Semantic-Based Approach for Cyber-Physical Cascading Effects Within Healthcare Infrastructures

Fatma-Zohra Hannou, Mohamad Rihany, Nadira Lammari, Faycal Hamdi, Nada Mimouni, Faten Atigui, Samira Si-Said Cherfi, Philippe Tourron

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 3, 2022, accepted April 19, 2022, date of publication April 29, 2022, date of current version May 23, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3171252

Semantic-Based Approach for Cyber-Physical Cascading Effects Within Healthcare Infrastructures

FATMA-ZOHRA HANNOU[1], MOHAMAD RIHANY[1], NADIRA LAMMARI[1], FAYÇAL HAMDI[1], NADA MIMOUNI[1], FATEN ATIGUI[1], SAMIRA SI-SAID CHERFI[1], AND PHILIPPE TOURRON[2]

[1]Laboratoire CEDRIC, Conservatoire National des Arts et Métiers, 75003 Paris, France
[2]Assistance Publique-Hôpitaux de Marseille, 13005 Marseille, France

Corresponding author: Fatma-Zohra Hannou (hannoufatmazohra@gmail.com)

This work was supported by the EU H2020 project SAFECARE—Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe, under the grant agreement 787002.

ABSTRACT This paper presents a framework for integrated cyber-physical security propagation study within critical infrastructures (hospitals use case). The framework includes an ontology for the semantic modeling of cyber-physical security. The impact propagation approach relies on propagation rules inferring the cascading effects of security incidents occurring in hospitals. An impact score module allows evaluating impacts' severity, considering implemented protection measures. This work is part of the European project SAFECARE, which provides a set of tests and demonstration sessions in partnership with 3 hospitals in Europe. During these tests, we measured effectiveness and efficiency metrics, as well as end users' satisfaction feedback. Experiments performed on real attack scenarios, show high effectiveness rates and a common agreement from end-users about the added value of the solution to enhance risks analysis practice and increase hospitals mitigation strategies efficiency.

INDEX TERMS Critical infrastructure, cyber-physical security, impact propagation, ontologies, semantic modeling.

I. INTRODUCTION

A. GENERAL CONTEXT

Critical infrastructures (CI) are of growing complexity since they are increasingly integrating Operational Technology equipment and the internet of things (IoT) devices. In parallel, sophisticated attacks continue to rise in frequency and effectiveness, exploiting the CI cyber systems vulnerabilities and spreading afterward to the physical ones (or vice-versa). If not mastered at the right time, these attacks can have detrimental effects on the hospital's patient care mission. Therefore, to ensure reliable service delivery and to be confident in their business continuity, hospitals must ensure effective management of their cyber and physical security.

Hospital risks are generally associated with various threats. The European Commission reported in [1] a generic classification of threats targeting critical infrastructures. It distinguishes natural hazards (floods, severe weather, wild/forest fires, earthquakes, pandemics/epidemics, livestock epidemics) from non-malicious man-made hazards (industrial accidents, nuclear/radiological accidents, transport accidents, loss of critical infrastructure) and malicious man-made hazards (those related to Cyber and terrorist attacks). Moreover, authors in [2] distinguish cyber-only attacks from physical-enabled cyber attacks and physical-only attacks from cyber-enabled physical attacks. They define the latter as physical attacks involving cyber activities and the first as a cyber-attack in which an attacker gains physical access to an on-site location from which the cyber-attack is then launched. In this paper, we are only concerned with deliberate threats (malicious man-made hazards) that exploit one or many vulnerabilities to trigger cyber and/or physical attacks leading to risks. When a cyber or physical attack (incident) occurs, it may provoke far-reaching cascading effects throughout the entire critical infrastructure, which need to be identified and estimated to ensure precise risk management [3]. Many critical assets could be compromised, and measures put in place to protect them could fail.

The associate editor coordinating the review of this manuscript and approving it for publication was Diana Gratiela Berbecaru.

This situation might cause harm, perceived as ''injuries or damages to people's health, or damage to property or the environment''.[1]

To increase situational awareness and ensure a quick and effective response to incidents and their cascading effects, hospitals must first have a comprehensive inventory of their critical assets and record their profiles, including their interconnections. The response to this requirement help, through risk analysis, to comprehend the nature of risks and to determine their magnitude. Hospitals must also have an integrated security solution for the prevention, detection, and response to incidents, whether they are cyber, physical, or a combination of both. These requirements are part of the requirements of the European project SAFECARE [2] in which the contribution of this paper fits. As an indication, this project brings together 20 partners from 10 different EU countries (industrial, academics, and governmental organizations), including 3 hospitals as end-users and demonstration sites for the produced solution. Thus, the work presented in this paper is a contribution to the SAFECARE objectives. It first consists of an ontology, named SafecareOnto, for a uniform representation and description of critical healthcare assets and their dependencies. This ontology is used to simulate the potential impact propagation of an incident under an impact propagation process we conceived and implemented. This process, named IPDSM (the Impact Propagation and Decision Support Model), provides the assets impacted by the incident and by those derived from the cascading effect, and the impact score of the incidents on the assets. This process, which is a cornerstone of the SAFECARE tool, serves for the triggering of the threat response process and feeds the process that gives information about the hospital availability status (Availability Management System).

This paper is organized as follows. The motivating example in Section I-B introduces a near-real attack scenario used to illustrate the different parts of the framework along the paper. Section II describes the ''SafecareOnto'' ontology, its building approach, formalization and related knowledge base. The semantic-based propagation model is explained in Section III. Since our solution is developed within the SAFECARE project, Section IV-A shows the global architecture of the project's modules and their communications. Section V reports main results of tests and demonstration sessions performed in the framework of the project. Research works related to security semantic modeling and propagation study approaches are discussed in Section VI. We conclude in Section VII, with a summary of contributions and future work.

B. MOTIVATING EXAMPLE

The following use case details a near-real cyber-physical attack scenario used to illustrate the research problem since real project data and scenarios cannot be revealed (confidentiality reasons). Figure 1 illustrates the different steps of the attack scenario.

During the ''COVID-19'' health crisis, the hospital dedicates part of its infrastructure to the vaccination campaign, which mobilizes medical staff to carry out vaccines and requires particular logistics. With malicious purpose, an attacker contacts a hospital staff member to identify his email address (step 1). Then, he sends a spear phishing email to break into the hospital's information system (step 2). Then, the attacker accesses the appointment scheduling system to modify the appointment planning and set them at one date `DD` and hour (step 3). Many patients gather in the hospital on the chosen day `DD`, claiming their vaccination, with the received phone confirmation. The attacker joins the crowd (step 4). Taking advantage of the situation, the attacker steps near the pharmacy to spy on the nurse when she types the security access code (step 5). The attacker enters the pharmacy (step 6), accesses the freezer, and steals the vaccines carrying them out in an isothermal backpack (step 7). Before leaving the hospital (step 9), the attacker attempts to erase his traces and create a diversion by lighting a fire (step 8). Since the pharmacy room is near to the technical room hosting the power supply device, the fire initiates a power cut in the entire hospital sector.

This attack's direct consequences are the theft of the hospital's vaccine stock and fire on the hospital's localities. The theft of the vaccine leads to a significant financial loss and the patient vaccination campaign's stopping, which seriously harms the hospital's reputation. It contributes to delaying the health crisis's release, with significant challenges, such as hospital resources unavailability, the scheduling of operations, etc. Besides, the fire can propagate to multiple localities in the hospital, threatening the lives of patients and employees. The attacker's actions lead to a series of indirect impacts, such as the non-availability of the hospital's information system following the cyberattack, the stopping of the care process, the theft of drugs from the pharmacy, or the power cut.

II. SafecareOnto, SEMANTIC MODELING

A. THE MODULAR ONTOLOGY

Several definitions of ontology exist, but only one predominates in the information system field. In [4], Gruber defines an ontology as an explicit specification of a conceptualization (an abstract representation of the world intended to represent).

The ontology ''SafecareOnto'' has been first designed as a modular ontology with three sub-ontologies (modules in the ontology engineering terms): a central ontology named `Asset ontology` and two related sub-ontologies `protection` and `impact` [5]. Each module supports one task dimension: The impact propagation task aims at determining the cascading effects resulting from an incident occurrence. This requires knowledge about the potential threats and how incidents evolve to impacts. On the other side, SAFECARE considers the presence of countermeasures to

[1] ISO 14971:2019

[2] https://www.safecare-project.eu/

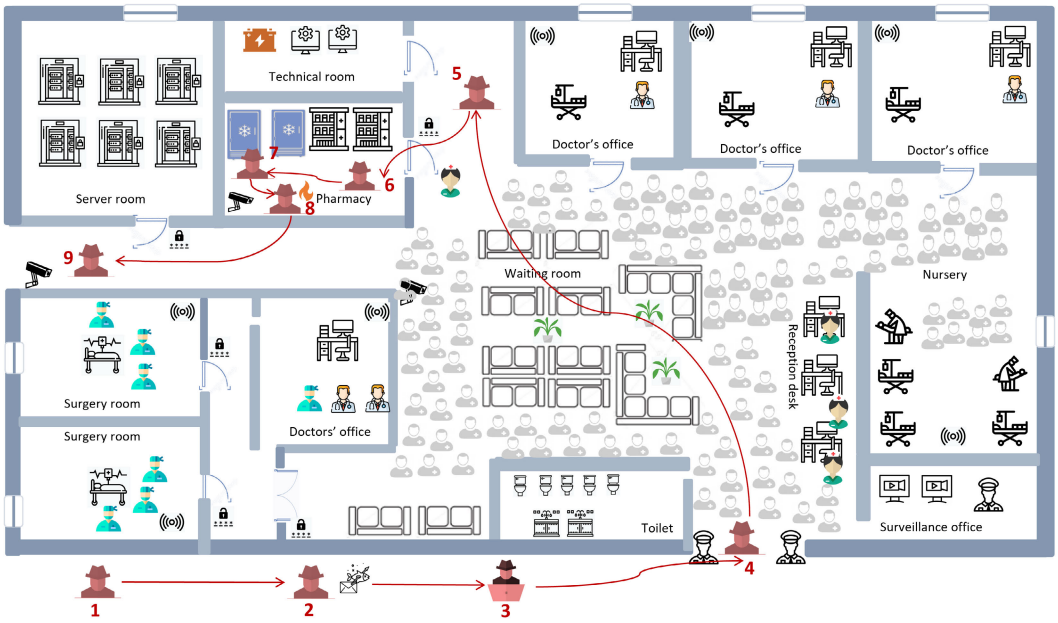

FIGURE 1. Steal "COVID-19" vaccine: the attacker path.

attenuate or eliminate incidents, which requires the solution to handle the implemented protection strategies for reducing asset vulnerabilities. The protection module manages this knowledge.

To create and refine this high-level modular ontology, we adopt a ''from scratch'' approach with a bottom-up fashion. This building technique allows formalizing partner experts' knowledge and fitting the propagation task. We drew on scenarios 1, 2, and 7 of the Neon methodology [6] and followed an incremental, iterative process. Existing semantic resources and standards were used to feed threats and protection modeling for better reusability and genericity. This section describes ''SafecareOnto'' following three steps: knowledge acquisition, formalization, and knowledge base creation. Further in Section IV-A, the implementation of the ontology is discussed within the internal architecture part.

B. KNOWLEDGE ACQUISITION

The knowledge acquisition phase is crucial for collecting the data required during the ontology design and population. The SAFECARE project gave the ground for a direct acquisition process from cyber-physical security experts employed by the hospitals (project end-users) or their stakeholders (security systems suppliers).

We had to manage several issues during the task, including the heterogeneity of terminologies since the interviewed experts came from several hospitals and countries. For genericity purposes, we integrated an alignment step to homogenize the vocabularies based on literature taxonomies and security standards (refer to Section VI). We also faced a classical issue with time-consuming tasks, as a difficulty to get experts' engagement. To maximize the collection of high-quality data, we created an acquisition methodology that mixes a passive collection process where experts autonomously fill pre-formatted files and active collection phases where ontology designers discuss with experts (online meetings) to check, complete, and validate the acquired data.

Within the project, twelve complex cyber-security attack scenarios have been developed with our partners, each describing a set of actions an attacker performs to accomplish his malicious aims. For each scenario, we carried out the following steps illustrated in Figure 2:

1) **Phase A:** identify the list of involved assets and the related risks engendered by the attacker actions.
2) **Phase B:** identify the assets inter-dependencies thanks to the hospital infrastructures (cyber and physical). The propagation scope is extended to the links connecting each involved asset within the cyber infrastructure of the hospital and its locality dependencies.
3) **Phase C:** Security experts indicate for all the assets the risks they are exposed to and potential protections implemented to secure them. Each protection is indicated with its corresponding efficiency degree.
4) **Phase D:** each incident occurring on a source asset might propagate to connected assets in different forms (impacts). Cyber and physical security experts indicate what are propagation vectors and how they enable the propagation of some incidents to specific threats impacts.

C. FORMALIZATION

The formalization phase corresponds to the definition of the logical and conceptual framework of the ontology. It includes identifying concepts, the description of relations and axioms

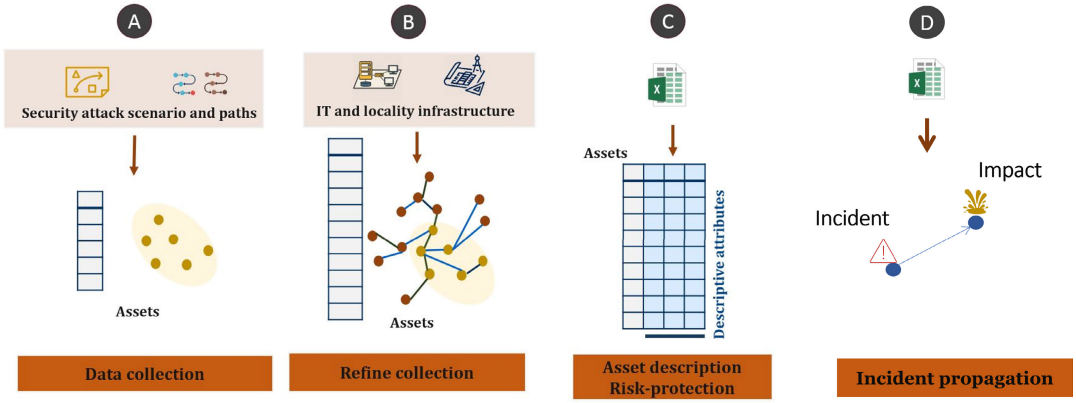

FIGURE 2. Knowledge acquisition methodology steps.

translating the dynamic knowledge on the constraints of concepts and relations.

1) CONCEPTS IDENTIFICATION

Concepts identification task is mainly supervised by the knowledge acquisition outputs. The issued terms have been generalized and semantically mapped to security management standards (refer to Section VI). This task enabled an iterative refinement cycle of the top-level modular ontology.

1) **Asset subontology** includes concepts corresponding to critical assets that the organization (healthcare infrastructure) aims to protect for delivering its tasks. The ISO/TS 11633-1:2019 [3] defines an asset as anything that has value to the organization, which includes technical data (credentials, passwords), non-health data (financial data), IT services, hardware, software, communications facilities, media, IT facilities, and medical devices that record or report data. It is considered critical if its malfunction induces a high impact on the overall system's operation and the patients [7]. Critical assets can be classified in two hierarchical levels, following their role to serve the organization's missions: **Business assets** and **Supporting assets**.
Business asset(*BusinessAsset* $\sqsubseteq$ *Asset*) or Essential asset in some standards, is according to [8] and [9], any information or processes deemed important for an organization, in the framework of a study. Business assets are intangible assets, and comprise **Services** and **Operations**. The security status of business assets can be evaluated according to key security needs: availability, traceability, integrity, and confidentiality.
   - **Service**, within the organization, the missions are carried out by different services. For a hospital, the surgery room service participates in the mission of providing healthcare. A service corresponds to a complex process involving a set of elementary operations.
   - **Operation:** Elementary task achieved as a part of one or more services. It encodes information or an act carried out using supporting assets. In the surgery room, medical acts, cleaning tasks, monitoring, patient data management are examples of operations.

Supporting asset concept (*SupportingAsset* $\sqsubseteq$Asset), is any element of the organization system serving one or several business assets. A supporting asset can be of a cyber (digital) or physical. Following the impact propagation task purposes, an asset is further specialized according to the nature of the incidents suffering from or impacts it creates.

- **Building** asset (*Building* $\sqsubseteq$ *Asset*), a geographical entity that corresponds to the building in which a hospital (or a part of it) is located. A building asset has a variable granularity going from ''room'' to a ''complex of buildings''. Buildings can be either: a **simple building** asset (a non-divisible location, *SimpleBuilding* $\sqsubseteq$ *Building*), or **complex building** asset that groups multiple simple building assets (*ComplexBuilding* $\sqsubseteq$ *Building*). The domain of the building assets corresponds to the hospital's physical infrastructure.
- **Network** asset (*Network* $\sqsubseteq$ *Asset*), a computer network denotes a communication and data exchange channel linking at least two devices (nodes). Networks connect the components of the hospital's cyber infrastructure.
- **Staff** (*Staff* $\sqsubseteq$ *Asset*), staff represents any physical person performing regular or occasional tasks within the hospital. In addition to direct employees, the staff includes external stakeholders acting on-site or remotely [10]. This concept willingly excludes patients since they are formalized as business assets.
- **Device** asset (*Device* $\sqsubseteq$ *Asset*): refers to any tangible equipment, whether associated to computer software with an automatic action

[3]https://www.iso.org/standard/69336.html

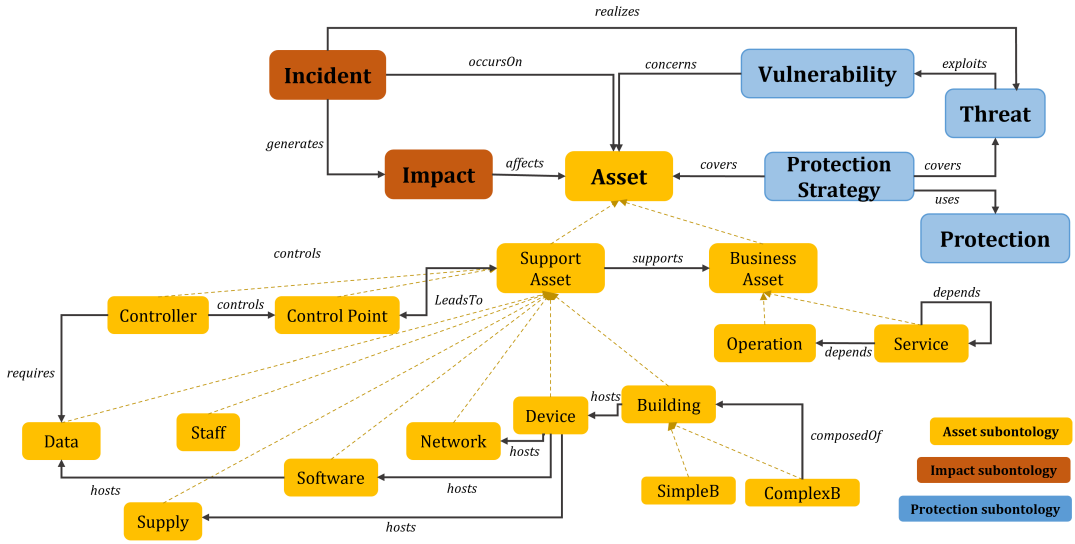

FIGURE 3. A global view of "SafecareOnto" concepts and relations.

(camera, sensor, server) or not (door, lamp). Computer device *ComputerDevice* $\sqsubseteq$ *Device*, building equipment such as doors, chairs, including those with an automated operating process *BuildingDevice* $\sqsubseteq$ *Device* (sensor, camera), medical devices *MedicalDevice* $\sqsubseteq$ *Device* (scanner, pacemaker).

- **Software** asset (*Software* $\sqsubseteq$ *Asset*), softwares are virtual programs (sequences of computer code) with data processing capabilities. They support a determined business process such as medical acts or human resources. Note that operating systems are also considered software.
- **Data** (*Data* $\sqsubseteq$ *Asset*): Data play a major role in security management since multiple attacks are carried out using or targeting data. We separate two context categories: **patient data**, and **operating data** used to support the hospital processes (access policies, camera flows, metadata, etc.).

Other supporting asset subconcepts are related to the access and control roles.

- **Access point** concept, the access points are the gateways that enable access to an asset and allow the occurrence of an incident. An access point can be either physical (door for room) or cyber (a port for network). The access point is an asset with a security access role (*AccessPoint* $\sqsubseteq$ *Asset*).
- **Controller** concept, controllers are physical equipment or virtual protocols implementing assets' access restrictions, formalized in predefined policies. Access to the surgery room requires a door (access point), supervised by a door access controller. A controller is a supporting asset that ensures safe use and anticipates a possible incident occurrence and propagation (*Controller* $\sqsubseteq$ *Asset*). Controller's scope can be very limited to one asset (as for door access controller), or can have a large control extent, in which case they are distinguished as specific classes: "electricity controllers", "phone controllers", **water controllers** are examples of strong roles that some devices and protocols own. This specification is essential for the propagation needs, as strong controllers propagate impacts to a larger set of assets, under particular constraints.

2) **The protection subontology**

- **Threat** (*Threat* $\sqsubseteq \top$), in this work, we use the **threat** and **attack** concepts interchangeably. A threat is an undesirable action that affects a security goal of the system. It can be a physical disaster ("Fire"), a fault, a failure ("denial of service"), or a human error [10], [11].
  A threat exploits one or several vulnerabilities, either earlier identified or emerging after incidents. The threats have been classified into physical threats and cyber threats. The cyber threat taxonomy corresponds to the "MITRE" attack cyber standard [12].
- **Vulnerability** (*Vulnerability* $\sqsubseteq \top$), vulnerability is a weakness that exposes the asset to threats and yields an incident's occurrence. In some security ontologies [13], vulnerability denotes the absence of protection measures against threats.
- **Protection** (*Protection* $\sqsubseteq \top$), is a countermeasure that protects the asset by preventing an incident's occurrence or attenuating its effect. Protection effectiveness varies following the threat nature and the asset. For the same asset, several protections can be aggregated to increase the effectiveness of the protection strategy. **Protections** are valuable resources of critical infrastructure and risk also to be targeted. They are **assets** too.

3) **The impact subontology**
   - **Incident** (*Incident* $\sqsubseteq \top$), according to the NIST [9], an incident is "an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of a system." An incident could be an attack against one or several assets by exploiting vulnerabilities. In SAFECARE, we handle both physical and cyber incidents, either with a criminal intention, human errors or natural events.
   - **Impact** (*Impact* $\sqsubseteq \top$), when an incident occurs, there is a risk that it propagates to related assets. An impact is the result of such propagation. This propagation needs to be precisely qualified and/or quantified to efficiently help decide about the mitigation plans. The cascading impacts is the subject of the task we describe in Section III.

2) RELATIONSHIPS IDENTIFICATION

The relationships depict how assets interact in the healthcare context and what are their properties. We have identified two families of relations. The first one corresponds to concepts attributes (data properties in Web Ontology Language [OWL]): a staff `hasRole`, a building `hasLevel`, a software `hasVersion`, etc. The second family of relations corresponds to concepts interactions (object properties in OWL). They are highlighted in Figure 3 with solid labeled arrows. We organized these relations in groups matching our propagation channels' analysis to fit the task purposes. This analysis revealed some structural patterns that support reasoning on incidents' propagation following their nature. Among patterns we can identify:

1) Operational dependency pattern reflects the dependence that two entities can have in order to function. For example, the SAMU[4] service depends on the telephone operation, this means that any malfunction in the telephone system implies the unavailability of the SAMU service. Operational dependency relations are: depends, supports and requires.
2) Leads to pattern captures the access and communication possibilities between assets. This access applies for both physical or cyber flows and is materialized through the `Leads To Access` and `Leads To Asset` relations. The access mechanism could be one-way or bidirectional.
3) The hosts-content pattern assumes that if an incident happens on an asset named `host asset` then the content, referred to as `content asset` could be affected by this incident. The structure of the pattern is enriched by rules to enhance the validity of the relations description. If the server (Device) suffers from "fire", the information system (Software) it hosts will be impacted (inaccessible).
4) Controls pattern allows specifying the conditions and mechanisms for granting or revoking access to cyber or physical assets. The pattern uses the `Controller` that `Controls` the `Access point`. The control patterns `requires Data` as access policies. For example, a physical Access Control system based on a smart card is composed of three elements: the access rights stored locally or remotely, door readers to check whether data on the card is consistent with the policy and the door (Access point) which would be unlocked when the card is approved.
5) The whole-part pattern assumes that if an incident happens on the whole, there could be an impact on its parts. Inversely, if parts are attacked, the whole could also suffer from the impact of the attack. In the healthcare structures, this pattern applies to locations `Building assets`, that are `Composed Of` smaller entities. Moreover, the propagation concerns in this case essentially "physical incidents" such as "unauthorized access", "fire" or "flooding". For example, if there is an intrusion on one floor of a hospital, it potentially affects all the rooms.

3) AXIOMS DEFINITION

Axioms allow defining the semantics of concepts, relations and express some restrictions on their values or cardinalities. The use of axioms enables representing specific capabilities or features of a concept and avoids adding new concepts that would not be reused [14]. For "SafecareOnto", a set of formal axioms is defined to specify some ontology elements. The following paragraph introduces some axioms examples and their corresponding description.

- $OperatingData \sqsubseteq Data$
  (subclass axiom, operating data are data)
- $ControlPoint \sqsubseteq Device \sqcup Building \sqcup Software \sqcup Network$
  (A control point can be either a device, a building, a software or a network. This excludes Data, Supply, and Staff from this asset role)
- $Controller \sqsubseteq \forall controls(AccessPoint)$,
- $Controller \sqsubseteq= controls(AccessPoint)$ All controllers necessary control an asset identified as a Control Point.
- $PhysicalIncident \sqcap CyberIncidents \sqsubseteq \bot$
  (Cyber incidents and physical incidents are totally disjoint concepts, same axiom for threats and protections)
- $Data \sqcap requiredbyController \sqsubseteq operatingData$
  (Data required by a Controller are exclusively OperatinData)
- $leadsToAsset$, $leadsToAccessPoint \sqsubseteq leadsTo$ leadsTo is a super relation for leadsToAsset and LeadsToControlPoint. This allows expressing constraints and propagation rules on the superRelation when it applies to both
- $ComplexBuilding \sqsubseteq \exists\ composedof\ Simplebuilding$
  ComplexBuilding is composed of at least one SimpleBuilding
- $ProtectionStrategy \sqsubseteq \exists\ uses\ Protection$
- $ProtectionStrategy \sqsubseteq \exists\ against\ Threat$
- $ProtectionStrategy \sqsubseteq \exists\ covers\ Asset$
- $ProtectionStrategy \sqsubseteq= covers\ Asset$

[4]Service d'Aide Médicale d'Urgence, health assistance service in French

Each protection strategy uses at least one protection, and is implemented against at least one threat. One protection strategy covers exactly one asset.

D. KNOWLEDGE BASE

A knowledge base is defined by an ontology and a set of facts. In SAFECARE, the knowledge base gathers all the information required to support the hospitals' cyber-physical security management, specifically the incident propagation task. The knowledge acquisition step produced three distinct knowledge types:

- Security standards used by industrial partners for qualifying cyber and physical threats and cyber protections. The ''MITRE'' dictionary [12] is used for cyber threats, which organizes them in two detail levels: each threat can have more than one sub-related threat (Spearphishing Link is a threat of type Spearphishing). The ''MITRE'' dictionary has also been used for cyber countermeasures. For physical threats, the physical threat detection system partner provided a list of physical threats as ''fire'', ''theft'', ''breaking through access control by force''.
- Hospital-related facts on assets and protection strategies implemented for each asset,
- Knowledge about incident-impacts mappings used for the construction of the rules base.

The Figure 4 shows an extract of the asset knowledge graph corresponding to the running example scenario.

III. IMPACT PROPAGATION APPROACH

A. PROPAGATION MECHANISMS

Estimating incidents propagation within critical infrastructures consists of identifying how an incident affecting a first infrastructure asset evolves by creating a series of cascading effects on physically or digitally connected assets.

Thanks to ''SafecareOnto'' and the knowledge acquisition task, hospitals' cyber and physical architectures are integrated into a single knowledge graph. The assets belong to the nodes of this knowledge graph, and the links of the graph encode their cyber and physical interdependencies. At the occurrence of the attack, the modules responsible for the threats detection (see section architecture), create security events as alerts. These alerts are subsequently confirmed and transformed into incidents. At the IPM level, each incident message received can affect one or more initial assets.

Starting with one asset, the propagation can operate through the knowledge graph links. Basically, any relationship between two assets is a potential vector of propagation. In fact, incidents do not necessarily propagate, and this depends on several factors: the nature of the threat, the nature of the asset, or the implemented protections. For example, if a virus attacks a computer's system, the virus would not affect the room hosting the computer, although the existence of the physical hosting link. However, the virus can affect the business process ''patient reception'' supported by the computer.

The propagation logic is more complex than the assumption that physical incidents only propagate to physical impacts and analogically for cybers. Some relationships could initiate a cyber impact with a physical incident (fire on a server inducing unavailability of information systems). Inversely, manipulation of the ATU (Air Treatment Unit) data results in an uncontrolled increase in room temperature, which is a potential risk for patients' health. This knowledge on the transformations of incidents is security expertise exclusively held by security experts evolving in the medical field, understanding the consequences of attacks. The following paragraph explains how this knowledge has been exploited to build the rules repository (initial model is to be consulted in [15]).

B. PROPAGATION RULES

The process of building the propagation rules repository, depicted in Figure 5 is composed of 4 steps:

- Knowledge acquisition: to build the propagation rule's base, experts' knowledge on incident transformation is gathered. This task is organized according to predefined attack scenarios in an incremental way. Each propagation case is analyzed, and the resulting rule is generalized to guarantee maximum coverage of similar propagation cases.
- Formalization: in this phase, the concepts and properties of the ontology that can be used to write rules are identified. A rule engine (we used in this work Jena inference[5]) is then used to implement these rules in the form of premises and conclusions that specify the conditions in which the propagation of impacts could occur.
- Validation and refining: the formalized rules are implemented, then tested on different scenarios on real data and test cases. Domain experts evaluate the inferred impacts on assets to determine whether the inference provides coherent and reliable results. At the end of the validation, rules could be refined to better meet the expected results.
- Learning: although the attack scenarios have been designed to cover as much as possible security incidents occurring within hospitals, the created rules repository is hardly exhaustive. New types of security incidents are constantly identified, new vulnerabilities are revealed, and new protections implemented. All these extensions need to be considered to study their consequences on the propagation that might require modifying or adding new rules. Currently, the incidents backup history is analyzed to identify possible changes. During the project, some rules have been added following a real security incident that occurred a few days before the final phase of the

[5]https://jena.apache.org/documentation/inference/index.html

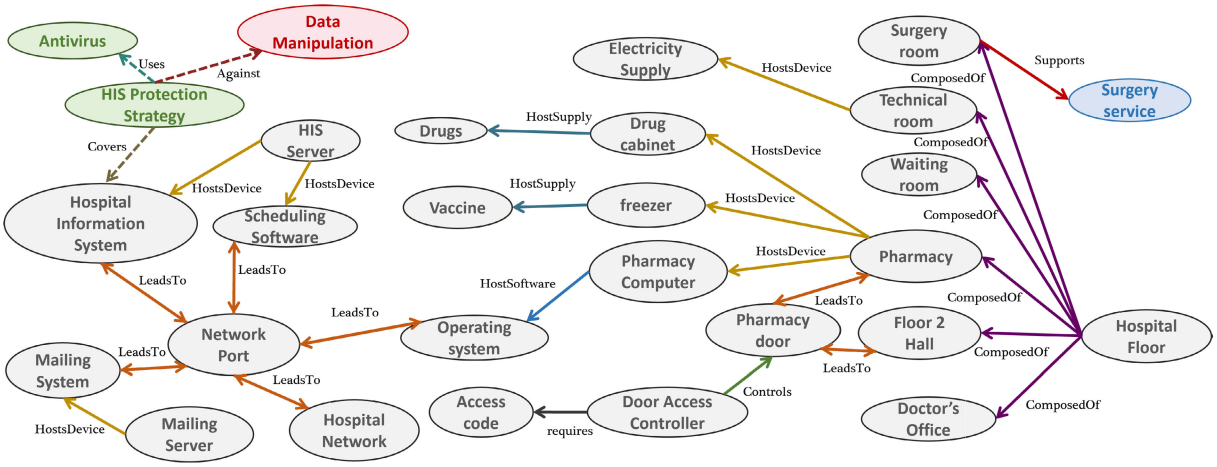

FIGURE 4. An extract form "COVID-19" scenario knowledge graph.

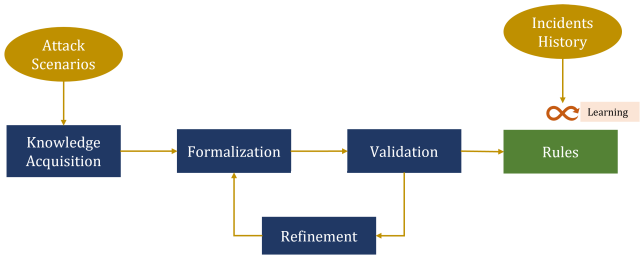

FIGURE 5. Propagation rules creation process.

tests in one of the pilot hospitals. The automation of this phase is possible and foreseen in future works.

The following examples present some propagation rules built during the project and illustrated in Figure 6 through the running scenario example. Each rule has a color code for the source asset and the target asset, where the source asset suffers from the initial attack while the target witnesses an impact of this attack. Notice also that the reception service (light blue in the figure), designates a business asset.

a: CYBER-CYBER RULE EXAMPLE

In step 2 of the attack scenario from Section I-B, after social engineering on a hospital employee, the attacker sends a spearfishing email. If successful, the incident risks spreading through the network. Spearfishing email initially affects the mailing system asset, and the first direct impact it may cause is a "network service scanning" on network assets, in order to identify the services and components connected to the hospital network. The following inference rule [6] expresses this propagation, highlited in Figure 6 as rule 1.

```
Incident(newIncident), realizes(newIncident, threat2),
NetworkScanning(threat2),occurs(newIncident, asset2) :-
occurs(incident1, asset1), realizes(incident1, threat1),
Spearfishing(threat1), software(asset1),
leadsToAsset(asset1, asset2), Network(asset2)
```

[6]For the sake of clarity, we use a simplified rule-based syntax similar to Datalog/Prolog.

b: CYBER-PHYSICAL RULE EXAMPLE

The patient reception service is managed by medical staff to organize patient visits to the hospital and facilitate their health care. This service is available thanks to several support assets such as the appointment management system and reception facilities. Any manipulation of the data on the hospital's appointment management systems could lead to a mass in the premises reserved for reception. In the figure, the scheduling software suffers from data manipulation and the waiting room providing the hosting service is crowded.

```
 Incident(newIncident), realizes(newIncident, threat2),
Crowding(threat2),occurs(newIncident, asset2) :-
occurs(incident1, asset1), realizes(incident1, threat1),
DataManipulation(threat1), software(asset1),
supports (asset1, asset3), Building(asset2),
supports (asset2, asset3)
```

c: PHYSICAL-PHYSICAL RULE EXAMPLE

A loitering incident can be detected by a camera and designates a suspicious movement of the attacker in a locality. Following loitering, many opportunities of attacks are possible: device destruction, supply theft, or breaking through access control by force. The later impact is shown as a result of the following propagation rule.

```
Incident(newIncident), realizes(newIncident, threat2),
UnauthorizedAccess(threat2),
occurs(newIncident, asset2) :-
occurs(incident1, asset1),
realizes(incident1, threat1),
Loitering(threat1), Building(asset1), leadsToAsset
(asset1, asset2), ControlPoint(asset2)
```

On the Figure 6, all purple nodes correspond to potentially impacted assets either with unauthorized access as in rule 3 or similar: theft of vaccines, drugs, or destruction of the freezer, computer, or cabinet.

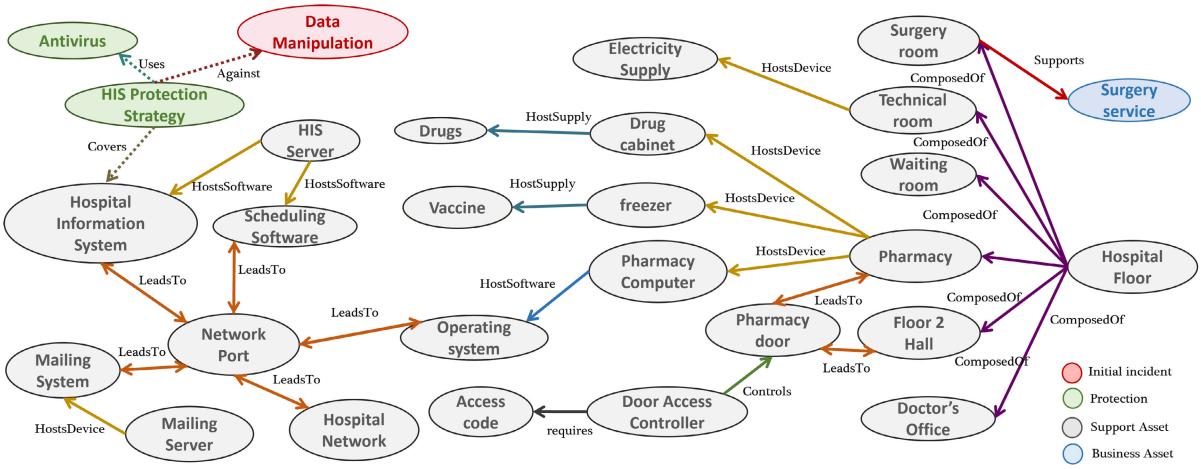

FIGURE 6. Propagation rules application on "COVID-19" scenario's knowledge graph.

d: PHYSICAL-CYBER RULE EXAMPLE

A suspicious interaction of an individual with an object is detected through the intelligence system equipping the camera. This interaction can lead to physical damage, such as deterioration or theft, but can also produce cyber impact if the device hosts software. The attacker who enters the pharmacy can seize the opportunity to plug a USB key in the computer and hack the authentication thanks to a malicious program to have access to the patients' data, for example. The following rule reflects the propagation of a physical incident (suspicious interaction, in light pink node) to a cyber incident (exfiltration over USB, in dark pink node)

```
 Incident(newIncident), realizes(newIncident, threat2),
 ExfiltrationOverUSB(threat2),
 occurs(newIncident, asset2) :-
occurs(incident1, asset1), realizes(incident1, threat1),
SuspiciousInteraction(threat1), Device(asset1),
hostsSoftware (asset1, asset2), Software(asset2)
```

e: BUSINESS ASSET RULE EXAMPLE

During surgery, the temperature of the surgery room should be kept at a fixed level to ensure the safety of patients during the medical procedure. Many threats can lead to an unsuitable temperature incident: data manipulation on sensor data, an electrical shutdown, failure of the ventilators: If the temperature of the surgery room increases, the health of the patient is threatened. The surgery service is therefore unavailable (dark green node on graph).

```
Incident(newIncident), realizes(newIncident, threat2),
Unavailable(threat2),occurs(newIncident, asset2) :-
occurs(incident1, asset1),
realizes(incident1, threat1),
SuspiciousInteraction(threat1), Building(asset1),
supports (asset1, asset2), Service(asset2)
```

C. PROTECTION INTEGRATION

As described in Section II, one or more protection strategies can be assigned to each asset. A protection strategy is specific to a threat type and can involve multiple protections. For example, a room can be protected against a "fire" threat thanks to a "fire door", and protected against "intrusion" using a "door access controller". Each protection attributed to an asset has properties as the efficiency degree. The efficiency of the door access controller depends on the integrated authentication system (biometric, imprint, code) and whether or not other access points exist. This efficiency is defined in our system as the "protection degree" an asset has against a threat. This parameter is a numerical value evaluated and provided by security experts. The existence of several protections leads to the aggregation of their corresponding protection degrees. Consequently, an asset can be identified as fully protected against a particular threat.

In our system, the "**full protection**" status is pre-evaluated and stored in the knowledge base. Knowing that an asset is fully protected is valuable for reporting its non-impact on the indicated threat, which affects the following propagation chain: If the asset is not impacted, the propagation stops at its level, which indirectly protects its neighbors. The following rule shows how the "fully protected" (or its inverse) predicate is integrated to impact propagation rules:

```
 Incident(newIncident), realizes(newIncident, threat2),
 NetworkServiceScanning(threat2),
 occurs(newIncident, asset2) :-
occurs(incident1, asset1), realizes(incident1, threat1),
Spearfishing(threat1), Software(asset1),
leadsToAsset(asset1, asset2), Network(asset2),
notFullyProtected (asset1, threat1)
```

In the graph of Figure 7, we observe that the use of the "Firewall" and the "Network segmentation" on the "Network port" prevents the "Network-Scanning" incident and therefore all subsequent cyber impacts on related softwares. The combined protection degree of the asset exceeds 100% which provides full protection, stopping the propagation of the threat.

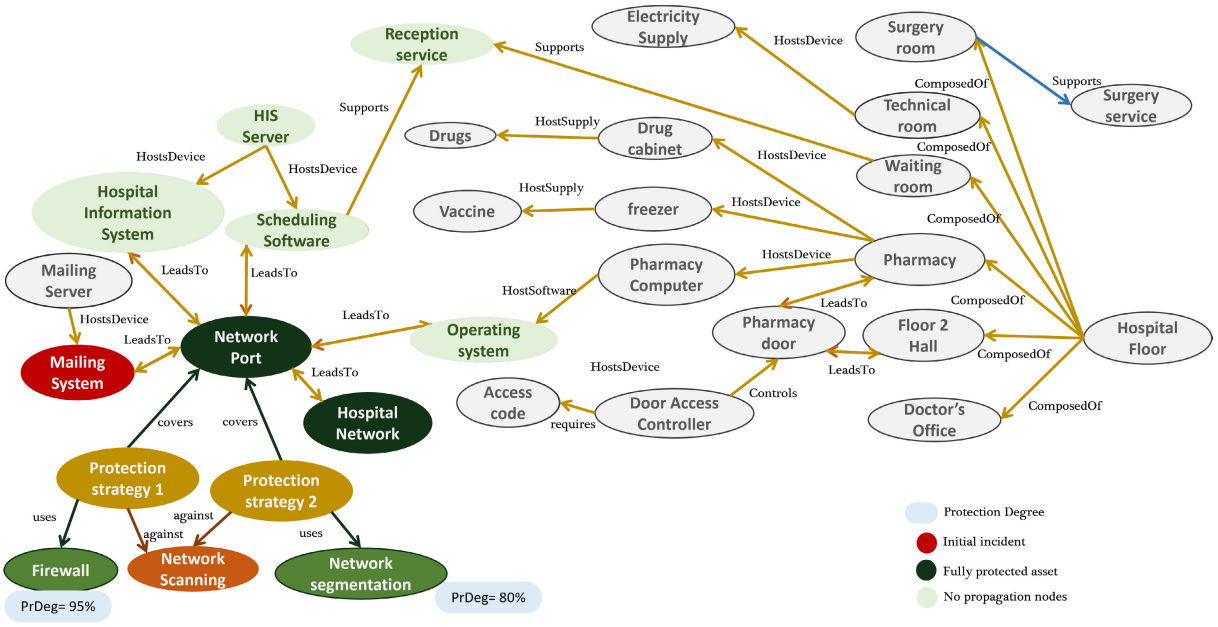

FIGURE 7. Propagation rules application of "COVID-19" scenario's knowledge graph, after integrating protection assets.

D. IMPACT SCORE

The protections implemented to protect assets do not always guarantee complete security coverage. Nevertheless, they allow attenuating the impacts' severity. As introduced in the previous section, the global protection degree related to an asset is a value provided by security experts referring to how the different implemented measures capabilities aggregate. The identification of this global value depends on the nature of the threat, the asset and the protection. The couple (camera (90%), human guard (95%)) has a global degree of protection that does not correspond to a trivial sum or maximum over their separate degrees of protection, and the addition of an intrusion detection system to this set does not guarantee a full protection either. In the same vein, implementing two different antivirus tools do not increase the protection degree if they both cover the same scope of attacks. These examples illustrate that the computation of the global protection degree rely on security experts knowledge and analysis of the system features. Accordingly, we define the impact score of an asset for a given threat and protections' set as follows:

$$impactScore_{th}(a) = 1 - \gamma_{j=1}^{p} protectionDegree_{th}^{j}(a) \quad (1)$$

where, p is the number of protections for an asset a per threat th, and γ is an aggregation function allowing to compute the global protection degree for an asset, associated with p protection measures. Considering that the aggregation of individual protection degrees to compute the global degree is specific to security solutions providers, the γ function is variable. This variation can be illustrated thanks to physical and cyber systems particularities for example. The protection degree ensured by a unique camera or when this camera completes a security guard varies. Global protection is also increased with the combined use of an intrusion detection system. This aggregation model that building security experts master is in no way comparable to that of cyber solution providers who aggregate for example different antivirus protection degrees by comparing the scope of viruses they cover. Examples of γ function can be: Max, weighted sum, probabilistic model output..

It is worth noticing here that if an asset a has numerous protections against threat th, it will be potentially less impacted by such a threat. Concretely, on equation (1), the second term expresses how much an asset a is protected against a threat th.

Recall that the propagation mechanism is implemented on top of the knowledge graphs built for each hospital.Following the aforementioned propagation rules, the potential impact navigate from an asset (graph node) to another through their cyber-physical relationships (graph edges).

The extent of an incident corresponds to the graph path (sequence of edges) it crosses. Which means that if an asset in the path is not impacted (its impact score for a given threat equals zero), it acts as a barrier stopping the propagation of the incident and the following assets in the path are saved. We generalize the impact score definition to any asset in the graph as follows.

$$impactScore_{th1}(a_t) = \begin{cases} 0, & \text{if } \exists a_i \in Path(a_s, a_t) \mid impactScore_{th2}(a_i) = 0 \\ 1 - \gamma_{j=1}^{p} protectionDegree_{th1}^{j}(a_t), & \text{otherwise} \end{cases} \quad (2)$$

where $Path(a_s, a_t)$ is the set of all the assets in the path connecting the asset source a_s to the asset target a_t. In the case of multiple paths connecting a_s and a_t, the impact could be propagated through all paths if the rules are applicable.

IV. IPM ARCHITECTURE

A. GLOBAL ARCHITECTURE

In this section, we describe the global architecture of SAFECARE. The project is composed of sixteen 16 different prototypes, those directly interacting with our module are depicted in Figure 8. First, there are the physical and cyber detection systems that will detect, validate and alert to all the other modules about an incident through the Data Exchange Layer (DXL). The data exchange layer implements publish-subscribe mechanisms to trigger notifications to the other components when new physical and cyber incidents or new impacts are sent. The impact propagation model is the aim of this paper, its role is to generate the cascading effect after receiving an incident from either physical detection system or cyber detection system and send the impact message through the DXL. The impact message will be sent to two different models, the threat response and alert system (TRAS), this model aims to alert in a timely fashion the relevant stakeholders when incidents and impacts occur. The second model that receives the impact message is the Hospital Availability Management System (HAMS). This service will improve the resilience of health services and the communication of availability information among hospital staff and first responders.

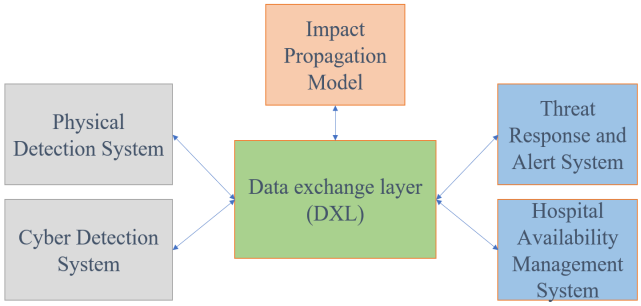

FIGURE 8. Extract of the SAFECARE project global architecture.

B. IPM COMMUNICATION

The impact propagation solution requires interacting with other project modules to acquire the necessary inputs to its functioning: a Central DataBase (CDB) gathering assets, protection lists, and security standards. This information is retrieved by using different APLs (Application Programming Interface). The module also interfaces both physical and cyber detection systems to get notified of incidents' occurrences. Each time IPM is notified about an incident, the model will analyze it and generate the impact cascading effect on all the other assets. These impacts need to be sent to the threat response and alert system and the hospital availability management system.

The IPM communicates with the other modules by exchanging JSON messages through the MQTT (Message Queuing Telemetry Transport) broker. When it receives an incident message from the detection systems, the impact module is triggered, and the JSON impact message is generated and published through the MQTT broker.

The MQTT broker of DXL has been implemented with Apache ActiveMQ client. The communication channels are secured using TLS 1.2 protocol (Transport Layer Security) over HTTPS. Implementation and tests have been conducted authenticating clients through X.509 certificates.

Figure 9 shows the communication between the IPM and the other modules.

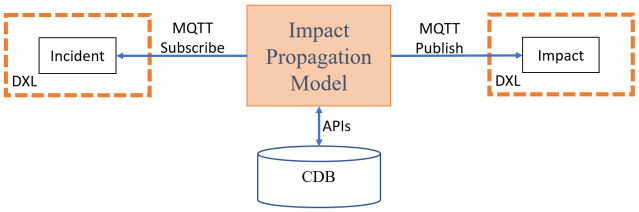

FIGURE 9. Architecture for the Communication between IPM and the other Models.

The module is organized into two parts, the online part, and the offline part. In the offline sub-module, the knowledge base is created by retrieving information from the central database using specific APIs. This information consists of the list of all assets, the types of the assets, and the list of protections associated with each asset. The online sub-module is triggered by the reception of an incident message. It consists of (i) propagating incidents and calculating impact scores and (ii) creating the impact propagation message that contains the list of impacted assets regarding threats in the incident message along with their impact score. Concretely, when an incident message is received, the CDB is queried to update the protection degree value for all the assets in the knowledge base. After that, the list of impacted assets is generated by running the inference rules. The impact score is calculated for each impacted asset based on the last updated value of the protection degree in the CDB. The final step is to publish the impact propagation message by using the MQTT broker.

The visualization of the propagation is made in a graphical way, where the nodes represent the assets, and the edges represent the relationship between them. The impact score on impacted assets is expressed by changing the color of the corresponding node. The red color represents a strong impact and the orange represents a moderate impact.

V. EXPERIMENTS AND EVALUATION

The SAFECARE project provides a set of regular tests for the different modules, including IPM. In addition, three real-life demonstration sessions were organized with the project pilot hospitals (Marseille,[7] Turin,[8] Amesterdam[9]). Each demonstration session was realized within the premises of the hospital and attended by all the project partners and the end-users (hospital employees or stakeholders). The session

[7]APHM: Assistance Publique Hopitaux de Marseille: http://fr.ap-hm.fr/
[8]ASLTO5: https://www.aslto5.piemonte.it/
[9]AMC: https://www.amc.nl/web/home.htm

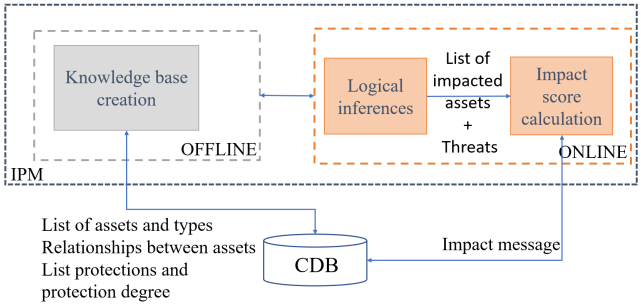

FIGURE 10. Overview of the IPM module global architecture.

aims to prove the efficiency and effectiveness of SAFECARE solutions for managing security events following 12 cyber-physical attack scenarios. The evaluation includes two dimensions: quantitative metrics evaluated by security experts and satisfaction questionnaires filled by the end-users. This section reports the results of both evaluations within the three hospitals.

While the cyber architectures of hospitals are similar (despite the varying number of assets), physical architectures differ. This variation is a crucial factor explaining the propagation patterns and impacts severity. Two types of physical architectures are represented across the partner hospitals:

- **Architecture A**: with small buildings spread over the hospital's geographical area.
- **Architecture B**: big connected building entities (high density).

A. SCENARIOS SUMMARY

Twelve security attack scenarios were designed with the project partners and end-users to organize the test and demonstration sessions. Each scenario has been described following the Ebios Risk Management method [16], including 4 steps:

- Know: the set of preparation actions the attacker achieves to target the hospital. In the "COVID-19" scenario introduced in Section I-B this corresponds to the social engineering effort.
- Get In: the incidents created as the attacker accesses physically or digitally the hospital's cyber or physical infrastructure. The intrusion uses access point assets as a network port to reach the hospital's network.
- Find: this step includes actions performed within the hospital to identify the targeted assets. Loitering around the pharmacy room enables the identification of the access code and the vaccine locality.
- Control: the achievement of the purposes of the attack such as the theft of the vaccine, the destruction of assets, or putting the fire.

The consequences of the scenarios explicit the attacker action impacts on the supporting and business assets. The Table 1 lists all the used scenarios with their corresponding attack objective.

TABLE 1. Summary of scenarios tested in SAFECARE demonstration sessions.

Scenario Label	Scenario Description
Sc1	Cyber-physical attack targeting power supply of the hospital
Sc2	Cyber-physical attack to steal patient data
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 on access control provider to steal medical devices
Sc9	Physical attack against hospital staff using a gun
Sc10	Physical attack to steal drugs
Sc11	Cyber-physical attack due to a personal laptop
Sc12	Cyber-physical attack to block national crises management

B. KNOWLEDGE BASE AND RULES STATISTICS

Table 2 reports a description of the knowledge graphs and rules built and derived for, respectively, hospital architectures A and B. For dense physical architecture B, the number of links between assets is greater due to the connectivity of physical elements, which also implies a dense cyber architecture. The size of the knowledge graph does not correspond to all the assets in the hospitals, but only a part used in demonstrations that is proportional to real attributes. This extraction was performed to study the propagation on particular dimensions. The module itself applies to the entire asset base of all hospitals.

On the other hand, the number of rules per architecture only indicates the number of rules built with the experts for each particular architecture type. However, the rules repository remains single, valid for any type of architecture without inconsistency. Rules will be activated automatically when they apply.

TABLE 2. IPM module demonstration settings.

Architecture	Graph Characteristics		Rules		
	Nodes	Edges	Physical	Cyber	Hybrid
Architecture A	1707	2677	11	12	2
Architecture B	3114	5644	29	22	4

C. IMPACTS GENERATION EFFECTIVENESS

In each tested scenario, at least one incident has been tested, with a total number of 23 incidents; 12 physical, and 11 cyber. Some of these incidents have been tested in the two different architectures (architecture A and architecture B) while others

are tested over only one. Table 3 summarizes the results of the demonstration. The columns incident label and incident type indicate the label of the received incident (in the JSON message) and its type (physical or cyber). The first column reports in which scenario this incident has been tested. An asset might suffer from more than one impact, that's why we report both the total number of impacts generated by IPM, overall assets, along with the number of distinct impacted assets. Following the loitering incident, if the room initially impacted hosts a set of devices, they can be impacted by either physical damage or stolen by the attacker. Consequently the number of impacts is greater than the number of impacted assets.

We derive from the results the impact that has the physical topology on the incident propagation. Dense building structures is an acceleration factor for the propagation of physical incidents such as loitering, for which we notice the largest propagation dynamic (20 for architecture B vs. 11 for architecture A). Connected rooms help the attacker access critical assets following a loitering action. For the same reasons, physically-enabled cyber incidents such as data manipulation on a computer's system are of greater occurrence and impact in architecture B.

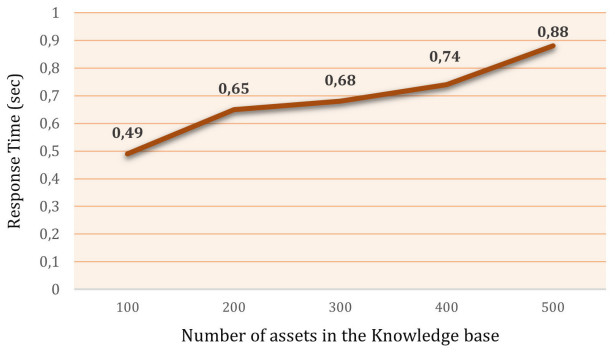

FIGURE 11. Evolution of the execution time following the knowledge graphs sizes.

D. IMPACTS GENERATION EFFICIENCY

1) EXECUTION TIME

The execution time in our module represents the global time needed to both generate impacts and calculate the impact score, after receiving an incident. To study the impact of the knowledge graph size on the execution time, we used 5 knowledge bases with similar characteristics (links' density, distribution of asset types), but a different number of assets. Figure 11 shows the execution time with respect to the graph size. We notice a linear-like evolution of the execution time following the increasing number of assets. This evolution is still reasonable since the global answer is less than 1 second for 500 assets. Further developments for diminishing this complexity are under investigation using parallel programming by isolating impacts computation for different asset types.

2) PRECISION AND RECALL MEASURES

An essential set of metrics about any estimation/prediction task is the evaluation of the exactness of the estimation: whether all expected impacts have been identified (true positives), the number of impacts that should not be identified (false positives), or the number of assets that should be impacted but were not computed by the IPM (false negative). The precision, recall and F-score are defined as follows:

- Precision: the proportion of true positives out of all predicted impacts.
- Recall: the proportion of true positive out of the real impacts.
- F-score: computed based on precision and recall as:

$$\text{F-score} = 2 * \frac{precision * recall}{precision + recall} \tag{3}$$

All these metrics were measured during demonstrations on 23 incidents. Table 4 reports their values for four significant incidents.

In general, the Table 4 shows satisfying results for the IPM; the F-score is always higher than 75%. We notice that IPM perform better when the initial incident is cyber, since the rule repository for cyber propagation patterns is better documented and based on rich cyber security standards and protocols.

E. KEY PERFORMANCE INDICATORS

A set of key performance indicators has been defined to evaluate the SAFECARE project, including sixteen (16) questions for the end-users. The purpose of these questions is to evaluate all the modules that are involved in the project. Two questions are the most relevant for IPM performance measuring: the first relates to the time needed by the agent to react after the detection of the event by the system. This time corresponds mainly to the necessary time for IPM to generate impacts. Sending the impact message faster will support the agent to take action quickly. The results of this questioner are presented in Figure 12.

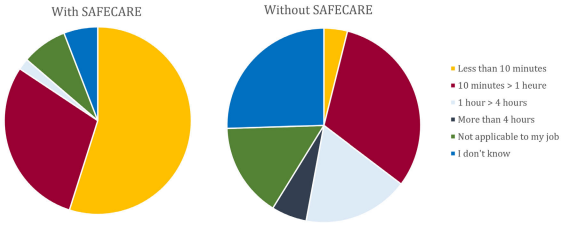

FIGURE 12. Reaction time following a security incident for end-users traditionally and with the use of SAFECARE.

According to the pie chart, more than 50% of the end-users report that the time needed to take the action with SAFECARE is less than 10 minutes and more than 78% answer that the same time is less than 1 hour. In comparison, without SAFECARE, only 32% of the end-users said that this time is less than 1 hour, and according to 67% of the end-users,

TABLE 3. The number of impacts and impacted assets following some incidents.

Scenario	Incident Label	Incident Type	Total Impacts		Impacted Assets	
			Architecture A	Architecture B	Architecture A	Architecture B
Sc1	Fire	Physical	-	20	-	14
Sc7 and Sc10	Loitering	Physical	11	20	5	11
Sc12	Malicious Link	Cyber	-	29	-	19
Sc2 and Sc5	Network Service Scanning	Cyber	12	26	8	9
Sc9	Weapons	Physical	6	-	4	-
Sc5	Data Manipulation	Cyber	-	7	-	6

TABLE 4. Precision, Recall and F-score measures.

Incident	Generated Impacts	False Negatives	False Positives	Precision	Recall	F-score
Fraudulent use of access control key	14	5	0	1	0.736	0.848
Loitering	18	7	0	1	0.72	0.837
Data Encrypted for impact	4	0	0	1	1	1
Network Service Scanning	27	4	0	1	0.857	0.922

more than 1 hour is needed to react after the detection of the event. We can conclude that end-users largely agree on the fact that SAFECARE diminishes agent reaction time to correct/intervene on the alert (without SAFECARE 1 to 4 hours and with SAFECARE less than 10 minutes).

The second questioner was to check whether the agents have a clear view of the impacts and potential escalation of the threat before presenting the SAFECARE and after presenting it. The results are presented in Figure 13

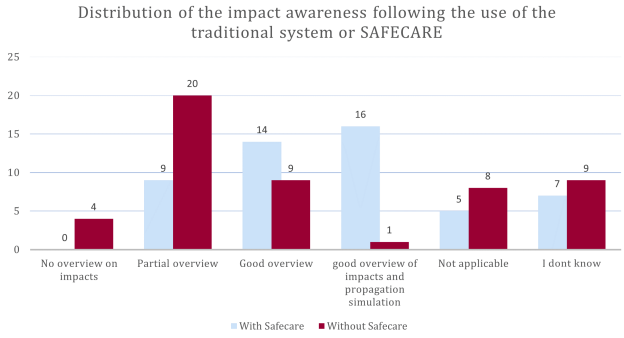

FIGURE 13. Quantification of the field of knowledge of the environment for the agent in charge of the alert.

The bar chart shows that 59% of end-users assert that alerted agent has a much better view and knowledge of impacted assets when using SAFECARE. Also, we can observe that the more we are providing information about the impact, the easiest the agent quantifies the alert and handles it.

F. END USERS SATISFACTION

At the end of each demonstration, questionnaires were asked to check two satisfaction elements: the end-users satisfaction regarding all the components of SAFECARE and the overall objectives of SAFECARE from the stakeholders' point of view. One hundred and twenty-five 125 questionnaire copies were provided in three different languages to the audience attending the demonstrations. These participants are from different professions like health practitioners, security experts, crisis managers, police, firefighter, technical operators, etc.

The system performance was tested based on two aspects: the detection level which is the ability of the system to detect cyber and/or physical threats and the response to this threat. The evaluation shows that 56% of the respondents completely agree that SAFECARE is a significant improvement over current solutions in the detection level for cyber threats while 81% of them agree on the detection level for physical threats. For the response to the threat the percentage is higher, 73% agree that SAFECARE is better than current solutions in responding to cyber threats and 87% in responding for physical threats.

1) SYSTEM USABILITY

A widely used metric for system usability evaluation is the System Usability Score (SUS) [17] which represents a reliable tool for measuring the usability of a software or a tool. The SUS provides ten (10) question items, each with five response options, from strongly agree to strongly disagree. The result of the SUS questionnaire is considered as good if above the value 68, and below the average otherwise. The SUS evaluation for the SAFECARE framework is displayed in Table 5, and demonstrates good global results for the usability, with a smooth variation between the two architectures, explained by the richness of demonstrated scenarios in architecture B compared to architecture A.

TABLE 5. System usability score.

	Architecture A	Architecture B	Total
SUS	64.325	76.042	73.125

Another evaluation was done which is the module specific performance, in this evaluation the participants fill a questionnaire about the understanding, efficiency and the useful of the module. The score varies from 1 to 7 where 1 means

strongly disagree and 7 refers to strongly agree. The results are shown in the Table 6.

TABLE 6. Module specific performance.

Module	Understood	Efficient	Useful
IPM	5.88	5.88	6.00

The end users were asked if the SAFECARE system meet all their requirements for the integration of cyber-physical security in the hospital and the results are depicted in Figure 14.

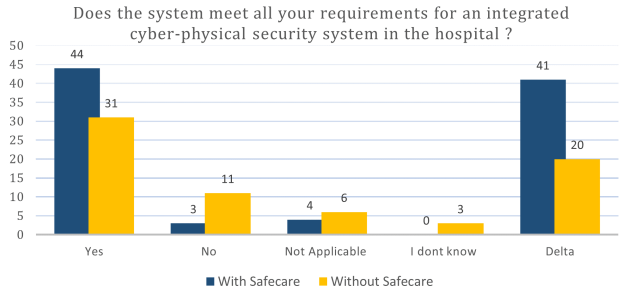

FIGURE 14. SAFECARE system compliance with end users' requirements.

We can observe from the figure Figure 14 that 44 out of 51 participants approve that these requirements can be reached with SAFECARE while 31 believe that the requirements can be reached without SAFECARE. The SAFCEARE system includes multiple modules in addition to the IPM. Some of them are enhancements of already existing security solutions which explains that some end-users had already the necessary tools to achieve some tasks without SAFECARE. On the other hand, and as stated in Figure Figure 13, the propagation module brings a significant gain in achieving the incident propagation task.

VI. RELATED WORK

Healthcare infrastructures are consensually agreed as critical. They are so vital assets for the maintenance of people's health. Their destruction or disruption would have a significant societal impact, hence the growing interest in securing them. Their adoption of more and more recent technologies raises a wide range of security issues and challenges that are the subject of several research papers. This section summarizes the research work related to our contributions. We have classified them into two categories: those describing models for asset management and analysis and those depicting incident propagation approaches.

A. MODELS FOR ASSET MANAGEMENT AND ANALYSIS

The hospital must hold perfect knowledge of its critical assets to maintain its mission despite the occurrence incidents. Assets identification and documentation fall within the scope of the risk analysis, a crucial process in risk management. The latter is described in a wide range of national and international standards: ISO/IEC 27000:2018, Common Criteria ISO/IEC 15408, ISO/IEC 27002:2013, IEC 80001-1:2021, and NIST SP 800-30. Some resources, like the HITRUST risk management framework [18] from the Health Information Trust Alliance (HITRUST) are associated with the healthcare sector. To achieve risk analysis, it is possible to rely on existing methodologies based on standards like LIRA methodology [19], CRISRRAM approach [1] and EBIOS RM methodology [8]. Some of these methodologies give descriptions of assets that are very often informal and light.

However, several models are presented in the literature for asset analysis ([20]–[25]). Authors in [22] propose an ontology called OLPIT, and claim that it reflects the layering suggested by the ITIL and CoBit frameworks. It defines hierarchical relationships between the three represented levels: process level, service level, and infrastructure level. Refs. [21] represents the assets dependence chain by an oriented graph where the assets are the nodes. They are organized hierarchically into the business system layer, information system layer, and system component layer. In [24] assets dependencies are arranged in a tree-based hierarchy with the ''building'' asset as the top-level node. There are two kinds of hierarchy links: the ''OR'' and the ''AND'' links. The ''AND'' is a normal link expressing the exclusive dependency that an asset has on its direct superior asset, while the ''OR'' link expresses redundant assets. In [23], a first version of a metamodel describing the Mission and Asset Information Repository (MAIR) is described. A representative set of assets is depicted with their type of dependencies on other assets through hierarchical layers from [26]: the mission layer for mission and business processes assets, the service layer containing common IT service, and asset layer gathering IT infrastructure assets. For asset analysis, in [20], four dependency layers are defined: the mission, the operational, the application, and infrastructure layers. In [25] where a survey of IoT-related solutions for COVID-19, threats in IoT-Based healthcare systems are gathered by layers: threats affecting the cloud computing layer, those affecting the fog computing layer and the ones affecting the healthcare sensor layer. A classification of solutions to combat COVID-19 threat is also provided. We can also find through the paper some covid-19 mobile applications and other IoT-based covid-19 assets that could be capitalized in our ontology in the same way as the identified threats and solutions. On another side, we can also mention for the description of assets ArchiMate 2.1, an open and independent Enterprise Architecture modeling language within TOGAF Framework 9.2 and the CIM standard produced by DMTF (formerly known as the Distributed Management Task Force) that is internationally recognized by ANSI and ISO.

The literature also provides a plethora of models constructed to serve a security purpose ([13], [27], [28]–[30]). Most of them are ontologies. In [30] the proposed ontology is used for generating attacks while [28] and [29] ontologies contribute to social engineering analysis and targeted attacks mitigation. These ontologies emphasize the link between the

asset concept and the other security concepts (threat, vulnerability, etc.). No description neither refinement of the concept ''asset'' is provided. Only dependency link is expressed between assets.

Finally, let us note that some earlier research works focused on the characterization of the dependencies between and within critical infrastructures. Although the terms ''dependency'' and ''inter-dependency'' are commonly used interchangeably, some of these research works distinguish them. The consensual distinction is this of Rinaldi *et al.* [31]. The authors define dependency as a relationship between two infrastructures in a single direction whereas inter-dependency is bidirectional (implicitly multi-directional) with two (implicitly more) infrastructures influencing each other. This definition is also shared by [32]. A more precise definition of the dependency concept is given by [33]. The European Union Agency for Cybersecurity (ENISA) proposes to consider dependencies within critical infrastructures (CIs) and dependencies between CIs. These kinds of dependencies are qualified as upstream, internal, or downstream dependencies in [34]. An upstream dependency expresses the fact that the products or services provided to one infrastructure by another external infrastructure are necessary to support its operations and functions. Downstream dependencies are the consequences to a critical infrastructure's consumers or recipients from the degradation of the resources provided by the critical infrastructure. Internal dependencies represent the internal links among the assets constituting a critical infrastructure. Therefore, upstream and downstream dependencies are between CIs whereas internal ones are within CIs. Several works have focused on the characterization of dependencies between CIs. Ref. [35] distinguishes spatial dependencies from functional ones. Refs. [31] and [33] propose a categorization of dependencies into physical, cyber, geographic, and logical ones. Refs. [36] and [37] consider physical, informational, geo-spatial, policy/procedural and societal dependency. For reasoning purposes, [38] propose another taxonomy of dependencies. They suggest considering five types of dependencies: generic, indirect, inter, co, and redundant dependency. Although the categorizations provided by the literature could be applied for the description of dependencies between assets within an infrastructure, they remain very generic. The complexity of dependencies in hospitals' real-life scenarios did not allow us to exploit these categorizations for a detailed description of the propagation of cyber or physical incidents inside a healthcare infrastructure.

B. INCIDENT PROPAGATION MODELS AND APPROACHES

Because of frequent threats whether they are natural hazards, non-malicious man-made hazards or malicious man-made hazards, risk propagation catches the attention of many scholars. Thus, manifold research efforts are devoted to the capture, modeling and assessing of cascading effects of incidents. The most recent ones are dedicated to critical infrastructures. Some of them analyze impacts within networks of interrelated critical infrastructures (e.g. [39]–[42], [43]). Others focus on a single critical infrastructure (e.g. [44]–[49] [50]–[53]). Moreover, some of the contributions are specific to a type of threat (ransomware, malware [54], spoofing attack [46], terrorist attacks [40], etc.). Others are a little less specific in the sense that they are interested in types of threats like natural disaster (flooding, heatwave, etc.) [44], cyber and/or physical attacks [47]–[49], [51], [55], etc. Some research works concentrate on a type of asset whatever its granularity (healthcare [44], civil aviation [46], power systems [50], [51], [53], [56], port infrastructure [48], airport infrastructure [57], supply chain [56], ADS-B system [46], etc.). However, to our knowledge, no research work is dedicated to the definition of an approach for cyber or physical incident propagation in a healthcare infrastructure as a whole.

Dependency graphs are frequently used to formalize the knowledge useful for analyzing cascading effects between and within critical infrastructures. In [49] the dependency graph represents causality relationships between components in a cyber-physical system. These relationships are quantified using statistical methods. Their approach to identifying these interdependencies relies on observation of the system's behavior in response to each set of failure cases. A failure sequence triggered from a failure case could be the data obtained from a simulation. Ref. [48] also chooses a dependency graph to represent interrelations between assets of the same critical infrastructure. To simulate the behavior of physical and cyber assets after an incident, it proposes to model assets (nodes of the graph) as a probabilistic automaton. In [42] the nodes of the graph are critical infrastructures. They are described by a finite number of different states representing their operational condition. A direct dependency between two critical infrastructures describes the semantics of supplier/customer and is tagged by a variable representing the probability that the source (customer) goes from one state to another state based on the current state of its supplier. In [39], the assessment of cascading effects of common-cause failures on critical infrastructure exploits an oriented graph where cyber and physical dependencies are represented and tagged by the likelihood that a source disruption effects, in cascade, the target. Other artifacts are also used to capture cascading effects. For instance, [58] proposes a domain ontology that captures the core concepts useful for the propagation of physical and cyber incidents in an airport system. They argue that through reasoning it is possible to automatically assess which assets are affected by a given incident. However, no propagation rules have been proposed and the approach to collect these rules is not described. Ref. [59] uses a matrix that gathers potential causal relationships between failures for a set of selected threat scenarios. Its content is produced following workshops bringing together experts. It is produced during a phase of the qualitative method called ISFI (infrastructure service failure interdependency) method focusing on the service level failure interdependencies between different infrastructure and that could be used for crisis management. As far as we are aware, excepting the latter method and ours, there is a lack of

approaches guiding the capture of the knowledge to be used for the identification of cascading effects. Moreover, most of the proposed artifacts for the representation of dependencies between assets also lack contextualization which would calculate the potential effects more precisely. Our contribution goes in this direction since we consider the protections put in place and could be enriched, without major changes by other elements of the context like the availability of the assets (connected or not for the devices, out of order, or in service for certain assets, etc.). The lack of methods for constructing artifacts is compensated by the proliferation of approaches that assess the cascading effects. Most of these approaches focus on interdependencies between critical infrastructures. They are sometimes domain-oriented. However, most of them are based on mathematical models (stochastic colored Petri net model [44], discrete event model [42], [46], Markov-chain model [54], [60], L-hop propagation model [61], etc.) and then requires a simulation step.

The approaches proposed for attack cascading effect mitigation can be grouped into two different sets. The first category focuses on physical infrastructure as in [62], where authors study the inter-dependency relationship among physical elements to detect indirect propagation of critical assets. Other works only focus on specific physical threats such as flooding [63]. In another hand, cyber incident propagation has been studied in [64] and [65]. The latter focuses on risks in administrative domains. Several approaches can be applied to deal with the risk assessment in cybersecurity, such as Bayesian networks [66]. These works do not cover incident propagation to connected infrastructure elements. The work of [67] addresses the impact propagation of cyber incidents using the Petri Nets model, to identify impacted elements and assess their impacts. In recent work, one of the only papers dealing with the propagation of incidents in an integrated cyber-physical context is that of [3]. It considers asset interdependencies for the estimation of the cascading effects of threats. Finally, the literature supplies contributions that generates attacks graphs to simulate a behavior of a information system when an attack occurs. As an example we can cite [30], [68], They often use a simulation environment like cyber ranges to improve, for example situational awareness, to help in risk analysis or teams training.Some of them are purely cyber. Others integrate cyber-physical systems (CPS) or the Internet of Things (IoT) systems. However, none of them take into account physical attacks. They also do not integrate physical assets like building.

To the best of our knowledge, there is no research work measuring the impact of cyber or physical incidents on the assets of healthcare infrastructure.

VII. CONCLUSION

Facing challenges related to the complex cyber-physical attacks targeting critical infrastructure, such as healthcare infrastructure, is of utmost importance given the disastrous damage that can have on organizations and individuals. The approach that we proposed within the SAFECARE project is a response to these challenges as it provides to agents on the front line, the tools to respond quickly and effectively to these complex threats. Indeed, our approach, based on a semantic model and a reasoning engine, allows anticipating impact propagation and helps mitigate potential harming effects while distinguishing highly and moderately impacted assets.

Experiments performed on real scenarios, in different EU hospitals, show effectiveness always higher than 80%, and a time saving reaching 95% which decreases the agent's reaction time after the incident has occurred. IPM guarantees a better view and knowledge of the impacted assets when processing an alert, or before alerts occur as part of the assessment of the risks to which hospitals are exposed. This represents a practical training tool for risk analysis.

The way the approach has been designed makes its extension easier and enables considerably improving its performances by enriching, for example, the rules repository with well documented cyber and physical propagation patterns.

As future work, we plan to expand our research by taking into account additional types of threats, as human faults and natural hazards, and proposing different metrics for the impact score computation that goes beyond protection degrees, as evaluating the severity according to vulnerabilities. We also plan to conceive a user-friendly GUI to help security experts add new propagation rules. To anticipate further complexity matters while expanding to large hospitals with big knowledge graphs and rule bases, we investigate some technical solutions to parallelize the computation of the impact for scaling purposes.

REFERENCES

[1] M. Theocharidou and G. Giannopoulos, "Risk assessment methodologies for critical infrastructure protection. Part II: A new approach," Tech. Rep. EUR 27332, 2015.

[2] J. Depoy, J. Phelan, P. Sholander, B. Smith, G. Varnado, and G. Wyss, "Risk assessment for physical and cyber attacks on critical infrastructures," in *Proc. IEEE Mil. Commun. Conf.*, Oct. 2005, pp. 1961–1969.

[3] S. Schauer, T. Grafenauer, S. König, M. Warum, and S. Rass, "Estimating cascading effects in cyber-physical critical infrastructures," in *Critical Information Infrastructures Security*. Springer, 2020, pp. 43–56.

[4] T. R. Gruber, "Toward principles for the design of ontologies used for knowledge sharing?" *Int. J. Hum.-Comput. Stud.*, vol. 43, nos. 5–6, pp. 907–928, Nov. 1995.

[5] F. Hannou, F. Atigui, N. Lammari, and S. S. Cherfi, "SafecareOnto: A cyber-physical security ontology for healthcare systems," in *Proc. 32nd Int. Conf. Database Expert Syst. Appl. (DEXA)* (Lecture Notes in Computer Science), vol. 12924, C. Strauss, G. Kotsis, A. M. Tjoa, and I. Khalil, Eds. Springer, 2021, pp. 22–34, doi: 10.1007/978-3-030-86475-0_3.

[6] M. C. Suárez-Figueroa, A. Gómez-Pérez, and M. Fernández-López, "The NeOn methodology framework: A scenario-based methodology for ontology development," *Appl. Ontology*, vol. 10, no. 2, pp. 107–145, Sep. 2015.

[7] ENISA. (2016). *Cyber Security and Resilience for Smart Hospitals*. [Online]. Available: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

[8] EBIO. (2019). *EBIOS Risk Manager—The Method*. Accessed: Feb. 18, 2022. [Online]. Available: https://www.ssi.gouv.fr/uploads/2019/11/anssi-guide-ebios_risk_manager-en-v1.0.pdf

[9] K. Stouffer, J. Falco, and K. Scarfone, "Guide to industrial control systems (ICS) security," *NIST Special Publication*, vol. 800, no. 82, p. 16, 2011.

[10] A. Herzog, N. Shahmehri, and C. Duma, "An ontology of information security," *Int. J. Inf. Secur. Privacy*, vol. 1, no. 4, pp. 1–23, Oct. 2007.

[11] A. Ekelhart, S. Fenz, M. D. Klemen, and E. R. Weippl, "Security ontology: Simulating threats to corporate assets," in *Proc. Int. Conf. Inf. Syst. Secur.* Springer, 2006, pp. 249–259.

[12] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas, "MITRE ATT&CK: Design and philosophy," Tech. Rep., 2018.

[13] S. Fenz and A. Ekelhart, "Formalizing information security knowledge," in *Proc. 4th Int. Symp. Inf., Comput., Commun. Secur. (ASIACCS)*, 2009, pp. 183–194.

[14] S. Staab and R. Studer, *Handbook on Ontologies*. Springer, 2010.

[15] M. Rihany, F. Hannou, N. Mimouni, F. Hamdi, P. Tourron, and P. Julien, "A semantic-based approach for assessing the impact of cyber-physical attacks: A healthcare infrastructure use case," in *Proc. 26th Int. Conf. Conceptual Struct. (ICCS)* (Lecture Notes in Computer Science), vol. 12879, T. Braun, M. Gehrke, T. Hanika, and N. Hernandez, Eds. Springer, 2021, pp. 208–215.

[16] ANSSI/ACE/BAC, *Ebios—Méthode de Gestion des Risques*, 2010.

[17] J. Brooke, "SUS-A quick and dirty usability scale," *Usability Eval. Ind.*, vol. 189, no. 194, pp. 4–7, 1996.

[18] HITRUST. (2016). *Healthcare Sector Cybersecurity Framework—Implementation Guide V1.1*. [Online]. Available: https://hitrustalliance.net/

[19] R. White, A. Burkhart, R. George, T. Boult, and E. Chow, "Towards comparable cross-sector risk analyses: A re-examination of the risk analysis and management for critical asset protection (RAMCAP) methodology," *Int. J. Crit. Infrastruct. Protection*, vol. 14, pp. 28–40, Sep. 2016.

[20] F. R. L. Silva and P. Jacob, "Mission-centric risk assessment to improve cyber situational awareness," in *Proc. 13th Int. Conf. Availability, Rel. Secur.*, Aug. 2018, pp. 1–8.

[21] X. Tong and X. Ban, "A hierarchical information system risk evaluation method based on asset dependence chain," *Int. J. Secur. Appl.*, vol. 8, no. 6, pp. 81–88, Nov. 2014.

[22] J. vom Brocke, A. M. Braccini, C. Sonnenberg, and P. Spagnoletti, "Living IT infrastructures—An ontology-based approach to aligning IT infrastructure capacity and business needs," *Int. J. Accounting Inf. Syst.*, vol. 15, no. 3, pp. 246–274, 2014.

[23] EU PROTECTIVE Project. (2017). *Delivrable D4.1*. [Online]. Available: https://protective-h2020.eu/

[24] J. Breier and F. Schindler, "Assets dependencies model in information security risk management," in *Proc. Inf. Commun. Technol.-EurAsia Conf.* Springer, 2014, pp. 405–412.

[25] M. A. Ferrag, L. Shu, and K.-K.-R. Choo, "Fighting COVID-19 and future pandemics with the Internet of Things: Security and privacy perspectives," *IEEE/CAA J. Automa. Sinica*, vol. 8, no. 9, pp. 1477–1499, Sep. 2021.

[26] G. Jakobson, "Mission cyber security situation assessment using impact dependency graphs," in *Proc. 14th Int. Conf. Inf. Fusion*, Jul. 2011, pp. 1–8.

[27] B.-J. Kim and S.-W. Lee, "Understanding and recommending security requirements from problem domain ontology: A cognitive three-layered approach," *J. Syst. Softw.*, vol. 169, Nov. 2020, Art. no. 110695.

[28] T. Li, X. Wang, and Y. Ni, "Aligning social concerns with information system security: A fundamental ontology for social engineering," *Inf. Syst.*, vol. 104, Feb. 2022, Art. no. 101699.

[29] R. Luh, S. Schrittwieser, and S. Marschalek, "TAON: An ontology-based approach to mitigating targeted attacks," in *Proc. 18th Int. Conf. Inf. Integr. Web-Based Appl. Services*, 2016, pp. 303–312.

[30] S. Wu, Y. Zhang, and X. Chen, "Security assessment of dynamic networks with an approach of integrating semantic reasoning and attack graphs," in *Proc. IEEE 4th Int. Conf. Comput. Commun. (ICCC)*, Dec. 2018, pp. 1166–1174.

[31] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *IEEE Control Syst.*, vol. 21, no. 6, pp. 11–25, Dec. 2001.

[32] R. F. Stapelberg, "Infrastructure systems interdependencies and risk informed decision making (RIDM): Impact scenario analysis of infrastructure risks induced by natural, technological and intentional hazards," *J. Systemics, Cybern. Inform.*, vol. 6, no. 5, pp. 21–27, 2008.

[33] W. Schmitz, "Simulation and test: Instruments for critical infrastructure protection (CIP)," *Inf. Secur. Tech. Rep.*, vol. 12, no. 1, pp. 2–15, 2007.

[34] F. Petit, D. Verner, D. Brannegan, W. Buehring, D. Dickinson, K. Guziel, R. Haffenden, J. Phillips, and J. Peerenboom, "Analysis of critical infrastructure dependencies and interdependencies," Argonne Nat. Lab. (ANL), Argonne, IL, USA, Tech. Rep., 2015.

[35] R. Zimmerman, "Understanding the implications of critical infrastructure interdependencies for water," in *Wiley Handbook of Science and Technology for Homeland Security*. 2008, pp. 1–25.

[36] D. Dudenhoeffer, M. Permann, and M. Manic, "CIMS: A framework for infrastructure interdependency modeling and analysis," in *Proc. Winter Simul. Conf.*, Dec. 2006, pp. 478–485.

[37] D. Clemente, *Cyber Security and Global Interdependence: What is Critical?* (Royal Institute of International Affairs). London, U.K.: Chatham House, 2013.

[38] A. O. Adetoye, M. Goldsmith, and S. Creese, "Analysis of dependencies in critical infrastructures," in *Proc. Int. Workshop Crit. Inf. Infrastruct. Secur.* Springer, 2011, pp. 18–29.

[39] P. Kotzanikolaou, M. Theoharidou, and D. Gritzalis, "Cascading effects of common-cause failures in critical infrastructures," in *Proc. 7th Int. Conf. Crit. Infrastruct. Protection (ICCIP)* (Critical Infrastructure Protection VII), vol. 417, J. Butts and S. Shenoi, Eds. Washington, DC, USA: Springer, Mar. 2013, pp. 171–182.

[40] B. Wu, A. Tang, and J. Wu, "Modeling cascading failures in interdependent infrastructures under terrorist attacks," *Reliab. Eng. Syst. Saf.*, vol. 147, pp. 1–8, Mar. 2016.

[41] R. Berariu, C. Fikar, M. Gronalt, and P. Hirsch, "Understanding the impact of cascade effects of natural disasters on disaster relief operations," *Int. J. Disaster Risk Reduction*, vol. 12, pp. 350–356, Jun. 2015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S221242091500028X

[42] S. Schauer, S. Rass, S. König, T. Grafenauer, and M. Latzenhofer, "Analyzing cascading effects among critical infrastructures: The CERBERUS approach," in *Proc. ISCRAM*, 2018, pp. 428–437.

[43] E. Pournaras, R. Taormina, M. Thapa, S. Galelli, V. Palleti, and R. Kooij, "Cascading failures in interconnected power-to-water networks," *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 47, no. 4, pp. 16–20, Apr. 2020, doi: 10.1145/3397776.3397781.

[44] N. Nukavarapu and S. Durbha, "GEO-visual analytics for healthcare critical infrastructure simulation model," in *Proc. IEEE Int. Geosci. Remote Sens. Symp. (IGARSS)*, Jul. 2017, pp. 6106–6109.

[45] D. Rehak, P. Senovsky, M. Hromada, T. Lovecek, and P. Novotny, "Cascading impact assessment in a critical infrastructure system," *Int. J. Crit. Infrastructure Protection*, vol. 22, pp. 125–138, Sep. 2018.

[46] M. Bin Kamaruzzaman, B. Sane, D. Fall, Y. Taenaka, and Y. Kadobayashi, "Analyzing cascading effects of spoofing attacks on ADS-B using a discrete model of air traffic control responses and AGMOD dynamics," in *Proc. IEEE Int. Conf. Cyber Secur. Resilience (CSR)*, Jul. 2021, pp. 241–248.

[47] W. Wang, S. Yang, F. Hu, H. E. Stanley, S. He, and M. Shi, "An approach for cascading effects within critical infrastructure systems," *Phys. A, Stat. Mech. Appl.*, vol. 510, pp. 164–177, Nov. 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0378437118308537

[48] S. König and S. Schauer, "Cascading threats in critical infrastructures with control systems," in *Proc. ISCRAM*, 2019, pp. 1252–1259.

[49] K. Marashi, S. S. Sarvestani, and A. R. Hurson, "Identification of interdependencies and prediction of fault propagation for cyber–physical systems," *Rel. Eng. Syst. Saf.*, vol. 215, Nov. 2021, Art. no. 107787.

[50] H. Liu, X. Chen, L. Huo, Y. Zhang, and C. Niu, "Impact of inter-network assortativity on robustness against cascading failures in cyber–physical power systems," *Rel. Eng. Syst. Saf.*, vol. 217, Jan. 2022, Art. no. 108068. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0951832021005688

[51] V. R. Palleti, S. Adepu, V. K. Mishra, and A. Mathur, "Cascading effects of cyber-attacks on interconnected critical infrastructure," *Cybersecurity*, vol. 4, no. 1, p. 8, Dec. 2021.

[52] X. Gao, M. Peng, and C. K. Tse, "Impact of wind power uncertainty on cascading failure in cyber–physical power systems," *Phys. A, Stat. Mech. Appl.*, vol. 583, Dec. 2021, Art. no. 126358.

[53] Z. Zhao, T. Zhou, Q. Wang, W. Gao, and Z. Zhou, "Research on modeling and simulation of CPPS and its cascading failure mechanism," in *Proc. IEEE 12th Int. Conf. Softw. Eng. Service Sci. (ICSESS)*, Aug. 2021, pp. 42–47.

[54] V. Karyotis, "A Markov random field framework for modeling malware propagation in complex communications networks," *IEEE Trans. Depend. Sec. Comput.*, vol. 16, no. 4, pp. 551–564, Jul./Aug. 2019.

[55] H. Orojloo and M. A. Azgomi, "A method for evaluating the consequence propagation of security attacks in cyber–physical systems," *Future Gener. Comput. Syst.*, vol. 67, pp. 57–71, Feb. 2017.

[56] Q. Zhang, H. Wang, X. Xie, B. He, X. Meng, and L. Huo, "Risk propagation on electric power supply chain networks based on blockchain technology," in *Proc. 6th Int. Conf. Intell. Comput. Signal Process. (ICSP)*, Apr. 2021, pp. 1019–1022.
[57] C. Köpke, K. Srivastava, L. König, N. Miller, M. Fehling-Kaschek, K. Burke, M. Mangini, I. Praça, A. Canito, O. Carvalho, F. Apolinário, N. Escravana, N. Carstengerdes, and T. Stelkens-Kobsch, "Impact propagation in airport systems," in *Cyber-Physical Security for Critical Infrastructures Protection*, H. Abie, S. Ranise, L. Verderame, E. Cambiaso, R. Ugarelli, G. Giunta, I. Praça, and F. Battisti, Eds. Cham, Switzerland: Springer, 2021, pp. 191–206.
[58] A. Canito, K. Aleid, I. Praca, J. Corchado, and G. Marreiros, "An ontology to promote interoperability between cyber-physical security systems in critical infrastructures," in *Proc. IEEE 6th Int. Conf. Comput. Commun. (ICCC)*, Dec. 2020, pp. 553–560.
[59] H. Seppänen, P. Luokkala, Z. Zhang, P. Torkki, and K. Virrantaus, "Critical infrastructure vulnerability—A method for identifying the infrastructure service failure interdependencies," *Int. J. Crit. Infrastruct. Protection*, vol. 22, pp. 25–38, Sep. 2018.
[60] M. Rahnamay-Naeini and M. M. Hayat, "Cascading failures in interdependent infrastructures: An interdependent Markov-chain approach," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 1997–2006, Jul. 2016.
[61] G. Da, M. Xu, and P. Zhao, "Multivariate dependence among cyber risks based on L-hop propagation," *Insurance: Math. Econ.*, vol. 101, pp. 525–546, Nov. 2021.
[62] C.-Y. Liu, A.-P. Jeng, C.-H. Chang, R.-G. Wang, and C.-C. Chou, "Combining building information modeling and ontology to analyze emergency events in buildings," in *Proc. Int. Symp. Autom. Robot. Construct. (IAARC)*, Jul. 2018, pp. 1–6.
[63] A. Serra-Llobet, E. Conrad, and K. Schaefer, "Governing for integrated water and flood risk management: Comparing top-down and bottom-up approaches in Spain and California," *Water*, vol. 8, no. 10, p. 445, Oct. 2016.
[64] N. Ben-Asher, A. Oltramari, R. F. Erbacher, and C. Gonzalez, "Ontology-based adaptive systems of cyber defense," in *Proc. STIDS*, 2015, pp. 34–41.
[65] M. Vega-Barbas, V. A. Villagrá, F. Monje, R. Riesco, X. Larriva-Novo, and J. Berrocal, "Ontology-based system for dynamic risk management in administrative domains," *Appl. Sci.*, vol. 9, no. 21, p. 4547, Oct. 2019.
[66] M. Szpyrka, B. Jasiul, K. Wrona, and F. Dziedzic, "Telecommunications networks risk assessment with Bayesian networks," in *Proc. IFIP Int. Conf. Comput. Inf. Syst. Ind. Manage.* Springer, 2013, pp. 277–288.
[67] M. Szpyrka and B. Jasiul, "Evaluation of cyber security and modelling of risk propagation with Petri nets," *Symmetry*, vol. 9, no. 3, p. 32, 2018.
[68] W. Nichols, Z. Hill, P. Hawrylak, J. Hale, and M. Papa, "Automatic generation of attack scripts from attack graphs," in *Proc. 1st Int. Conf. Data Intell. Secur. (ICDIS)*, Apr. 2018, doi: 10.1109/icdis.2018.00050.

FATMA-ZOHRA HANNOU received the Diploma degree in computer science engineering from the École nationale Supérieure d'Informatique, Algeria, in 2013, and the master's degree in artificial intelligence and the Ph.D. degree in computer science from Sorbonne University, Paris, in 2015 and 2019, respectively. She has been a Postdoctoral Researcher with CNAM Paris, since February 2020. She carries out her research work within the ISID team on the European project SAFECARE. She completed her thesis on the representation and evaluation of data quality. She authored seven papers in international conferences, animated several talks, and earned a Best Paper Award from DBKDA, in 2019. Her research topics include data management and quality, semantic web, and data analysis.

MOHAMAD RIHANY received the master's degree in computer science from Lebanese University, Hadat, Lebanon, in 2016. He is currently pursuing the Ph.D. degree in computer science under the title of exploring RDF data sources from the Versailles Saint-Quentin-en-Yvelines University, Versailles, France. In 2020, he joined the Cérdic Laboratory, Conservatoire National des Arts et Métiers (CNAM), Paris, as a Research Engineer, to work in a European project SAFECARE that integrated cyber-physical security for health services. He is the author of four papers in international conferences. His research interests include semantic web, data analysis, and linked data.

NADIRA LAMMARI received the Ph.D. degree in computer science from CNAM University, Paris, France, in 1996. She has been an Associate Professor with CNAM University, since 1998, where she has been a Researcher with the CEDRIC Laboratory, since 1992. Her research interests include information system security engineering, data anonymization, and ontology engineering. She participated to different French and EU research projects. Some of them are related to information system security domain.

FAYÇAL HAMDI received the M.Sc. degree and the Ph.D. degree in computer science from the University of Paris-Sud, in 2008 and 2011, respectively. He is currently an Associate Professor with the Information and Decision Systems Engineering (ISID) Group, Conservatoire National des Arts et Métiers (CNAM), Paris. His research works include semantic web technologies, ontology alignment, ontology engineering, data integration, and large-scale ontology matching and linked data. He was involved in the last few years in different semantic web projects in collaboration with academic and industrial partners.

NADA MIMOUNI received the Engineering degree in computer science from the University of Tunis, the M.S. degree from Nancy II University, in 2008, and the Ph.D. degree from Sorbonne Paris Nord University, in the framework of the FUI project "Légilocal" on semantic modeling and querying of French legal text networks. She has been a Lecturer in computer science with the Conservatoire National des Arts et Métiers (CNAM), Paris, since 2019. Before joining CNAM, she participated in several projects as a Postdoctoral Researcher at Télécom Paris, in 2018 and 2019, for the "Data & Museum" project, aiming at using semantic web technologies for the exploitation and enrichment of cultural heritage data, and at Paris Dauphine University, from 2016 to 2018, for the "Governance Analytics" project in the framework of the Interdisciplinary and Strategic Research Initiatives (IRIS) led by Paris Sciences et Lettres (PSL) Research University. Her research interests include knowledge extraction and representation and the semantic web with the use of automatic language processing methods for data analysis and exploration.

FATEN ATIGUI was born in Montélimar, France, in 1984. She received the B.S. degree in information and hypermedia from the University of Gabès, Tunisia, in 2008, the M.S. degree in computer science and telecommunication from the University of Toulouse 3, Paul Sabatier, France, in 2009, and the Ph.D. degree in computer science from the University of Toulouse 1 Capitole, France, in 2013. From 2012 to 2014, she was an Assistant Professor with the University of Toulouse 1 Capitole. Since 2014, she has been an Associate Professor with the Conservatoire National des Arts et Métiers (CNAM), Paris, and a member of the CEDRIC Laboratory. She is the author of more than 21 conference papers and three journals articles. Her research interests include business intelligence methods and tools, business analytics and big data, and semantic web.

SAMIRA SI-SAID CHERFI received the Ph.D. degree and her accreditation to supervise research from the University of Paris 1-Panthéon Sorbonne. She is currently a Full Professor and the Head of the Department of Computer Science, Conservatoire National des Arts et Métiers. Her research interests include information systems methodologies, information systems quality and security, methods and tools for information systems engineering, method engineering, and quality assessment and improvement. She supervised several Ph.D. students and has more than 60 papers published in international conferences and journals. She chaired several international events within conferences of her interest domain (RCIS, CAiSE, and ER). She was involved in several projects on data quality, data privacy, and information systems security.

PHILIPPE TOURRON received the Engineering degree in computer science and various postgraduate programs (certified ISO/IEC 27001 lead auditor, ISO/IEC 27005 Risk manager, forensic expert, risk analysis method Ebios professor at Aix-Marseille University). Accustomed to risk analysis and cyber crisis management, he has worked both in the private industry (Michelin Group—seven years) and in the public sector (university and research—18 years). He is also a member of different cyber security groups: Club Ebios (risk analysis method), club 27001 (exchange around ISO 27001 implementation), government groups working to improve standardization of security in health structures (ASIP), and a consultant for the ministry of health (privacy and critical systems). Moreover, he has also been a professor for more than 20 years, teaching networks, risks, and cyber-crisis management. He is a CISO for ten years in one of the three main hospitals in France: APHM. He is also a Coordinator of the Safecare project (European H2020 project: https://www.safecare-project.eu/).