Integrated cyber-physical security for health services

ECSCI Virtual workshop – 24 June 2020

SAFECARE: Integrated Cyber-Physical Security

Fabrizio Bertone

LINKS Foundation, Turin - ITALY

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

HORIZON 2020

Characteristics of hospitals

- High presence of external persons
  - Support staff (cleaning, food, students)
  - Patients
  - Visitors
- Structures of large size
- Complex ICT systems and devices
  - Support systems and databases
    - HIS hospital information system
    - PACS picture archiving and communication system
    - LIS laboratory information systems
  - Various networks
  - Medical devices (networked)

SAFECARE

Integrated cyber-physical security for health services

Assets

- Highly skilled personnel
- Patients

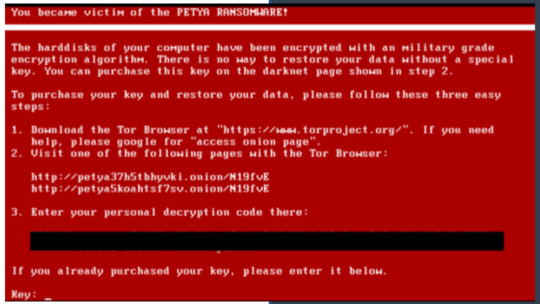
- Valuable equipment
  - Devices, drugs, PPEs

- Valuable data

Threats

- Aggressions
- Kidnapping/Coercion

- Theft
- Vandalism
- Sabotage



```
You became victim of the PETYA RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade
encryption algorithm. There is no way to restore your data without a special
key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy
steps:

1. Download the Tor Browser at "https://www.torproject.org/". If you need
   help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

   http://petya37h5tbhyvki.onion/N19fvE
   http://petya5koahtsf7sv.onion/N19fvE

3. Enter your personal decryption code there:

   [redacted]

If you already purchased your key, please enter it below.

Key: _
```

- Unauthorized access
  - Data breach
- Destruction/modification
  - ransomware

Motivations for integrated security system

- Updated knowledge of the global status
- Links between assets of different domains
- Cyber-Physical “kill chains”

SAFECARE Methodology and Approach

- Threat analysis, Risk assessment

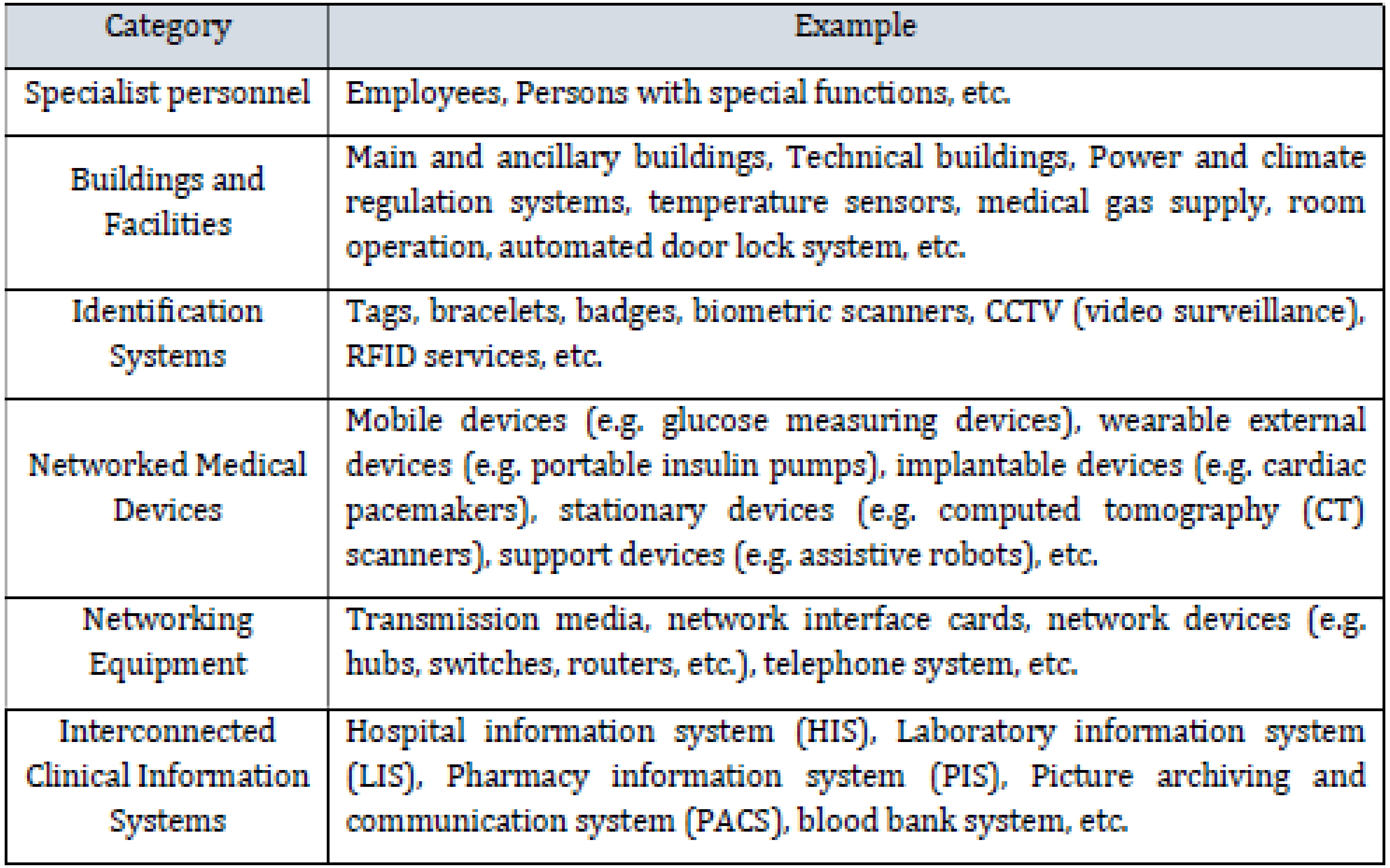
- Attack scenarios definition
- Integrated architecture, communication and storage

SAFECARE
Integrated cyber-physical security for health services

- Impact propagation
- Holistic view and management

- Information sharing

Hospital assets categories sample



Category	Example
Specialist personnel	Employees, Persons with special functions, etc.
Buildings and Facilities	Main and ancillary buildings, Technical buildings, Power and climate regulation systems, temperature sensors, medical gas supply, room operation, automated door lock system, etc.
Identification Systems	Tags, bracelets, badges, biometric scanners, CCTV (video surveillance), RFID services, etc.
Networked Medical Devices	Mobile devices (e.g. glucose measuring devices), wearable external devices (e.g. portable insulin pumps), implantable devices (e.g. cardiac pacemakers), stationary devices (e.g. computed tomography (CT) scanners), support devices (e.g. assistive robots), etc.
Networking Equipment	Transmission media, network interface cards, network devices (e.g. hubs, switches, routers, etc.), telephone system, etc.
Interconnected Clinical Information Systems	Hospital information system (HIS), Laboratory information system (LIS), Pharmacy information system (PIS), Picture archiving and communication system (PACS), blood bank system, etc.

Threat and vulnerability landscape

Threats

Cyber attacks:

- Social engineering
- Spear phishing
- Malware
- RATs
- DDoS
- Vulnerability exploits

Physical attacks:

- Intrusion
- Aggression
- Material destruction
- Bombing
- Manmade fire

Natural hazards:

- Flood
- Earthquake
- Storm

Targets

- Building
- Power supply
- Air cooling system
- Water heating system
- Patients data
- IT systems
- Medical devices
- Health practitioners
- Patients and population

…

Motives

- Political
- Terrorism
- Harm
- Financial
- Intelligence
- Reputation damage

Vulnerabilities

Cyber vulnerabilities:

- Application &OS vulnerabilities
- Control Gaps & Design Flaws
- Unpatched devices
- Weak credential
- Lack of cyber threat prevention
- Lack of cyber threat detection
- Lack of security policy

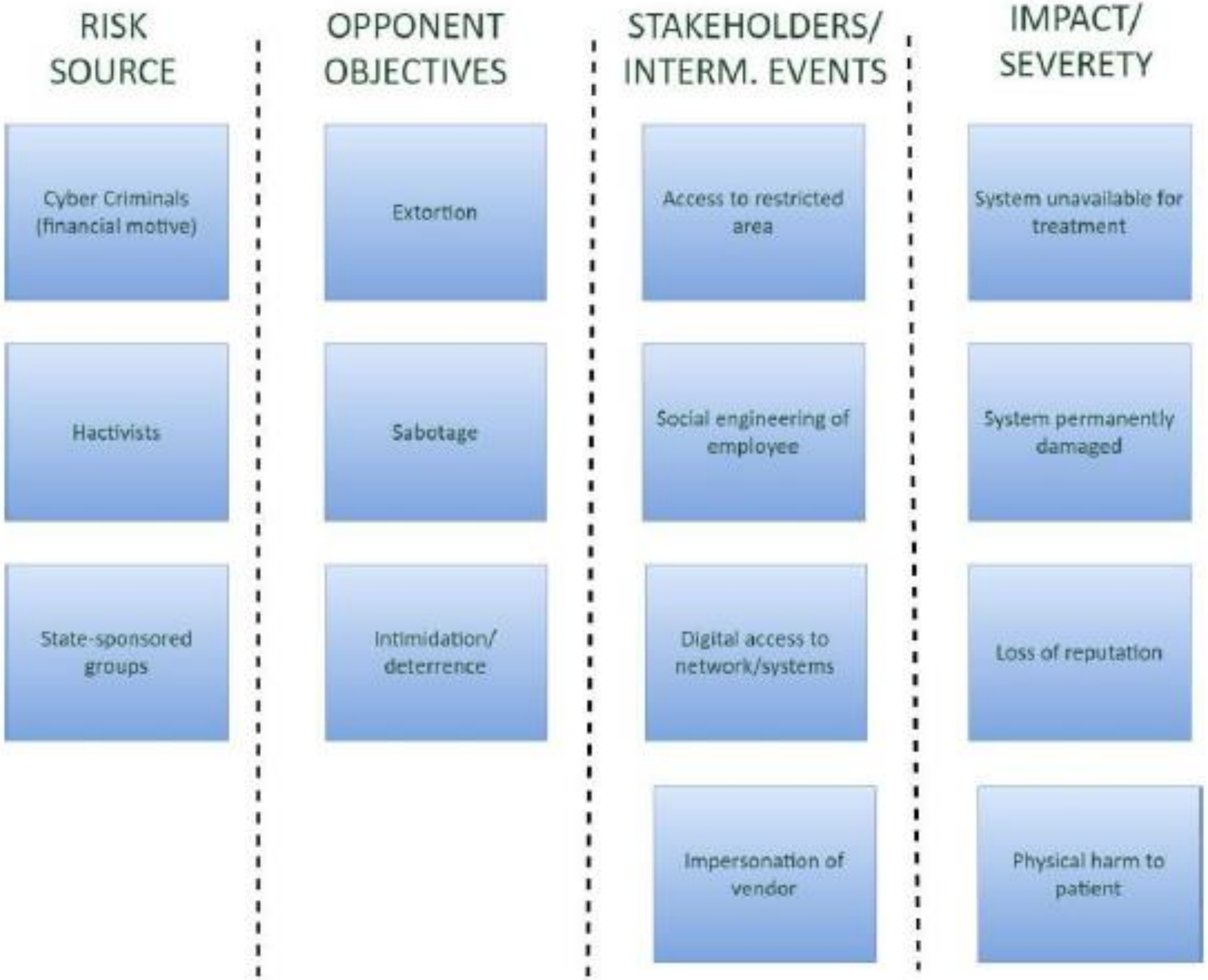
Physical vulnerabilities:

- Lack of access management
- Lack of video monitoring
- Lack of fire detection
- Lack of smart sensors
- Lack of security agents
- Lack of security policy
- Lack of collaboration with police and firefighters

SAFECARE

Integrated cyber-physical security for health services

Strategic Scenario Example [1]



RISK SOURCE

- Cyber Criminals (financial motive)
- Hactivists
- State-sponsored groups

OPPONENT OBJECTIVES

- Extortion
- Sabotage
- Intimidation/ deterrence

STAKEHOLDERS/ INTERM. EVENTS

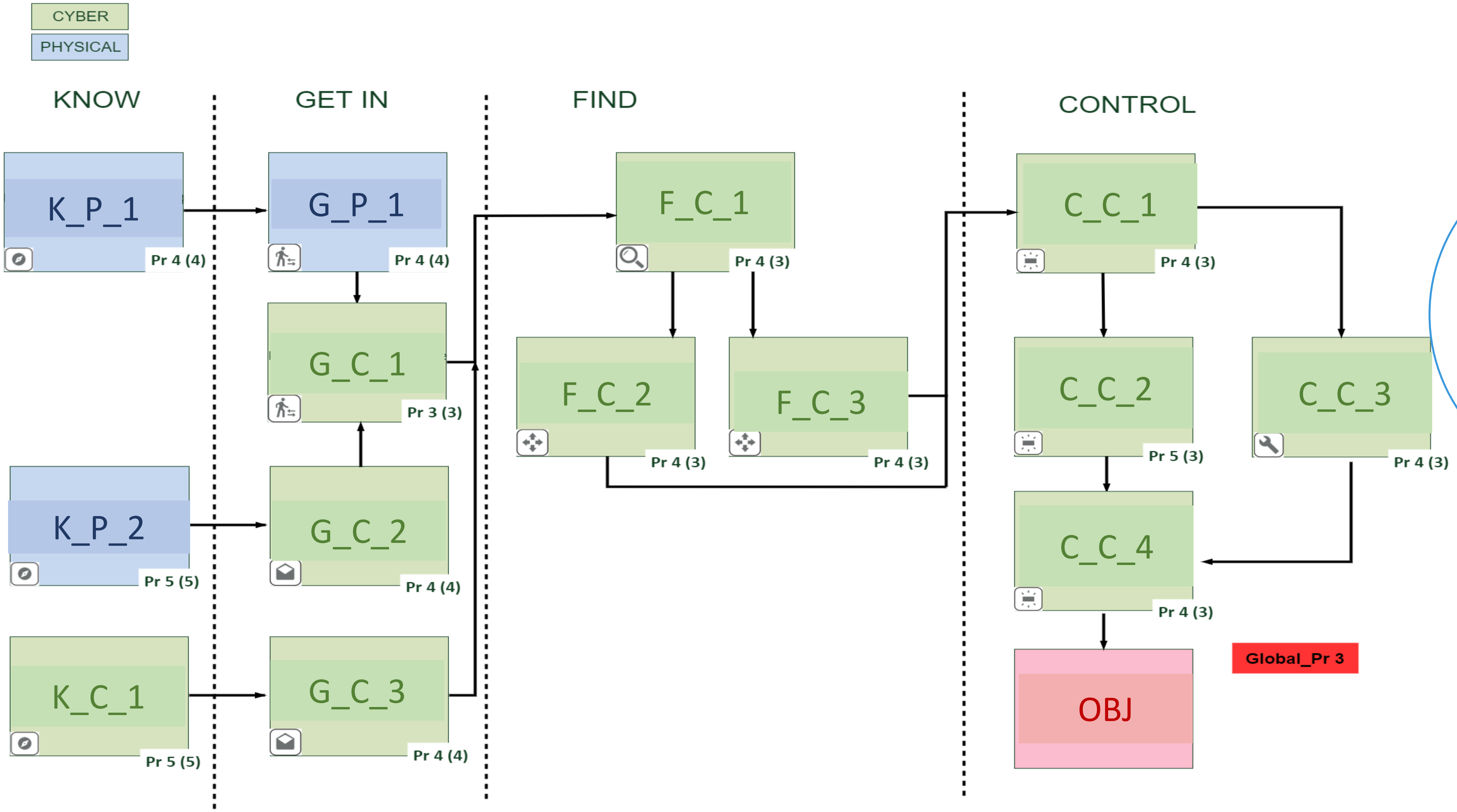
- Access to restricted area
- Social engineering of employee
- Digital access to network/systems
- Impersonation of vendor

IMPACT/ SEVERETY

- System unavailable for treatment
- System permanently damaged
- Loss of reputation
- Physical harm to patient

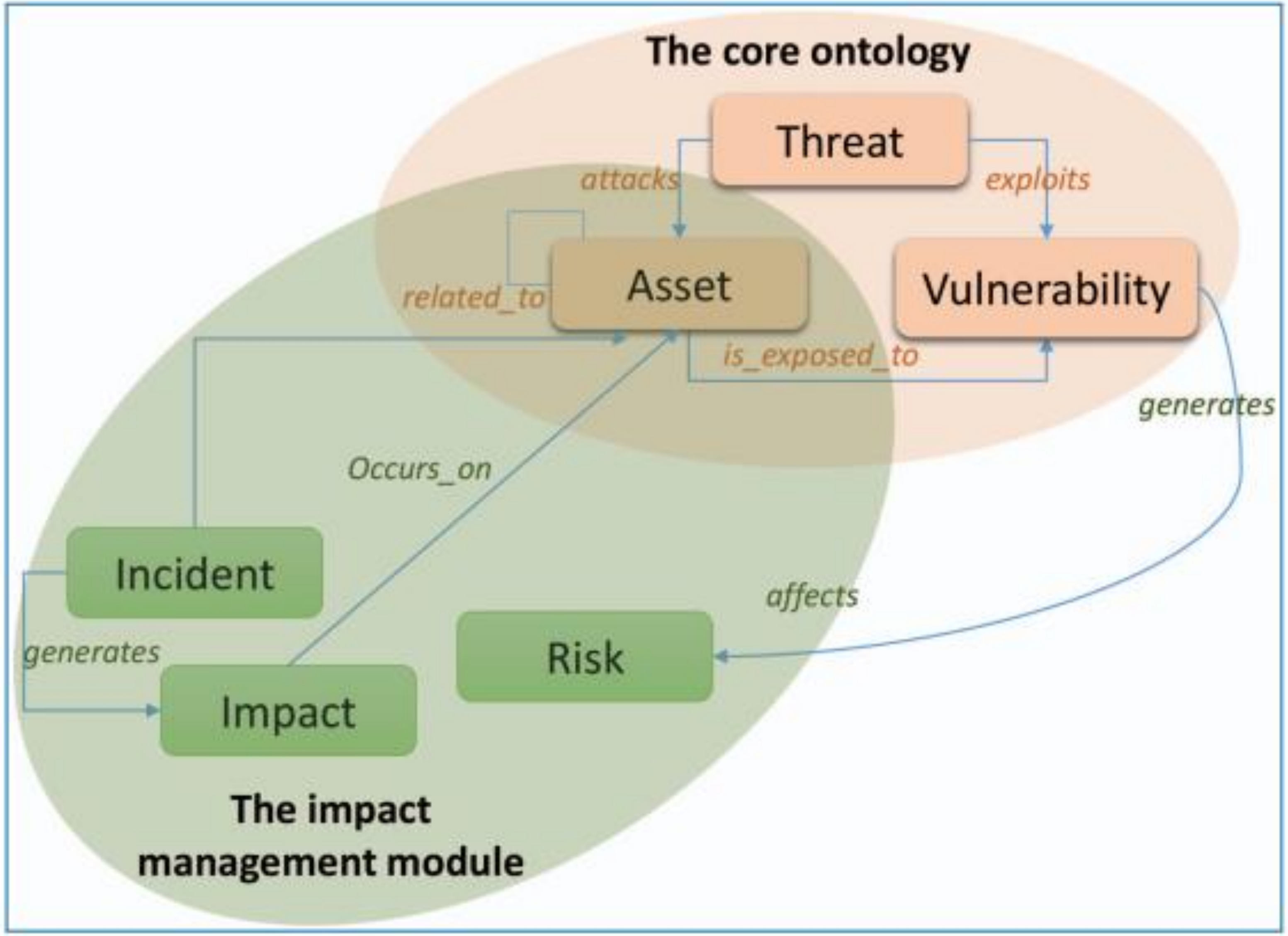
SAFECARE
Integrated cyber-physical security for health services

Attack Technical Scenario Example (KC)

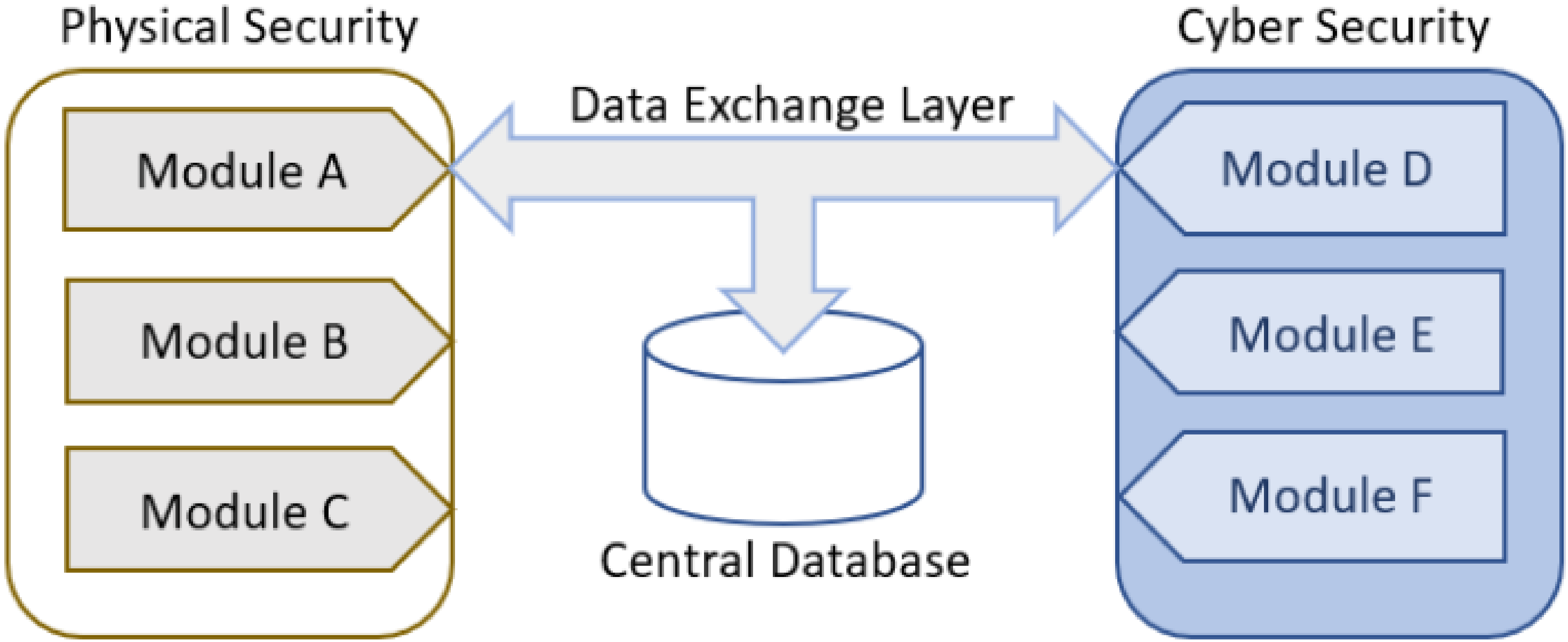


SAFECARE
Integrated cyber-physical security for health services

SAFECARE Ontology [2]



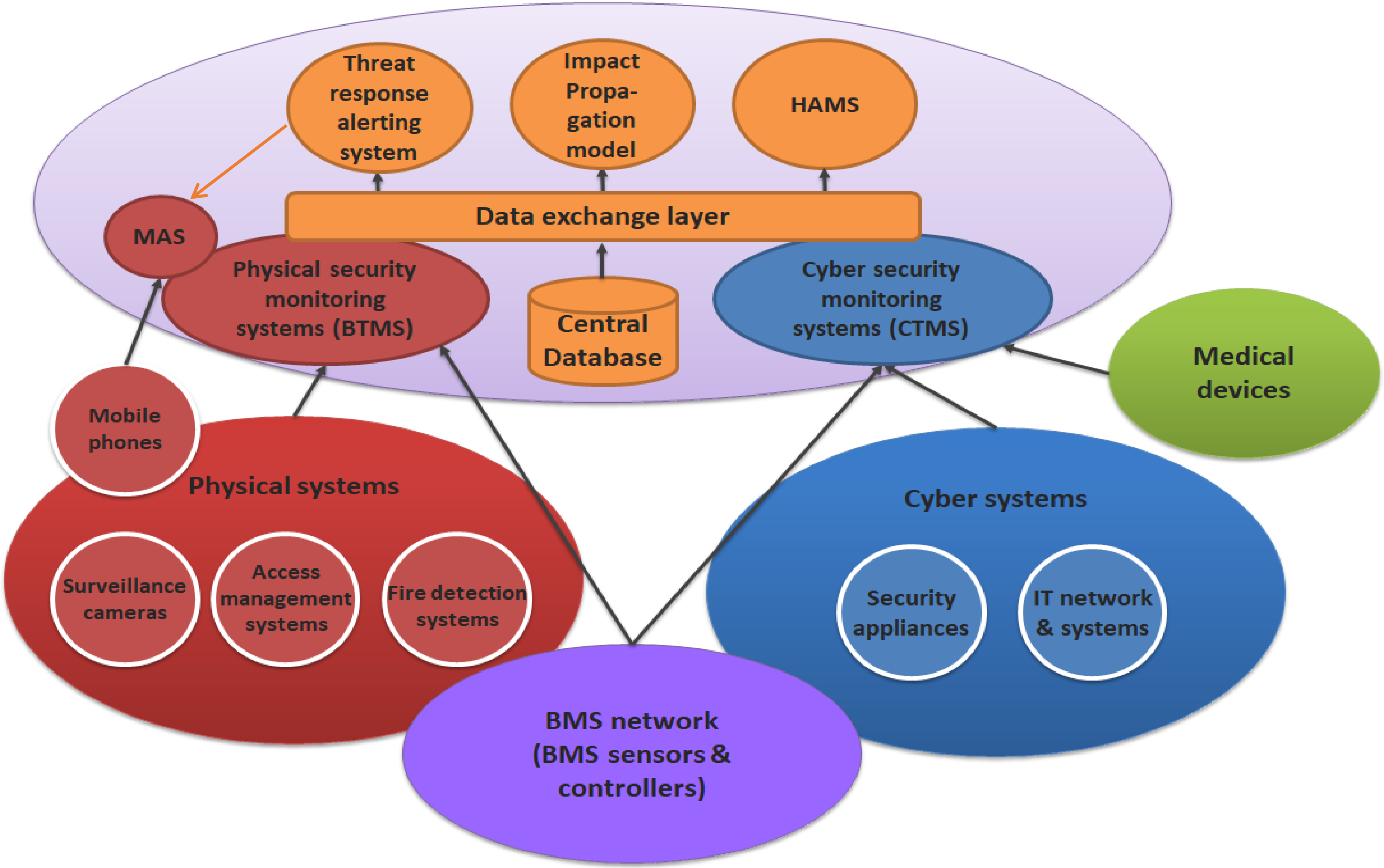
High-level Architecture for Integration



SAFECARE

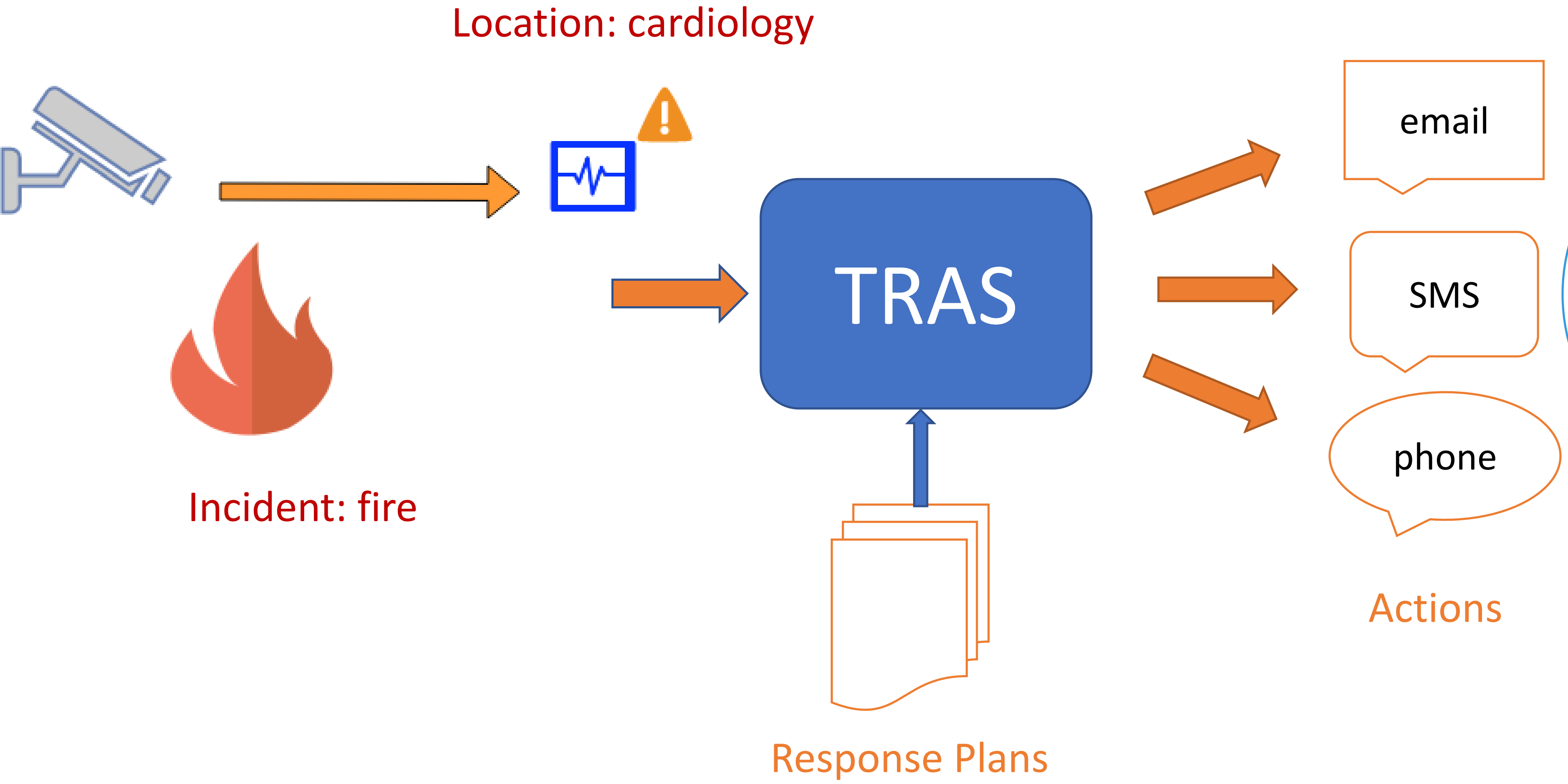
Integrated cyber-physical security for health services

SAFECARE Global Architecture [3]


Threat response alerting system
Impact Propa-gation model
HAMS
MAS
Data exchange layer
Physical security monitoring systems (BTMS)
Central Database
Cyber security monitoring systems (CTMS)
Medical devices
Mobile phones
Physical systems
Surveillance cameras
Access management systems
Fire detection systems
Cyber systems
Security appliances
IT network & systems
BMS network (BMS sensors & controllers)

SAFECARE
Integrated cyber-physical security for health services

Threat Response Alerting System



Location: cardiology

Incident: fire

TRAS

email

SMS

phone

Actions

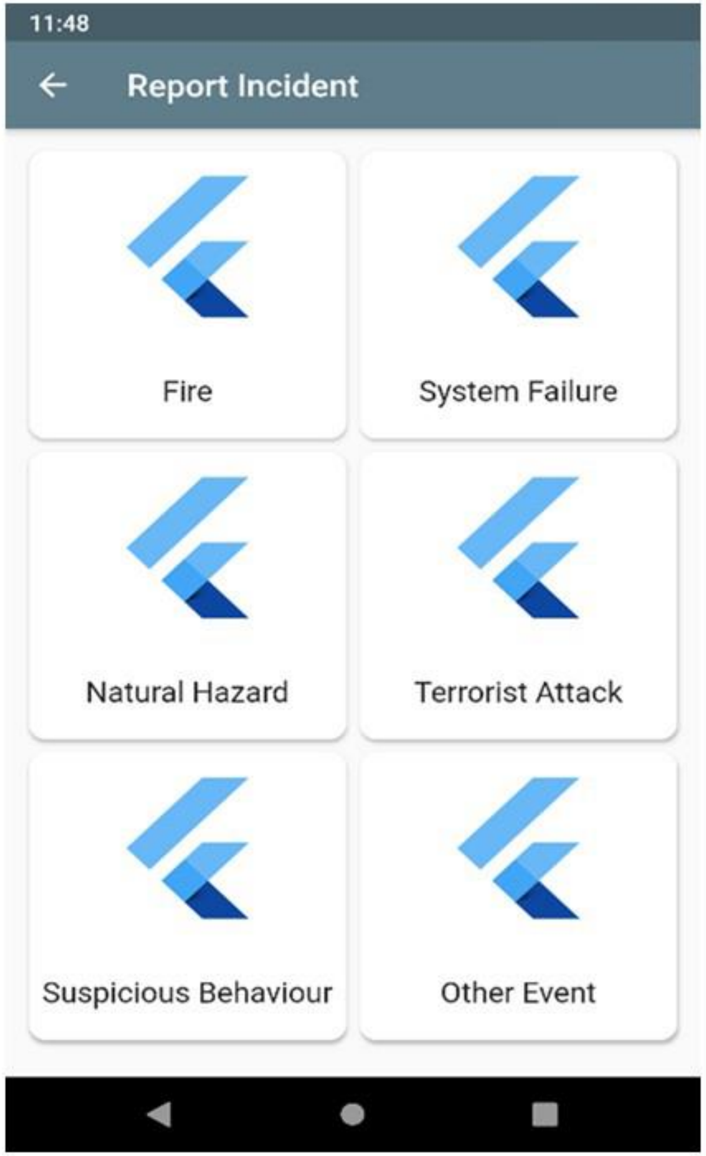
Response Plans

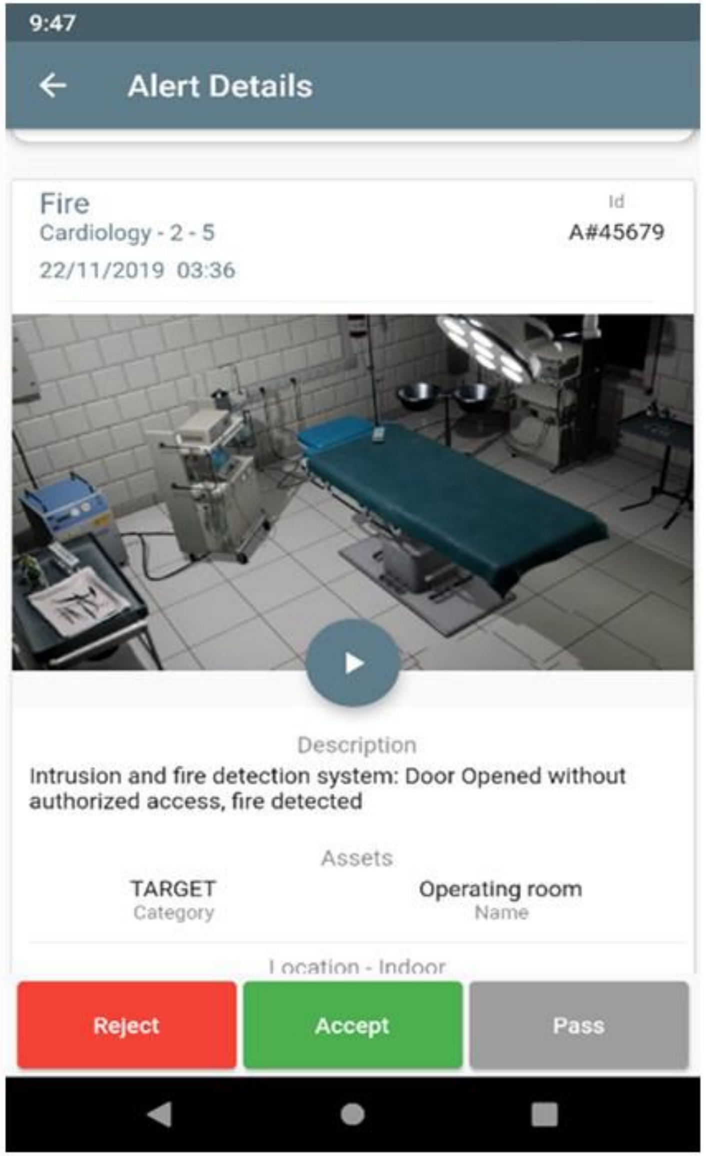
SAFECARE

Integrated cyber-physical security for health services

Mobile Alerting System [3]

REPORTING





Fire
Cardiology - 2 - 5
22/11/2019 03:36

Id
A#45679

Description
Intrusion and fire detection system: Door Opened without authorized access, fire detected

Assets

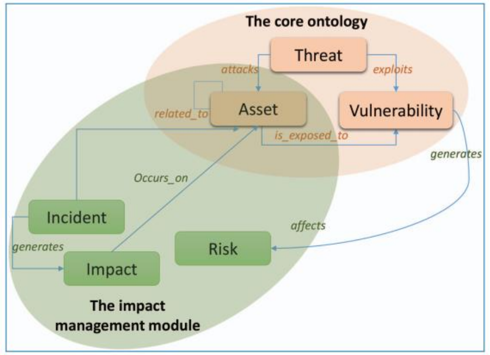
TARGET	Operating room
Category	Name

Location - Indoor

VALIDATION

Impact Propagation

Location: cardiology



Initial event of: fire incident

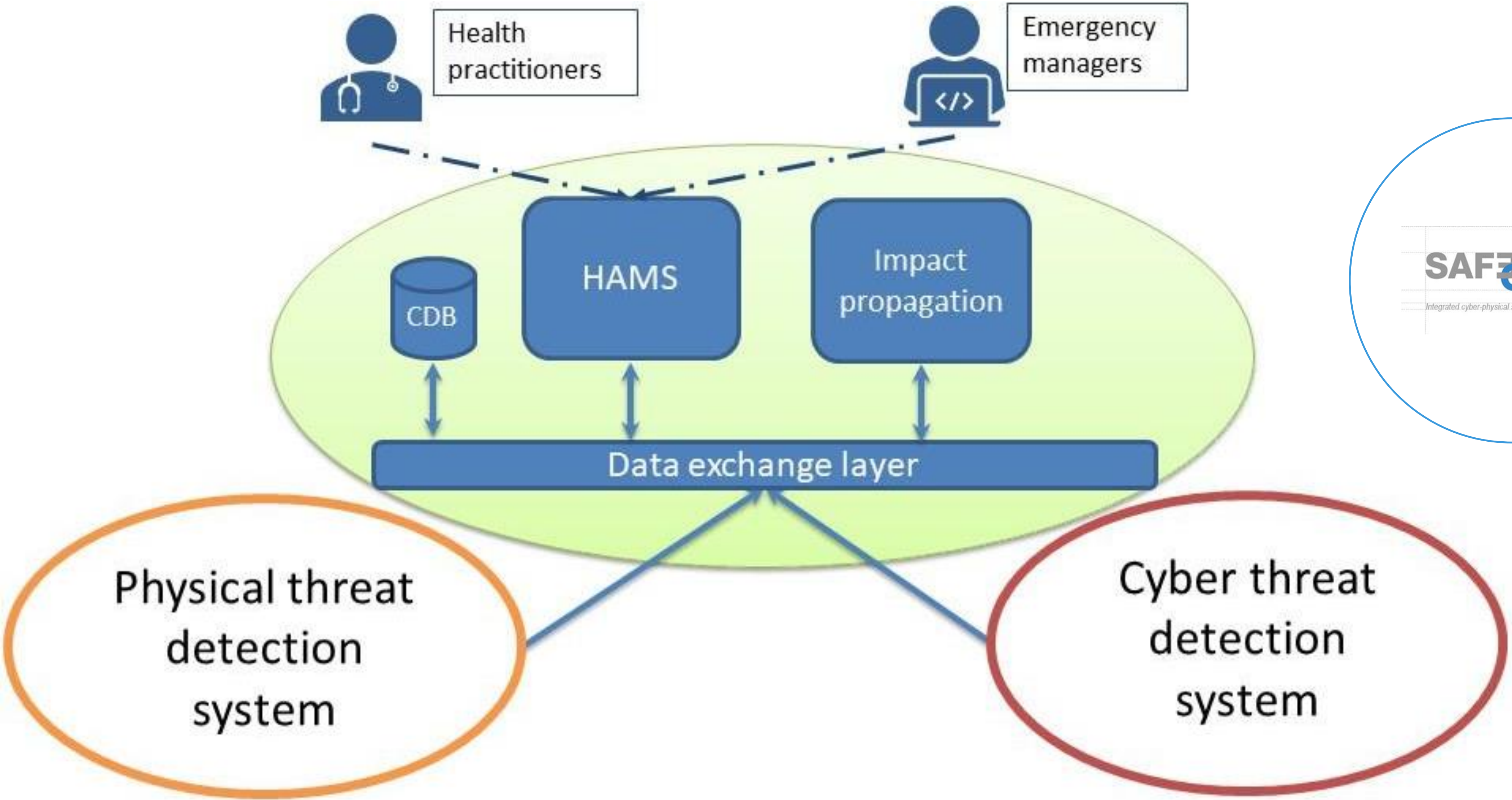
Assets relationship analysis

SAFECARE

Integrated cyber-physical security for health services

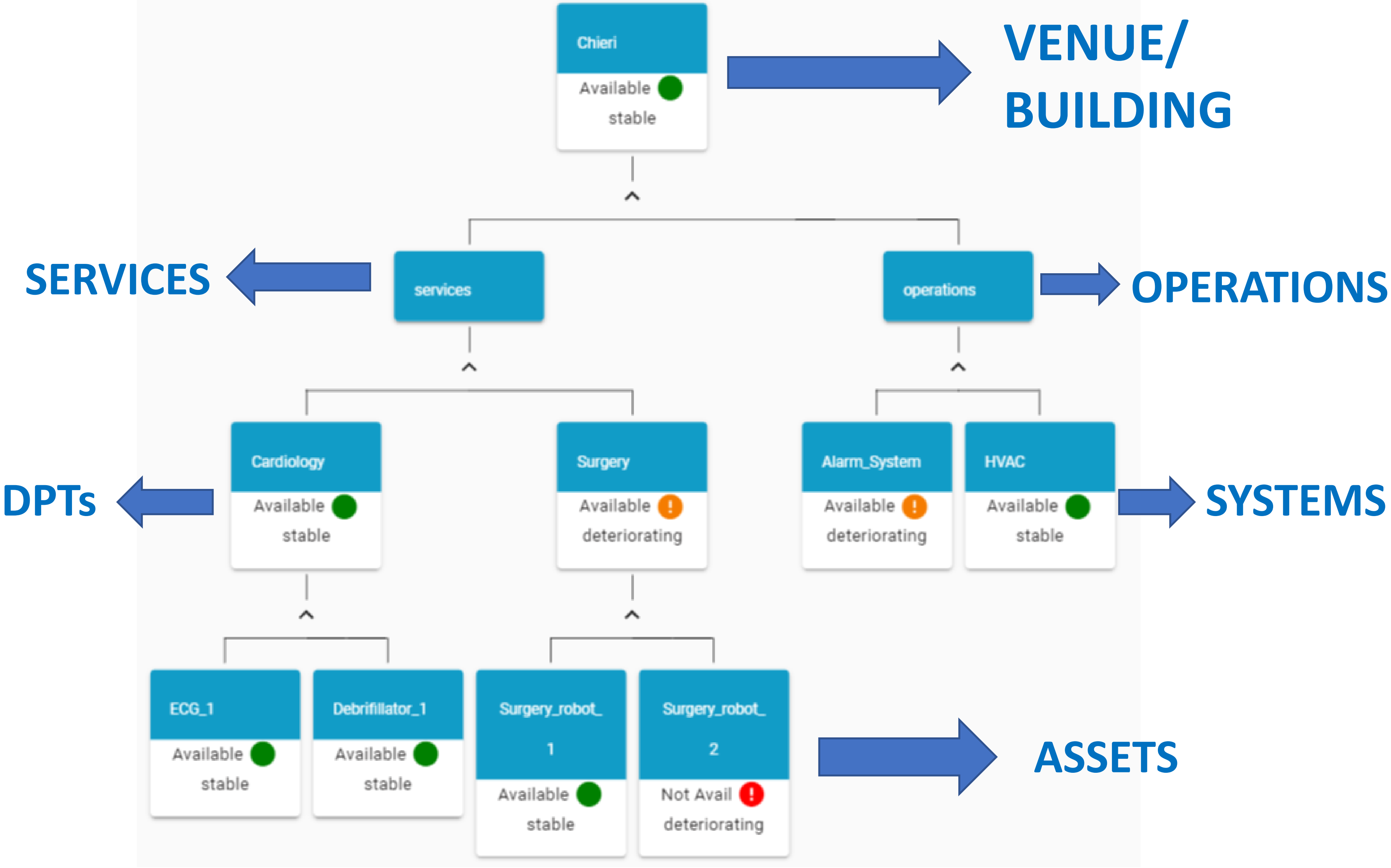
Cascading Impacts Propagation

Hospital Availability Management System [4]



SAFECARE
Integrated cyber-physical security for health services

Assets graph view



VENUE/ BUILDING

SERVICES

OPERATIONS

DPTs

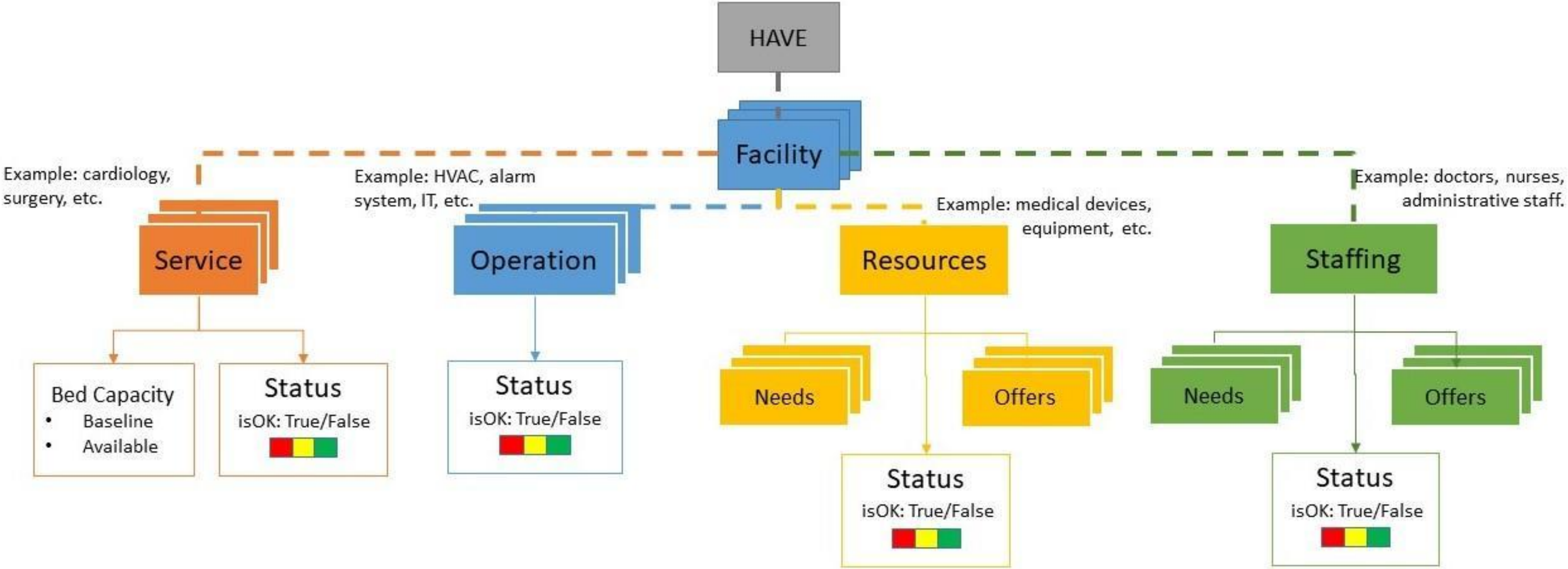
SYSTEMS

ASSETS

SAFECARE

Integrated cyber-physical security for health services

Interoperable Information Sharing [4]



HAVE

Facility

Example: cardiology, surgery, etc.

Example: HVAC, alarm system, IT, etc.

Example: medical devices, equipment, etc.

Example: doctors, nurses, administrative staff.

Service

Operation

Resources

Staffing

Bed Capacity

- Baseline
- Available

Status

isOK: True/False

🟥🟨🟩

Status

isOK: True/False

🟥🟨🟩

Needs

Offers

Status

isOK: True/False

🟥🟨🟩

Needs

Offers

Status

isOK: True/False

🟥🟨🟩

Conclusions

- Hospitals are complex environments
  - Not always easy to monitor security
- Criminals target specifically hospitals, especially during crisis
- Holistic knowledge increases threats detection and decrease reaction time
- Data sharing is key in emergency situations

SAFECARE

Integrated cyber-physical security for health services

References

1. Eva Maia et al. 2020. “Security Challenges for the Critical Infrastructures of the Healthcare Sector” *
2. Faten Atigui et al. 2020. “Vulnerability and Incident Propagation in Cyber-physical Systems” *
3. Fabrizio Bertone et al. 2020. “Integrated Cyber-physical Security Approach for Healthcare Sector” *
4. Francesco Lubrano et al. 2020. “HAMS: An Integrated Hospital Management System to Improve Information Exchange”. CISIS 2020

* in “_Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated CyberPhysical Protection of Modern Critical Infrastructures_”

SAFECARE

Integrated cyber-physical security for health services

https://www.safecare-project.eu/

@SafecareP

SAFECARE Project

Fabrizio Bertone

Researcher @ LINKS Foundation

Fabrizio.Bertone@linksfoundation.com