

SAFECARE

Integrated cyber-physical security for health services

SAFECARE Results: Innovations & Scientific Point of View

Commercial Event

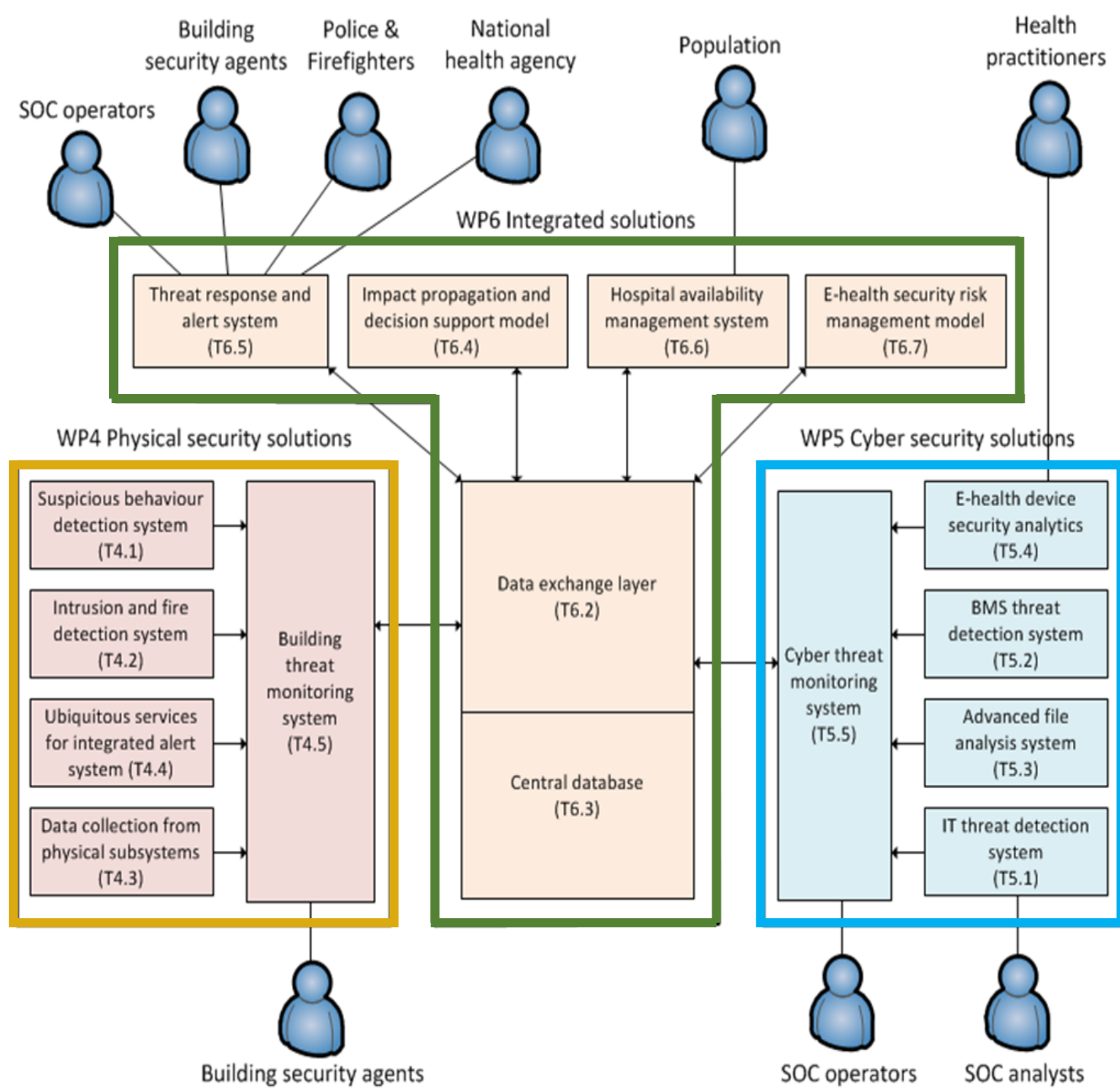
Eva Maia, ISEP

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



Physical Security



COMING UP
NEXT!



Detection

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
- Complete integrated and automated system

COMING UP
NEXT!



Physical Security



Alert & Response

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



ITDS concentrates the functions to **detect security events**.
offers both common **non-supervised IDS/IPS** methods and
innovative supervised ML methods



SOC's analysts:
correlate information
understand threats
improve response capacities and shorten time response
mitigate the consequences of attacks, especially in case of large data and APT.



Cyber Security



Detection

SAFECARE Innovation Elements

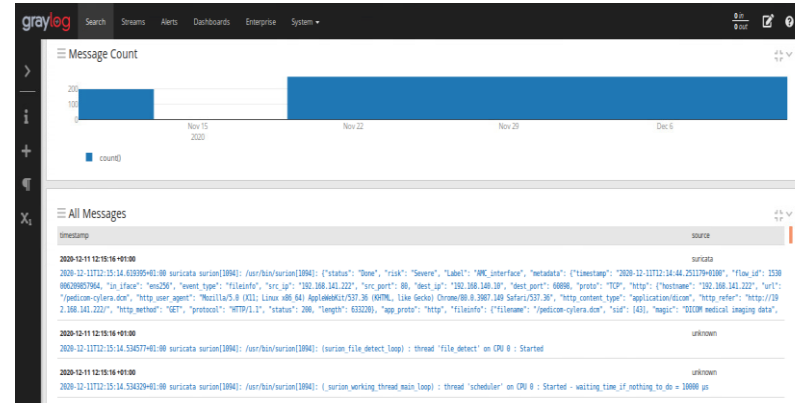


Cyber Security

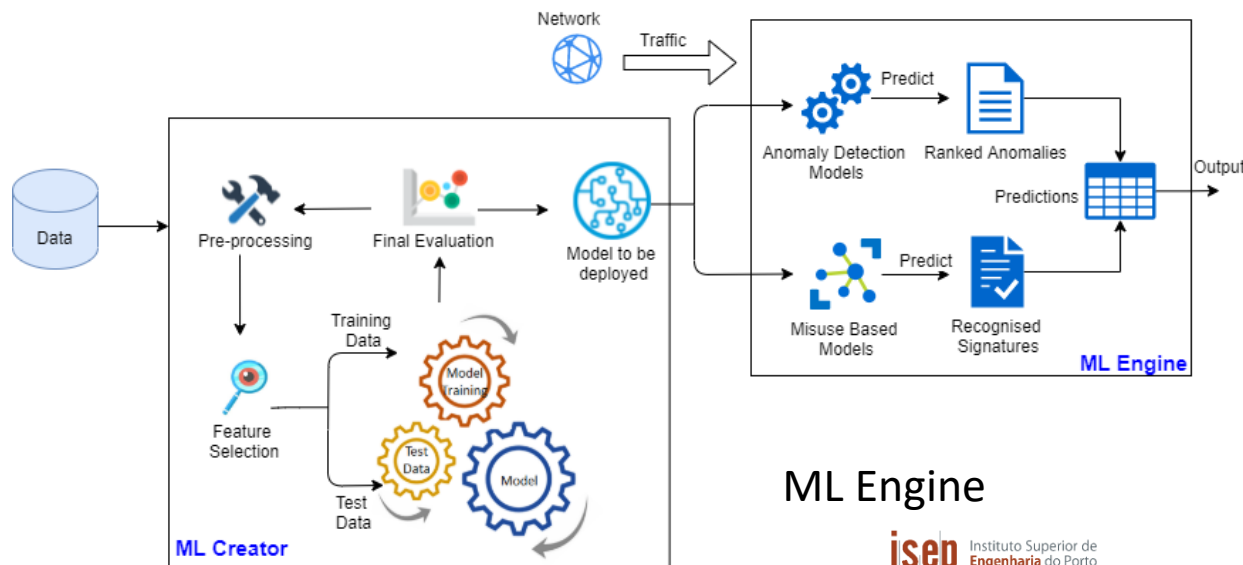
```

-rw-r--r-- 1 root root 1.9K Apr 28 2020 app-layer-events.rules
-rw-r--r-- 1 root root 20K Apr 28 2020 decoder-events.rules
-rw-r--r-- 1 root root 468 Apr 28 2020 dhcp-events.rules
-rw-r--r-- 1 root root 1.2K Apr 28 2020 dnsp3-events.rules
-rw-r--r-- 1 root root 1.8K Apr 28 2020 dns-events.rules
-rw-r--r-- 1 root root 16M Oct 21 14:38 emerging-all.rules
-rw-r--r-- 1 root root 4.8K Jan 27 18:35 files.rules
-rw-r--r-- 1 root root 13K Apr 28 2020 http-events.rules
-rw-r--r-- 1 root root 2.7K Apr 28 2020 ipsec-events.rules
-rw-r--r-- 1 root root 585 Apr 28 2020 kerberos-events.rules
-rw-r--r-- 1 root root 2.1K Apr 28 2020 modbus-events.rules
-rw-r--r-- 1 root root 558 Apr 28 2020 nfs-events.rules
-rw-r--r-- 1 root root 558 Apr 28 2020 ntp-events.rules
-rw-r--r-- 1 root root 1.3K Apr 28 2020 smb-events.rules
-rw-r--r-- 1 root root 5.1K Apr 28 2020 smtp-events.rules
-rw-r--r-- 1 root root 13K Apr 28 2020 stream-events.rules
-rw-r--r-- 1 root root 58 Jul 21 2020 test.rules
-rw-r--r-- 1 root root 5.1K Apr 28 2020 tls-events.rules
    
```

Network threat detection engine
(based on Suricata) **AIRBUS**



Correlation engine (based on Graylog) **AIRBUS**



ML Engine

isep Instituto Superior de Engenharia do Porto



Detection

SAFECARE Innovation Elements



Cyber Security

The screenshot displays the SAFECARE interface within a remote console. The main window shows a table of alerts and incidents with the following data:

Severity	Status	Identifier	Last Update	Title	Operators	Detector
Low	Opened	01FG6ZZB8XKM ZSPTMCMWV8K NRN	32s	Machine learning detect attack		newgraylog1
Low	Opened	01FG6ZVWA81F QWBRP86N293 JR	1m	Network service scanning		newgraylog1
Medium	Opened	01FG6ZSXM4Y Q48FG738HYKN M7	3m	Network Denial of Service		newgraylog1
Low	Opened	01FG6ZS6WD9E 2GGNVT06VTFZ DD	3m	Network service scanning		newgraylog1
Low	Opened	01FG6ZRW00NJ VAA9E9TY9MEH W0	4m	Malicious Link		newgraylog1
Medium	Opened	01FG6ZEYJS2Y WWNSSQJRJB7 72C	9m	Data Manipulation		newgraylog1
Info	Opened	01FG6ZCFK9E07 5A6Y8JMHE9V4 7	10m	New Cyber Impact received		newgraylog1

The interface also includes a sidebar with navigation icons, a top navigation bar with the AIRBUS CYMERIUS logo, and a right-hand panel showing details for the selected incident, including sections for 'LAST OPERATOR EVENT', 'ANALYSIS', 'EQUIPMENTS (3)', and 'REACTIONS (1)'.



Detection



- Use of **non-supervised IDS/IPS methods** and **innovative supervised ML techniques**

SAFECARE Innovation Elements

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.

COMING SOON

the
afternoon
session



Cyber Security



Detection



- 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



Cyber Security

COMING SOON

the
afternoon
session



- Superior detection accuracy and remediation, by leveraging security 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



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 of the system
- Identification precursor events and next critical scenarios.

COMING SOON

the
afternoon
session



Cyber-physical
Security



Detection

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.



- Alerting solution combining multi-channel notification delivery systems

COMING SOON

the
afternoon
session



Cyber-physical
Security



Alert & Prevention
& Response

SAFECARE Innovation Elements

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



Cyber-physical
Security



COMING SOON

the
afternoon
session

- Combination of different data sources, from static data (such as incident and impact messages), to estimate in near real-time potential impact on the asset availability, improving the awareness and providing context to users during incident management
- Asset-centric views and incident-centric interface to support users to analyze the overall situation and if needed inspect all the details of incidents, estimated impacts and report of alert campaign
- Training and simulation functionalities to support the adoption and the easy-of-use
- Developed as a web application with the possibility to deploy it locally or in Cloud (SaaS)



Alert & Prevention
& Response

SAFE CARE Solution

The image displays the SAFE CARE solution interface, which is an integrated cyber-physical security system for health services. The central logo features the text "SAFE CARE" in a large, blue, stylized font, with the tagline "Integrated cyber-physical security for health services" below it.

The interface is composed of several overlapping windows and panels:

- Top Left:** A window titled "AIRBUS CYMERIUS" showing a list of incidents. The table includes columns for "Sévérité", "Statut", "Identifiant", "Dernière MAJ", "Titre", and "Opérateur".
- Top Center:** A "Command Center" window with a "FORESCOUT" section, displaying filters and alert management options.
- Top Right:** A "Remote console - HAMS test front-end" window showing a network diagram with nodes like "SC2-NETWORK-RADIOLOGY-C-1" and "SC2-PORT-RAD_NETWORK-C-1".
- Bottom Left:** A configuration window for "SC2-PORT-RAD_NETWORK-C-1" with various settings and a "Save" button.
- Bottom Center:** A detailed incident view for "Loitering for 20" with a "Description" field and a "Sensor id 28374" field.
- Bottom Right:** An "Incidents Data" table with columns for ID, Type, Severity, Date, Status, Message, and Impacts. It shows two incidents with "very high" severity.

The overall interface is designed for real-time monitoring and response to cyber threats in a healthcare environment.

Scientific Dissemination



Scientific Dissemination

Academic Activities

- Students projects and Thesis
- 11 final grade projects; 3 MsC; 5 PhD

- Milestone Research Programme @ AAU



AALBORG UNIVERSITY

- Presentations in  Greek,  Portuguese and  Romanian Universities



Scientific Dissemination

Conferences / Journals

- 25 publications

Publications

Risk Assessment and Solution Requirements

Stakeholders involved in Hospitals' Crisis Management Processes – KEMEA, APHM, EOS

Body Area Network (BAN) for Healthcare by Wireless Mesh Network (WMN) – BEIA

Lego Methodology Approach for Common Criteria Certification of IoT Telemetry – BEIA

Physical Security Solutions

Digital Twins and Semantic Data Fusion for Security in a Healthcare Environment – MILESTONE

Cyber Security Solutions

A Matter of Life and Death: Analyzing the Security of Healthcare Networks – FST (Conference Paper)

Cyber Threat Monitoring Systems – Comparing attack detection performance of ensemble algorithms – ISEP, ACS (Conference Paper, Coming Soon).

Selection and Performance Analysis of CICIDS2017 Features Importance – ISEP

Integrated cyber-physical security solutions

Cyber-physical Threat Detection Platform Designed for Healthcare Systems – BEIA, KEMEA, LINKS, CSI

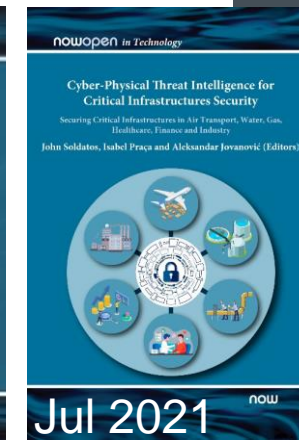
Towards a global CIs' cyber-physical security management and joint coordination approach – KEMEA (Conference Presentation)

Cross-Domain Security Asset Management for Healthcare – LINKS, ASLTO5 (Conference Paper, Coming Soon)



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
- International Conference on Transport and Smart Cities, 17-19 September 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
- SAFECARE Commercial Event, November 2021





Eva Maia



egm@isep.ipp.pt

SAFE CARE

Integrated cyber-physical security for health services

SAFECARE Results: Innovations & Scientific Point of View

Commercial Event

Eva Maia, ISEP