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 **N**etworked **A**gents for **S**ecurity and **T**rust **A**ssessment in **C**PS/**I**oT **A**rchitectures

Project Overview

Giannis Ledakis
UBITECH

SAINT workshop 20/03/2018

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**

ANASTACIA

softeco sismat information technology

THALES

Atos

ERICSSON

United Technologies Research Center

UBITECH ubiquitous solutions

montimage

MANDAT INTERNATIONAL

Odin S

UDG

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.

IoT Networks

- "Internet of Things"
  - Ubiquitous (it is present everywhere)
  - Highly distributed
  - Brings logic to any "thing"
- These features allow to integrate every day objects with embedded systems
  - This allows controlling new types of systems

IoT Challenges

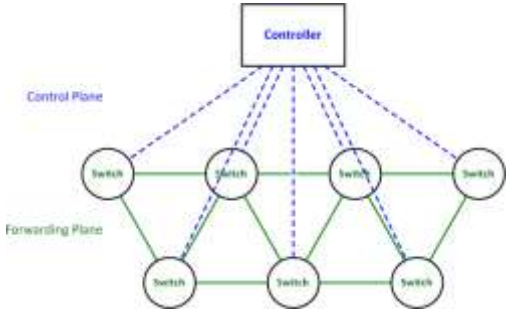
- Complexity of operation
  - Highly distributed systems are hard to operate
- Security issues
  - Critical systems handled by IoT require security enforcement
- Dynamic adaptability
  - IoT networks have to dynamically adapt to dynamic envirnoments

The big picture so far

IoT Platforms

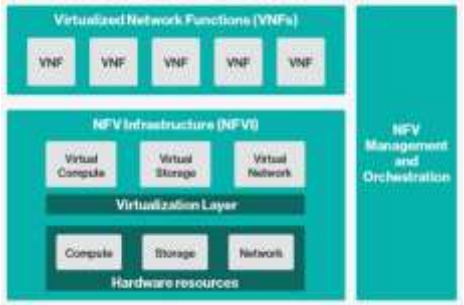
- Ubiquitous
- Capable of monitoring wide areas

SDN Technologies



- Network flows organization
- Centralized flow management

NFV Techniques



- Topology flexibility
- Adapt the network elements to new requirements

Challenges

- SDN and NFV complement each other
  - But there is not an standard way
- IoT networks can enhance the Quality of Life and are gaining popularity
  - But security issues are still an open research and innovation field
- Moreover, the dynamic nature of IoT-based CPS networks makes security enforcement a challenge
  - A dynamic security enforcement approach is required.

ANASTACIA Project Mission

- 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.

- Combine the SDN and NFV techniques for IoT networks
- The goal is generate both:
  - A self-reacting security platform
  - Secure-by-design development methodologies

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

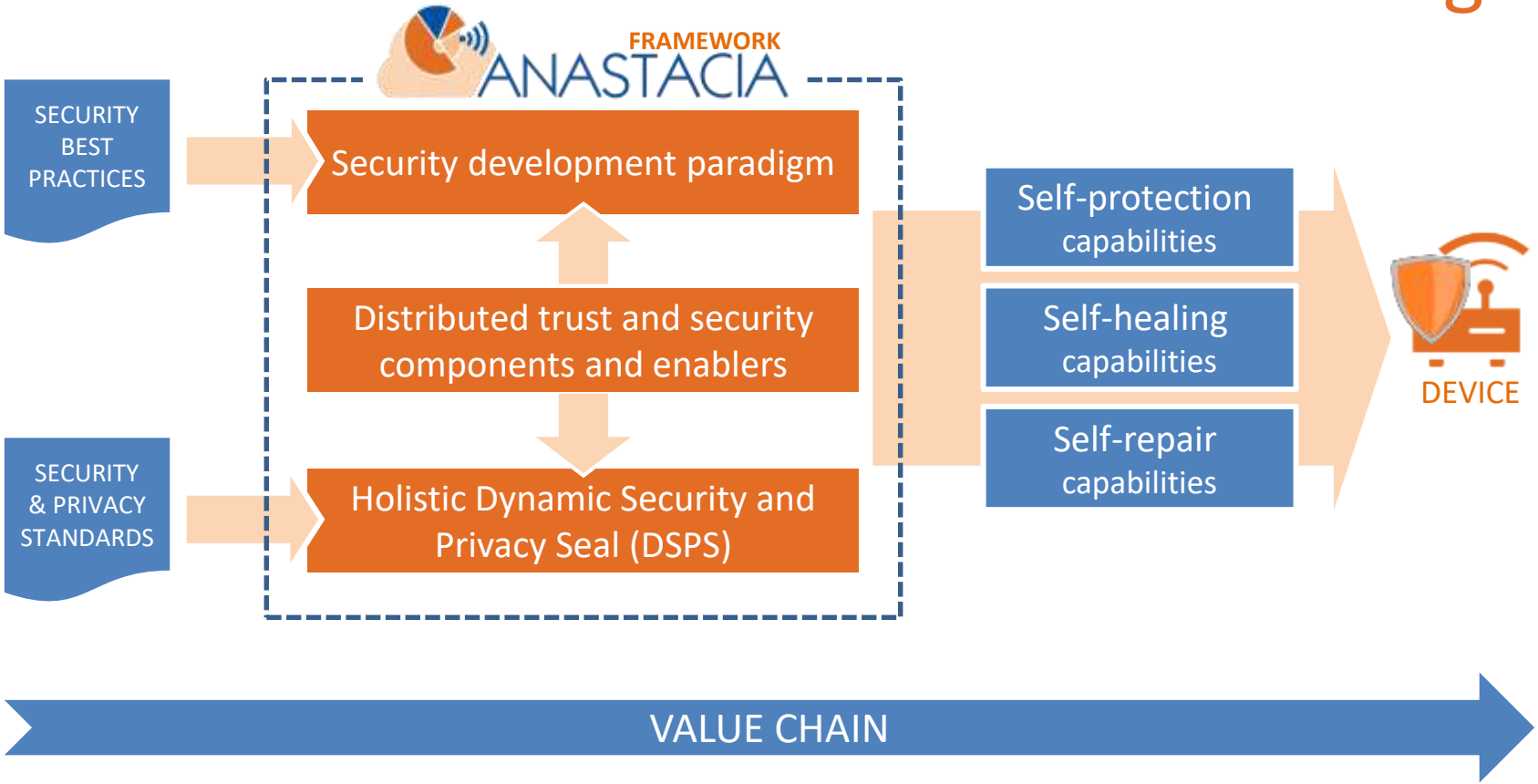
Holistic Dynamic Security and Privacy Seal (DSPS)

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)

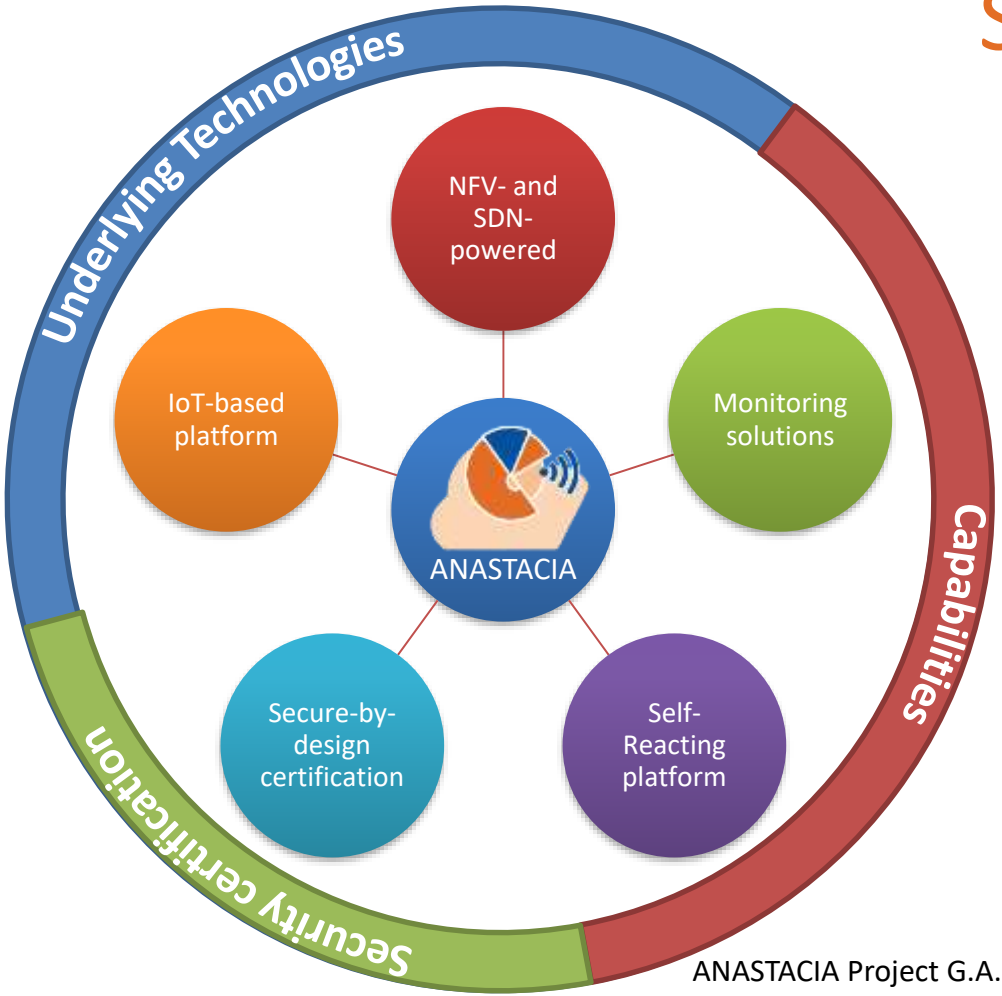
ANASTACIA's sub-objectives

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.

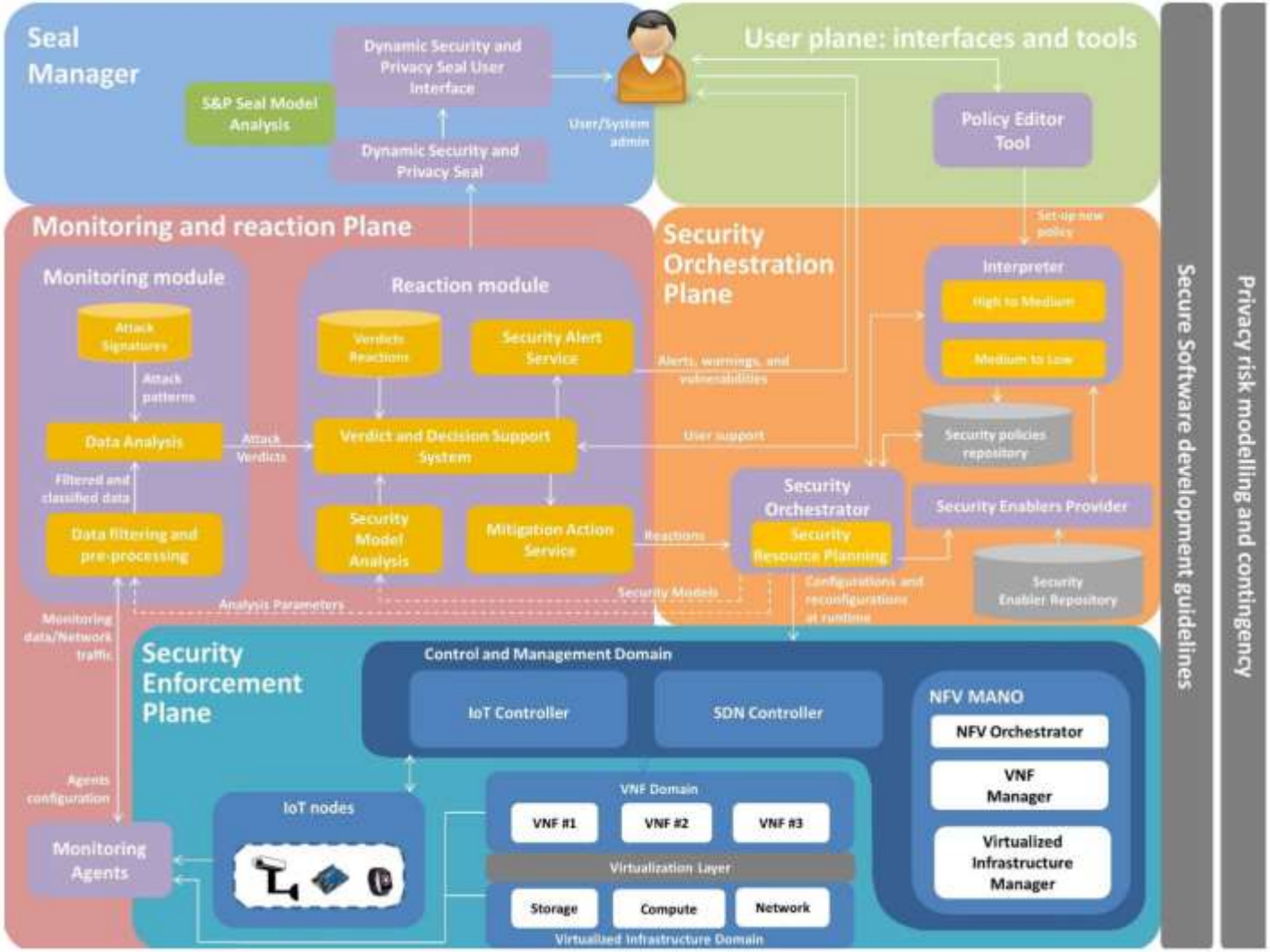
Summarizing…



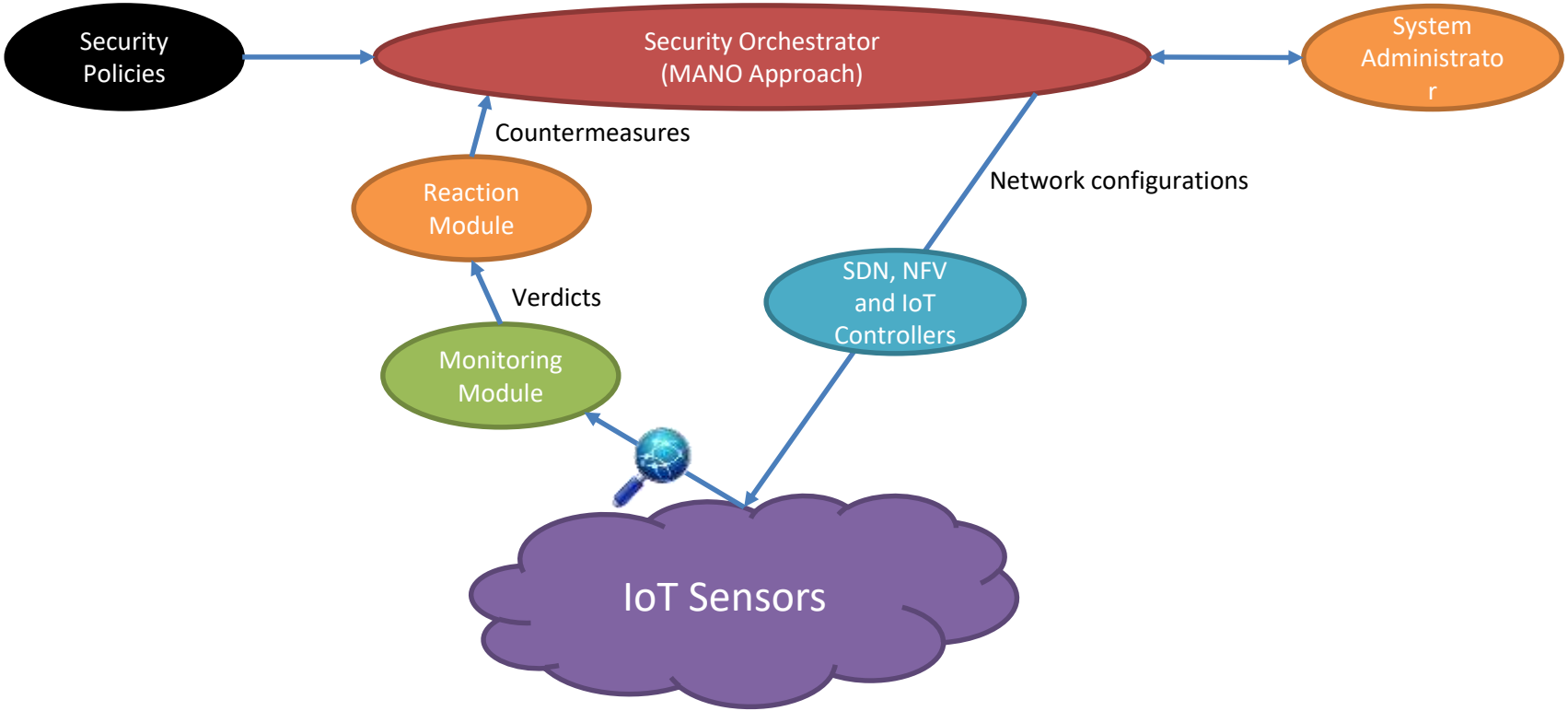
Summary


Underlying Technologies
Capabilities
Security certification
NFV- and SDN-powered
IoT-based platform
Monitoring solutions
ANASTACIA
Secure-by-design certification
Self-Reacting platform

ANASTACIA framework architecture



ANASTACIA Workflow



ANASTACIA Workflow

In Anastacia the security is driven and managed by security policies

• High-level Security Policy Language (HSPL) and the Medium-level Security Policy Language (MSPL)

– HSPL: The policy language suitable for expressing the general protection requirements of typical non-technical end-users.

– MSPL: Expreses specific configurations by technically-savvy users in a device-independent format.

➢ Supported Policies

– Authentication
– Authorization
– Filtering/Forwarding
– Channel Protection (e.g. IpSec)
– General Security

➢ Current Plugins Approaches

– Anonymity
– Antiphising
– Brologging
– Bromalware
– Dansguardian
– IPTables
– ReconduceBandwidth
– Reencryption
– Squid
– Strongswan

ANASTACIA Workflow

To enforce these security properties, ANASTACIA's Security Orchestrator component translates policies and interacts with:

- SDN controllers
- NFV MANO stack modules,
- IoT controllers

➢ Virtual Security Functions

– vFirewall (e.g. netfilter Linux iptables)
- Filtering rules

– vRouter (e.g. OpenVirtualSwitch in OpenWRT)
- Traffic forwarding, traffic mirroring, traffic diversion …

– vChannelProtection
- Level3 encryption IPSec, SSL e.g. openVPN, DTLs

– vIDS (Intrusion Detection System, e.g. Snort)

Current Status

Consortium is working for the implementation of a full cycle of the ANASTACIA workflow.

- Monitoring Data are collected
- Reactions are created
- Many security plugins already available

Security Plugins of ANASTACIA	
CoojaPlugin	ODLPlugin
IoTControllerPlugin	OnosPlugin
IoTControllerPlugin	OvsFwPlugin
KippoPlugin	PFSensePlugin
LimitBwPlugin	QuaggaPlugin
m2l_plugins (authorization)	SnortPlugin

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

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