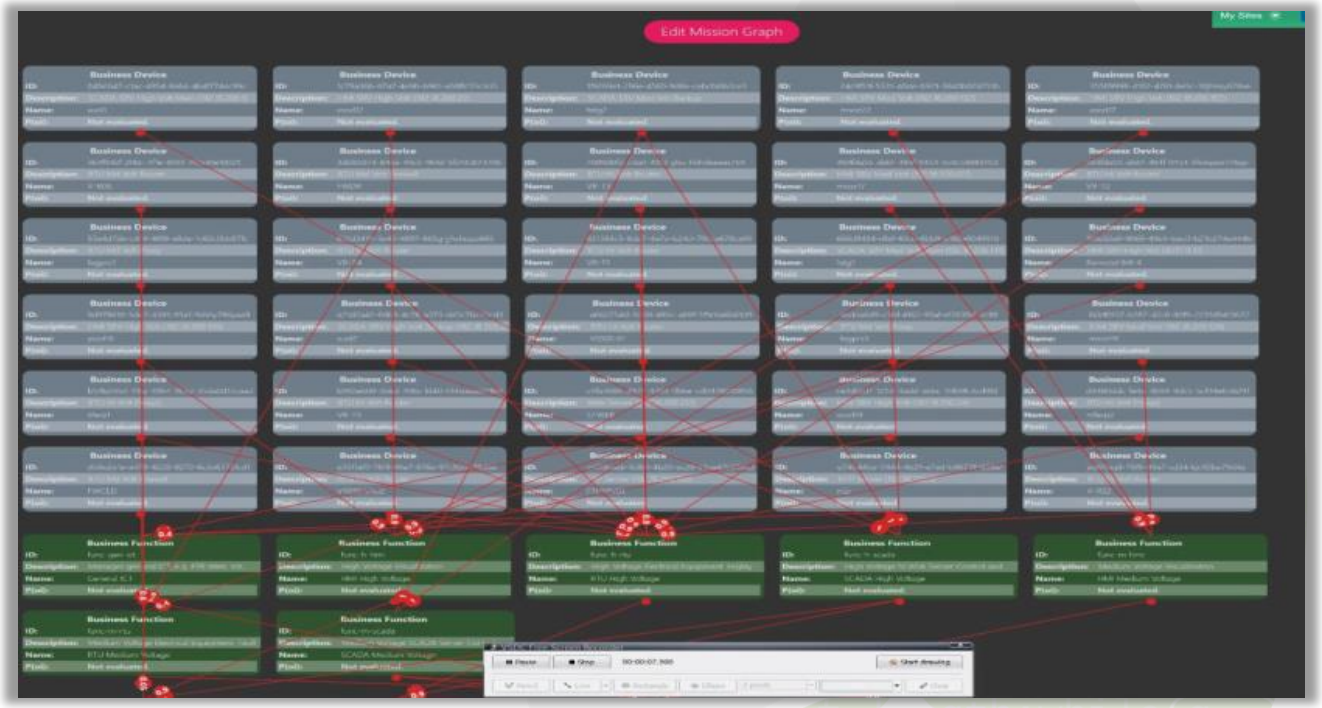
DRMP - Data Collection

- Acquisition of network knowledge (scans, topology data-flows, assets characteristics)
- Acquisition of vulnerability surface knowledge (scans)
- Flexible and open interface to COTS sensors and systems
- Acquisition of governance models and any relevant human behaviour data
- Normalization of multiple data sources to a common data model
- Based on a previous FP7 experience



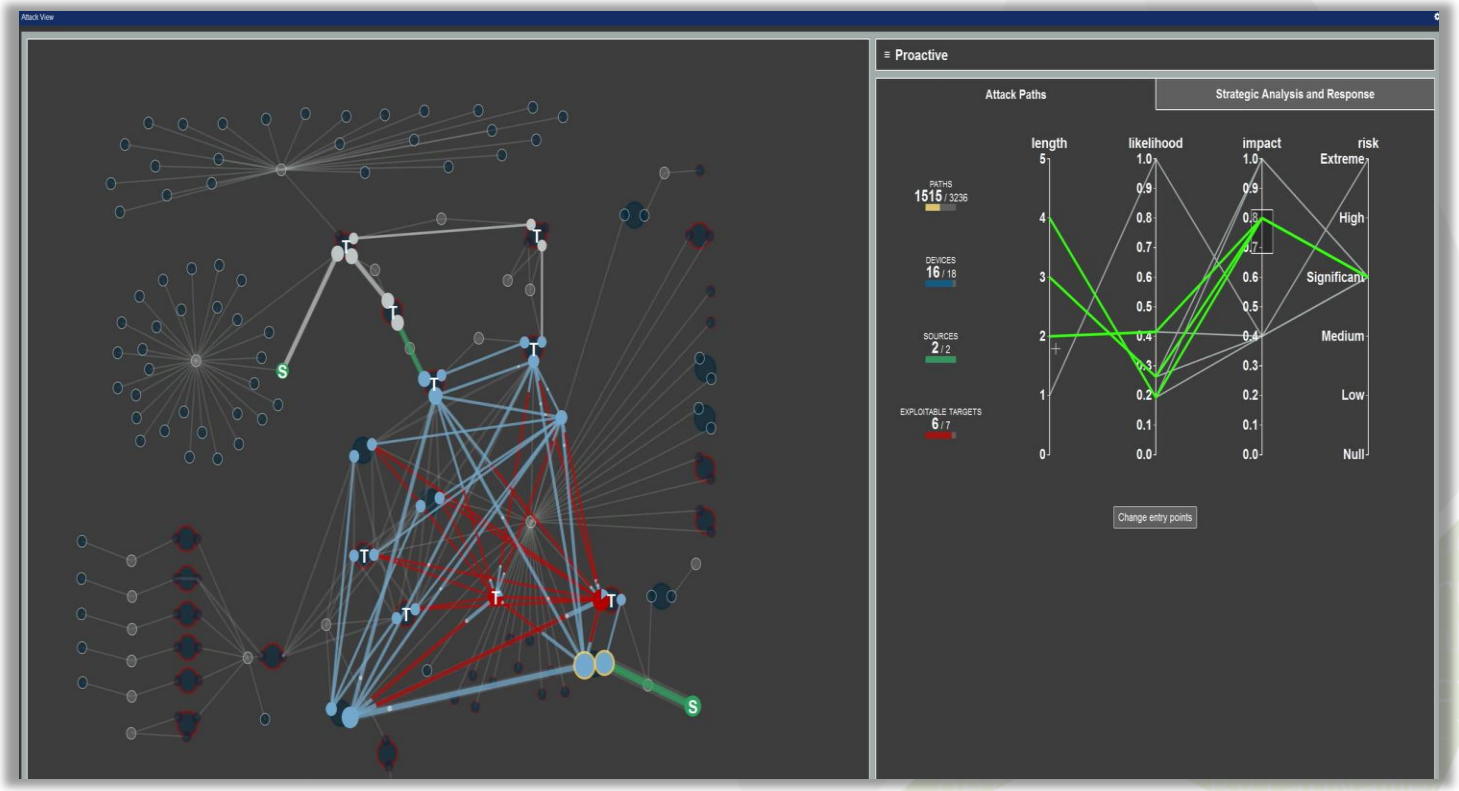
DRMP – Mission Impact Evaluation

- A quantitative evaluation of the business impact
- Calculated from a precise mapping of key business processes vs infrastructural assets
- Providing impact component for the risk computation
- Based on a previous FP7 experience



DRMP – Attack Graph Evaluation

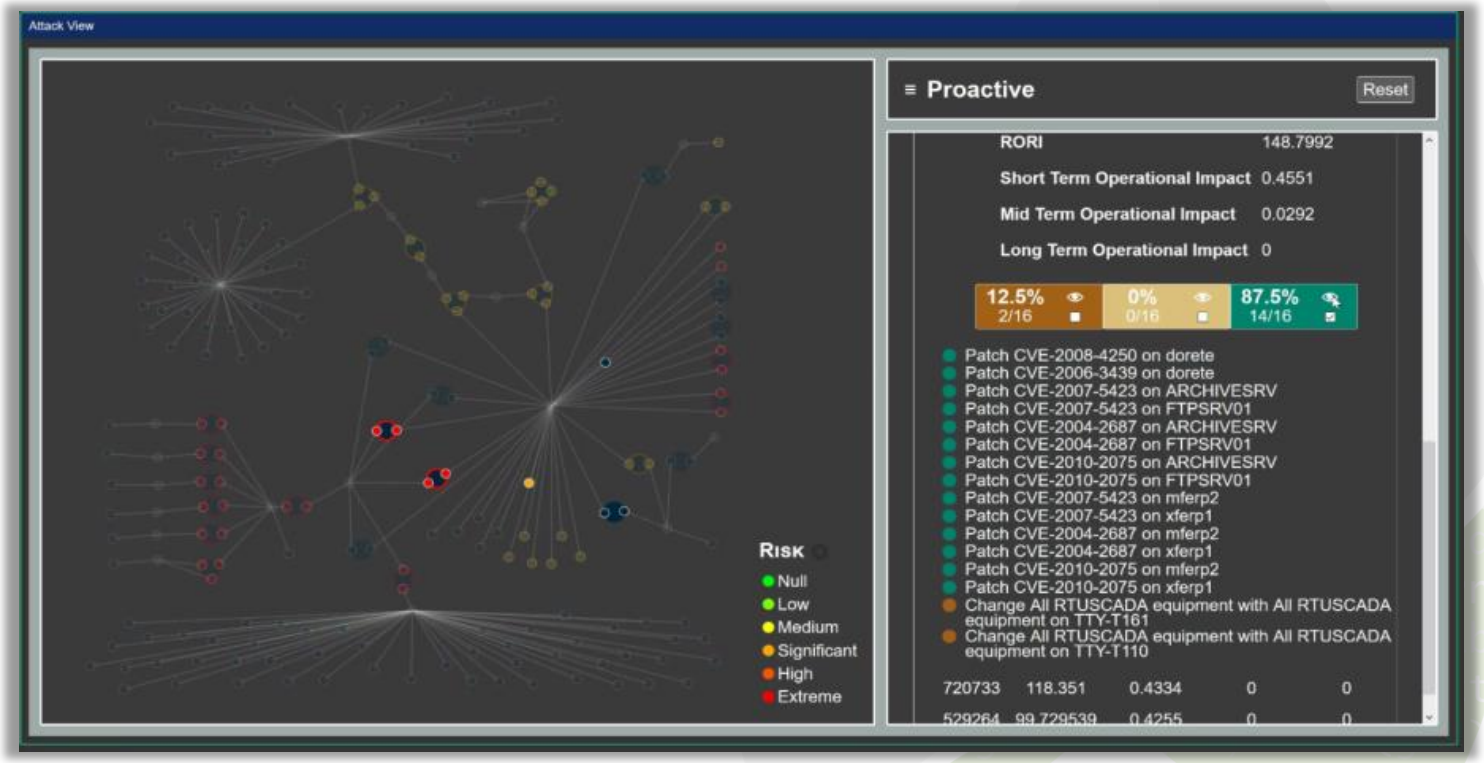
- Calculating and prioritizing possible attack paths within a graph
- An attack graph represents possible ways via which a potential attacker can intrude into the target network by exploiting a set of vulnerabilities on various network hosts and gaining certain privileges at each step



The attack graph will consider multidimensional threats (not only due to technical vulnerabilities but also human behaviour)

DRMP – Response Evaluation

- Generating and prioritizing mitigation actions
- A list of prioritized, specific and actionable risk-mitigation actions is then generated, based on cost / impact / risk reduction trade-offs

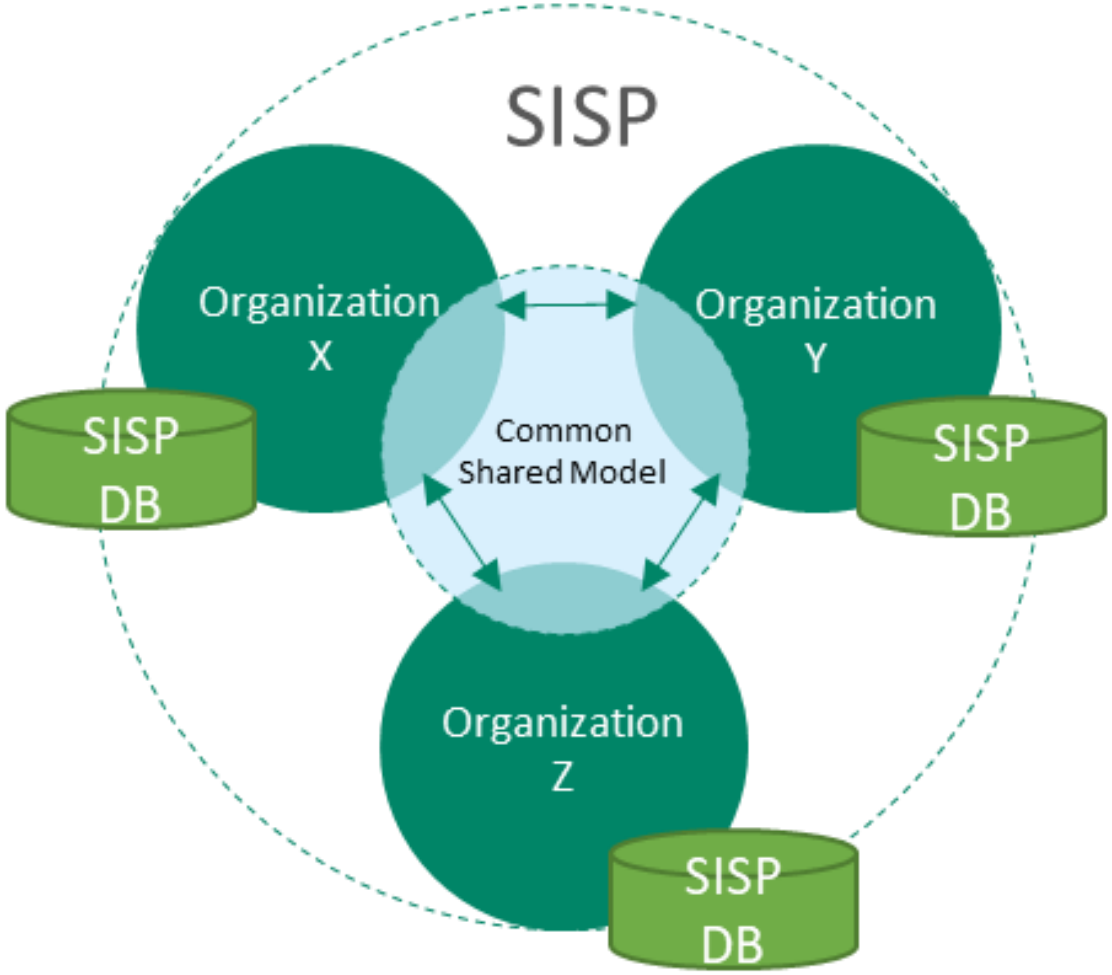


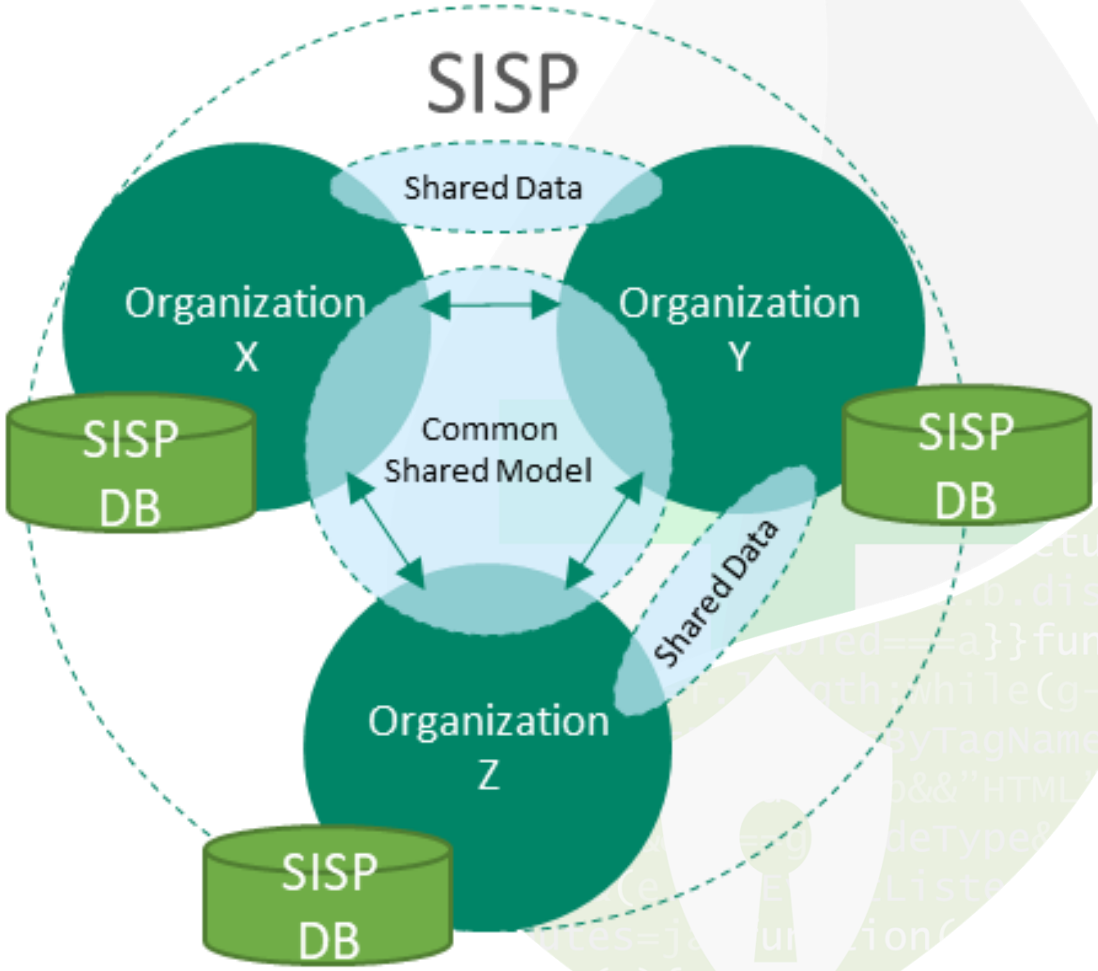
Secure behaviours nudging

Resilience governance

Not only technical, but also governance and 'human' mitigation actions (nudging) to be considered

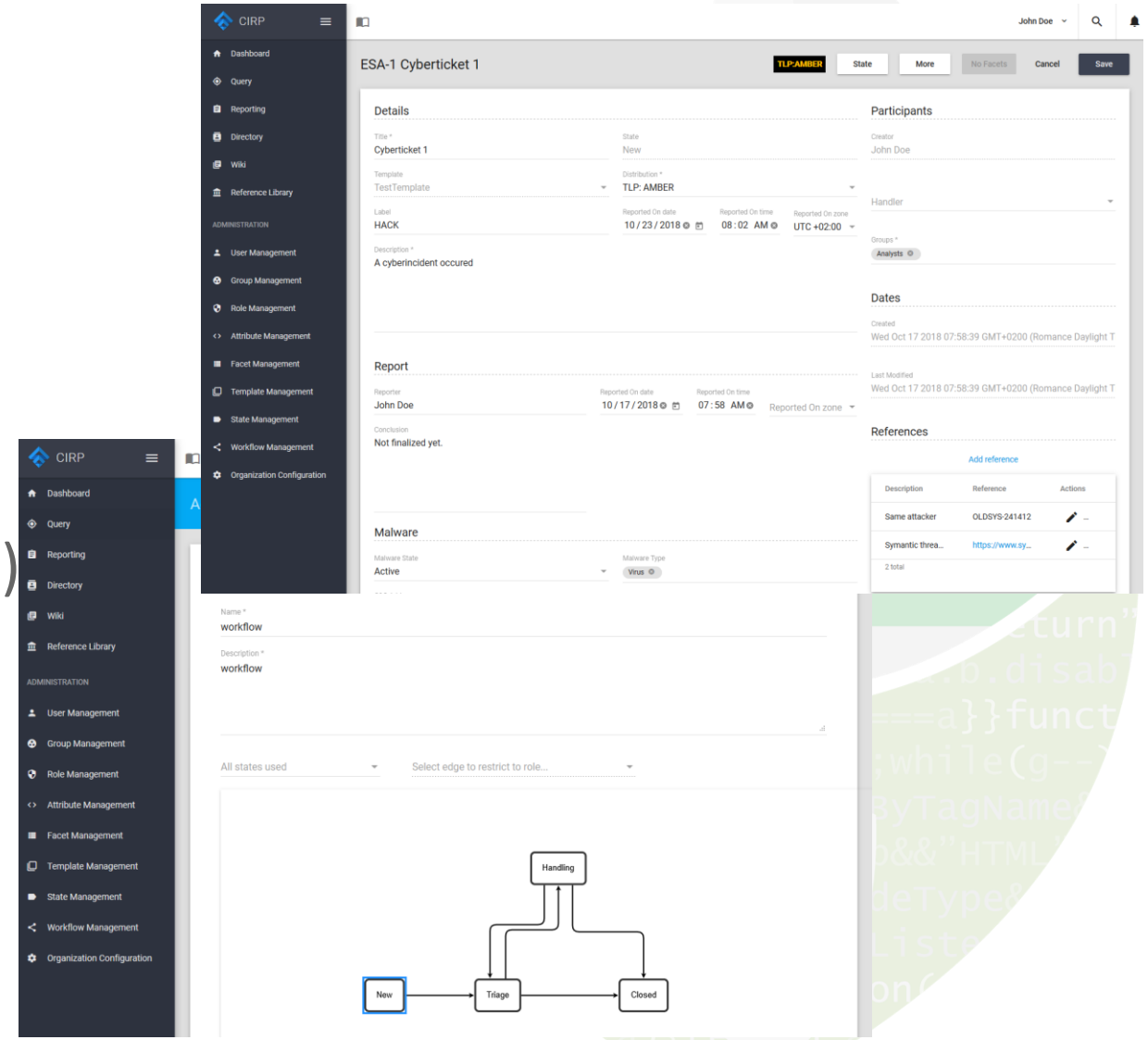
Secure Information Sharing Platform (SISP)





Secure Information Sharing Platform (SISP)

- Secure information sharing
- Customizable templates and data model
- Customizable workflow
- Customizable dashboard views
- Customizable reporting
- Shared knowledge management (wiki)
- Internationalization and localization
- GDPR compliant
- Multitenant/Multiorganization
- Cross border (multi regulation regulations compliance)

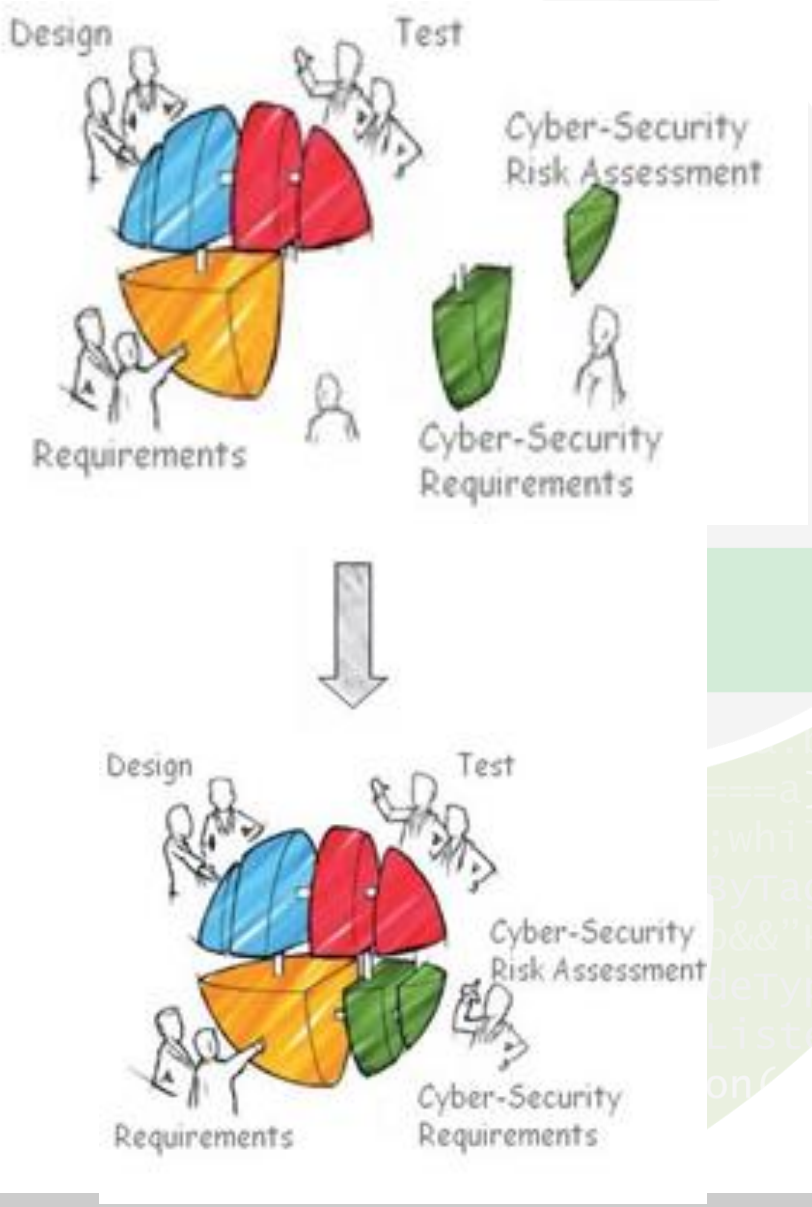


SISP – Use of blockchain for information sharing

- Data is nowadays a key asset
- Appealing target for cyber-attacks to undermining data C.I.A. properties
- Data Integrity issues are exacerbated when data must be shared between collaborating but independent parties
  - Data owners have hardly control of them
  - Where data are stored? Who can actually access them? In which way?
  - Trusting data has become crucial
- Other similar example scenarios
  - Supply chain management
  - Forensics data
  - …

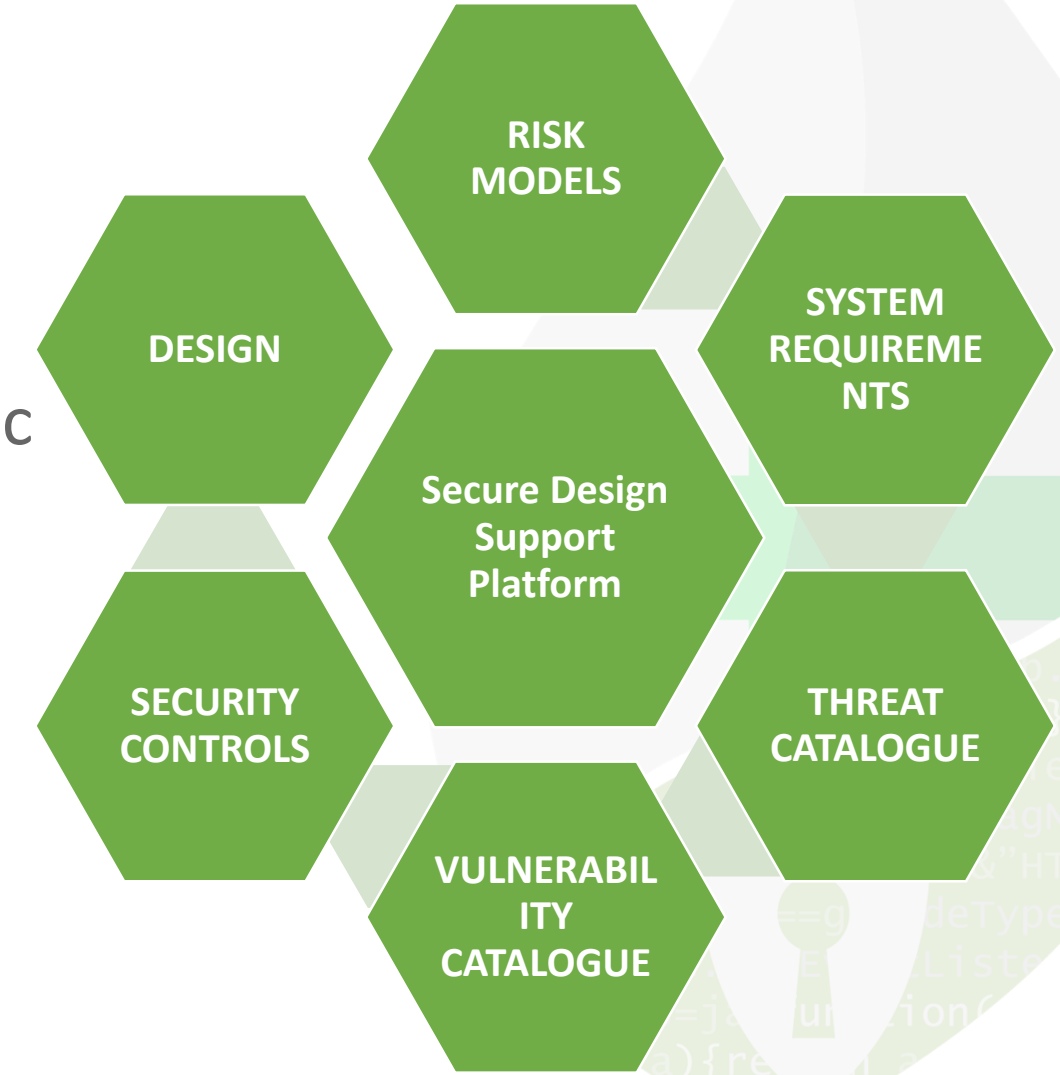
Secure Design Support Platform (SDSP)

- Software and system engineering lifecycles are a fundamental component of mission-critical systems and medical devices development
- As software and systems become more complex, security-related risks are also increasing
- Traditional security-engineering rely on addressing security risks during the operation and maintenance of systems, increasing costs
- Secure system and software engineering best practices recommend that security risk assessment is included from the earliest phase



Secure Design Support Platform (SDSP)

- Enabling security-by-design of complex systems
- Following ESA ECSS standard
- Integrating into the system engineering life-cycle, with a specific focus on medical devices
  - Requirements
  - Design
- Configurable with ad-hoc
  - Vulnerabilities, threats and security controls catalogues



Identity Management Platform (SDSP)

- PANACEA aims to develop a novel concept of digital identity for the patient/healthcare professional
- A combination of a biometric feature and a digital signature of the patient's mobile device (including some randomness)
- The result will be a master key that could be derived in multiple secondary digital identities for multiple applications by adding a third element (third factor authentication) specific to the application (pin, passphrase or anything else)
- Features:
  - It solves the entropy problem with biometric keys thanks to the combination with another key (the Smartphone's signature randomly generated)
  - It enables creating the conditions for a repudiation of biometrics: if the master key is compromised, another key can be generated from the same biometric feature but using another signature from the mobile device
  - It facilitates management of non-repudiation: transactions are signed using this digital identity allowing the authentication of parties for that transaction and the generation of logs with legal value so parties cannot repudiate the transaction – possible storage in blockchain to be explored
  - It supports privacy-preservation: the digital identity certifies the identity of actors without disclosing any personal information. Only the ID is important (unique, verifiable, repudiation capacity)

Panacea
People-centric cybersecurity in healthcare

Thank you for your attention! *Questions?*

Website: ***www.panacearesearch.eu***

Contacts:

Pasquale Mari, Policlinico Gemelli, pasqualemari3@gmail.com

Matteo Merialdo, RHEA System S.A., m.merialdo@rheagroup.com

Ivan Tesfai, RINA, ivan.tesfai@rina.org