# SAFECARE NEWSLETTER May 2021

## Message from SAFECARE Coordinator, Philippe Tourron

A final straight line is in front of us. After this start of the year marked by the testing phase, we will start the on-site demonstrations. Of course, the conditions are still disrupted by the COVID-19 crisis, but we are staying the course with some essential adaptations.

The test phase could not take place under the Porto sun and we therefore had to create a completely virtual environment based on the ACS CyberRange (thanks to their team, who allowed this reactivity). We also had to limit the scenarios tested and split the tests into several sessions to validate all the sequences between the Safecare modules and, therefore, between the partners involved. All the participating partners consistently dedicated their time and energy, with remarkable leadership by the CSI and ISEP teams.

We were able to discover the need for some adaptations and the importance of the central database, which allows consistency between all the modules. This kind of discovery was the objective of the tests.

We are retaining the following lessons for our final stages:

• Preparation, with data validation between all partners involved, is essential before launching the risk scenario.

• Each test phase requires a facilitator who sets the pace of the attack paths for each risk.

• The definition of evaluation criteria, appropriate questionnaires, and the designation of actors to play the role of observers is the guarantee of being able to identify all the elements of improvement.

The virtual demonstration of a scenario in the context of the Amsterdam hospital allowed us to continue our evaluation and should lead us to calmly approach the on-site demonstrations for Turin (ASLTO5) and Marseille (AP-HM). This time around, we will have hybrid environments with components in a CyberRange connected on site, components in cloud mode, and components (software and hardware) from each site, as well as local actors. This unforeseen adaptation gives us the opportunity to imagine and confirm the feasibility of future on-premises and cloud integration.

The partners will be largely remote, which will be a new challenge for our consortium.

I have confidence that our teams will successfully integrate Safecare into our hospital environments.

Have a good home straight everyone. Now is the time to accelerate.

## SAFECARE Research Online

The result of SAFECARE partners research has been made available online for sharing and study by practitioners in the field. It is available on the website, and includes the first set of deliverables accepted by the European Commission, related to the requirements of healthcare infrastructure security and preliminary designs of the SAFECARE system, as well as scientific papers and articles submitted on the basis of the SAFECARE research. The research can be found here:

Deliverables and publications

Risk Assessment and Solution Requirements

Physical Security Solutions
Cyber Security Solutions
Integrated Cyber-Physical Security Solutions

## Updates

SAFECARE 2nd Awareness Event - On Monday 1st of February, 2021 the SAFECARE Project Consortium held its 2nd Awareness Event with the aim of presenting the main results achieved within the project. The event was chaired by Mr. Philippe Tourron, from the Assistance Publique – Hôpitaux de Marseille and Coordinator of the project, and it represented a unique opportunity to gain an in-depth knowledge from, and also to contribute to, the discussions on key technological trends, best practices, emerging threats and other relevant issues in the sector of Healthcare Infrastructure security. The press release of the event is available here.

Third edition of the Leuven AI Law and Ethics Conference (LAILEC) - On 25-26 March 2021 took place the third edition of the LAILEC. The conference, organized by the KU Leuven Centre for IT & IP Law (CiTiP), gathered security experts in various fields and proposed sector-specific panels and exclusive workshops. Elisabetta Biasin, a Researcher in Law at CiTiP, and member of the SAFECARE consortium, was one of the speakers at the Healthcare cybersecurity panel on Day 2: '*Regulating complexity: cybersecurity of AI-driven technology in the healthcare sector*'. The panel discussed the ethical and legal challenges of regulating cybersecurity for healthcare AI-driven technologies. Therein, Elisabetta gave a presentation on medical device cybersecurity regulatory challenges based on the research carried out in SAFECARE.

SAFECARE in the news - The SAFECARE project has been mentioned in the French newspaper "La Provence", featuring an interview with Philippe Tourron, project coordinator and responsible for the protection of security systems at AP-HM. This article shows how topical is the work of SAFECARE for healthcare infrastructure security.

SAFECARE project of the week 22-26 March 2021 on cybewatching.eu, The European watch on cybersecurity & privacy.

Security Incidents in Healthcare Infrastructure during COVID-19 Crisis - SAFECARE Partners are tracking the rise in security incidents affecting healthcare infrastructure during the crisis.

## Project Progress

### Physical Security Solutions:

- The Suspicious Behaviour Detection System, Intrusion and Fire Detection System, Data collection System and Mobile Service have been integrated with the Building Threat Monitoring System.
- Virtual cameras, door access controls and fire alarms have been added to the virtual hospital for test simulation.
- The Data Collection System (including virtual sensors), Mobile Alerting System and Building Threat Monitoring System have been installed on CyberRange. Suspicious Behaviour Detection System and Intrusion and Fire Detection System have been connected to CyberRange remotely.

The deliverables for T4.1 (Suspicious behaviour detection system), T4.2 (Intrusion and fire detection system), T4.3 (Data collection system) and T4.5 (Building monitoring system) have been delivered. But those tasks are extended due to a lack of data collection delay caused by Covid-19. T4.4 (Mobile service for integrated alerting system) is complete.

### Cyber Security Solutions:

All the tasks of WP5 (Cyber security solutions) are complete. The following prototypes have been successfully implemented:

- IT threat detection system:

The solution is able to detect known malware and attacks as well as suspicious behaviours that may be the work of a new unknown method for an attacker to slip into or harm the system.

- BMS threat detection system:

The solution is conceived as a network intrusion detection system (NIDS) based on passive monitoring detection modules. This means that the NIDS does not inject any traffic into the monitored network, it only observes the traffic generated by other devices. This reduces interference with critical network operations.

- Advanced file analysis system:

The solution is able to detect the malicious files in critical health infrastructures by performing a thorough analysis - both statically and dynamically - of files that transit through the IT (Information Technology) and BMS (Building Management System) networks.

- E-health devices security analytics:

The solution aims at performing data analytics for medical devices. Its architecture focuses on acquiring, monitoring, and analysing medical device log data to detect security events. Furthermore,

it generates alerts when such events or vulnerabilities are detected and sends alerts to the relevant stakeholders.

- Cyber threat monitoring system:

The solution collects and centralizes cyber security events, displays information in an organized way and provides user-friendly interfaces to SOC (Security Operations Center) analysts so that they can analyse and visualise threats and impacted assets.

The prototypes have been deployed on the Test Platform (WP7) to validate that each prototype is operational and to test their interconnections. To conclude, all the WP5 objectives have been achieved.

**Integrated Cyber-Physical Solutions**:

The development of Integrated cyber-physical security solutions has been completed, according to the SAFECARE project schedule. This resulted in the achievement of two SAFECARE milestones: i) Data Exchange Layer(DXL) and Central Database(CDB) are deployed and ii) Impact Propagation and Decision Support model(IPDSM) is ready and integrated with DXL and CDB. The three above-mentioned software are the basis of the integrated solution, which can manage cyber and physical incidents communicated by detection solutions and evaluate how they can impact on hospital critical assets.

Additional systems for data visualization, management of asset availability, alerting and the security risk management model have been developed and tested within the SAFECARE testing platform.

Tests done gave us the possibility to improve the readiness and the maturity of this integrated solution, in order to be ready for the final demonstrations AMC, ASLTO5 and APHM.

## Testing the SAFECARE Solution

SAFECARE will carry out operational demonstrations to test the global solution under live conditions, through three demonstrations in hospitals (Turin, Marseille and Amsterdam) and one large scale pilot (Marseille).

The first step to fruitful demonstrations was to have a simulation environment where all prototypes are represented. Therefore, to ensure the security and reliability of the entire SAFECARE solution, a test platform, representative of the target environment, was built to validate that each prototype is operational, and the interconnections between prototypes are working as expected. Moreover, this first step also allowed the training of security practitioners and health practitioners to use the prototypes, the deployment of the test bed in an operational environment and, finally, the evaluation of the security impact of the prototype on risk assessment.

All the partners worked hard in the last months to ensure the success of this test phase. The most representative scenarios to test the SAFECARE solution were selected, and through the selected scenarios, most of the components were tested.

From the several simulation sessions performed, the correct functioning of the SAFECARE components was ensured and the interconnections between them were fine-tuned. All the technical issues that arose were solved and it was also possible to explain to the end-users the operation of the SAFECARE platform, not only from a user's perspective but also explaining all the workflow of an incident. This allowed the discovery of new features that were very useful to the user and that were not initially planned. Most of them will be developed to guarantee the completeness of the SAFECARE solution in the demonstration phase.

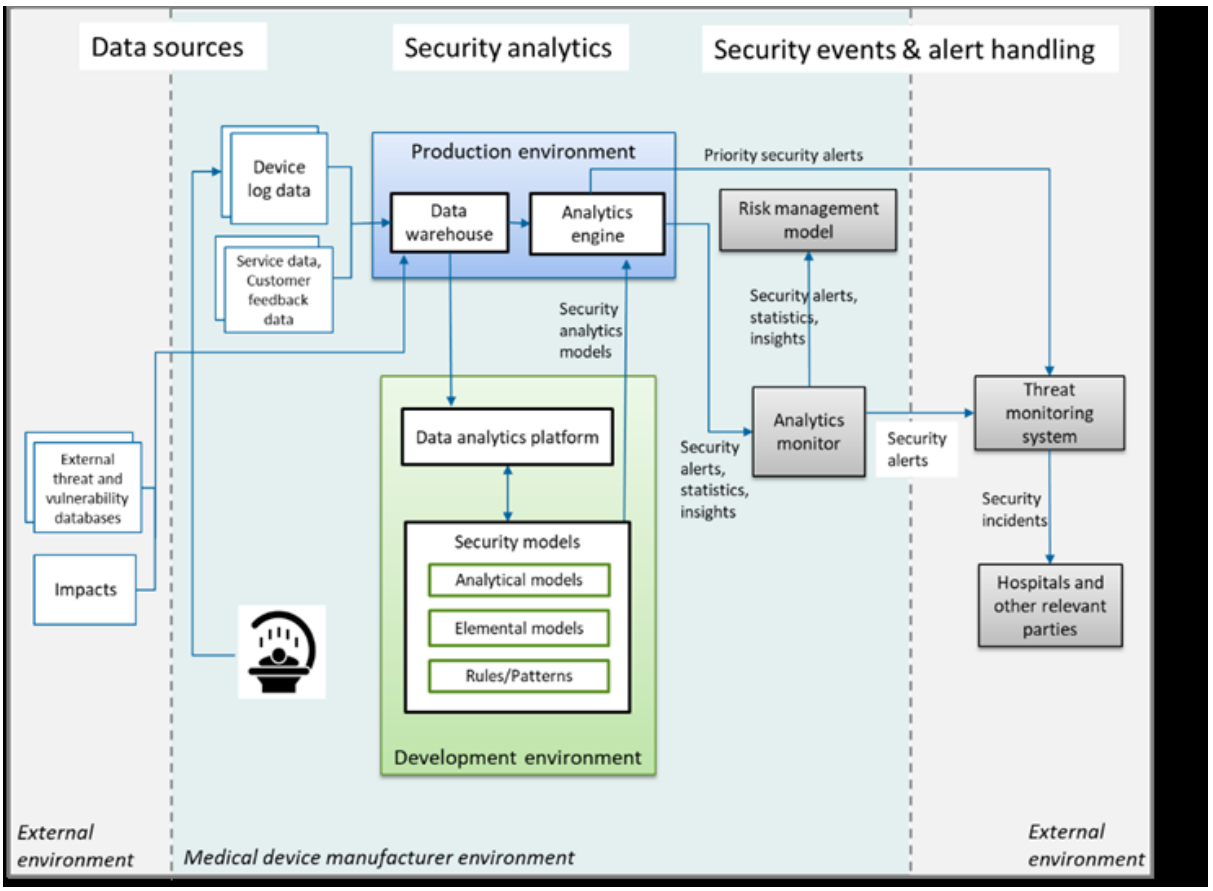
## Focus on health innovation

### E-health Device Security Analytics and Monitoring

One of the innovations in SAFECARE is medical device security analytics and monitoring. This addresses a significant blind spot in security monitoring in hospital environments and consequently healthcare as a critical sector. The introduction of E-health Device Security Analytics – EDSA in short – leverages the medical device to monitor the medical device and its operational environment.

Traditionally, medical devices are not designed for this, EDSA has been designed, specified, prototyped and tested. As a first feature, logging capabilities of the medical device have been extended together with means to retrieve and extract-transform-load the resulting security relevant data in a data warehouse in a way that does not interfere with the clinical function of the medical device. As a second feature, security analytics-based alerting models process incoming data and generate alerts where alerts are optimized for actionability by parties responsible for remediation. For example, for medical device service engineers alerts are designed for a near-zero false positive rate and unambiguous fix. As a third feature, EDSA interfaces with security management systems with routing organized such that alerts go to the right management system for remediation. For example, alerts related to vulnerabilities or threats in the operational environment of the medical device go to the hospital cyber threat management system and alerts related to the security controls of the medical device go to the vendor service dashboard.

The prototype implementation has been tested positively. Security alerting models based on medical device logs provide meaningful alerts to make medical devices and hospitals more secure, e.g. detect security misconfiguration vulnerabilities and user behaviour anomalies and threats. Integrations with management systems have been successfully demonstrated in a multi-partner hospital testbed setup. Thereby, it further demonstrated the innovation value potential through its combination with other IT, OT, physical monitoring means, optimally addressing the current blind spot in context and integrally improving hospital security and risk management.




*E-Health Device Security Analytics architecture (source: SAFECARE deliverable D5.7)*

## BMS threat detection system

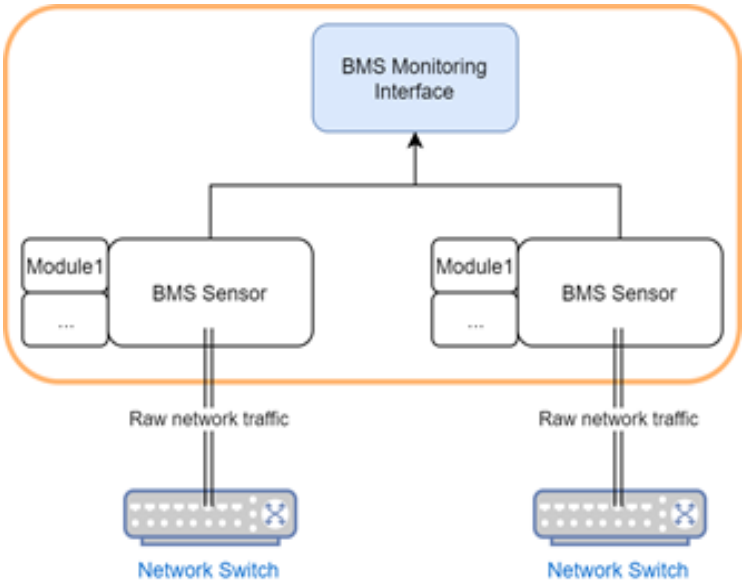
One of the main outcomes of the SAFECARE project is a cyber threat detection system that aims at improving the detection of attacks on IT networks and Building Management Systems (BMS).

Forescout Technologies has developed an innovative network-based Intrusion Detection System (NIDS) that leverages in-depth protocol parsing and is specifically designed to protect healthcare BMS from cyber-attacks. This NIDS, called BMS probe in the context of SAFECARE, combines whitelisting (learning-based) approaches and blacklisting (attack-specific) approaches to detect a wide range of possible attacks to BMS.

This NIDS is capable of parsing widespread (standard and proprietary) BMS, IoT, and Healthcare protocols such as MQTT, Modbus, RTP, DICOM, HL7, LIS02 and Philips Data Export. It not only allows detecting attacks that directly target building automation and management systems, but also enables the monitoring of network traffic from medical devices, which can be the targets of attacks that leverage the building automation equipment. The NIDS relies on multiple engines to detect ongoing cyber-attacks, including: signature-based detection from in-depth protocol parsing of industry-specific protocols for both building automation systems and healthcare equipment; anomaly-based detection for local networks by learning normal communication flows and alerting on

deviations from these; and attack-specific detections, such as malformed packets, port scans, and man-in-the-middle.

One of the main performance requirements was not to disrupt the operational continuity of the building automation network in Healthcare Delivery Organizations (HDO), therefore the NIDS does not inject any traffic into the monitored network, it only observes the traffic generated by other devices. The architecture of the NIDS is as follows:

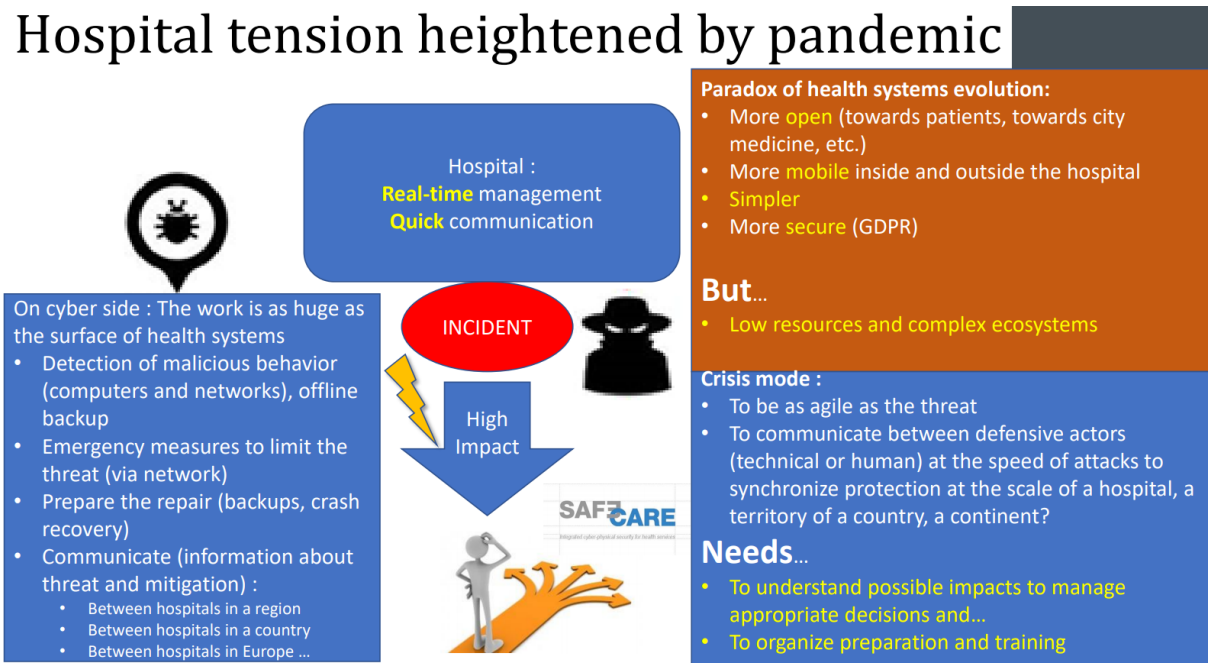



*NIDS architecture (source: SAFECARE deliverable D5.4)*

## Communication and Dissemination

SAFECARE partners have participated in several events recently, including the CERIS workshop on enhancing European resilience in case of pandemics, organised by the European Commission - DG HOME on the 22nd of April.

During the CERIS workshop SAFECARE partners (AP-HM and ISEP) presented the project's main outputs. Particular emphasis was put on the collection of security incidents during the pandemic and on the solutions designed to mitigate cyber and physical attacks in hospitals.




*Hospital tension heightened by pandemic (source: SAFECARE presentation at CERIS workshop)*

## Upcoming events

On June 29th, the SAFECARE consortium will hold the General Assembly and Board members meeting.

Additionally, the project's consortium is organising two commercial events to present the global solution to potential customers and health practitioners. These events will be held in September and October 2021.