WISG

Workshop interdisciplinaire sur la sécurité globale

21 & 22 mars 2023 • Palais du Pharo **Marseille**

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

anr agence nationale de la recherche
AU SERVICE DE LA SCIENCE

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE
Liberté Égalité Fraternité

SGDSN

Sécurité des infrastructures de santé critiques contre les menaces cyber et les attaques physiques avec SAFECARE

M. Philippe Tourron, AP-HM et GHT Hôpitaux de Provence

SAFECARE
Integrated cyber-physical security for health services

Hôpitaux Universitaires de Marseille | ap·hm

Safecare: Defend critical healthcare systems

Philippe Tourron - Coordinator

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

Project Identity

GA Number	**787002**
Starting date	01/09/2018
Duration in months	39
Topic	CIP-01-2016-2017
Consortium	21 partners - 10 EU countries Technical providers, hospitals, national public health agencies and security bodies
Project Coordinator:	Philippe Tourron, Marseille Public University Hospital (AP-HM)
Technical coordinator:	David Lancelin, Airbus CyberSecurity (CCS)
Scientific coordinator:	Isabel Praça, Instituto Superior de Engenharia do Porto (ISEP)

SAFECARE
Integrated cyber-physical security for health services

Context reminder Challenge for health systems managers

- **3 perimeters that overlap and collaborate :**
  - Medical devices
  - Building management
  - Medical data and software

Share data and infrastructure

- Polymorphic, agile, and combined threats : today and tomorrow, a strong attraction for cybercriminals and potentially terrorists

- A strong dependence between assets and complex impact chains... that can affect the lives of patients and staff

- A Paradox : A lot of information in specialized supervision systems without communication or integration

Need for a global view in anticipation, protection, and crisis management

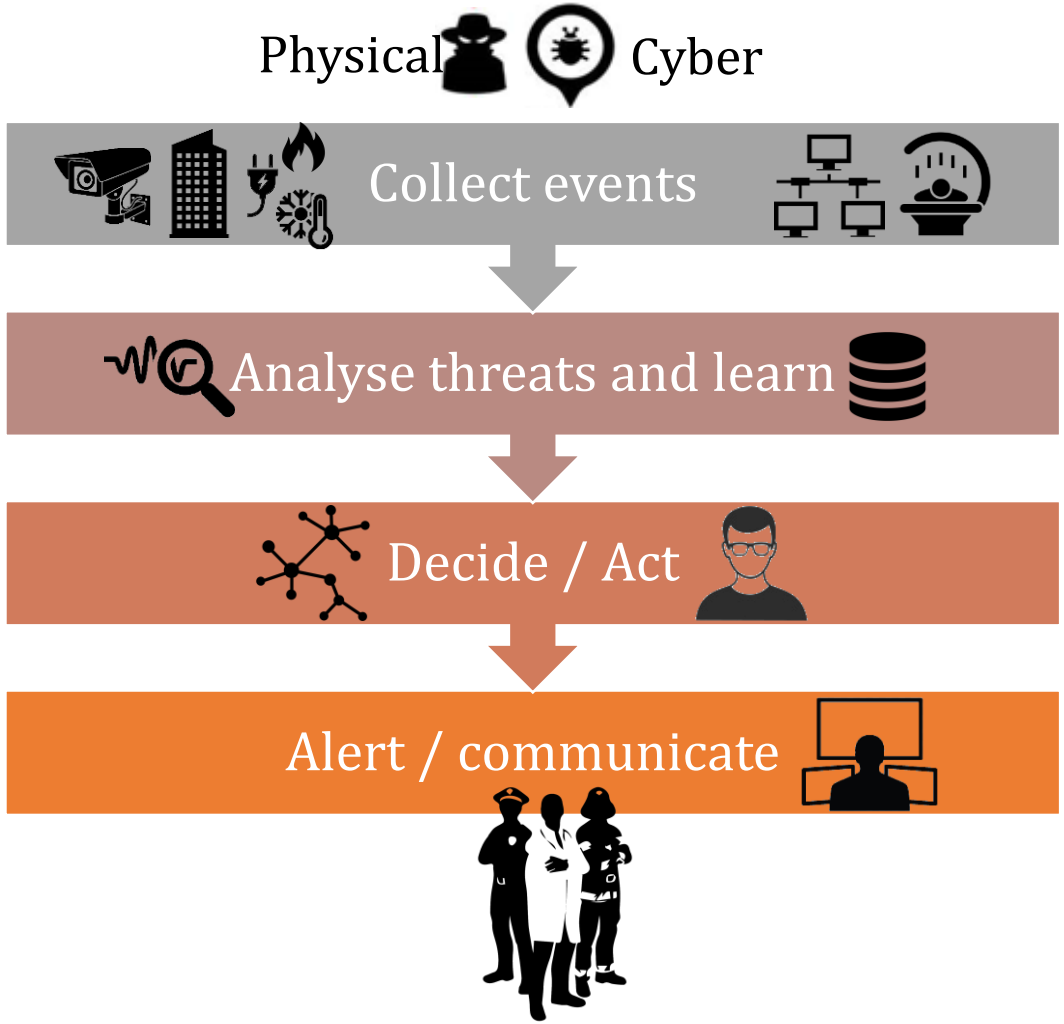
Addressing the challenge…

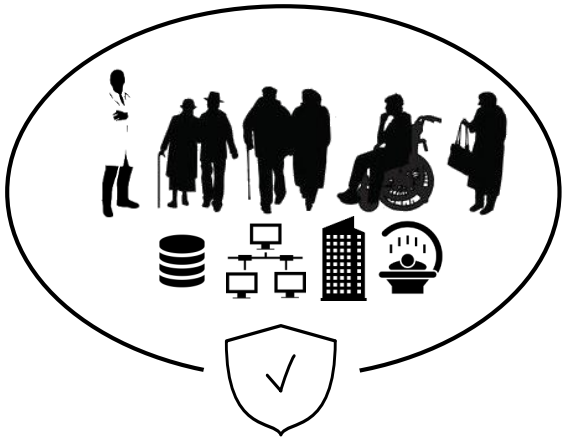
SAFECARE aims to:

- Provide high-quality, innovative, and cost-effective solutions that will improve physical and cyber security; and
- Enhance threat prevention, threat detection, incident response, and mitigation of impact in healthcare infrastructures, through the creation of a global protection system.

Over the course of 39 months, SAFECARE will design, test, validate and demonstrate 13 innovative elements optimizing the protection of critical infrastructure under operational conditions

Four steps to manage the security

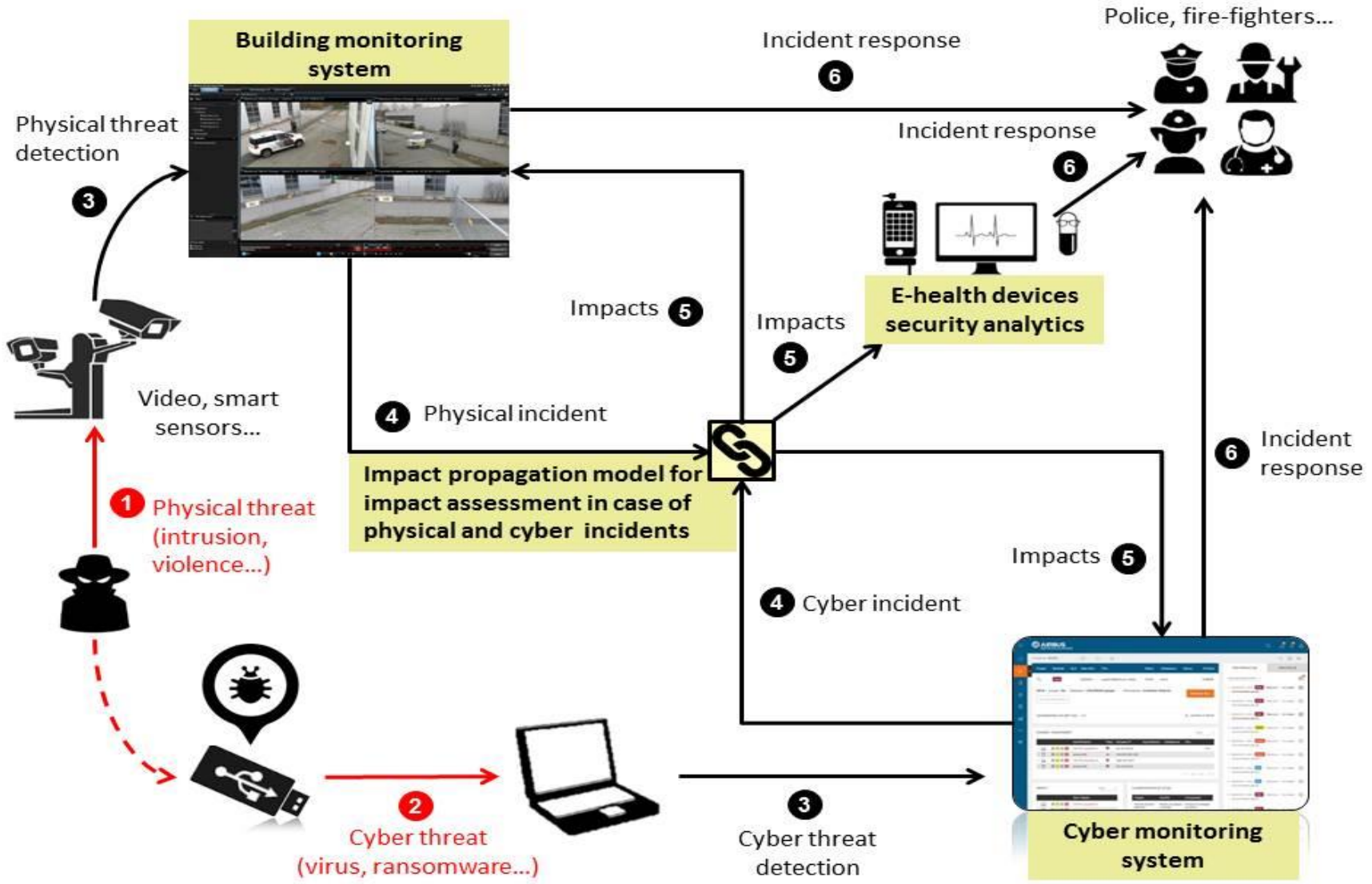




Patients, employees, assets, and services to protect

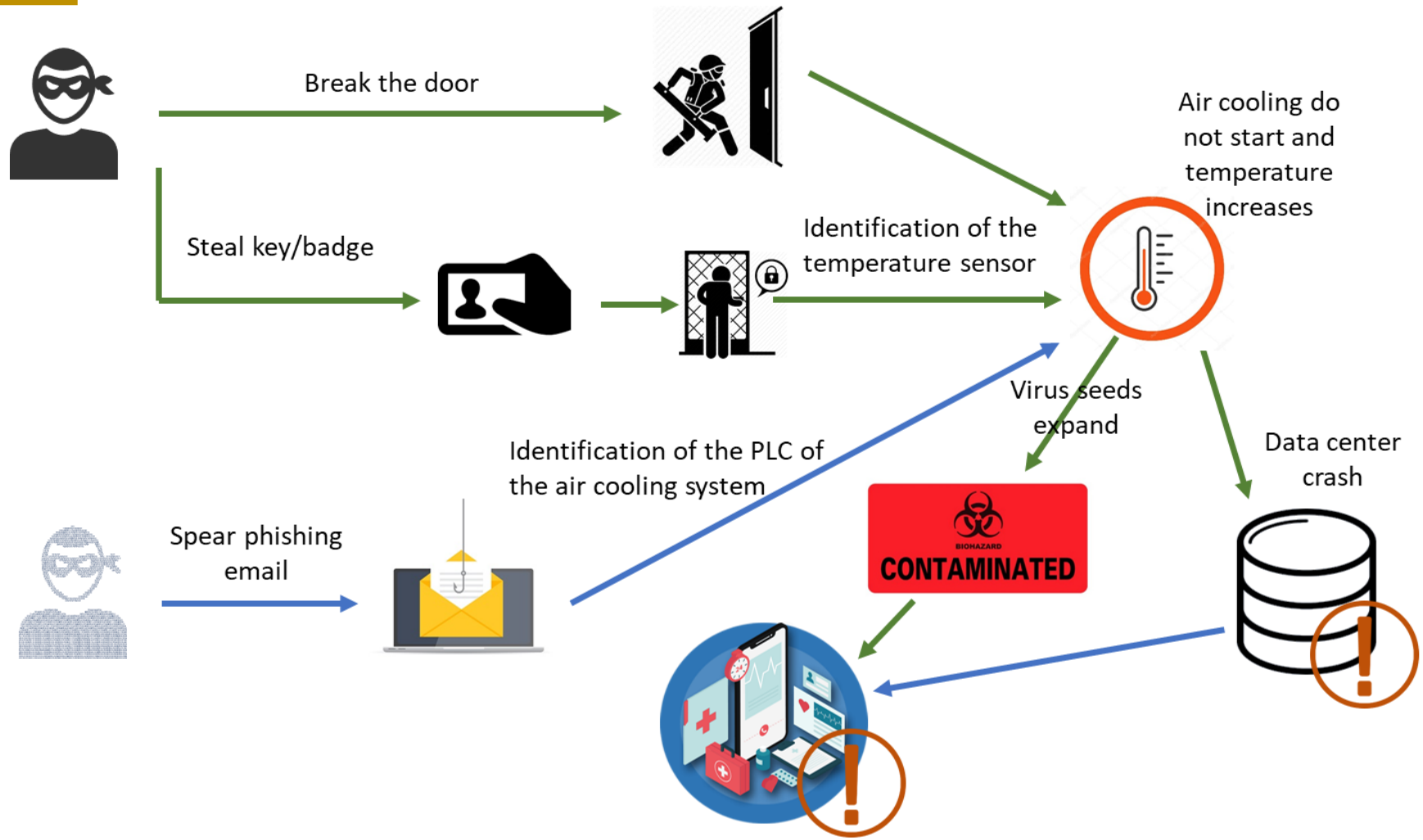
SAFECARE
Integrated cyber-physical security for health services

Overall concept



Cyber Physical Scenarios

Cyber-physical attack targeting the air-cooling system of the hospital



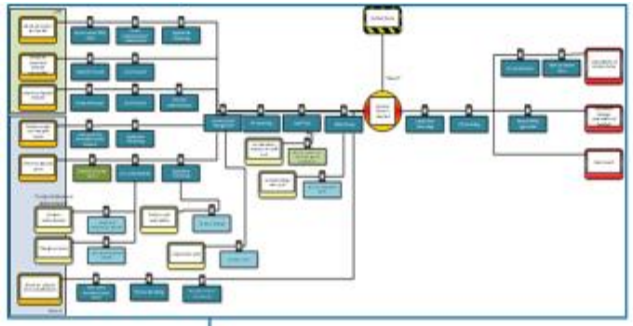
SAFECARE
Integrated cyber-physical security for health services

Risk Assessment

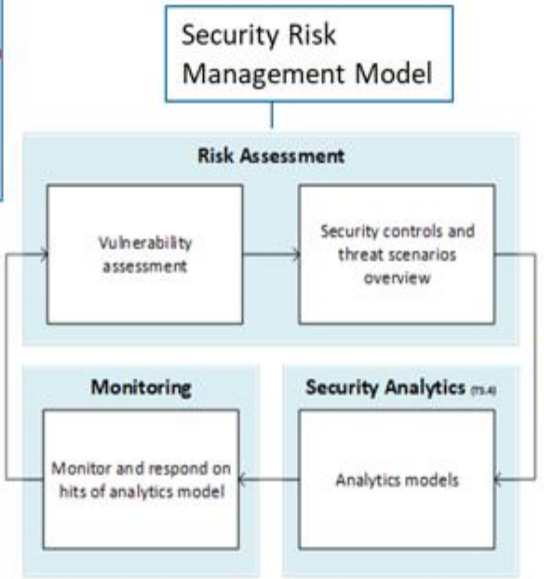
EBIOS RISK MANAGER

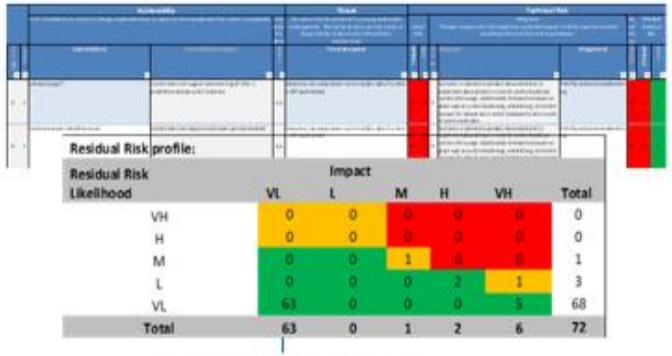
Expression of Needs and Identification of Security Objectives

EBIOS attack paths



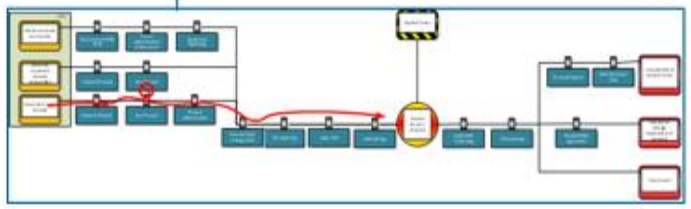
BowTie defense paths





Security Risk Assessment and risk profile

Monitoring Field data using BowTie



SAFECARE
Integrated cyber-physical security for health services

Scenarios

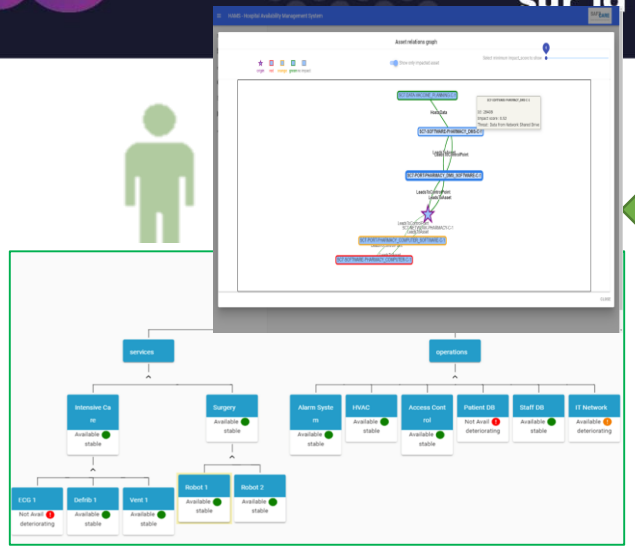
- Sc1: Cyber-physical attack targeting **power supply** of the hospital
- Sc2: Cyber-physical attack to steal **patient data** in the hospital
- Sc3: Cyber-physical attack **targeting IT systems**
- Sc4: Cyber-physical attack to cause a **hardware fault**
- Sc5: Cyber-physical attack targeting the **air-cooling system** of the hospital
- Sc6: Cyber-physical attack on **medical devices**
- Sc7: Cyber-physical attack to **steal credentials** to access IT systems
- Sc8: Cyber-Physical attack in access control provider to **steal medical devices**
- Sc9: Physical attack against hospital staff using a **gun**
- Sc10: Physical attack ~~**to steal drugs**~~ **vacines (COVID)**
- Sc11: Cyber-physical attack due to a **personal laptop**
- Sc12: Cyber-physical attack to **block national crisis management**

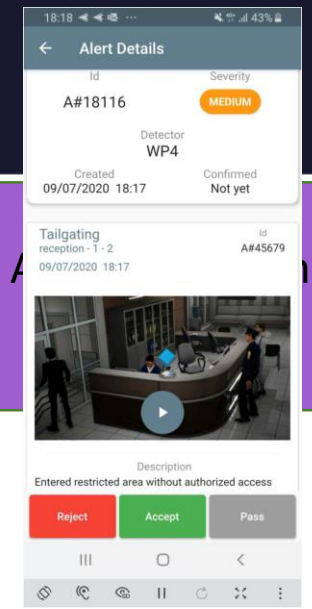
SAFECARE
Integrated cyber-physical security for health services

WISG

Workshop interdisciplinaire sur la sécurité globale

SAFECARE Four tools for End-Users

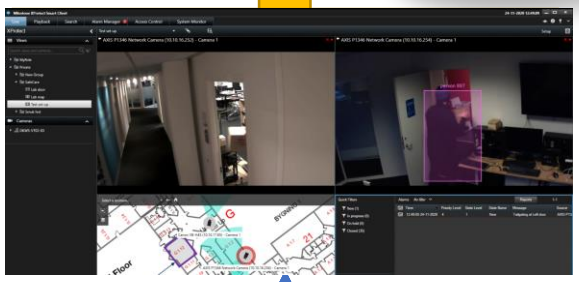


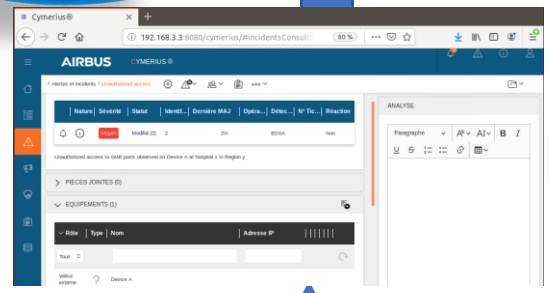


Cascading impacts calculation (IPM Ontology)

INCIDENTS

INCIDENTS





Access control

Video protection

Building monitoring system

Fire detection system

...

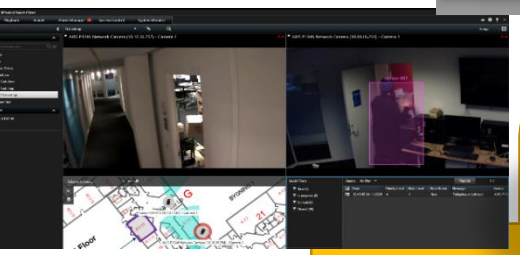
FW-IPS-IDS

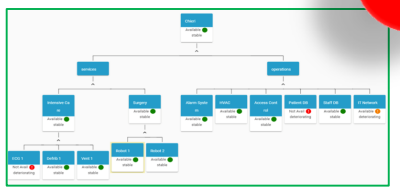
SIEM

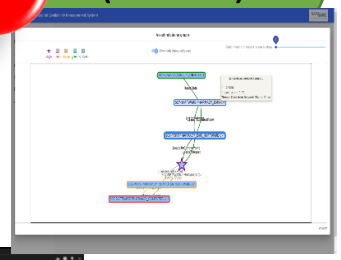
Threats detection systems

E-health AI

SAFECARE Four tools for End-Users

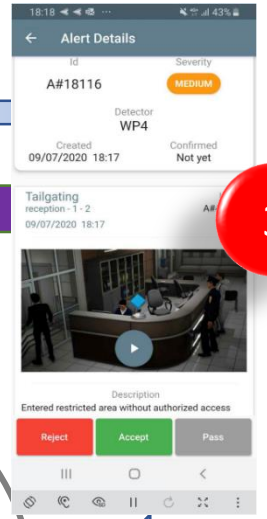






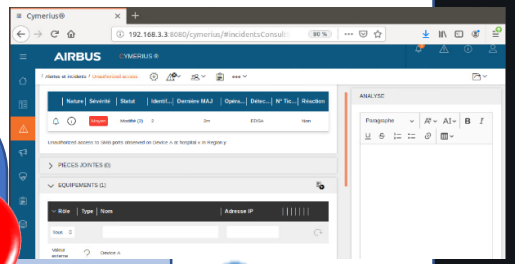
Global Supervision (HAMS)

4



3

Alerting system (TRAS-MAS)



2

INCIDENTS

INCIDENTS

1

Cascading impacts calculation (IPM Ontology)

Physical security supervision (BTMS – MAS)

Cyber sécurity supervision (CTMS)

Access control

Video protection

Building monitoring system

Fire detectio n system

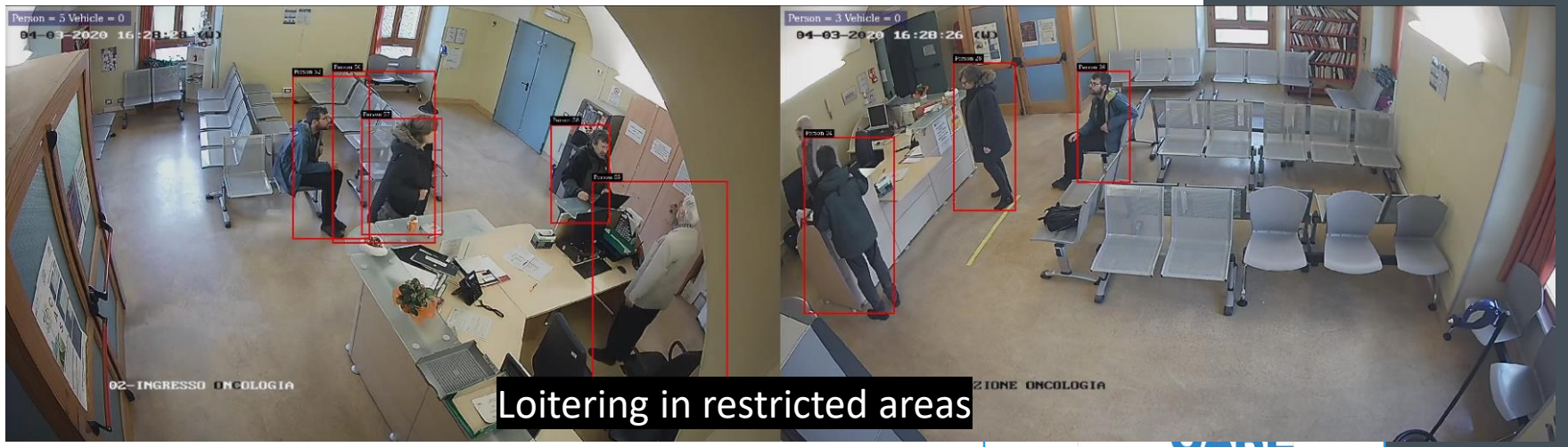
...

FW-IPS-IDS

SIEM

Threats detection systems

E-health AI

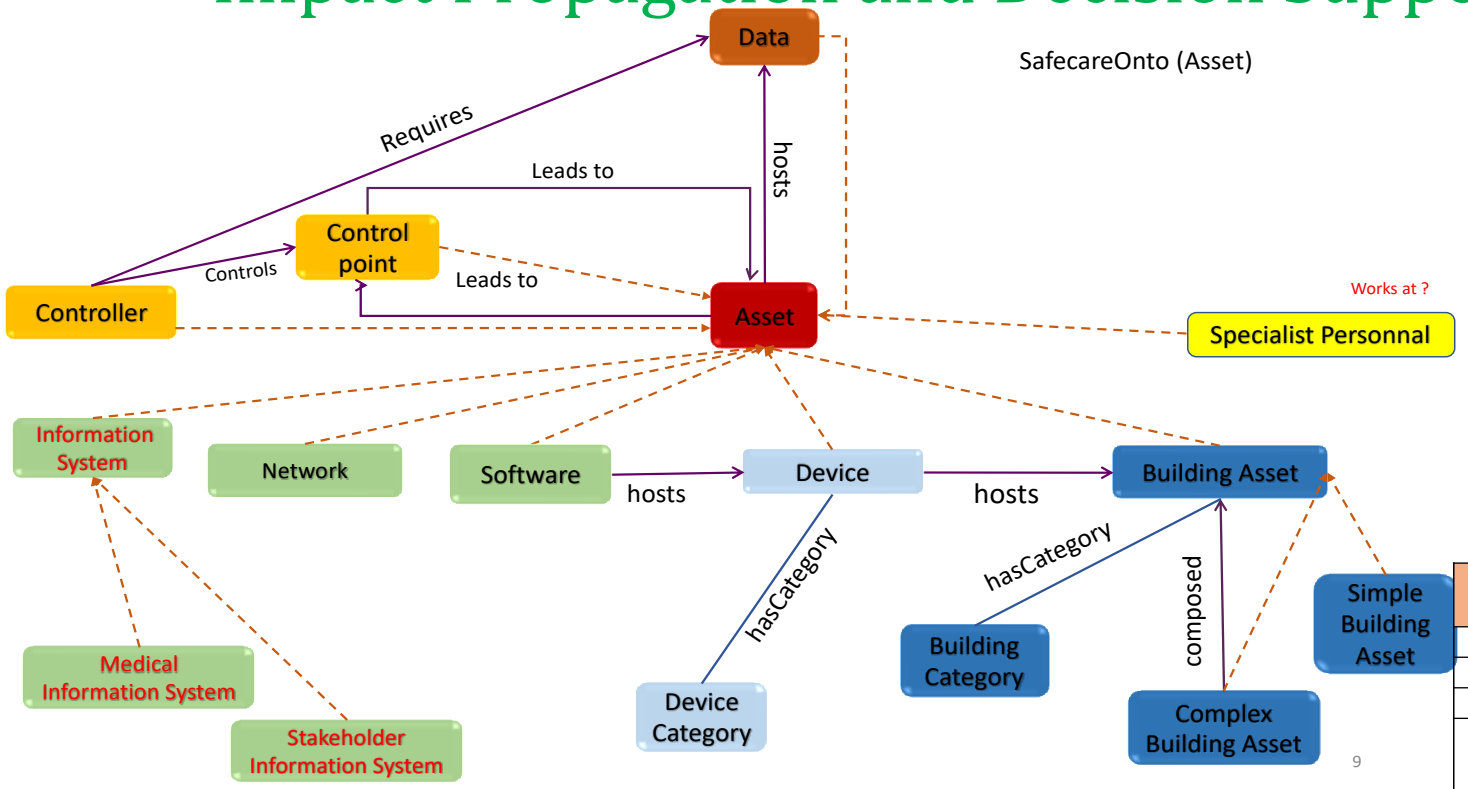


Physical Security Solutions

Integrated Solutions : focus on

Impact Propagation and Decision Support

le cnam



SAFECARE
Integrated cyber-physical security for health services

A model capturing assets, theirs relationships and related security concepts

A set of rules managing impacts propagation

Asset category	Incident category	Link category	propagableVia (yes, no)	Asset category	Incident category
Network	Virus	leadsTo	yes	Network	Virus
Network	Virus	leadsTo	yes	Device	Virus
Network	Saturation	leadsTo	yes	Network	Saturation
Network	Saturation	leadsTo	yes	Device	Non operational Device
Network	Abnormal behavior	leadsTo	yes	Network	Abnormal behavior
Network	Abnormal behavior	leadsTo	yes	Device	Non operational Device
Network	Scan	leadsTo	yes	Network	Scan
Network	Scan	leadsTo	yes	Device	Indentification
Network	Data exfiltration	leadsTo	yes	Network	Data exfiltration
Building	Physical	locatedIn	yes	Asset	Physical

IPM knowledge management

EBIOS RISK MANAGER

le cnam

BOWTIE

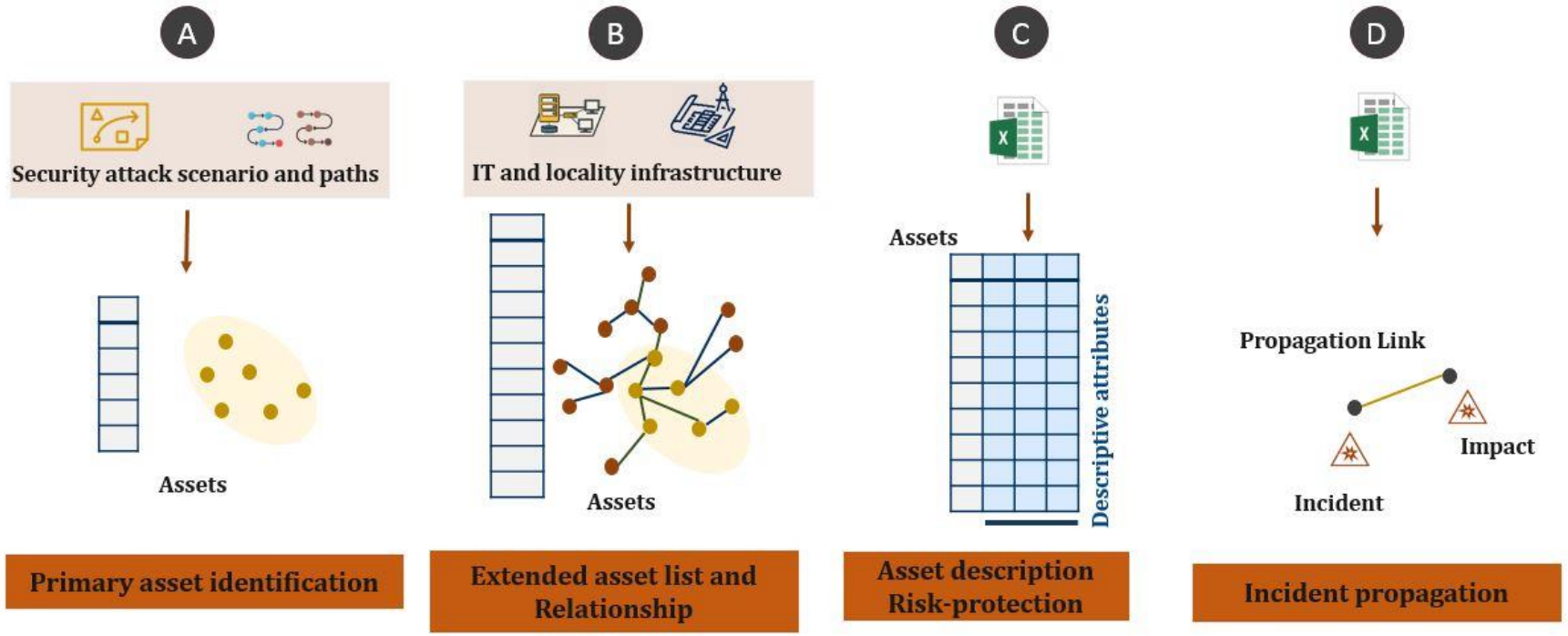


Figure 3 Data Acquisition Methodology Phases

SAFECARE
Integrated cyber-physical security for health services

IPM impacts … to decide

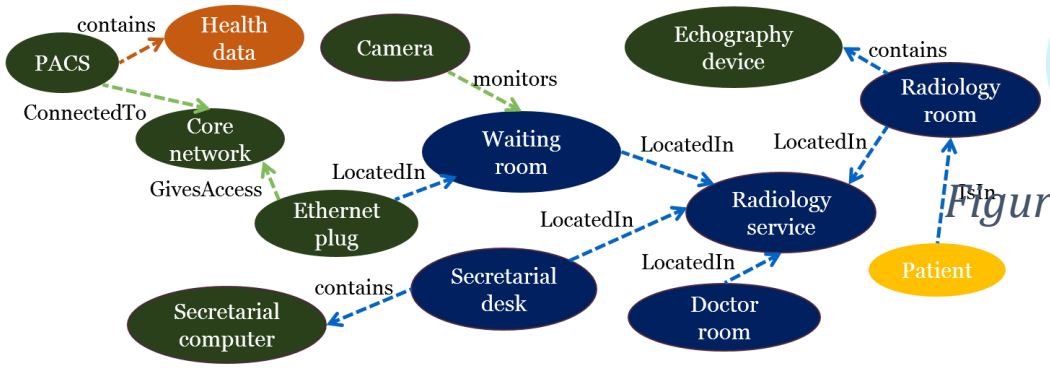


Figure 4 Assets relationships extracted from cyber and physical architectures

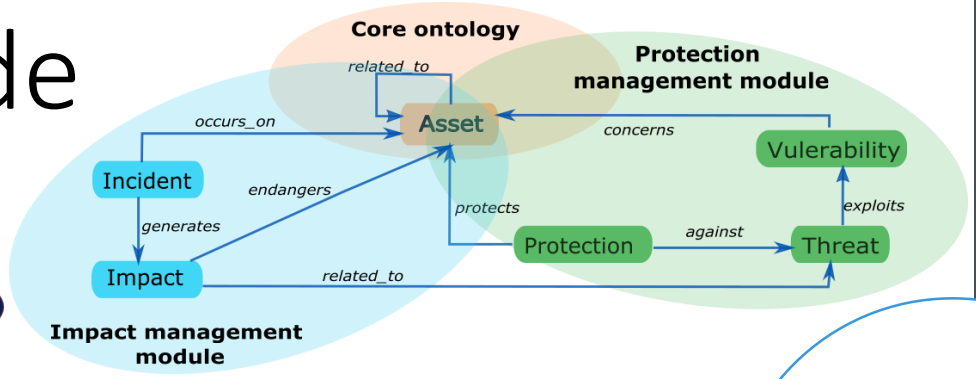


Figure 5 The Modular Structure of the SafecareOnto

Formula

$$impactScore_{th1}(a_t)$$

$$= \begin{cases} 0 \; if \; \exists a_i \in Path(a_s, a_t) \; s.t. \; impactScore_{th2}(a_i) = 0 \\ 1 - \sum_{j=1}^{p} protectionDegree_{th1}^{j}(a_t), otherwise \end{cases}$$

Where $Parh(a_s, a_t)$ is the set of all the assets in the path

Impact Propagation Module

For an effective anticipation, the following knowledge must be acquired:

- Cyber and physical architectures to identify critical assets exposed to threats (scope of damage),
- Risks engendered by the attacker's actions,
- Protecting measures implemented to stop potential attacks or reduce their impacts.

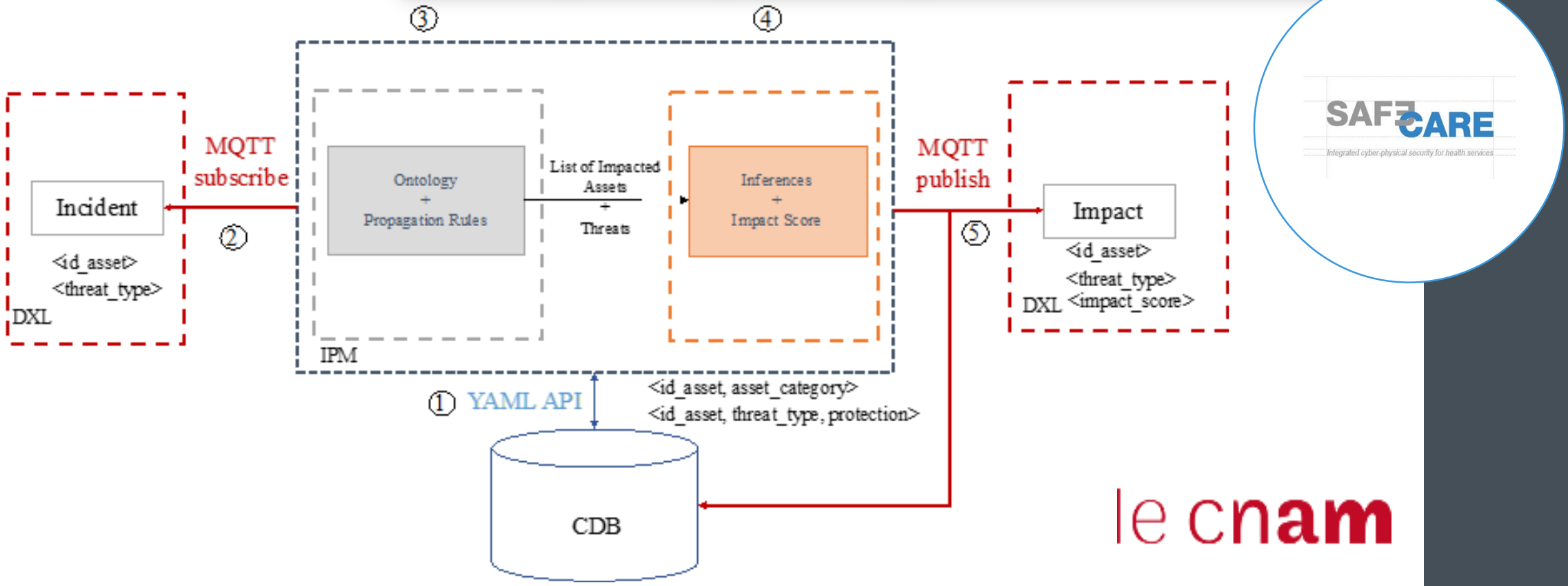
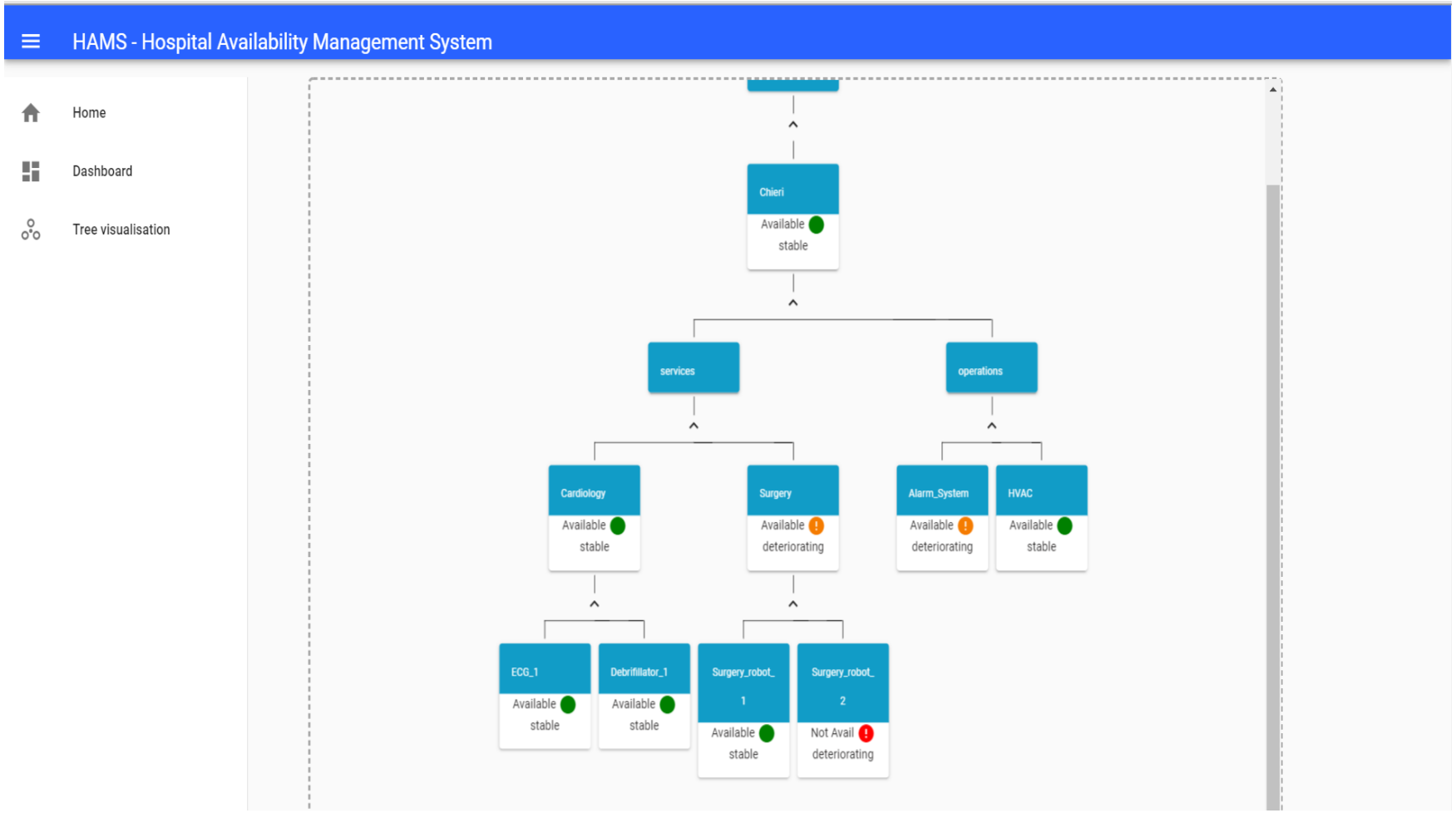


Figure 2 IPDSM module global architecture and interactions with other modules of SAFECARE

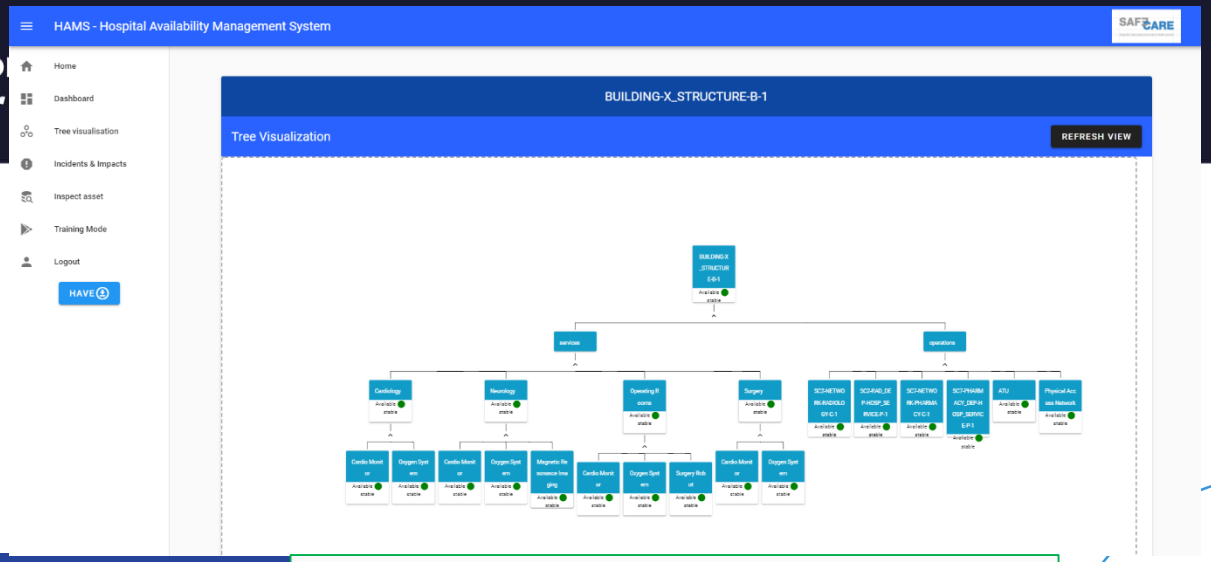
Interfaces for crisis management

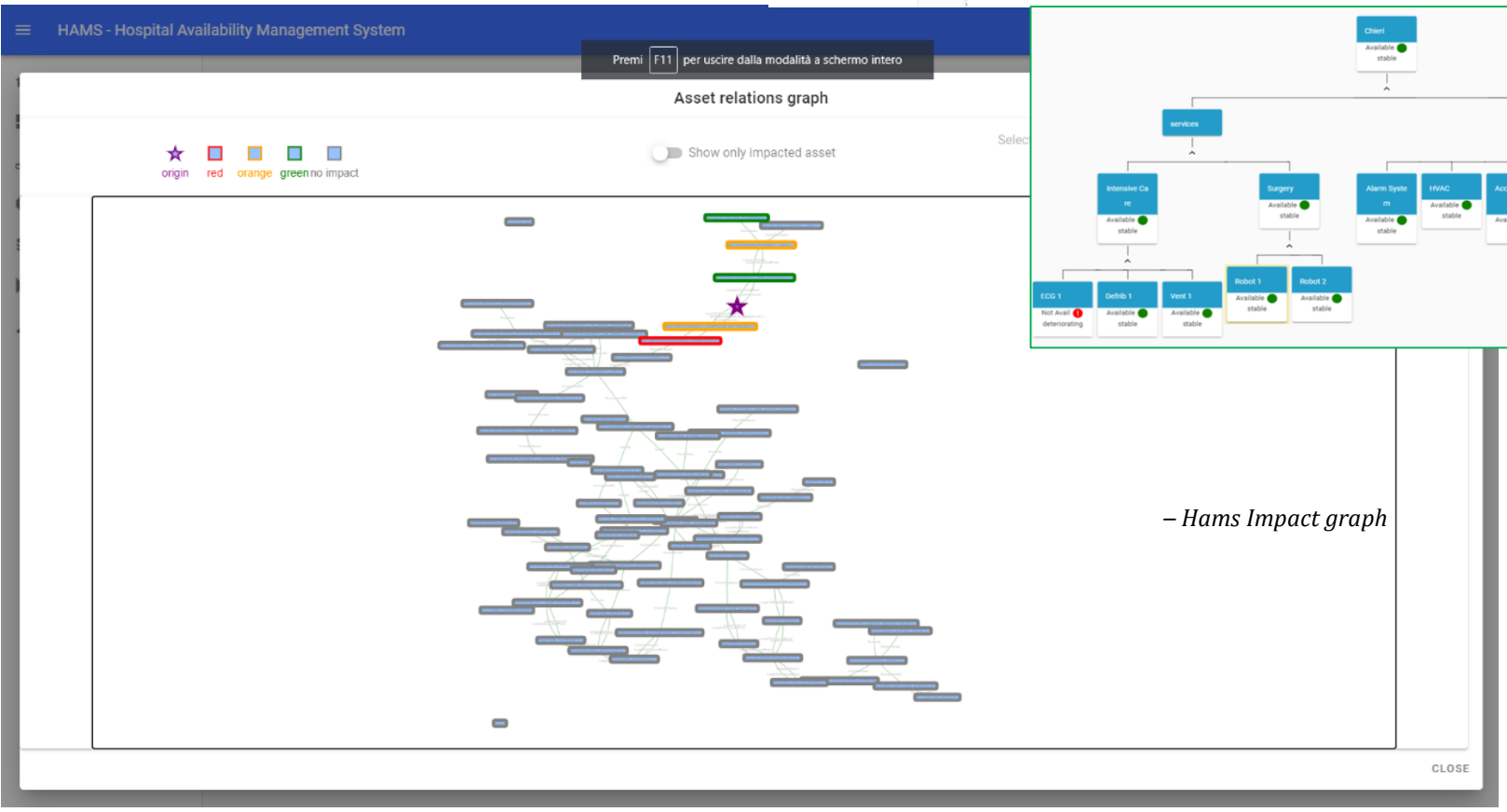
Hospital availability management system



SAFECARE
Integrated cyber-physical security for health services

HAMS interface incidents and impacts





– *Hams Impact graph*

Tests and Demonstration

Test Platform

Cyber Range

SAFECARE
Integrated cyber-physical security for health services

Pilots

Hôpitaux Universitaires de Marseille | ap hm

Marseille

A.S.L. TO5
Azienda Sanitaria Locale di Chieri, Carmagnola, Moncalieri e Nichelino

Turin

amc
Academisch Medisch Centrum
Universiteit van Amsterdam

Amsterdam

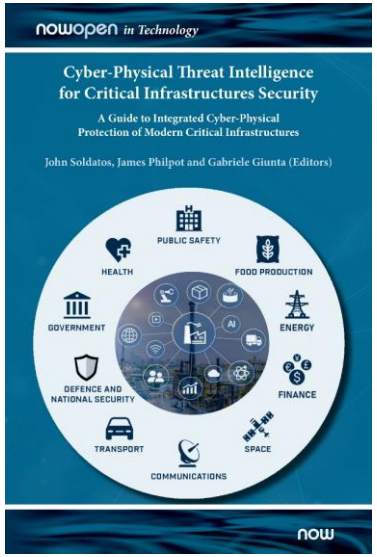
Scientific activities

Focus events organised.

Cyber-Physical Security for Critical Infrastructures Protection

Co-located with ESORICS 2020

Workshop organised in September 2020



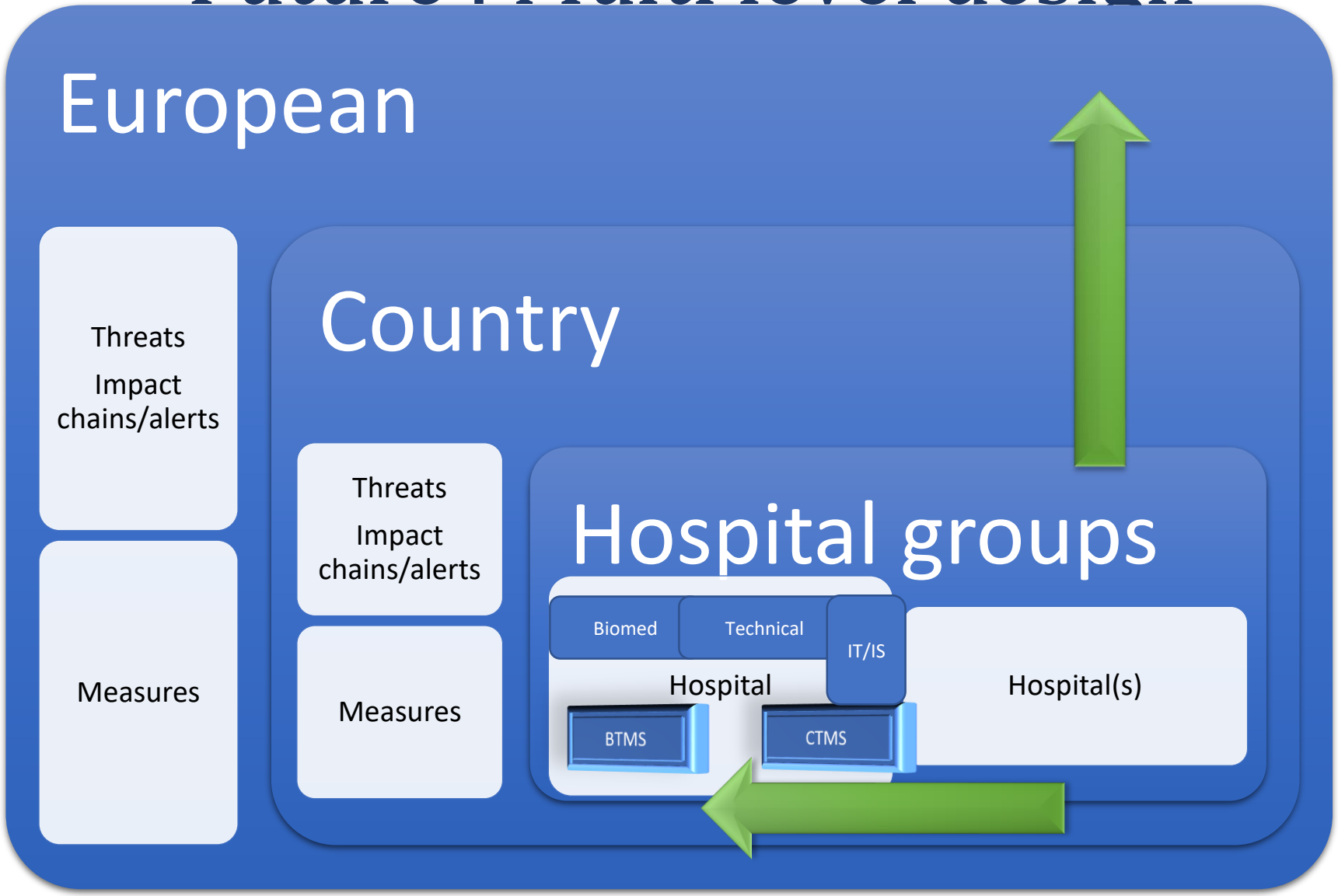
4 chapters written for ECSCI book;
7 open access publications and extra conference proceedings.

Security Incidents in Healthcare Infrastructure during COVID-19 Crisis

Posted on 18 November, 2020 by James Philpot

Website traffic growth.

Future : Multi level design



Suite du projet à l'APHM par étapes

Real time /life use

(4) Vidéosurveillance et sécurité physique

(3) Connexion aux capteurs existants

IPM +HAMS + Module CDB et module DXL (+ TRAS)

(2) Simulation

Module HAMS

Module DXL

Interface développée par l'APHM

À travers l'IPM

CDB adaptée

(1) Training : module de training étendu (12 risques)

Module training

extension aux autres risques et risques spécifiques

APHM inclut la liste des actifs, type d'incident…

Training : module de training existant

Module training

Utilisation du code source du HAMS sous licence

publicly available version:
https://hams-training-mode.s3.eu-west-1.amazonaws.com/index.html#/training

Thank you

More details available on:

- Our website: https://www.safecare-project.eu/
- Twitter: @SafecareP
- -LinkedIn: SAFECARE Project

Philippe.tourron@ap-hm.fr