Panacea

People-centric cybersecurity in healthcare

PANACEA Project focus on User Requirements

Matteo Merialdo, Technical PM
RHEA System S.A.

WORKSHOP ON CYBER SECURITY SITUATION AWARENESS FOR HEALTH ORGANIZATIONS
Brussels, 10 June 2019

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

Panacea
People-centric cybersecurity in healthcare

Scope

- Project coordinator is Universita' Cattolica del Sacro Cuore – Sabina Magalini
- PANACEA will deliver a **suite of technological and organizational tools** which help users to assess and reduce the vulnerability to cyberattacks of their "system in scope"
- Systems in scope include
  - **Healthcare providers** (single Hospital, Group of Hospitals, Healthcare region)
  - **Medical Device lifecycle**
- PANACEA delivers nine tools, clustered in two integrated toolkits :
  - the **Solution Toolkit: four technical tools, three organizational tools**
  - the **Delivery Toolkit: two tools**

PANACEA Solution Toolkit

- The **Solution Toolkit** comprises
  - **four technical tools** for

    I-dynamic risk assessment & mitigation,

    II-secure information sharing,

    III-security-by-design & certification,

    IV-identification & authentication
  - **three organisational tools** for

    V-training & education,

    VI-resilience governance,

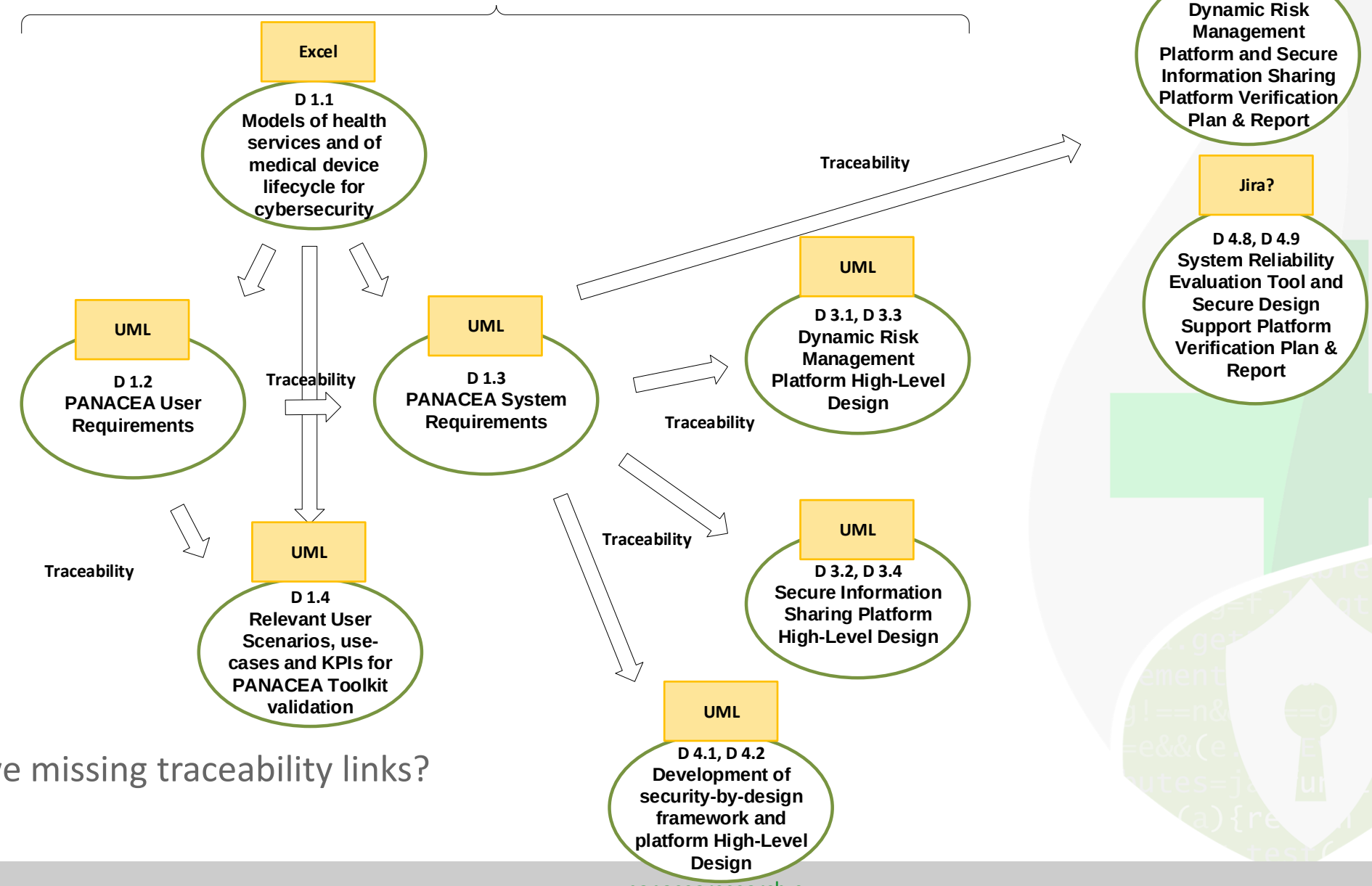
    VII-secure behaviours nudging

PANACEA Requirements, Design

- A single Model Based System Engineering approach is adopted for managing
  - Models (for example, WP 1.1)
  - Requirements (User and System requirements)
  - Software design of the four technological platforms
  - Overall traceability (System Requirements must *cover* User Requirements, Design must *realize* System Requirements)

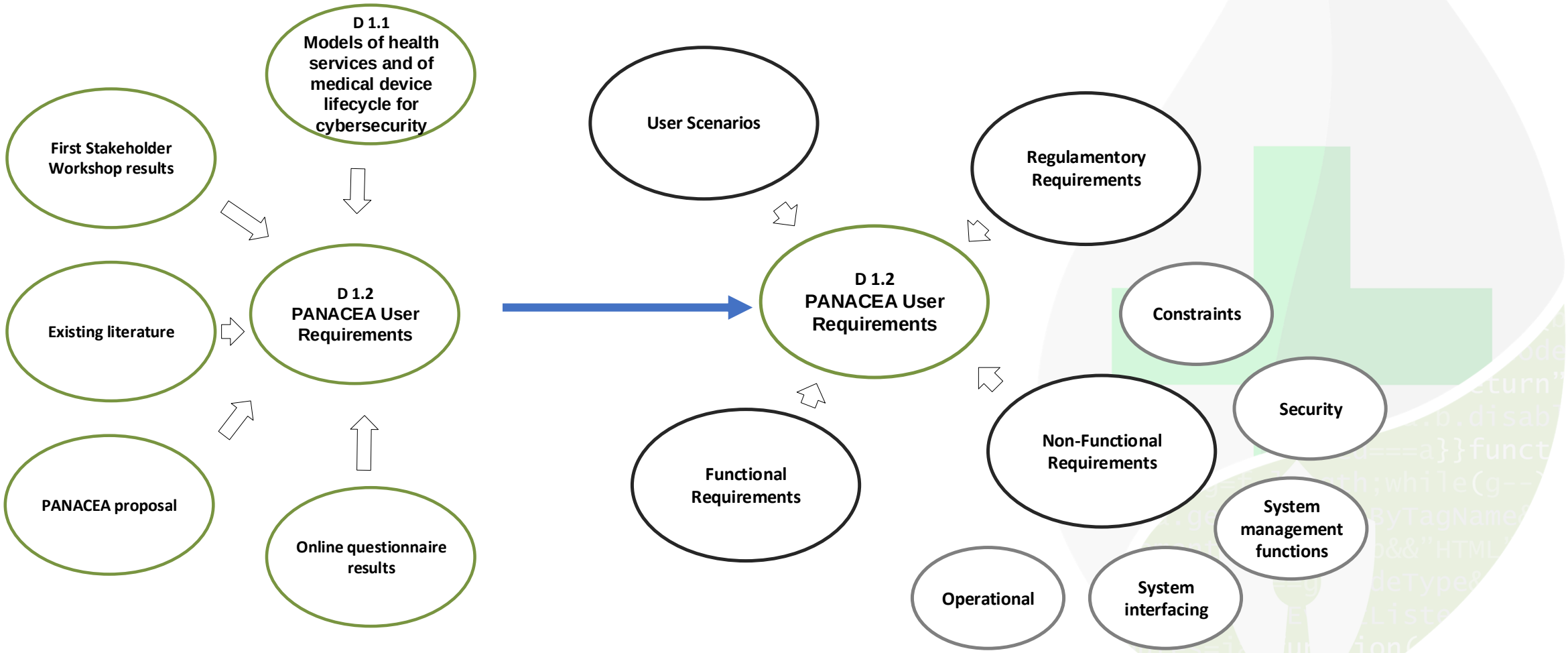
Models, Requirements, Design

Single modelling project

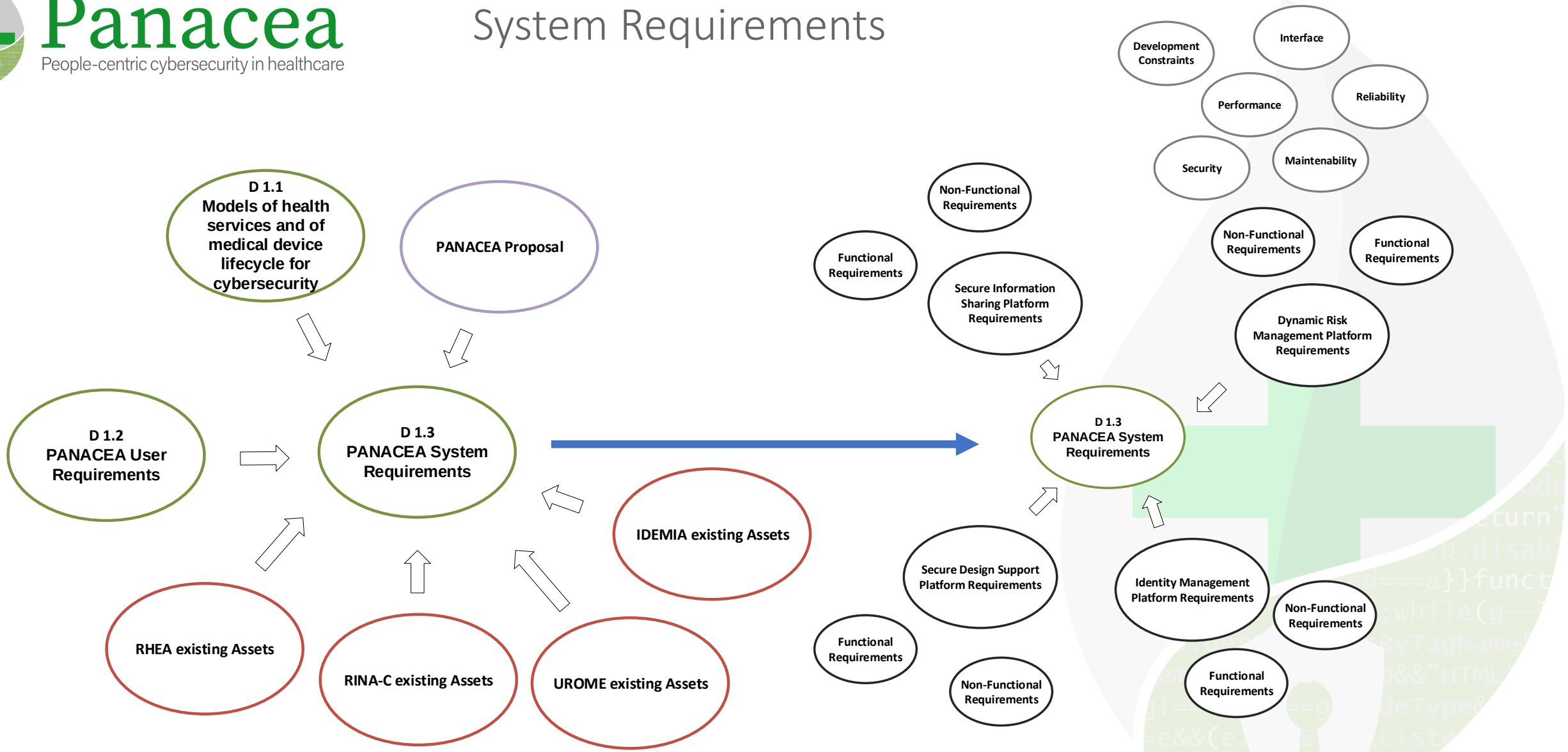


- Are we missing traceability links?

PANACEA User Requirements



System Requirements



User Requirements, sources

- PANACEA End Users
  - Fondazione Policlinico Universitario Agostino Gemelli
  - 7th Health Region Crete
  - Irish Centre for Emergency Management
  - Innovation Sprint Sprl
- PANACEA users workshop (28-29 May, Rome)
  - 55 attendees
    - PANACEA end users
    - HC H2020 projects (Sphinx, Curex, SecureHospitals, ECHO)
    - ECSO WG 3.6 (healthcare) members
    - Various hospitals representatives (IT teams, HC personnel including management)
- PANACEA proposal
- Online survey – coming soon on www.panacearesearch.eu

User Requirements, sources

- Scenario elicitation
  - Attack scenarios
  - Behaviours driven scenarios
  - Regulatory driven scenarios

User Requirements, risk scenarios

- Among the scenarios
  - Social engineering attacks
  - Phishing attacks
  - Ransomware attacks
  - Attacks against critical medical systems
  - Attacks against connected medical devices
  - Attacks against HC IT infrastructure
  - Distributed denial-of-service attacks
  - Loss or theft of equipment
  - Insider, accidental or intentional data loss
  - Lack of security-by-design good practices for medical devices, HC IT infrastructure or critical medical devices
  - Misconfiguration of identification means (including biometrics)

User Requirements, main highlights

- ~200 User Requirements are being collected (actually in refinement) in different areas
  - General
  - Risk Assessment and mitigation
  - Information sharing
  - Security-by-design
  - Identification & Authentication
  - Governance
  - Human factor
  - Value assessment
  - Implementation guidelines

User Requirements, main highlights

- From the elicitation, some main highlights
  - The perception of the importance of cyber-security in HC is increasing, but it is still seen mainly as a technical issue
  - The perception of the importance of the human behavior (of patients and HC personnel) is still limited
  - One of the main worries is the perception of the invasiveness of cyber-security solutions and trainings
  - The cyber-security awareness divide across EU is evident
    - While the technology divide seems less evident
    - Technology excellence does not proceed in parallel with cyber security excellence

User Requirements, main highlights

- From the elicitation, some main highlights
  - In the elicited cases, almost no business impact analysis is performed regularly
    - Lack of updated awareness of the criticality of the processes
    - Lack of awareness of the dependencies between IT infrastructure, human behavior and critical processes (from HC IT teams and HC personnel)
  - Lack of cyber-security training and training curricula is evident
    - We divided the HC personnel in different categories in order to start identifying ad-hoc training curricula
    - It is evident that cyber sec trainings need to be tailored to the HC domain, encompassing all HC personnel (from simple awareness to complex cyber-range exercises)

User Requirements, main highlights

- From the elicitation, some main highlights
  - Security-by-design for HC systems and medical devices is listed as a priority by HC IT teams or HC personnel
    - But in practice, there is not much investment or QA
    - It is evident a lack of basic awareness and training
    - The impact of IoT is not clearly understood or perceived
    - Need for a EU-wide certification scheme for medical devices is perceived

User Requirements, main highlights

- From the elicitation, some main highlights
  - Identification and authorization are perceived topics (in particular by the HC IT teams), in particular for what regards physical security
    - Need for lightweight and simple identification mechanisms is evident, because rules are usually broken
    - M2M and H2M identification and authorization are not perceived as a major issue
  - From both HC IT Teams and HC personnel, it has been highlighted the need of tailored governance schemes for HC organizations
    - Existing governance frameworks does not seem to be perfectly applicable in the HC sector
    - The perception of a disconnection between cyber-security needs and its necessary procedures and the HC organization is evident
    - The need of a specific separate process for managing cyber security governance has been raised
    - The perception of the value and ROI of cyber-security is not clear

PANACEA Solution Toolkit

- The **Solution Toolkit** comprises
  - **four technical tools** for

    I-dynamic risk assessment & mitigation,

    II-secure information sharing,

    III-security-by-design & certification,

    IV-identification & authentication
  - **three organisational tools** for

    V-training & education,

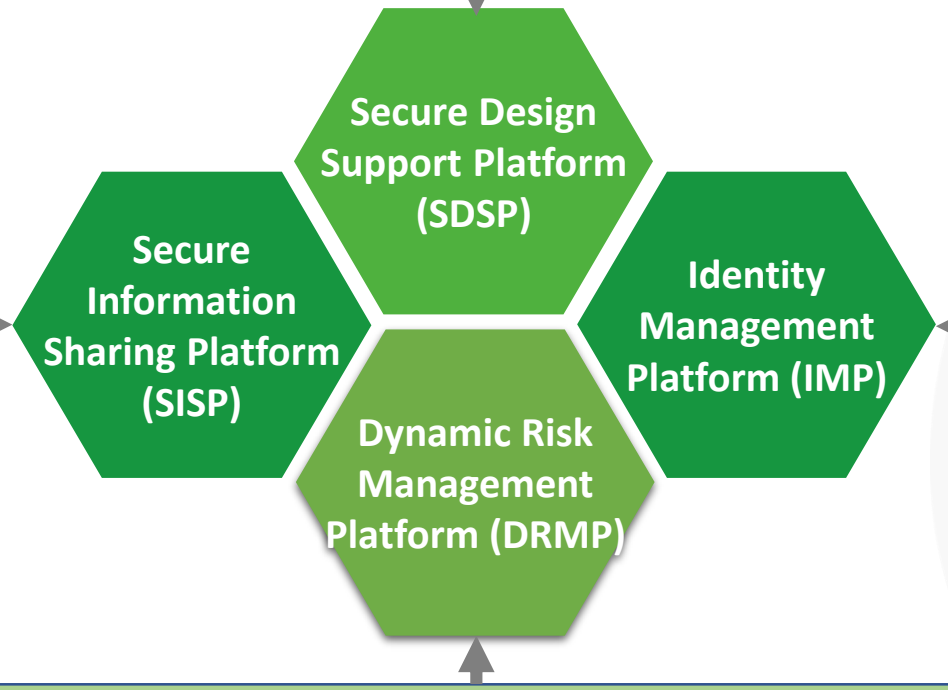
    VI-resilience governance,

    VII-secure behaviours nudging

Solution Toolkit *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

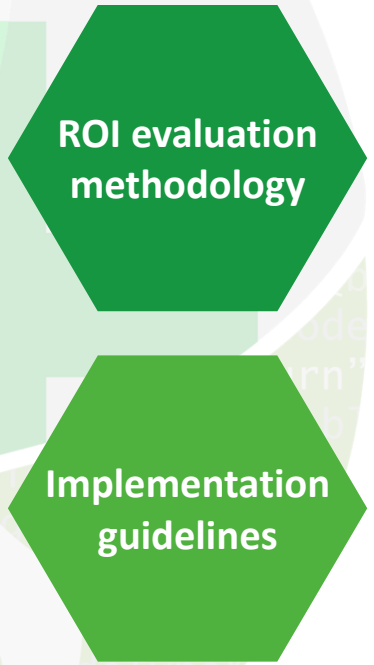
Multidimensional threat modelling, dynamic risk assessment with business impact dynamic computation, technical and organisational response for complex infrastructure

Solution Toolkit *Organizational tools*

- **Training and education for cybersecurity**: organized **activity and packages** aimed at imparting information and/or instructions to help the recipient to **attain a required level of knowledge or skill** with regard to appropriate **secure behaviours, targeted on HCOs**
- **Resilience governance:** set of organizational arrangements (**roles, responsibilities, policies, plans, procedures**) ensuring the capability to **identify** cyber risk, **prevent** and **detect** cyber-attacks, **recover** after a cyber-attack, **tailored on HCOs**
- **Secure behaviour nudging**: set of **interventions, in addition to the training**, aimed at influencing the behaviours of the **HCO staff and patients and other staff involved in the medical device lifecycle**

Delivery Toolkit

- The **Delivery Toolkit**, will specifically **support the adoption of the solution toolkit or similar cybersecurity solutions**. It includes **two tools.**
  - **ROI evaluation methodology:** a **structured process** for evaluating the return of investing in cybersecurity solutions (such as the PANACEA toolkit or parts of it). Its purpose is **to support the HCO decision makers** in taking the investment decision. It considers both **economic and non-economic returns**.
  - **Implementation guidelines:** consist in **procedures, check-lists, methods, project organization models** do be used during the adoption process. Their purpose is to **ensure that the solution fits with the needs and the context of the HCO, are implemented effectively and efficiently, produce the expected results**.



Panacea
People-centric cybersecurity in healthcare

Thank you for your attention! *Questions?*

Website: www.panacearesearch.eu

Contacts:

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