ANASTACIA has received funding from the European Union's **Horizon 2020 Research and Innovation Programme** under Grant Agreement N° 731558 and from the Swiss State Secretariat for Education, Research and Innovation.

ANASTACIA

Advanced Networked Agents for Security and Trust Assessment in CPS/IoT Architectures

IoT privacy risk management in ANASTACIA project

Stefano Bianchi
Softeco Sismat – ANASTACIA Project Coordinator

IoTWeek 2017
IoT Risk Management

ANASTACIA has received funding from the European Union's **Horizon 2020 Research and Innovation Programme** under Grant Agreement N° 731558 and from the Swiss State Secretariat for Education, Research and Innovation.

ANASTACIA

Advanced Networked Agents for Security and Trust Assessment in CPS/IoT Architectures

TYPE:	Research & Innovation Action
CALL:	H2020-DS-LEIT-2016
TOPIC:	DS-01-2016 Assurance and Certification for Trustworthy and Secure ICT systems, services and components
DURATION:	36 MONTHS (Jan 2017 → Dec 2019)
COSTS:	€ 5,420,208.75
FUNDING:	€ 3,999,208.75
G.A.:	731558

Rationale

- The heterogeneous, distributed, and dynamically evolving nature of Cyber Physical Systems (CPS) based on Internet of Things (IoT) and virtualised cloud architectures introduces new and unexpected risks that cannot be solved by current state-of-the-art security solutions.
- ANASTACIA will deliver paradigms and methods that
  - build security into the system at the outset;
  - adapt to changing conditions;
  - reduce the need of finding flaws and repairing them when the system is already deployed;
  - provide the assurance that ICT systems are secure and trustworthy at all times.

Mission

- To develop a trustworthy-by-design autonomic security framework which will address all the phases of the ICT Systems Development Lifecycle (SDL) and will be able to take autonomous decisions through the use of new networking technologies such as Software Defined Networking (SDN) and Network Function Virtualisation (NFV) and intelligent and dynamic security enforcement and monitoring methodologies and tools

- holistic solution enabling trust and security by-design for Cyber Physical Systems (CPS) based on IoT and cloud architectures

The ANASTACIA framework includes

1

Security development paradigm

based on the compliance to security best practices and the use of the security components and enablers (this will provide assisted security design, development and deployment cycles to assure security-by-design)

2

Distributed trust and security components and enablers

able to dynamically orchestrate and deploy user security policies and actions within complex and dynamic CPS and IoT architectures (online monitoring and testing techniques will allow more automated adaptation of the system to mitigate new and unexpected security vulnerabilities)

3

Holistic Dynamic Security and Privacy Seal (DSPS)

combining security and privacy standards and real time monitoring and online testing (this will provide quantitative and qualitative run-time evaluation of privacy risks and security levels, which can be easily understood and controlled by the final users)

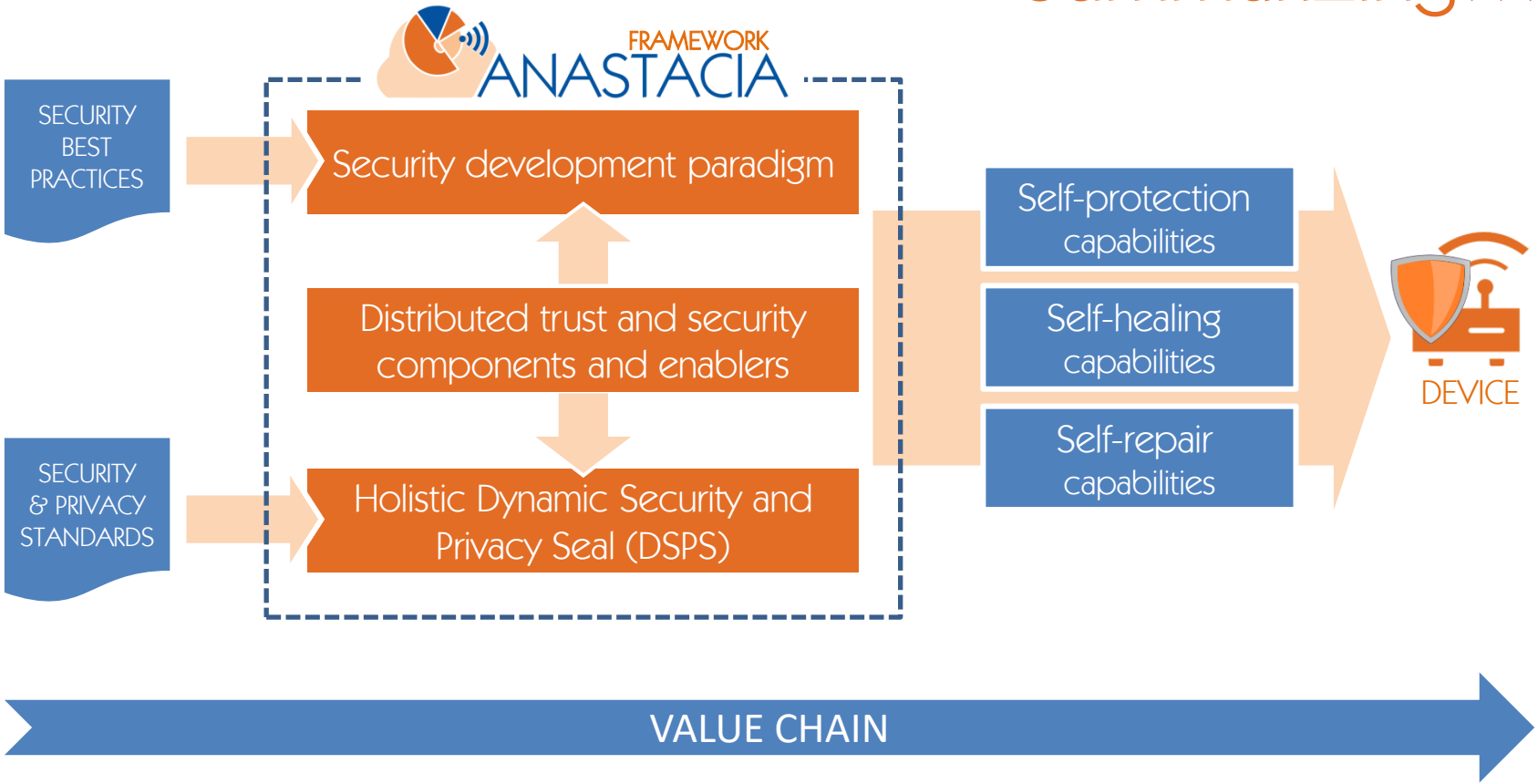
The ANASTACIA framework provides

1. Self-protection capabilities
2. Self-healing capabilities
3. Self-repair capabilities

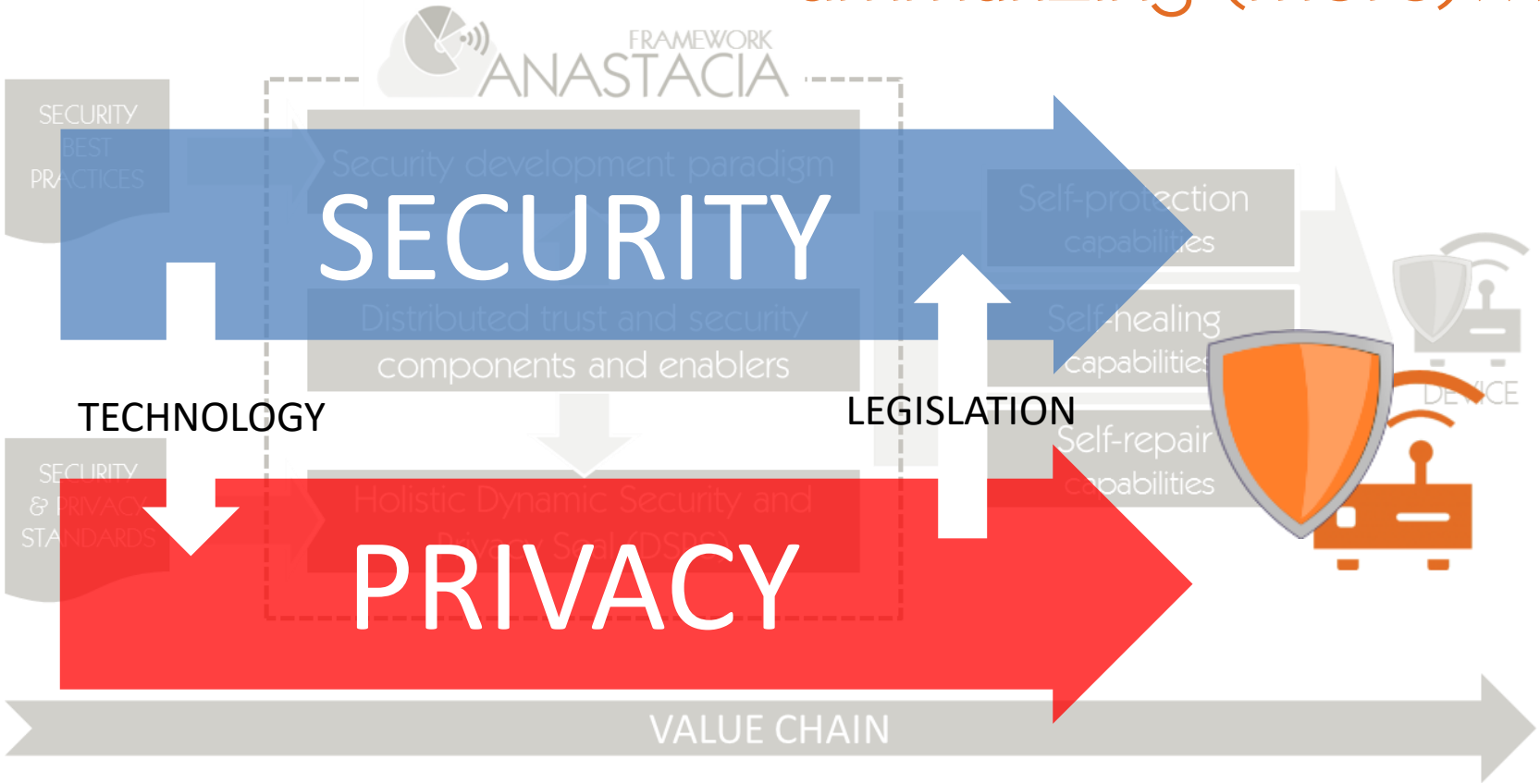
ANASTACIA's sub-objectives

1. To provide the end users with intuitive and user-friendly tools and solutions to model and configure policies governing the configuration of the security in decentralized and virtualized architectures.
2. To leverage cloud and SDN/NFV functionalities to allow easy deployment and provide security solution for highly connected CPS/IoT; and, more generally, smart objects communications.
3. To develop a dynamic Security Enforcement Manager, based on Monitoring and Reaction components, using beyond state-of-the-art vulnerability analysis and security monitoring techniques.
4. To develop a Dynamic Security and Privacy Seal (DSPS) combining normative requirements (GDPR, ISO standards, etc.) with monitoring functionalities to provide real-time indication on the trustability of a deployed system.
5. Validation and evaluation of the overall approach in two realistic industrial case studies with high societal and economic impact.
6. To maintain a strong link to relevant standards and standard bodies.

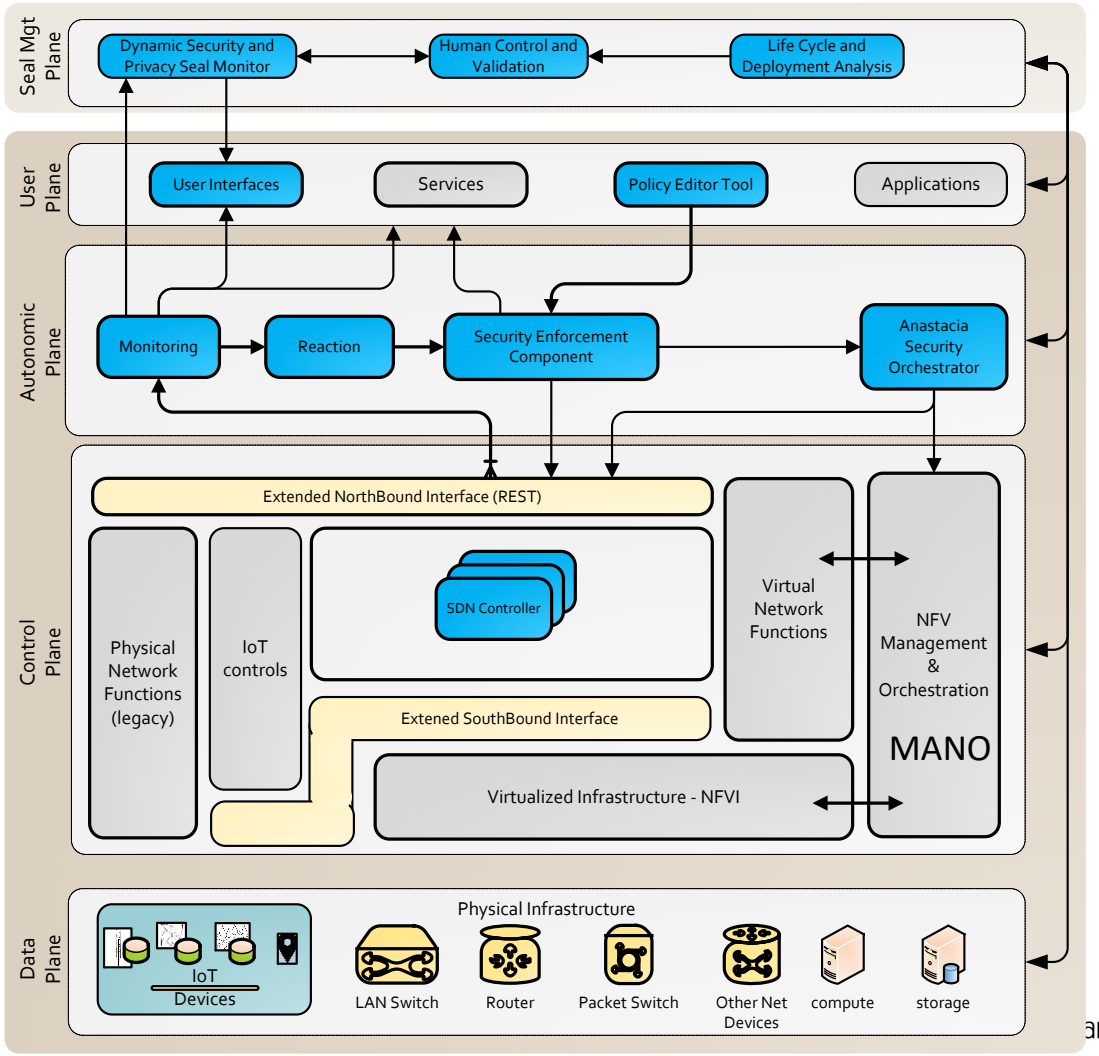
Summarizing…



Summarizing (more)…

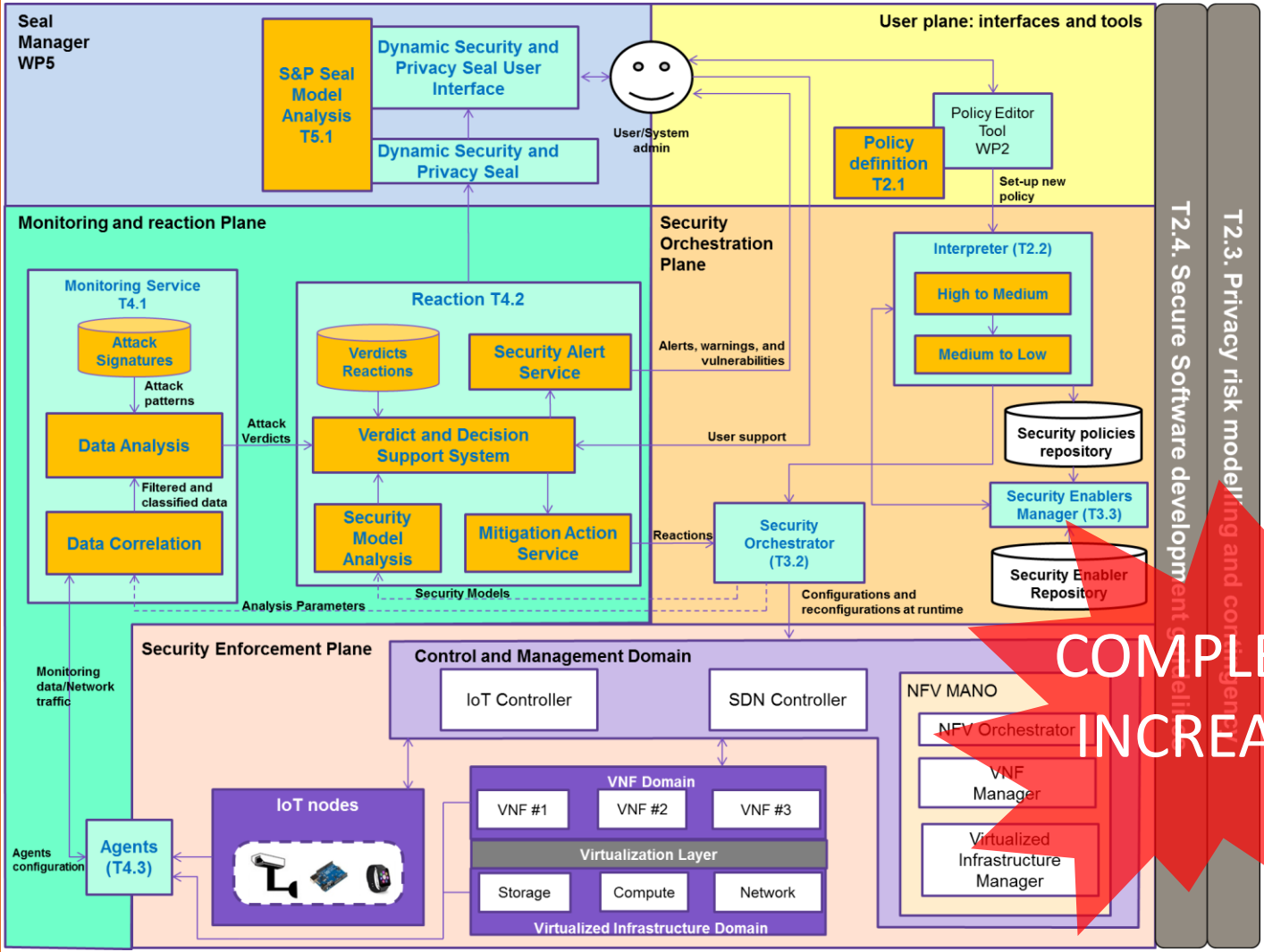


ANASTACIA framework architecture

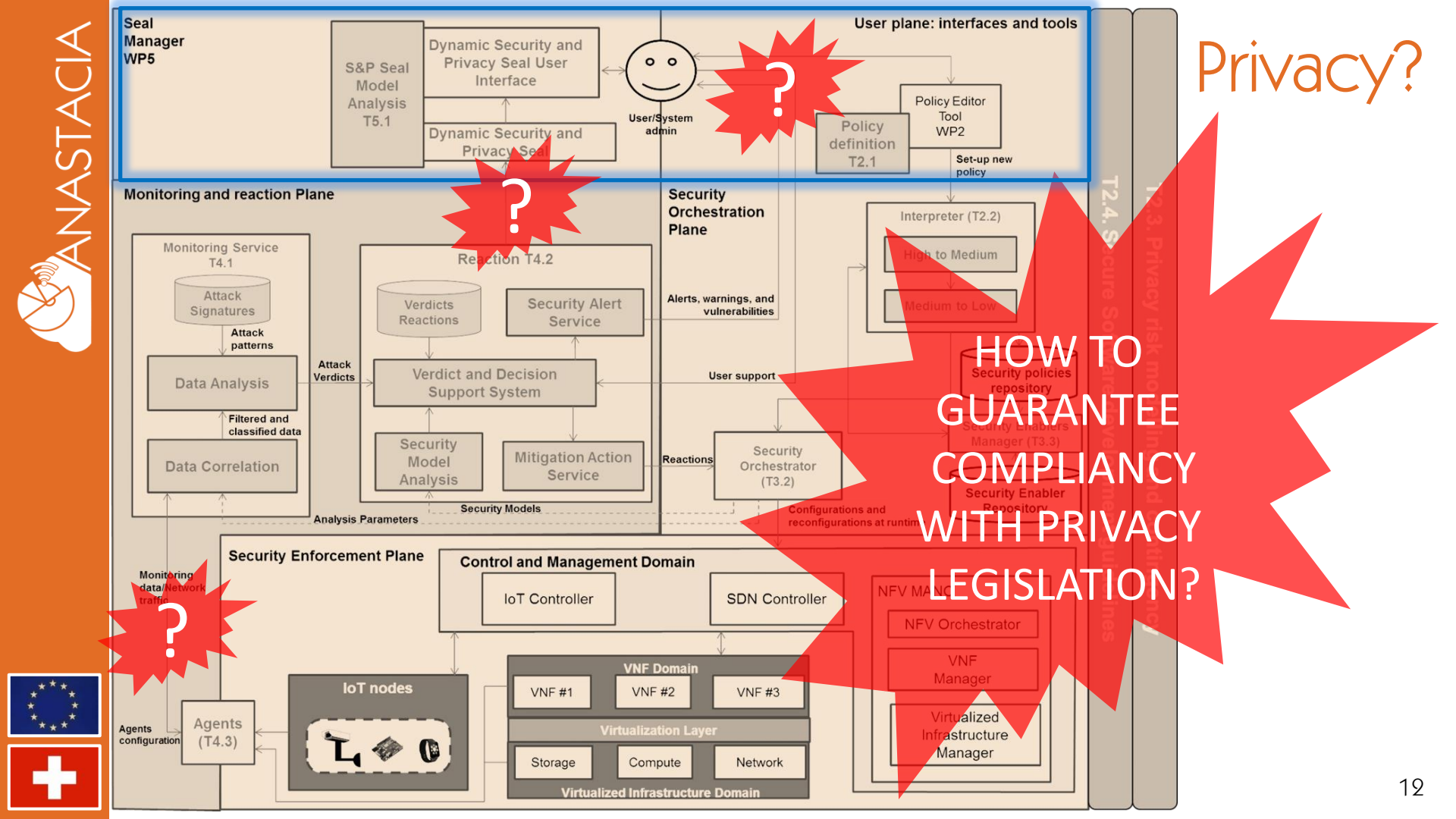


PLANES

ANASTACIA framework architecture



COMPLEXITY INCREASED


Seal Manager WP5
S&P Seal Model Analysis T5.1
Dynamic Security and Privacy Seal User Interface
Dynamic Security and Privacy Seal
User/System admin
User plane: interfaces and tools
Policy Editor Tool WP2
Policy definition T2.1
Set-up new policy
Monitoring and reaction Plane
Security Orchestration Plane
Monitoring Service T4.1
Attack Signatures
Attack patterns
Data Analysis
Filtered and classified data
Data Correlation
Reaction T4.2
Verdicts Reactions
Security Alert Service
Attack Verdicts
Verdict and Decision Support System
Security Model Analysis
Mitigation Action Service
Analysis Parameters
Security Models
Alerts, warnings, and vulnerabilities
Interpreter (T2.2)
High to Medium
Medium to Low
User support
Security policies repository
Security Enablers Manager (T3.3)
Security Orchestrator (T3.2)
Reactions
Security Enabler Repository
Configurations and reconfigurations at runtime
Security Enforcement Plane
Control and Management Domain
IoT Controller
SDN Controller
NFV MANO
NFV Orchestrator
VNF Manager
Virtualized Infrastructure Manager
Monitoring data/Network traffic
IoT nodes
Agents configuration
Agents (T4.3)
VNF Domain
VNF #1
VNF #2
VNF #3
Virtualization Layer
Storage
Compute
Network
Virtualized Infrastructure Domain
T2.4. Secure Software Management
T2.3. Privacy risk monitoring and mitigation
HOW TO GUARANTEE COMPLIANCY WITH PRIVACY LEGISLATION?

Privacy?

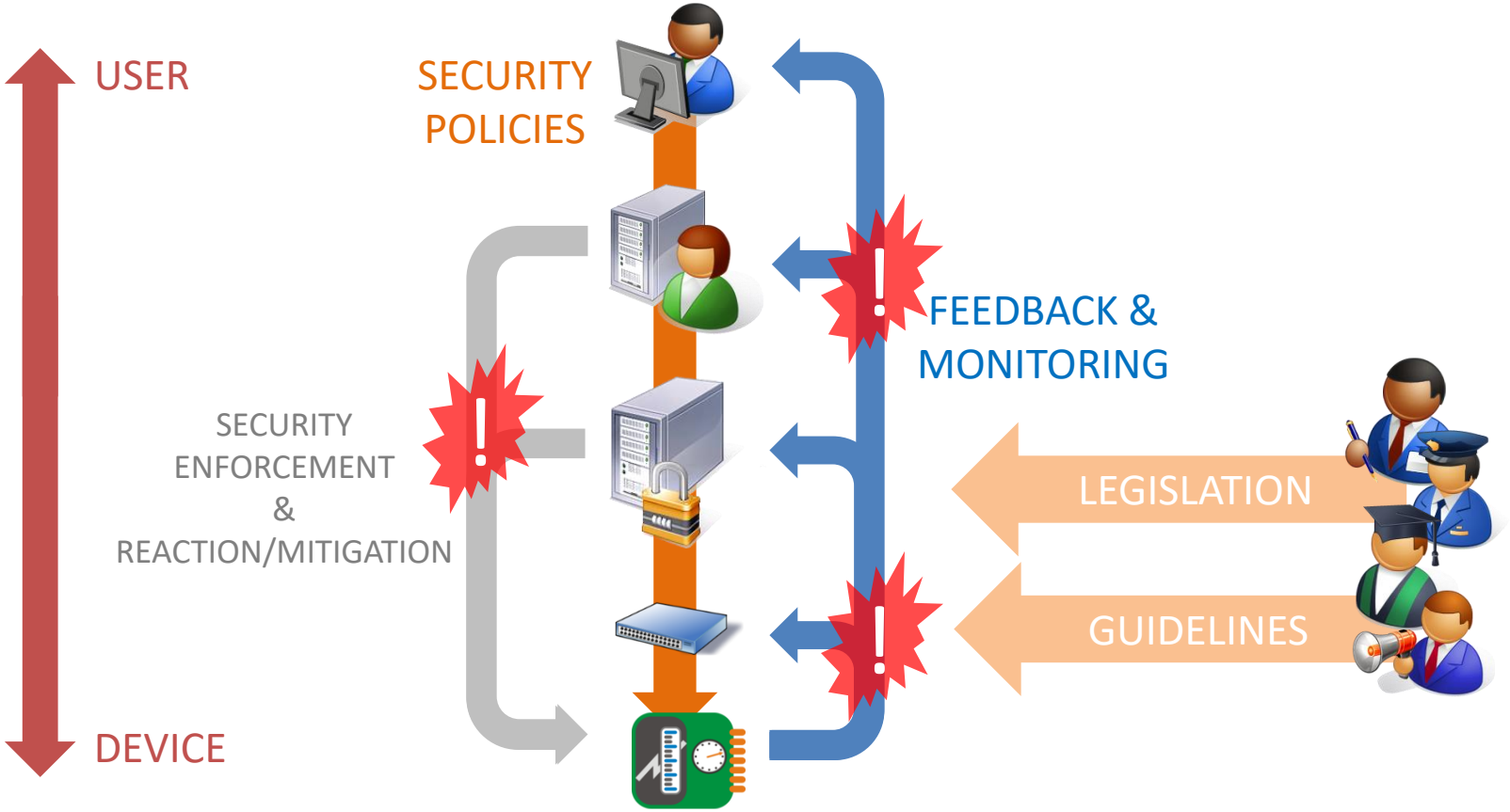
Holistic approach combining security and privacy

- ANASTACIA will endow end users and security experts with intuitive and user-friendly tools, models, guidelines and solutions to manage security, privacy and risk in decentralized and virtualized architectures.
- ANASTACIA will provide a set of novel security and trust by design enablers tailored to cope with heterogeneous and holistic scenarios that may combine SDN-NFVs and IoT, implementing:
  - policy based security management models
  - threat analysis and contingency mechanisms
  - privacy risk modelling
  - secure software development guidelines
- The privacy risk analysis and modelling will identify measurement points as well as contingency measures to mitigate the risk.

DYNAMIC SECURITY AND PRIVACY SEAL (DSPS)

- Instantaneous view and understanding on the trust level of the system, combining real-time dynamic security and privacy monitoring with conventional certification schemes applying ISO certification models, plus normative requirements from General Data Protection Regulation (GDPR) and ISO standards
- The first ICT-based seal addressing GDPR
- New models of secured certificate registry will be also researched in order to prevent the risk of counterfeiting

ANASTACIA's challenge on privacy-compliant security



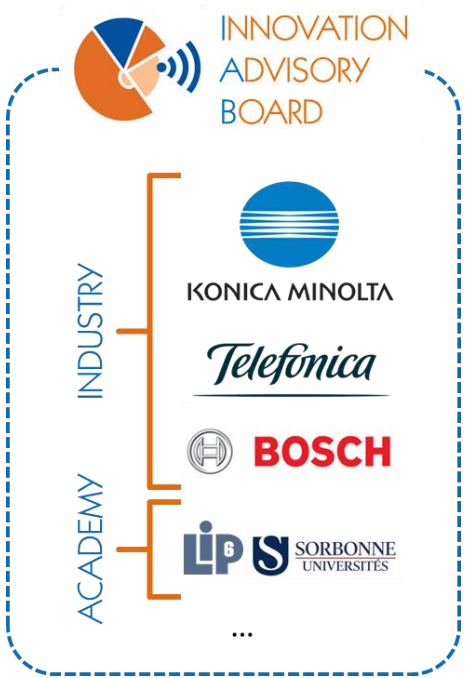
Use Cases

- Mobile Edge Computing applications
  - **Test Case**: MEC on video cameras
  - **Scenario**: Spoofing attack on the security camera system

- Smart Building Management Systems applications
  - **Test Case**: Resilient cyber-physical systems in smart buildings
  - **Scenario**: Cyber-attack at a hospital building

Innovation Advisory Board (IAB)

To support the Consortium in the identification and implementation of the strategy to maximize the impact of results, overviewing and aligning the released outcomes with the industry's and standardization bodies' requirements



IAB members

KONICA MINOLTA

Christian Mastrodonato
Chief Technologist
Konica Minolta Inc

https://www.linkedin.com/in/cmastrodonato/

Telefónica

Diego R. Lopez
Senior Technology Expert
Telefonica I+D

https://es.linkedin.com/in/dr2lopez

BOSCH

Jesus Luna
Security Architect
Robert Bosch Inc

https://www.linkedin.com/in/jlunagar/

LIP6 SORBONNE UNIVERSITÉS

Stefano Secci
Associate Professor
Pierre and Marie Curie University (UPMC)
Paris VI - LIP6
https://www.linkedin.com/in/stefanosecci/

Contacts

- **Project Coordinator**

  Stefano BIANCHI (Softeco Sismat)

  stefano.bianchi@softeco.it

- **Scientific and Technical Project Manager**

  Antonio SKARMETA (Universidad de Murcia)

  skarmeta@umu.es

ANASTACIA has received funding from the European Union's **Horizon 2020 Research and Innovation Programme** under Grant Agreement N° 731558 and from the Swiss State Secretariat for Education, Research and Innovation.

ANASTACIA

Advanced Networked Agents for Security and Trust Assessment in CPS/IoT Architectures

www.anastacia-h2020.eu

http://youtube.anastacia-h2020.eu

http://twitter.anastacia-h2020.eu

http://linkedin.anastacia-h2020.eu

http://www.anastacia-h2020.eu

http://youtube.anastacia-h2020.eu

http://twitter.anastacia-h2020.eu

http://linkedin.anastacia-h2020.eu

ANASTACIA

ANASTACIA

softeco sismat information technology

THALES

Atos

ERICSSON

United Technologies Research Center

UBITECH ubiquitous solutions

montimage

MANDAT INTERNATIONAL

OdinS

UDG UNIVERSAL DEVICE GATEWAY

Consiglio Nazionale delle Ricerche

Aalto University

UNIVERSIDAD DE MURCIA

ANASTACIA has received funding from the European Union's
Horizon 2020 Research and Innovation Programme under Grant Agreement N° 731558
and from the Swiss State Secretariat for Education, Research and Innovation.