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

Dynamic Cybersecurity for IoT/CPS based Environments

Antonio Skarmeta

Universidad de Murcia (Spain)

ANASTACIA

ANASTACIA

SOFTECO
SIMPLY YOUR TECH SOLUTIONS

THALES

Atos

ERICSSON

United Technologies Research Center

UBITECH
ubiquitous solutions

montimage

MANDAT INTERNATIONAL

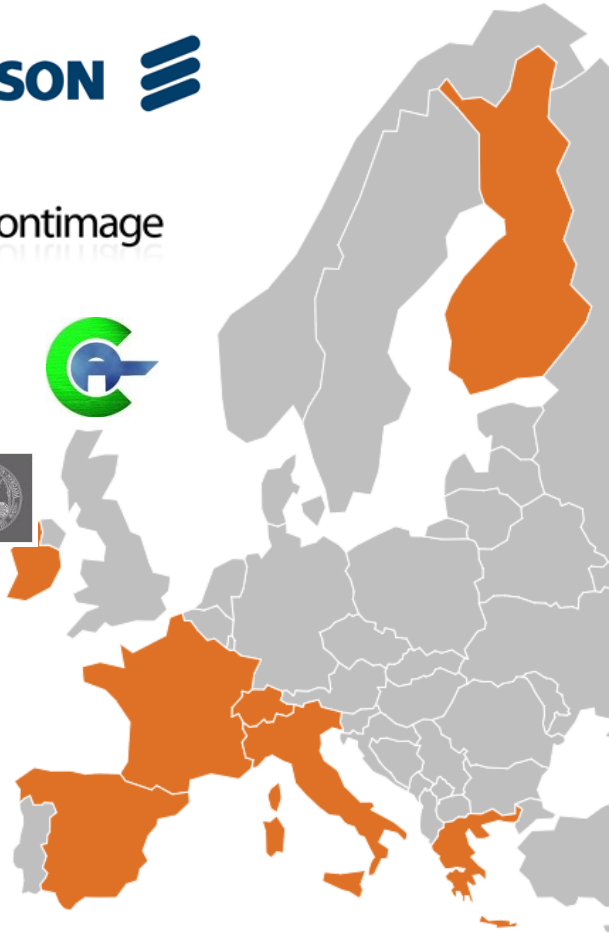
OdinS

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.

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)

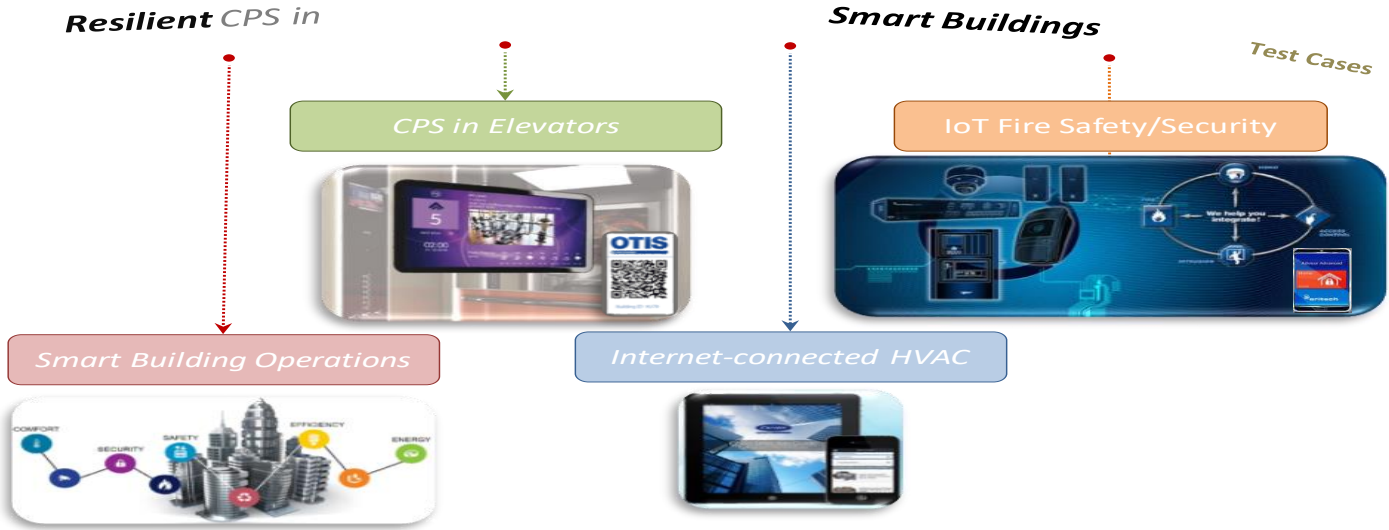
Attacking IoT

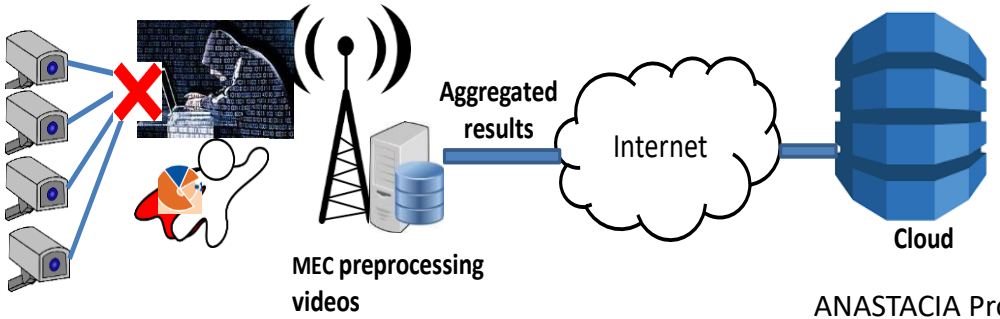
- Default, weak, and hardcoded credentials
- Difficult to update firmware and OS
- Lack of vendor support for repairing vulnerabilities
- Vulnerable web interfaces (SQL injection, XSS)
- Coding errors (buffer overflow)
- Clear text protocols and unnecessary open ports
- DoS / DDoS
- Physical theft and tampering

Why ANASTACIA is needed

- Cyber-attacks on IoT are getting more and more widespread because of:
  - Dynamically evolving nature of systems
  - Increased internet-connectivity of equipment's
  - Constrained capabilities of IoT systems, misconfigurations, absence of software updates…
  - Lack of interoperability of devices deployed on **distributed smart IoT deployments**.
- Thereby, new types of attacks and 0-day vulnerabilities, such as Slow DoS Attacks (SDA) are emerging and evolving
- However, current network security solutions monitoring, management and reaction systems/tools present low responsiveness and can unlikely cope with the dynamic IoT environments
  - Besides, the deployment and management of NSFs (Network Security Functions) to mitigate cyber-attacks have not yet properly studied and exploited in NFV/SDN-enabled IoT networks.
- All these security vectors claim for new **context-aware security frameworks to allow orchestrating NFV managers, SDN controllers and IoT controllers across IoT domains**, thereby providing security chaining, as well as dynamic reconfiguration and adaptation of the virtual security appliances according to monitoring and reaction mechanisms.

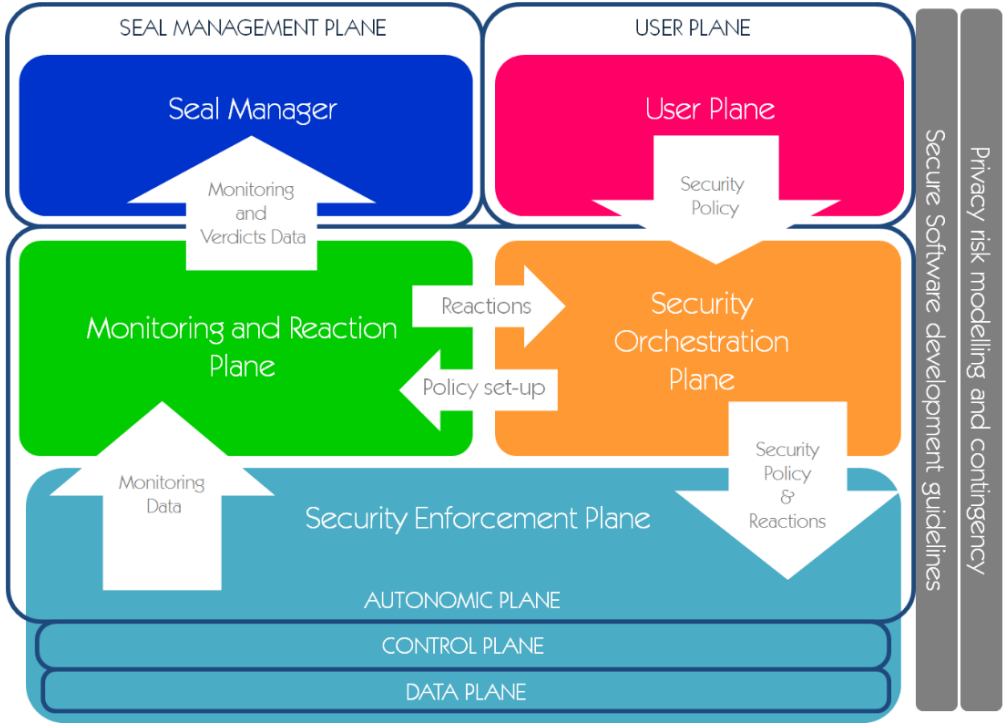
Scenario and Use Cases





ANASTACIA's Approach

- To cope with those challenges Anastacia is designing, implementing and evaluating a holistic and dynamic SDN/NFV-based Security framework for IoT



ANASTACIA's main Key Innovations (KI)

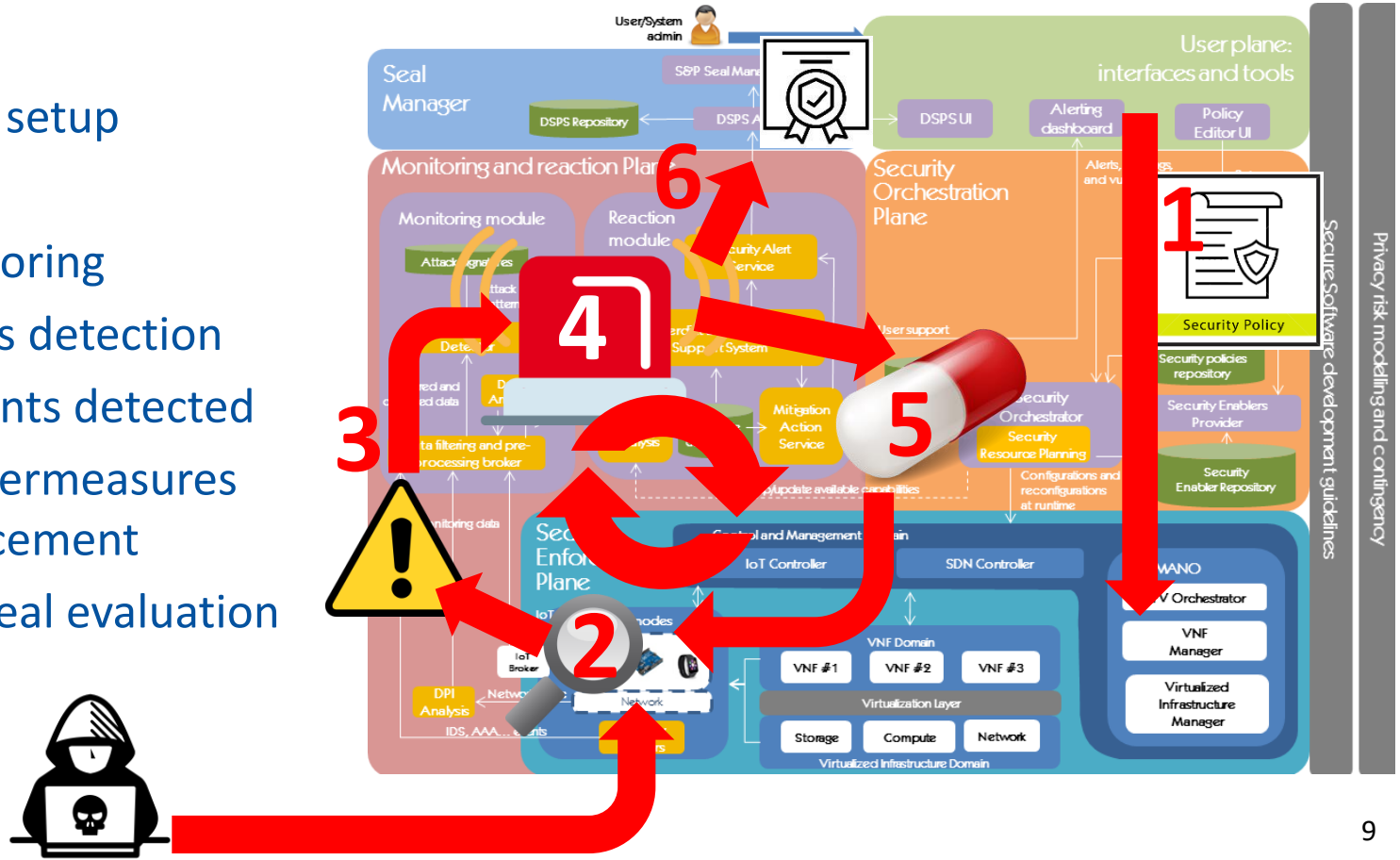
1. Holistic policy-based security management and orchestration in IoT
2. Investigation on innovative cyber-threats
3. Trusted Security orchestration in SDN/NFV-enabled IoT scenarios
4. Dynamic orchestration of resources planning in Security-oriented SDN and NFV synergies
5. Security monitoring to threat detection in SDN/NFV-enabled IoT deployments
6. Cyber threats automated and cognitive reaction and mitigation components
7. Behaviour analysis, anomaly detection and automated testing for the detection of known and unknown vulnerabilities in both physical and virtual environments
8. Secured and Authenticated Dynamic Seal System as a Service

ANASTACIA architecture

1. Policy setup

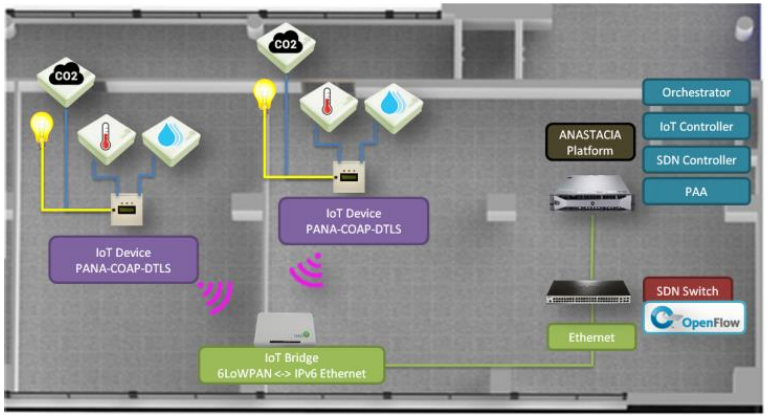
Attack

2. Monitoring
3. Probes detection
4. Incidents detected
5. Countermeasures enforcement
6. S&P Seal evaluation



BMS area

- **BMS Cascade Attack on a Megatall Building (Man in the middle attack – temperature sensor change)**
  - **OBJECTIVE:** protecting the system from a remote manipulation for sensitive sensor data.
  - **THREAT:** a hacker plans to gain control over critical temperature sensor to falsificate high values and hence triggering the evacuation alarms.
  - **DETECTION:** data monitoring, machine learning models and data analysis to detect anomaly behavior of temperature value.
  - **MITIGATION**: Security orchestrator requests to the SDN controller and IoT controller to stop the malicious data traffic.
- **OpenFlow SDN switches**
- **Distributed architecture of access control**
- **PANA network authentication**
- **IoT Broker server**
- **Wireless IoT/CPS devices**
  - Sensors of Temp and Hum.
  - Actuators of Fire Alarm



Conclusion

- ANASTACIA addresses the security management of distributed IoT scenarios, such as Smart Buildings or Smart Cities, that can benefit from policy-based orchestration and management approach, NFV/SDN-based solutions and novel monitoring and reaction tools to cope with new kind of cyber-attacks
- Security VNFs can be timely and dynamically orchestrated through policies to deal with heterogeneity demanded by these distributed IoT deployments, than can be deployed either at the core of at the edge, in VNF entities, in order to rule the security in IoT networks
- Dynamic and reactive provisioning of Security VNFs towards the edge of the network can enhance scalability, necessary to deal with IoT scenarios
- Dealing with this general problem statement and use case raises several research challenges, being faced in ANASTACIA

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