SAFECARE Outcomes: Scientific Point of View

3S Clustering Event

Eva Maia, ISEP

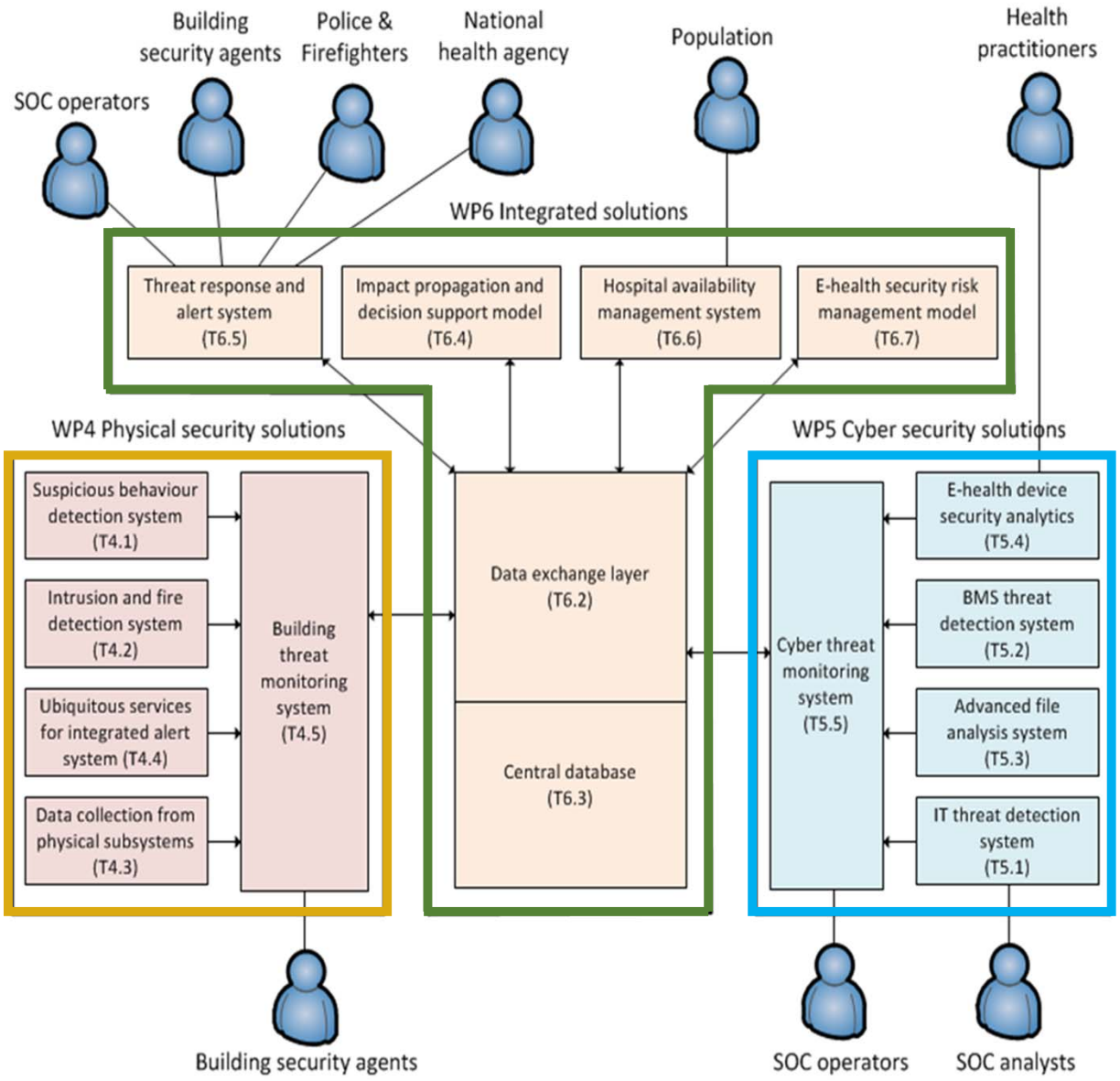
SAFECARE has received funding as part of the "Secure societies – Protecting freedom and security of Europe and its citizens" challenge of the Horizon 2020 Research and Innovation programme of the European Union under grant agreement 787002

SAFECARE Architecture

Three different modules:

- **physical** security solutions,
- **cyber** security solutions and
- **integrated** solutions

that allow the combination of cyber and physical systems



SAFECARE Innovation Elements

13 Innovation Elements

3 Domains

Physical Security

Cyber Security

Cyber-physical Security

2 Capabilities

Detection

Alert & Prevention
& Response

SAFECARE Innovation Elements

Suspicious behaviour detection system to improve physical security

captures video streams from surveillance cameras, and with a near real-time analysis triggers security alerts in case of crowding, loitering or other suspicious activities

Intrusion and fire detection system to improve physical security

correlated video monitoring system with existing access management and fire detection systems to notably extend threat detection capacities and reduce number of false positive incidents

- improve pattern detection techniques
- process a huge quantity of data in near-real time.
- hardware and software architecture optimization

SAFECARE Innovation Elements

Mobile services for increased awareness of the building security agent

informs key personnel of a suspicious activity in the hospital assuring the interoperability with the project ecosystem and the encompassing approach to physical threats, cyber threats and related impacts

A building monitoring system with an enlarged view about the combination of cyber-physical threats and impact assessment

centralize security events from the suspicious behaviour detection system, intrusion and fire detection system, access management system, air cooling system, power supply system

- Improvement of reaction times
- Enrichment of the communication infrastructure in case of physical threats
- Complete integrated and automated system

SAFECARE Innovation Elements

An IT oriented threat detection system and analytics tools to improve cyber threat investigation

network traffic near-real time analysis in order to detect suspicious behaviour and scale up security events to the cyber threat monitoring system

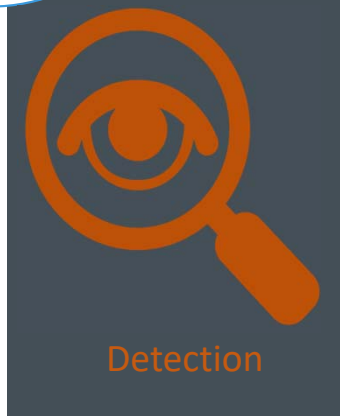
An OT oriented threat detection system and analytics tools to improve cyber security of BMS

Network protocol parsing in order to detect specific threats and 0-days attacks to building automation systems.

An advanced file analysis system to improve cyber security

Dynamic detection of malicious files.

- Use of non-supervised IDS/IPS methods and innovative supervised ML techniques
- Building automation threat hunting to detect intrusions
- Dynamic file analysis update considering new file formats



SAFECARE Innovation Elements

An analytics solution to monitor e-health devices and improve cyber security

pro-active security monitoring and detection services for medical solutions and their environment.

A cyber threat monitoring system with an enlarged view about the combination of physical and cyber security threat and impact assessment

collects cyber security events from multiple security assets and centralizes them on a unique dashboard

- Superior detection accuracy and remediation, by leveraging security relevant data from the medical device
- Increase of SOC operator awareness and improvement of support decision making by proposing an appropriate response plan to solve the incident and mitigate the aftermaths

Cyber Security

SAFECARE

Integrated cyber-physical security for health services

Alert & Prevention & Response

SAFECARE Innovation Elements

A central database storing incidents and impacts and enabling analytics together with a scalable and standardized data exchange layer to protect and regulate the database access

An impact propagation model to simulate potential cascading effects and a decision support model to help decision makers to collect evidence

formalizes the relations between physical and cyber assets and threats in health services with a view to simulating cascading effects propagation between these assets.

- Evaluate the real or potential impacts of an attack on a component on other components
- Identification precursor events and next critical scenarios.

SAFECARE Innovation Elements

A threat response and alert system managing multi-step processes and a wide spectrum of communication channels

real-time multi-channel notification and alerting system that combines the ability to deliver notifications, alerts and mobilize resources based on the incoming event.

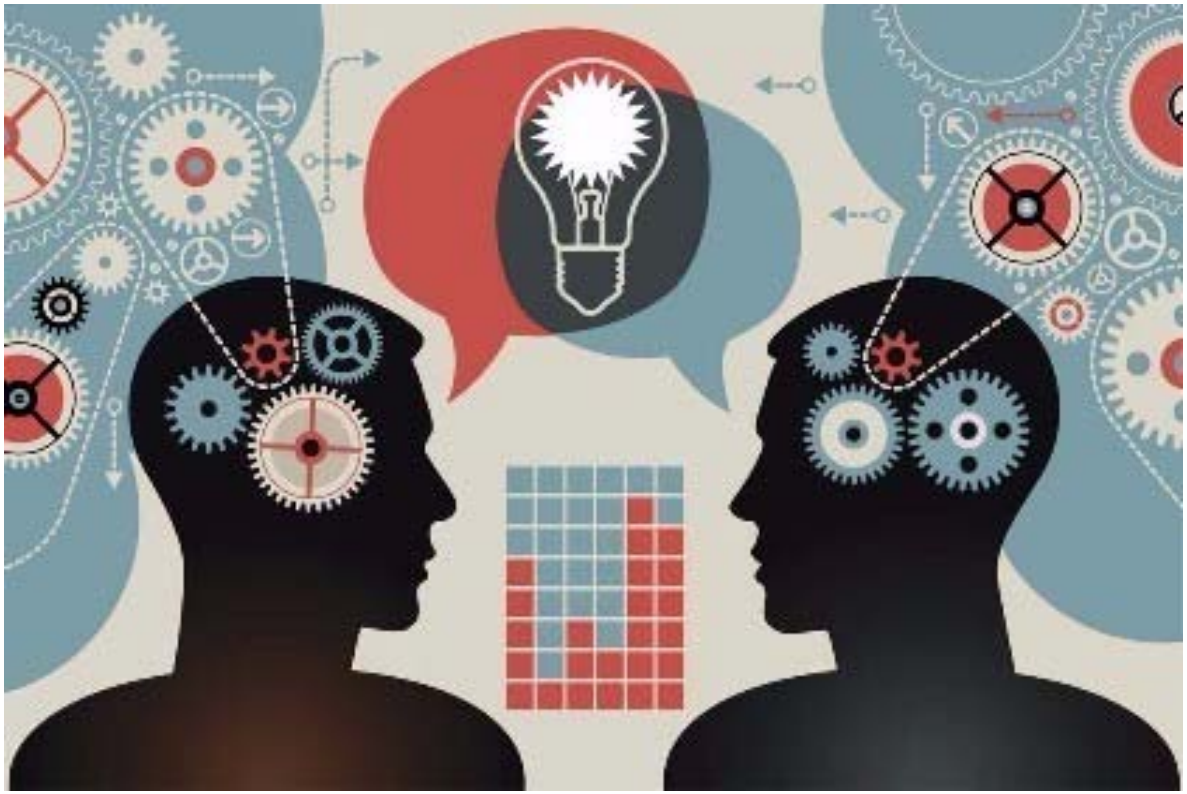
A Hospital Availability Management System to reroute the flow of patients with the capability to manage cross border crisis events

provides hospital availability, aiming to improve the health service resilience and the data availability in case of emergency

- Alerting solution combining multi-channel notification delivery systems
- Ability to manage in real time the emergencies, with a higher level of context and awareness and providing support to emergency managers

SAFECARE Solution

Scientific Dissemination



Scientific Dissemination

Academic Activities

- Students projects and Thesis
- 11 final grade projects; 3 MsC; 5 PhD
- Milestone Research Programe @ AAU

AALBORG UNIVERSITY

- Presentations in Po se and Ro n Universities

Scientific Dissemination

Conferences / Journals

- 25 publications

Publications

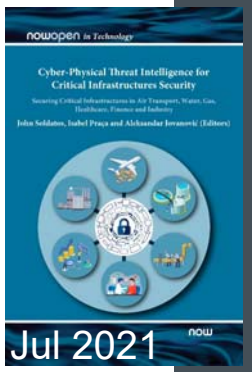
Risk Assessment and Solution Requirements	Physical Security Solutions	Cyber Security Solutions	Integrated cyber-physical security solutions
Stakeholders involved in Hospitals' Crisis Management Processes – KEMEA, APHM, EOS	Digital Twins and Semantic Data Fusion for Security in a Healthcare Environment – MILESTONE	A Matter of Life and Death: Analyzing the Security of Healthcare Networks – FST (Conference Paper)	Cyber-physical Threat Detection Platform Designed for Healthcare Systems – BEIA, KEMEA, LINKS, CSI
Body Area Network (BAN) for Healthcare by Wireless Mesh Network (WMN) – BEIA		Cyber Threat Monitoring Systems – Comparing attack detection performance of ensemble algorithms – ISEP, ACS (Conference Paper, Coming Soon).	Towards a global CIs' cyber-physical security management and joint coordination approach – KEMEA (Conference Presentation)
Lego Methodology Approach for Common Criteria Certification of IoT Telemetry – BEIA		Selection and Performance Analysis of CICIDS2017 Features Importance – ISEP	Cross-Domain Security Asset Management for Healthcare – LINKS, ASLTO5 (Conference Paper, Coming Soon)

SAFECARE

Integrated cyber-physical security for health services

Books

- *"Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber- Physical Protection of Modern Critical Infrastructures"* *(4 Chapters)*
- *"Cyber-Physical Threat Intelligence for Critical Infrastructures Security: Securing Critical Infrastructures in Air Transport, Finance, Gas, Healthcare, and Industry"* *(3 Chapters)*



Scientific Dissemination

Critical Infrastructure Protection Projects Cluster Workshop/Event

ECSCI Virtual workshop

24-25 June 2020

Scientific Dissemination

Presentations

- CoU Meeting, Brussels, Sept 2019
- Mediterranean Security Event, Oct 2019
- Critical Infrastructure Protection Projects Cluster Workshop, Virtual, 24-25 June 2020
- International Conference on Cyber Defense and Security, October 2020
- RSNA 2020, Philips Cybersecurity Services, Nov 2020
- Community of European Research and Innovation for Security (Ceris) Disaster Risk Societies – State-of-play and Way Forward, June 2021
- HIMMS 2021, Cybersecurity - Philips One Services Portfolio, August 2021

Scientific Dissemination

Events

- Awareness Event, Leuven, Sept 2019 (involvement of other CIP – SATIE, FINSEC)
- Workshop *"Cyber-Physical Security for Critical Infrastructures Protection",* Co-located with ESORICS 2020 (PC Chair; PC members)
- IEEE CBMS Special Track on: *Security of e-Health Systems and Connected Medical Devices*, *June 2021*
- Workshop *"Cyber-Physical Security for Critical Infrastructures Protection"*, Co-located with ESORICS 2021
- The 3S Clustering Event, October 2021

Eva Maia

egm@isep.ipp.pt

SAFECARE Outcomes: Scientific Point of View

3S Clustering Event

Eva Maia, ISEP

SAFECARE has received funding as part of the "Secure societies – Protecting freedom and security of Europe and its citizens" challenge of the Horizon 2020 Research and Innovation programme of the European Union under grant agreement 787002