SAFECARE

Integrated cyber-physical security for health services

Specification of the impact propagation and DS models

Deliverable 6.6

Lead Author: CNAM

Contributors: CNAM, CCS, MS, BEIA, SEM, CSI, ISEP, ENC, PMS, PEN

Deliverable classification: (PU)

Co-funded by the Horizon 2020 Framework Programme of the European Union

Version Control Sheet

Title	*Specification of the impact propagation and DS models*
Prepared By	*Samira Cherfi, Nadira Lammari, Fayçal Hamdi, and Faten Atigui*
Approved By	*KUL and ENC*
Version Number	*0.6*
Contact	Samira.Cherfi@lecnam.net

Revision History:

Version	Date	Summary of Changes	Initials	Changes Marked
0.1	14/11/2019	Initial Version	SC, NL, FH, FA	
0.2	27/11/2019	Review KUL	EB	
0.3	28/11/2019	Comments CSI	SA, LV	
0.4	28/11/2019	Review ENC	DF	
0.5	29/11/2019	Adding new content from PEN & PMS	BH	
0.6	15/12/2019	Final revision	SC, NL, FH, FA	

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement no 787002.

Contents

List of Figures

List of Tables

The SAFECARE Project

Over the last decade, the European Union has faced numerous threats that quickly increased in their magnitude, changing the lives, the habits and the fears of hundreds of millions of citizens. The sources of these threats have been heterogeneous, as well as weapons to impact the population. As Europeans, we know now that we must increase our awareness against these attacks that can strike the places we rely upon the most and destabilize our institutions remotely. Today, the lines between physical and cyber worlds are increasingly blurred. Nearly everything is connected to the Internet and if not, physical intrusion might rub out the barriers. Threats cannot be analyzed solely as physical or cyber, and therefore it is critical to develop an integrated approach in order to fight against such combination of threats. Health services are at the same time among the most critical infrastructures and the most vulnerable ones. They are widely relying on information systems to optimize organization and costs, whereas ethics and privacy constraints severely restrict security controls and thus increase vulnerability. The aim of this project is to provide solutions that will improve physical and cyber security in a seamless and cost-effective way. It will promote new technologies and novel approaches to enhance threat prevention, threat detection, incident response and mitigation of impacts. The project will also participate in increasing the compliance between security tools and European regulations about ethics and privacy for health services. Finally, project pilots will take place in the hospitals of Marseille, Turin and Amsterdam, involving security and health practitioners, in order to simulate attack scenarios in near-real conditions. These pilot sites will serve as reference examples to disseminate the results and find customers across Europe.

Executive Summary

This document is part of the WP6: "Integrated cyber-physical security solutions" and contains the specification of the Impact propagation and decision support model (IPM) to be later implemented in continuation of Task 6.4.

The document structure is the following:

Chapter 1 introduces the context of this deliverable and the objectives of the related task.

Chapter 2 contains state of the art analysis for models, methods, standards and tools dealing with similar problems of risks modeling and risk propagation.

Chapter 3 details the specification of the IPM module and the interaction with the other modules from the overall architecture. Since hospitals host a variety of assets dedicated to internal and specific needs, it is necessary to define a model that establishes the set of characteristics necessary for impact propagation specific usage. This model needs to be instantiated on the bases of the data stored in the central database and thus it has to be compliant with the storage structure. The communication with the central database relies on the data exchange layer. The impact propagation should also take into account the degree of risk and incidents severity.

Chapter 4 provides a validation of the specification using real scenarios collected from business partners (hospitals). The details of the scenarios are confidential as they describe real assets and their details (vulnerabilities, configurations and location information etc.). Consequently, as this deliverable is public, the data simulation will not be included. We include, instead, a section of conclusions and lessons learned from this validation exercise.

Chapter 5 summarizes and concludes the deliverable.

1 Introduction: IPM in the global architecture

The impact propagation and decision support model is the cornerstone of the project achievement because it is the component where cyber and physical security management artefacts' interlinking is highlighted.

Hospitals are cyber-physical systems that are vulnerable by nature to a multitude of attacks that can occur at their communication, networking, and physical entry points. Such cyber-physical attacks can have detrimental effects on their operation and the safety of their patients. Thus, to properly secure these systems, it is of utmost importance to: (i) understand their underlying assets with related vulnerabilities and associated threats, (ii) quantify their effects, and (iii) prevent the potential impacts of these attacks.

The challenge addressed by the IPM is to understand the tight relationships between the assets' characteristics and the propagation of attacks' effects to better prevent the impacts and consequences of incidents. Thus, an effective reaction to attacks needs a detailed knowledge of intrinsic and contextual assets properties. However, hospitals host a variety of medical and IT assets with very different characteristics.

The IMP addresses three main objectives:

a) Provide a model that is able to capture the essential characteristics related to incidents understanding and propagation,
b) Take into account the fact that, within the SAFECARE project, this knowledge could evolve as the work with partners, and especially with hospitals, evolves,
c) Propose an impact propagation mechanism specification that considers the assets, their vulnerabilities, their interdependencies, their contextual knowledge and the incidents that occurred in their environment.

1.1 Deliverable 6.6 overview

The aim of task 6.4 is to describe the relations between physical and cyber assets in health services. The objective is to evaluate the impact propagation of both cyber and physical incidents coming from the e-health monitoring system (Task 5.4, D5.8 to be submitted at M25), the cyber threat monitoring system (Task 5.10), and the building monitoring system (D4.10).

This deliverable is dedicated to the IPM specification. The IPM relies on: (1) a model that formalizes the assets semantic interdependencies, and (2) an impact propagation engine that reasons on these relationships to compute potential impacts of cyber and physical incidents and thus anticipate further incidents on the whole system. The model takes into account the variety of the assets such as infrastructures (power supply, air cooling, etcetera), IT systems, medical devices, as well as patients' and personnel's data. The objective is to help improving the safety and security of hospitals and their patients.

As shown in Figure 1, the IPM interacts with the other modules of the system through the Data exchange layer module (D6.3) and the Central database (D6.5). The Central database contains: (1) the descriptions of assets, which are stored through an "ad-hoc" application managing static data, and (2) incidents from BTMS (Building Threat Monitoring System) and CTMS (Cyber Threat Monitoring System) stored through the data exchange layer (DXL). The IPM accesses this data through DXL.

Figure 1: The Impact propagation and decision support model within the global architecture.

2 State of the art

This section presents existing work on impact propagation of incidents and the methods used to assess the severity of incidents and risks.

2.1 Impact propagation analysis in critical infrastructures

ISO/IEC 27005:2008[1] defines the risk of information assets (or systems) as a possibility that the existing threat explores assets' (or systems) vulnerabilities leading to organization damages. According to Kaplan and Garrick [1], the risk assessment requires answering three questions: (1) 'What can go wrong?' (2) 'What is the likelihood?' and (3) 'What are the consequences?'.

To answer the first question, it is necessary to be able to define scenarios on assets and their interdependencies. This relies essentially on correctly modeling the system. The second question identifies the probability of a scenario and the last question refers to the identification of impacts and eventually prevention.

In a cyber-physical system, the analysis, the good understanding, and the representation of the relevant interdependencies will dominate the modeling activity. In fact, the variety of assets, their potential vulnerabilities, and the protection mechanisms associated to them makes the evaluation of potential attacks and the impacts of attacks very complex. The propagation of incidents impacts depends on the nature of dependencies. We could find in the literature a distinction between dependency and interdependency. In the first case, the relationship between assets or critical infrastructure is unidirectional; whereas it is bidirectional in case of interdependency. For sake of conciseness, we will use in this section, the term "interlinking" in both situations.

To categorize critical infrastructures interdependencies, different classifications have been provided in the literature. For more details, author could refer to the review of Ouyang [2] on critical infrastructures interdependencies. To explore the propagation mechanisms, we have adopted the classification from Rinaldi et al. [3] who categorize interdependencies into physical, logical, cyber and geographical (see section 2.3).

From the previous classification, we notice that the interdependencies rely essentially on a high-level categorization of the relationships without going deeper in the characterization of the

[1] ISO, E. (2011). IEC 27005: 2011 (EN) Information technology--Security techniques--Information security risk management Switzerland. ISO/IEC.

nature and the semantics of these interdependencies. This is one of the objectives of the IPM that will be discussed later in this deliverable.

The interdependencies play an important role in increasing the operational efficiency of systems. However, they increase their vulnerabilities by introducing additional channels for risk propagation within sub systems and components. In the literature, there exist several approaches for the propagation of impacts analyzing. As detailed below, we propose to classify these approaches into three categories: empirical approaches, agent-based approaches and network-based approaches.

2.1.1 Empirical approaches

Empirical approaches analyze assets interdependencies relying on experts' opinions and on traces from past incidents. The underlying assumption is that it is difficult to identify assets' interdependencies in normal situations. Thus, analyzing the incidents could help rising intangible relationships among assets under extreme situations such as disasters, failures or attacks. From a theoretical point view, this kind of approaches could be used to extract frequent interdependency failure patterns with their occurrence probabilities. From a practical point of view, to be efficient and reliable, these approaches require uniform data collection method for both incidents and assets description with a sufficient level of details. Moreover, the nature of these interdependencies and their strength have to be precisely qualified and quantified.

In [4] authors defined accuracy, comprehensibility, timeliness and accessibility of data as key characteristics to be able to store, analyze, query, and visualize critical incident information. The analysis of such data could then be analyzed through a rigorous process to mine records of frequent failure patterns as presented in Chou and S. Tseng [5].

Concerning the relationship between interdependencies and propagation of impacts, Mendonça and Wallace conducted [6] a study on the 9/11 World Trade Center attacks and their impact on critical infrastructures and the services they provide. The study showed that approximately 20% of reported disruptions involved interdependency. The authors argued that their study provided some empirical evidence for viewing critical infrastructures as "systems of systems" may help improving response to incidents.

An interesting aspect, not very well investigated in the literature, is the analysis of cascading effects based on the nature of interdependencies and also the combination of incidents effects. The method presented by Kotzanikolaou et al. [7] combines common-cause and cascading events in order to assess the potential risk caused by complex situations. The author considered the cumulative dependency risk of cascading chains.

To conclude on this section, it seems that empirical methods based on the analysis of collected data from traces of incidents and failures, provides a valuable knowledge that could help preventing impact propagation and managing risks.

2.1.2 Agent based approaches

These approaches consider a critical infrastructure system (CSI) as a complex adaptive system. The whole system is analyzed as a complex phenomenon emerging from many individual and autonomous agents. This kind of approaches enables to capture all types of interdependencies among CIS by event simulations. It also provides scenario-based what-if analysis and the effectiveness assessment of different control strategies.

Barret et al. [8] investigated cascading effects in three closely coupled systems that are cellular networks, transportation networks and social phone call networks. They studied the interaction between these systems and the challenges raised by their co-evolution and reaction to incidents. Gomez et al. [9] proposed a method for clustering a network into agents called decision units. This method aims to deal with complexity by exploring relationships between agents' local decisions and their impact at the global level.

These approaches have two main weaknesses. The first one concerns the quality of simulation that is highly dependent on the assumptions made by the modeler regarding agent behaviors. The second one is the sensitive nature of the detailed information about each subsystem

2.1.3 Network based approaches

These approaches enable the dependencies of the connected infrastructures to be represented as a graph. This structure is further used to identify critical paths for incidents propagation. When network-based approaches rely on flow analysis and if detailed information is available, these methods could lead to reliable results with a heavy impact on the method computational cost.

Shah et al. [10] propose to evaluate the resilience of a system under attacks. The infrastructures are modeled using networks of interdependent processes. Simulations on this model attempt to provide the network behavior prediction in the face of different attacks or disturbance magnitudes.

Other approaches for impact propagation analysis exist but are less suitable for our investigations.

2.2 Incidents and impacts assessment

In this section we present existing methods and tools for incidents and/or impacts assessment. Some of them are applied in the industry sector. They generally support monitoring systems.

The cyber threat monitoring system of CCS (Airbus CyberSecurity) uses two main scales (see Figure 2):

- The criticality scale, used to characterize assets, has four levels: low, medium, high and highest.
- The severity scale, used to characterize alerts, has five levels: none, info (for informational messages), low, medium and high. Each alert sent to the cyber threat monitoring system is characterized by the cyber security system's SIEM (security information and event management) using this scale.

If an asset is defined as a group of several components, a specific security assessment is determined based on one of the three aggregation methods below:

- Maximum: this method highlights the dependency link between assets. The asset's security status value will then be the highest value of the components.
- Weighted average: this method is based on the full independence of the assets it includes. The asset's security status value will then be the average value of its components weighted by the sum of the criticality's weights.
- Criticality: this method is based on the full independence of the assets it includes.

In addition to the global criticality of an asset, criticalities in terms of confidentiality, integrity and availability need also to be assessed.

Figure 2: List of devices defined in the cyber threat monitoring system and their associated criticality

Devices | Unreferenced | Sites | Networks | Services | Security

Name ^1	Type	Criticality	C	I	A	Classification	Description	Last modified
79546_eqpt00001	Device	High	Low	Medium	High	Defence - secret		2016-07-04 14:30
79546_eqpt00002	Device	Highest	Highest	Highest	Highest	EU Confidential		2016-07-04 14:30
79546_eqpt00003	Device	High	High	High	High	Restricted Information		2016-07-04 14:30
79546_eqpt00004	Device	Highest	Highest	Highest	Highest	EU Restricted		2016-07-04 14:30
79546_eqpt00005	Device	Highest	Highest	Highest	Highest	NATO Restricted		2016-07-04 14:30
79546_eqpt00006	Device	Low	Low	Low	Low	NATO Confidential		2016-07-04 14:30
79546_eqpt00007	Device	Low	Low	Low	Low	Other		2016-07-04 14:30
79546_eqpt00008	Device	High	High	High	High	Level 3		2016-07-04 14:30
79546_eqpt00009	Device	Highest	Highest	Highest	Highest	NATO Unclassified		2016-07-04 14:30
79546_eqpt00010	Device	Highest	Highest	Highest	Highest	Level 4		2016-07-04 14:30

Pages: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

The Cybersecurity and Infrastructure Security Agency[2] proposes a Cyber Incident Scoring System called the NCCIC Cyber Incident Scoring System (NCISS). This system is based on the NIST Computer Security Incident Handling Guide [11]. It helps experts to determine the priority of limited incident response resources and the level of support required for each incident. This is done by generating incident scores (between 0 and 100) calculated using a weighted arithmetic average. This system's inputs are discrete and analytical assessments of incident characteristics. Its weakness is that it is not currently designed to support cases where multiple correlated incidents may increase overall risk.

The NIS Cooperation Group (NIS CG) proposes a guide for assessing the impact of an incident. This guide concerns incidents that affect the security of network and information systems, in any sector of society. The NIST for the National Vulnerability Database (NVD) uses the Common Vulnerability Scoring System to evaluate the severity of the stored vulnerabilities. This scoring system is based on the evaluation of the vulnerabilities according to a set of metrics.

Finally, we can also cite qualitative assessment of the severity of impacts proposed by risk analysis methodologies like EBIOS RM [12].

In the context of building sector, we can cite XProtect® VMS[3] of Milestone. As part of the core functionality of this tool, impacts scales are distinguished on two levels: events or alarms. Events are any type of information that may be provided to the security agents representing something that happened in a device connected to the VMS. Events do not require the agent attention and do not need to be managed. Originally, alarms are events, but they require the security agents' attention. According to the user's rules defined by the XProtect Rule Engine, events can be considered as alarms. Partners integrating the XProtect VMS are enabled to provide more sophisticated alarming systems and implementing a more structured alarm handling. For

2 https://www.us-cert.gov/CISA-Cyber-Incident-Scoring-System
3 https://www.milestonesys.com/solutions/platform/video-management-software/xprotect-corporate/.

example, in USA, Nemours Children's Health System[4] uses Everbridge[5] partner to contact a broader range of people (security staff, medical staff, patients and their relatives, etc.) according to the severity of the situation. Figure 3 shows the Everbridge template for creating incidents, with the priority "high" for this example. Figure 4 shows an example of launching an actual incident in Everbridge.

Figure 3: Example of template for creating incidents in Everbridge[6]

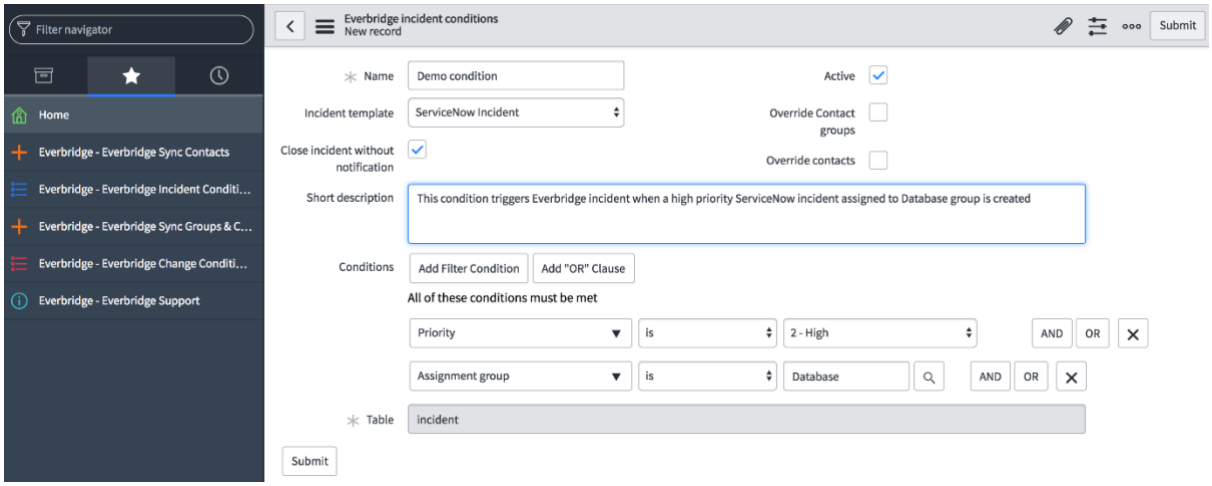
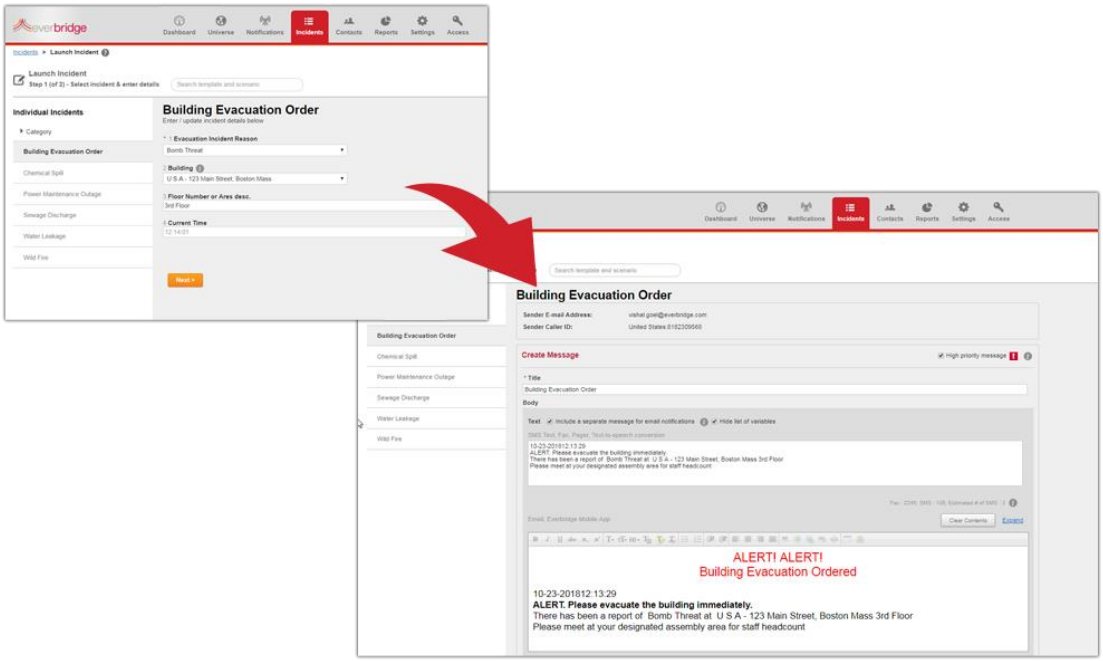


Figure 4: Example of launching an incident in Everbridge[7]



From an academic point of view, several contributions have dealt with the issue of assessing incidents and their impacts. We can mention for instance, a quantitative methodology named SYNEFIA [13]. This methodology evaluates synergistic effects of critical infrastructure failures.

4 https://www.nemours.org/.
5 https://www.everbridge.com/products/visual-command-center/.
6 https://www.everbridge.com/wp-content/uploads/servicenow-screenshot-2-1.png.
7 https://www.everbridge.com/wp-content/uploads/workflow-intelligence-PROD_MN_IC.png

The authors define the synergetic effects as an aggregation effect of impacts' interactions called synergetic impacts. The latter are impacts caused by disruptions or failures of two or more components/ sub-sectors/sectors of the critical infrastructure at the same time. This type of impact could arise from the lack of resilience of a critical infrastructure with respect to the impact of an incident, causing accumulative effects that increase the impact on the system and society. In [14], a quantitative method to assess cascading impacts in critical infrastructures is presented. This method takes into account the typology of incident's impacts. It is a multi-criterial assessment approach based on static stochastic models of the elements/ sub-sectors/ sectors of the critical infrastructure.

2.3 Asset interdependencies

The Council Directive 2008/114/EC (European Union 2008) defines a critical infrastructure as: "*an asset, system of part thereof located in Member States which are essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions*". Therefore, the examination of a critical infrastructure as a whole is crucial while assessing its business or supporting assets [15]. Indeed, dependencies among assets of the internal context of a critical infrastructure must be considered because of cascading effects that a disruption of an asset may have on other assets. It is also required to consider the dependencies that critical infrastructure has with the external context. Among type of dependencies that the ENISA proposes to consider, we can mention the dependencies within a critical infrastructure and the dependencies between critical infrastructures. These kinds of dependencies are qualified either upstream or internal or downstream dependencies in [16]. 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 a critical infrastructure. Internal dependencies represent the internal links among the assets constituting a critical infrastructure. Therefore, upstream and downstream dependencies are between critical infrastructures whereas internal ones are within critical infrastructures.

The following two sections characterize these kinds of dependencies.

2.3.1 Characterization of dependencies between and within critical infrastructures

Although the terms "interdependency" and "dependency" are commonly used interchangeably in the literature related to security, some research work distinguish them. The consensual distinction is this of Rinaldi et al. The authors define a dependency as a relationship between two infrastructures in a single direction, that is, one infrastructure influences the state of another, whereas interdependency is bidirectional (and implicitly multidirectional) with two (and implicitly more) infrastructures influencing each other [3]. A more precise definition of the dependency concept is given by [17].The authors define this concept as *the complete or partial dependence* of an infrastructure on commodities or services of one or more other infrastructures. For [18] the infrastructure interdependencies means a bi-directional relationship between multiple different infrastructures in a general system of systems through which the state of each infrastructure influences or is influenced by or correlated to the state of another.

Several works have been interested in the characterization of the mono/bidirectional dependencies between infrastructures. Table 1 presents the different categorizations with the related definitions.

Table 1 - categorizations of the mono/bidirectional dependencies between infrastructures

Authors	Infrastructure relationship	definition
[19]	Spatial dependency	refers to the proximity of one infrastructure to another
	Functional dependency	refers to a situation where one type of infrastructure is necessary for the operation of another
[3] **[17]**	Physical dependency	arises from a physical linkage between the inputs and outputs of two infrastructures: a commodity produced or modified by one infrastructure (an output) is required by another infrastructure for it to operate (an input)
	Cyber dependency	arises when a state of an infrastructure depends on information transmitted through the other infrastructure
	Geographic dependency	occurs when elements of multiple infrastructures are in close spatial proximity
	Logical dependency	refers to dependency where the state of one infrastructure depends on the state of the other via a mechanism that is not a physical, cyber, or geographic connection
[20] and [21]	Physical dependency	defines an engineering reliance between infrastructures
	Informational dependency	Defines an informational or control requirement
	Geospatial dependency	Defines a relationship that exists due to the proximity of the infrastructures
	Policy/ Procedural dependency	Exists due to the policy or procedures relating an event or state change for an infrastructure to subsequent effect in another infrastructure
	Societal dependency	occurs when an event on an infrastructure component may impact on societal factors of the other infrastructure.

Since these kinds of infrastructure characterization don't allow reasoning about and extracting dependencies, [22] propose another taxonomy of dependencies. They suggest considering five

types of dependencies: generic, indirect, inter, co and redundant dependency. Let A, B and C be three infrastructures. "A" is related to "B" by a generic dependency if some event associated with "A" (source infrastructure) influences "B" (target infrastructure). An entity "C" is indirectly dependent on an entity "A" when events in "A" indirectly influence events in "C" by first inducing events in "B", which in turn induce the events in "C". An interdependency is a two-way relationship where "A" and "B" are mutually dependent on each other. A co-dependency exists between "B" and "C" when they mutually depend on "A" (the source infrastructure), whose failure can lead to a simultaneous failure of "B" and "C". We say in this case that there is a co-dependency of "B" and "C" on "A". If "B" and "C" are related to a target infrastructure "A" ("B" and "C" influence "A") and if the two source infrastructures "B" and "C" must fail before "A" is sufficiently impacted, we say that there exists a redundant dependency of "A" on "B" and "C".

Although initially defined to describe relationships between infrastructures, the defined categorization has also been used for asset dependencies characterization. However, this characterization requires the asset inventory where semantic links between assets are exhibited. The following section tackles this aspect. It presents models describing semantic links between assets.

2.3.2 Models describing semantic links between assets

Several models are presented in the literature for representing semantic links between assets. In [23], four dependency layers are defined: the mission, the operational, the application and infrastructure layers. The mission layer defines the enterprise and organizational entities where the "mission objective" is the essential entity. The latter captures the enterprise level business objectives of the organization. The operational layer gathers two essential assets expressed respectively through the business process entity and the information entity. The business process entity captures business functions and services essential for the organization to function operationally while the information entity models the various information assets that the business uses. Each of these entities can be decomposed into lower level sub-entities as required. The application layer is dedicated to the main information system services represented by the IT services entity. The infrastructure layer represents the software, hardware and networking entities that host and execute the IT services.

The two first layers constitute the enterprise model and the two last ones the IT model. The two models are constituting the mission dependency model where intra and inter layers dependencies are exhibited. Let us note that the inter layer dependencies are hierarchical dependencies. Hereafter an extract of the mission dependency model.

[24] proposes an ontology called OLPIT. According to the authors, the OLPIT ontology reflects the layering suggested by the ITIL [25] and COBIT [26] frameworks. It defines hierarchical relationships between the 3 represented levels: process level, service level and infrastructure level.

In the deliverable D4.1 of the EU project, PROTECTIVE[8], a first version of the metamodel describing the Mission and Asset Information Repository (MAIR) of the Mission impact Management System (MIM) is presented. A representative set of assets is depicted with their type of dependencies to other assets. These assets are distributed among hierarchical layers defined

[8] https://protective-h2020.eu

in [27]: the mission layer comprising mission and business processes assets, the service layer containing common IT service and asset layer gathering IT infrastructure assets. For more details see the EU project, PROTECTIVE.

For asset analysis, [28] represent the Assets Dependence Chain by an oriented graph where the assets are the nodes of the graph. They are organized hierarchically into business system layer, information system layer and system component layer. The business system layer gathers the organizations 'core assets described in terms of business processes, business activities, business data, etc. Information system layer is constituted of assets achieving a variety of business functions and business processes. System components layer represents assets that make up the information systems and maintain their operations. Compared to the above models, this model is poor. Indeed, the only represented relationships between assets are those linking assets from different layers. Moreover, any relationship is generic since it expresses the transfer value of the assets.

Jakobson's graph is a little different from that of Tog and Ban. Indeed, in addition to the nodes representing the assets, this graph has two other special nodes: AND nodes and OR-nodes that represent logical dependencies. The AND-node defines that the parent node depends on all of its children nodes, while the OR dependency defines the required presence of at least one child node.

Breier and Schindler present in [29] dependencies between assets arranged in a tree-based hierarchy with the "building" asset as the top-level node. The hierarchy links are of two kinds: the "OR" and the "AND" links. The "AND" link is a normal link. It expresses the fact that the dependent asset depends exclusively on its direct superior asset in the hierarchy. The "OR" link is used to express redundant assets.

To define models allowing to represent critical infrastructure assets and the semantic links which exist between them, one can rely on Enterprise Architecture (EA) frameworks and standards or methodological guides existing in the industrial world. As an example of EA framework, we can mention TOGAF Framework 9.2[9] which is a standard of the Open Group[10] It aims improving organization business efficiency. Within TOGAF is proposed ArchiMate 2.1, an open and independent EA modeling language. This language provides metamodels for the construction of the architecture repository that allows an enterprise to distinguish between different types of architectural assets existing at different levels of abstraction in the organization: Business, Application, Data, and Technology levels. It also presents a clear set of relationships between and within architecture layers.

We can also mention the CIM standard[11] produced by DMTF (formerly known as the Distributed Management Task Force) and which is internationally recognized by ANSI (American National Standards Institute)[12] and ISO (International Organization for Standardization)[13]. This standard provides a common definition of management information for systems, networks, applications, services and devices using UML language. Dependencies between IS components are expressed.

9 https://pubs.opengroup.org/architecture/togaf9-doc/arch/
10 https://www.opengroup.org/
11 https://www.dmtf.org/standards/cim
12 https://www.ansi.org/
13 https://www.iso.org/

There also exist several security risk analysis methodologies that give description of assets. Most of them are based on standards. These descriptions are very often informal and sometimes accompanied by catalogs. This the case of EBIOS RM [12], MAGERIT 3.0 [30], methodologies. MAGERIT methodology, for example, proposes a catalogue where assets are organized into trees showing dependencies, where the security of the assets higher up in the tree depends on assets in the lower positions. A "higher asset" is said to depend on the "lower asset" when the security requirements of the higher one, are translated into the security needs of the lower one. EBIOS RM gives an informal description of assets where very semantic links could be extracted.

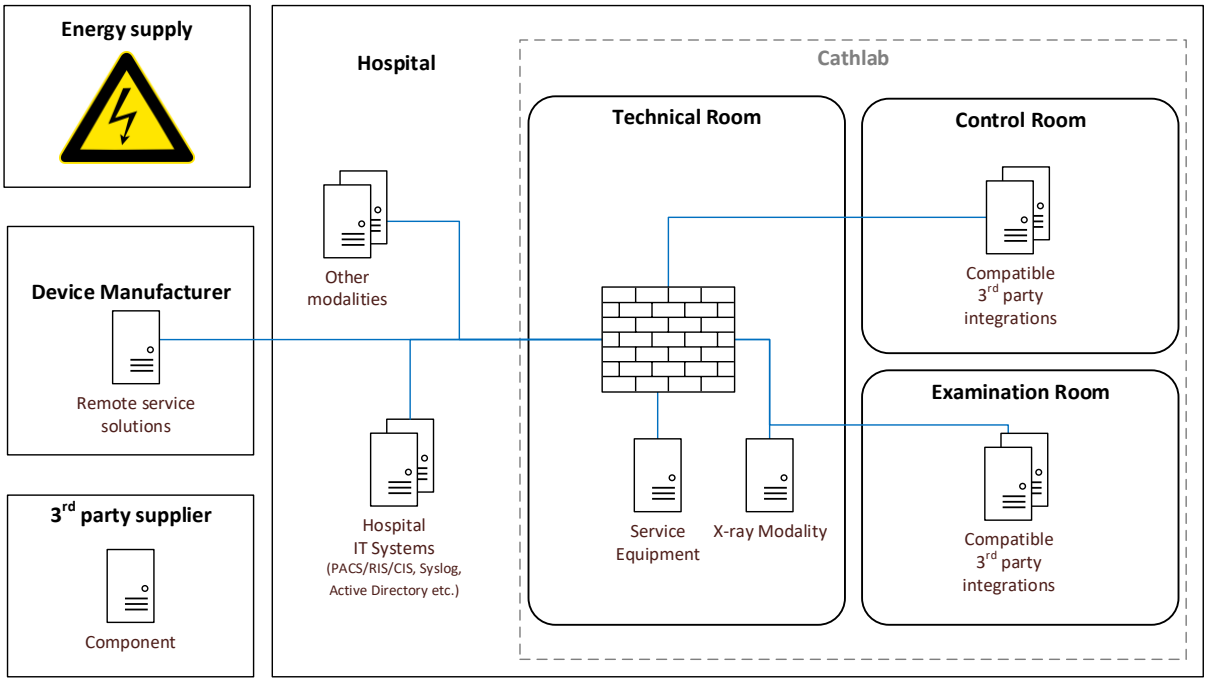
Finally, the National Cybersecurity Agency of France (ANSSI) published a guide helping organizations mapping their Information system (IS). According to the ANSSI, this IS map contributes to the cyber-protection, Cyber-defense and cyber-resilience of Information systems. It supports either vital importance operators like hospitals or public or private organizations. This guide gives a generic, informal and non-exhaustive description of an IS map where dependencies between IS objects are mentioned. This description allows presenting an IS according to three perspectives (business, application and infrastructure perspectives) where each of them is composed by two views. Each view describes IS objects belonging to it and the relationships with other objects of the same view of with another view (of the same perspective or another perspective). For example, the business perspective gathers 2 views: the business view of the eco-system (entities with which the IS interact) and the business view of the IS (the essential/business assets). The infrastructure perspective is structured into two views: the logical and the technical view. The logical view illustrates the logical networks partitioning (IP addresses, VLAN, filtering functions, etc.). The technical view gathers physical equipment's. We can also mention the metamodel proposed by the General Secretariat of the French Government [31], defining the common framework for urbanization of the state information system (IS). This metamodel is organized into five view: strategic, business, functional, application, infrastructure views. Each view exhibits some assets of the IS and semantic relationship between them and between assets of other views.

2.3.3 Assets interdependencies: the special case of healthcare and medical devices

This part will detail the risk induced by interdependencies in healthcare sector for medical devices.

2.3.3.1 System under consideration

Figure 5: Healthcare system from a medical device manufacturer's perspective.



System under consideration (cf. Figure *5*) enables healthcare practitioners to provide minimal invasive image guided diagnosis and treatment of e.g. cardiac diseases. The system is physically divided over multiple rooms which also can contain additional product options and/or compatible third-party medical devices and IT equipment. From an infrastructure perspective the system requires electricity and for optimized workflow a network connection to the hospital network to interact with other modalities and hospital IT systems to exchange patient/examination data, audit trails and more. A remote connection with the device manufacturer can be an option depending on remote service capabilities of the system and if a related service offering is obtained by the healthcare practitioner.

Different types of interdependencies between the infrastructures, systems, and assets within the healthcare system and their potential implications are described with examples in the sections below.

2.3.3.2 Emerging areas of concern in healthcare sector for medical devices

Table 2 below lists the major issues of concern with respect to medical devices in the healthcare critical infrastructure sector structured along the emerging infrastructure themes from [32].

Table 2 - The major issues of concern with respect to medical devices in the healthcare critical infrastructure sector

Selected critical assets	Major critical infrastructure theme	Examples for potential implications
Medical devices	Vulnerability	Medical devices are prone to physical attack e.g. they can be stolen if kept in unlocked room. As most devices are highly connected to systems inside and outside the hospital, they may be vulnerable to cyber-attacks.

	Dependency	Medical devices may depend on operations in other critical infrastructures, including electricity, and information technology.
	Exposure	Medical devices in a healthcare facility may be exposed to natural threats (e.g., hurricane) and human-initiated cyber threats via ubiquitous computing and telecommunications technologies
	Fragility	Medical device operations may be influenced by elements outside the control of the medical device manufacturer and the healthcare facility (e.g., changes in applicable standards and regulations).
	Susceptibility	Operability of medical devices may depend on its ability to resist extraneous events (e.g., continuity of service after a cyber-attack or a power glitch). Resistance to such extraneous events is a joint responsibility of the devices and the healthcare.
	Reliability	Medical devices must be able to perform its intended missions of disease diagnosis and treatment when needed despite threats that may hinder the expected reliability (e.g. malware outbreak in hospital network).
	Resilience	A healthcare facility must enable medical devices to quickly recover from the effects of a natural event (e.g. power outage due to a storm) or human-initiated event (e.g., power outage due to sabotage) because prolonged failures could have a debilitating impact on society.

2.3.3.3 Identifying risks with use cases in healthcare for medical devices

Structured along the interdependency types introduced in 2.3.1, Table 3 below summarizes a representable set of dependency risks associated with medical devices.

Table 3 - Set of dependency risks associated with medical devices

Interdependency type	Implications for risk management
Requires-dependency	Use of a medical device such as radiology device requires connection to hospital network and related IT assets such as a PACS (Picture Archiving and Communication System) to store medical data, Hospital information system that contains patient personal data and patient scheduling information. In addition, medical devices require electricity and an environment which complies to the basic infrastructure needs (power, climate control). These systems and resources have requires-interdependency with the medical devices as a

	risk in these systems affect the hospital operations availability and workflow.
Exclusive-dependency	Interoperability between medical devices might be limited based on device type or dedicated products and software versions. Functionality of the medical devices therefore can be licensed and/or only available in specific combinations.
Hints-dependency	Adoption of technology upgrade program (e.g. operating system, latest security software) ensures that the healthcare industry adopts technologies that have a positive impact on the security, user experience and effectiveness of healthcare operations.
Hinders-dependency	Adoption of new support systems or incompatible interfaces to the existing medical devices may produce unintended negative consequences. For instance, they may require more hospital staff training and/or have configuration incompatibilities.

2.3.3.4 Risks due to interdependency concerns in the healthcare sector for medical devices

Table 4 below presents instances of risks associated to medical device interdependencies.

Table 4 - Risks associated to medical device interdependencies

Type of healthcare interdependency for medical devices	Relevant Themes	Implication for risk management
Physical interdependency	What commodities are produced in other sectors that are consumed by the healthcare system?	Physical access control for medical devices, climate control mechanism (e.g. to maintain appropriate room temperature for ideal device operation), energy sources such as electricity and related safeguards (e.g. UPS). Any disruption in these systems may have implications on the medical device operations. This will in turn affect healthcare operations that depend on these devices.
Cyber interdependency	What data and information are produced and transmitted via information and communications technologies?	Health related personal data of e.g. patient, operator, physician or service engineer in databases, images, reports, logging with ePHI (On media, in memory, in transit and on display). Disruptions in the IT sector may lead to the loss of the above information. This can have a significant impact on medical device operations e.g. incorrect patient scheduling for the use of medical devices.

		There may also be costs associated with data storage, retrieval and transmission, including updating and hacking. This must account for bidirectional risk in interdependent systems.
Geographical interdependency	What are the systems that share the same environment with the healthcare system?	Medical devices are located in hospitals which may share corridors with other structures (e.g. electricity, cables, gas). A vulnerability in the adjacent structure may pose a physical threat to the medical devices that can compromise their operations.
Logical interdependency	On what other interdependent system does the state of the healthcare system depend?	Economic challenges, regulatory submissions of new or upgrades of existing medical devices can possibly affect local healthcare operations.
Policy and/or procedural interdependency	What policy changes can affect healthcare operations?	International, national or regional policy changes (e.g., new procedures or laws) with significant influence on healthcare operations such as GDPR, FDA Cybersecurity guidance and EU MDR (Medical Device Regulation).
Societal interdependency	What public opinions can affect healthcare operations?	Publicly known and/or exploited vulnerabilities in medical devices can have a negative impact on public opinion/trust related to medical devices.

3 Solution description

This part describes the impact propagation model and decision support model solution that includes the specification of the IPM ontology and the IPM rules.

3.1 SAFECARE ontology

This section presents the concepts and properties of the Safecare ontology called *SafecareOnto* as well as its creation process. The Safecare ontology describes both cyber and physical assets, their vulnerabilities and their interdependence as well as the risks and threats. It is the cornerstone of the knowledge graph used by the Impact Propagation and Decision Support Model module to infer the propagation of impacts over cyber and physical assets. In the following section we will, first, describe the construction process of this ontology, and secondly, give details about the concepts and properties of SafecareOnto.

3.1.1 Overview of our ontology building process

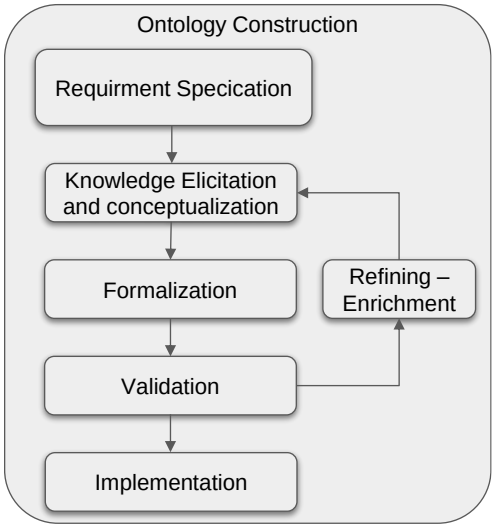
The word “ontology” is used with different meanings in different fields. In the field of computer science, an ontology is “an explicit and formal specification of a shared conceptualization” [33].

The conceptualization corresponds to an abstract model in which the domain knowledge has been captured in a generic way [34]. This domain knowledge is conveyed using the ontology component: concepts, relationships, axioms (rules) and instances. There are several kinds of ontologies. As part of the SAFECARE project, we are concerned with the construction of an application ontology that gathers constructs that depend on both a domain (security of a healthcare infrastructure) and a task (impact propagation).

Transforming the designing ontologies art into an engineering activity has attracted the interest of many researchers. Several methods have been proposed. However, they lack genericity and they essentially include guidelines. For instance, the NeOn methodological framework [35] suggests an ontology design through four phases (requirement specification, knowledge acquisition, conceptualization, formalization and implementation) and identified nine scenarios that could be involved in this process.

For the determination of our approach to build the IPM ontology described in Figure 10, we have been inspired by NeOn methodological framework.

Figure 6: Construction process of the IPM ontology



In the first phase, we provided information about the scope of the ontology (its purpose, the language to be used during its implementation, the target users for which it is intended, its requirements expressed under competency questions).

In the second phase we started by studying the available resources (ontological and non-ontological) favorizing the elaboration of the IPM ontology. The lack of ontological resources that perfectly meet our requirements, led us to choose the option of building a first draft of our ontology from portion of non-ontological resources through an abstraction process in order to identify a core of basic concepts and relationships that must be part of our ontology. As an example of non-ontological resources, we can mention the description of EBIOS RM methodology [12] and the description of medical devices of the MITRE [36]. The conceptualization activity consisted on summarizing, organizing and structuring the knowledge required into a meaningful model. In our case, for representing knowledge conceptual modelling, we opted for the UML class diagram. The benefits of such model for ontology conceptualization have been acknowledged in several studies. One of its main advantages is that it is widely used. Furthermore, users are likely

to be more familiar with a class diagram representation of the ontology (since it is a semi-formal model) than with OWL which representation is purely textual. Thus, it is more relevant for the verification of the ontology scope.

The resulting conceptual model (the first draft of our IPM ontology) has been translated, during the formalization phase into a formal model using the ontology language OWL2. The latter has been initially chosen in the first phase of the building process. This has been, in our opinion, a good choice as it offers a highly expressive language and inference capabilities.

The last phase is under execution. It consists on evaluating the IPM ontology regarding the ability of the impact propagation module to deal with the threat scenarios defined in the SAFECARE project (see for that the deliverable D3.6). The validation step will lead to a refinement and enrichment of the ontology.

3.1.2 SafecareOnto: concepts and properties

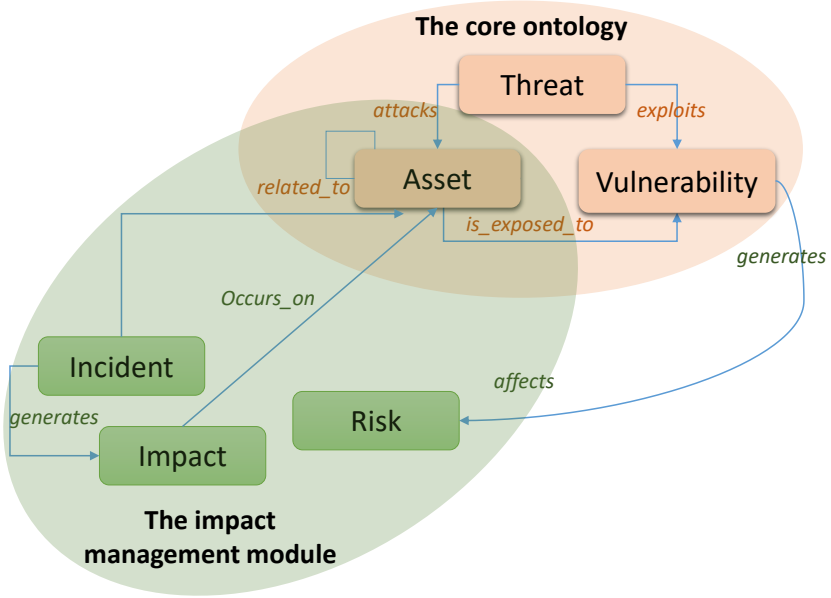
The Safecare ontology called SafecareOnto aims at capturing information about assets and their related knowledge (vulnerabilities, risks, related incidents etc.) that is necessary and sufficient to support risk analysis process addressed by the Safecare project. It therefore abstracts the "semantic" content that is provided by academic literature, standards, hospital partners, open databases about healthcare and IT devices etc.

3.1.2.1 SafecareOnto, a modular ontology

The impact propagation and decision support model relies on both structural information about the assets; their intrinsic properties and their structural relationships as well as on knowledge about the incidents that they suffered from. It also holds knowledge about how to infer and propagate impacts. This second knowledge evolves continuously and is more dynamic that the structural knowledge. For example, the software of a medical asset could be updated to correct a known vulnerability. This kind of operations is less dynamic and more predictable that the occurrence of incidents.

To cope with the static and dynamic knowledge and to confer more stability to the IPM module, we have adopted a modular vision of the ontology. At a high level of abstraction, we could view the whole picture as depicted in Figure 7.

Figure 7: The modular structure of SafecareOnto



The core ontology captures essentially the static and is centered essentially on three concepts that are Asset, Vulnerability and Threat.

An ***asset*** is any "thing" that has value. Within the Safecare projects assets could be ***business assets*** such as personal data about patients and personnel or the patients themselves or ***support assets*** such as medical or IT devices or medical staff. Assets are related to other assets through several kinds of relationships (see section 2.3).

A ***vulnerability*** is any weakness of an asset that could be used to generate a threat. A vulnerability assesses the protection of an asset against attacks. A threat could be accidental or malicious. As an example for "a radiology room" could have as vulnerability "likely to be subject to unauthorized access" and a "patient report" could have as vulnerability "lack of encryption".

A ***threat*** is the operationalization or a materialization of a vulnerability. An asset could be exposed to several vulnerabilities that are known or that could emerge after incidents occurrence. The information about vulnerabilities is updated consequently to regular maintenance operations or after incidents analysis. "Unauthorized access" or "personal data disclosure" are examples of threats. The more we know about the threats that relates to an asset, the more efficient could be its protection and the better we could react when incidents occur.

These basic concepts are further refined and characterized. An excerpt is formalized in section 3.1.2.2. This formalization is done in such a way that it can easily be extended to meet emerging requirements.

The impact management module is an extension to the core ontology that relies on the previous concepts. It allows defining the concepts that are essential to impact propagation computation and provide indicators to help deciding about the suitable countermeasures to face attacks consequences. It relies on concepts such as incident, risk and impact.

An ***incident,*** according to NIST [37], is "an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security

policies, security procedures, or acceptable use policies". An incident could be an attack against one or several assets by exploiting vulnerabilities. In Safecare, we handle both physical and cyber incidents. We also have to assess the severity of an incident to better computer its propagation.

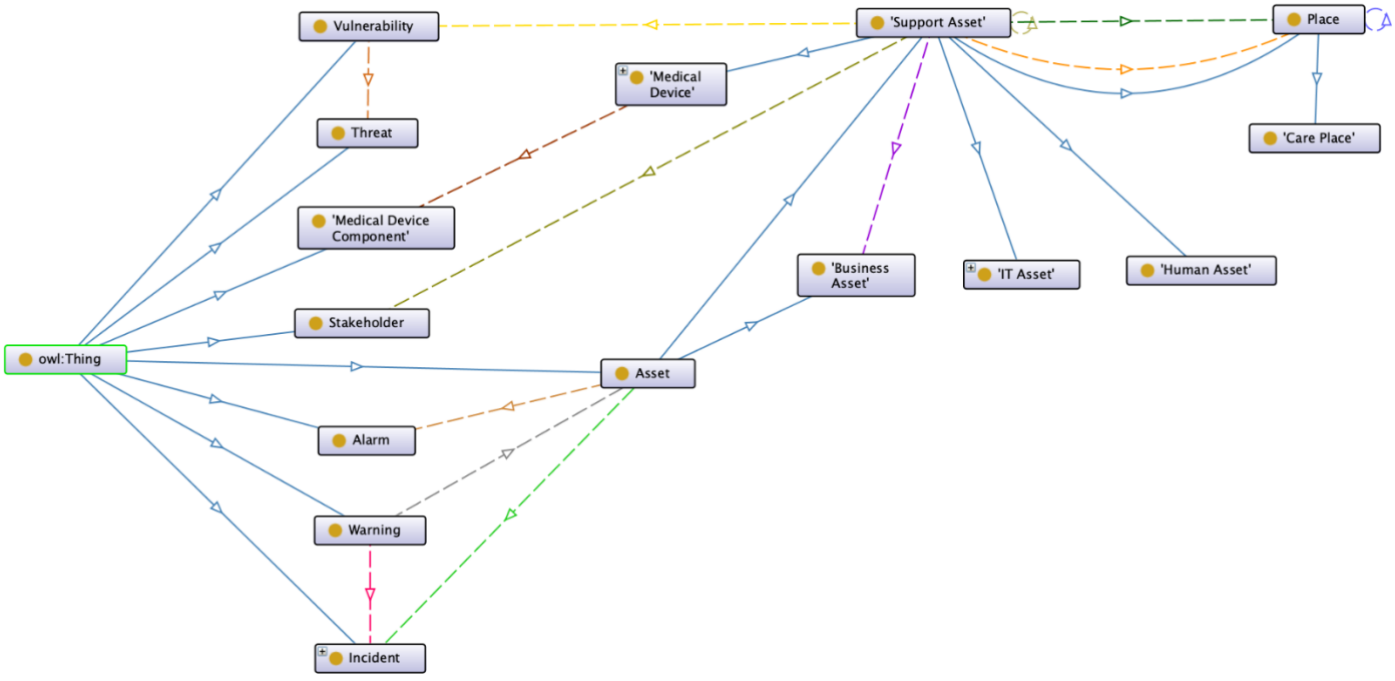
An incident could be the expression of a known ***risk*** or completely unexpected. Indeed, a risk is the probability that a threat will exploit a vulnerability.

When an incident occurs, it is likely to have ***impacts*** on assets. An impact needs to be qualified and/or quantified to efficiently help deciding about the mitigation plans (see section 2.2).

3.1.2.2 Formalization of SafecareOnto

The first version of the SafecareOnto includes the principal classes and properties describing the healthcare physical and cyber assets, their vulnerabilities, their risks and their threats. To avoid deep changes in the future versions, the CNAM has tried to represent as possible the general classes and properties of the domain (e.g. Asset, Vulnerability, Threat, etc.). Hence, classes and properties that will be extracted from new scenarios will be easily integrated in the ontology (for example as sub-classes or sub-properties). Figure 8 represents an excerpt of the SafecareOnto.

Figure 8: Excerpt of the SafecareOnto



The classes and properties defined in the SafecareOnto are presented respectively in Table 5 and Table 6:

Table 5 - Classes of the IPM Ontology

Class	SubClass of
Asset	owl:Thing
Business Asset	Asset

Support Asset	Asset
Human Asset	Support Asset
IT Asset	Support Asset
Medical Device	Support Asset
Medical Impact	Medical Device
Network-connected Medical Device	Medical Device
Standalone Medical Device	Medical Device
Wireless Medical Device	Medical Device
Place	Support Asset
Care Place	Place
Medical Device Component	owl:Thing
Stakeholder	owl:Thing
Incident	owl:Thing
Threat	owl:Thing
Vulnerability	owl:Thing
Alarm	owl:Thing
Warning	owl:Thing

Table 6 - Properties of the IPM Ontology

Property	Domains	Ranges
attachedTo	Warning	Asset
closedTo	-	-
hasAlarm	Asset	Alarm
hasCause	Warning	Incident
hasIncident	Asset	Incident
hasLocation	Support Asset	Place
hasManager	Support Asset	Stakeholder
hasPart	-	-
hasThreat	Vulnerability	Threat
hasVulnerability	Support Asset	Vulnerability
hasWarning	Asset	-

interactWith	-	-
isSupportFor	Support Asset	Business Asset
hasAddress	Support Asset	xsd:string
hasDescription	-	xsd:string
hasId	-	xsd:string
hasManufacturer	Medical Device	xsd:string
hasModel	Medical Device	xsd:string
hasModelVersion	Medical Device	xsd:string

3.2 IPM rules specification

As reported in section 2.1, there are several approaches for impact propagation management. Within the Safecare project, as we do not have any detailed data on previous incidents with the related assets descriptions the empirical approach could not applied and it is not feasible during the project to collect real detailed data on both the hospital configurations (assets and interdependencies) and incidents traces.

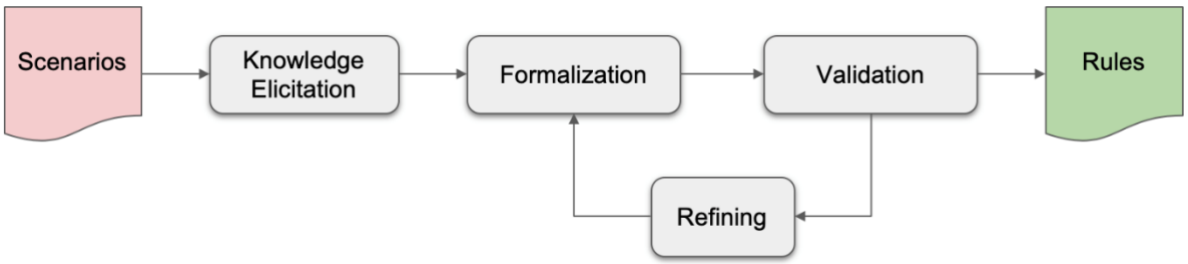
The two other approaches namely agent-based and graph-based are mainly structure oriented. However, from our investigations it appears that a real added value that could be brought by the project to combine cyber and physical incidents and to take into account the variety of interdependencies is by providing a semantic oriented approach based on semantic web technology.

A first solution is consequently based on the exploitation of the ontologies' expressiveness expanded by the usage of inference rules.

This section describes the IPM rules used to automatically infer the impact propagation. Actually, the idea of the IPM module is to use axioms describing the concept and properties of the IPM ontology as well as a set of rules to deal with different threat scenarios. The creation of these rules follows the steps below (cf. Figure 9):

- *Knowledge elicitation*: in this phase, threat scenarios are analyzed and discussed with domain experts to identify, on the one hand, all the assets that could be impacted in each scenario, and on the other hand, the relationships between assets that lead to the propagation of impacts. Moreover, all the situations of a given scenario are analyzed to see if it is possible to generalize common parts. The objective is to avoid redundant rules.
- *Formalization*: in this phase, the concepts and properties of the IPM ontology that can be used to write rules are identified. A rule-engine (e.g. SWRL, JENA) is then used to implement these rules in the form of premises and conclusions. As existing rule-engine are often equipped with semantic reasoners, the implemented rules can be applied to automatically infer impact propagation.
- *Validation and refining*: in this phase, implemented rules are tested on different scenarios and inferred impacts on different assets are evaluated by domain experts. At the end of the validation, IPM rules could be refined to better meet the expected results.

Figure 9: IPM Rules Construction Process



a near-real scenario (cf. Figure 10). Based on the knowledge graph and on IPM rules, a reasoner is used to infer impacts propagation on assets. In this prototype, the IPM rules were expressed in terms of OWL concepts (classes, properties, individuals) using the JENA rule engine[14]. Each rule is composed of a list of body terms (premises), a list of head terms (conclusions). The following example presents a JENA rule that propagates warnings in case of assets located in the same places:

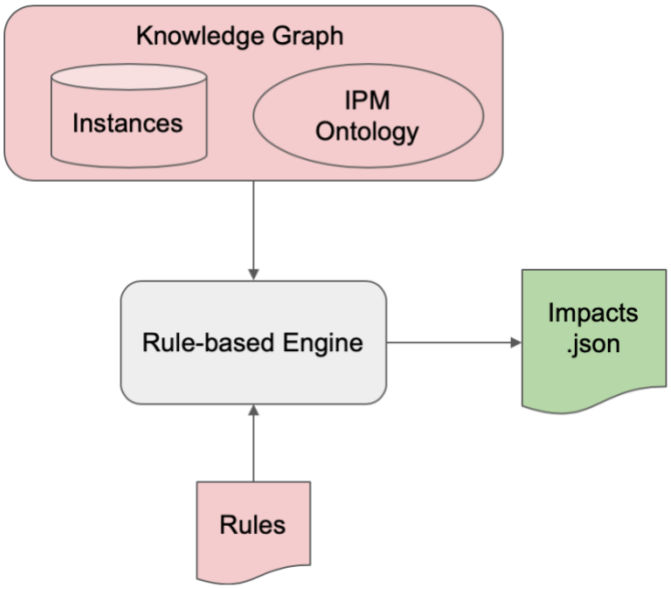
(?asset ipm:hasLocation ?place), (?warning ipm:attachedTo ?place), (?warning ipm:hasCause ?incident), makeSkolem(?new_warning, ?warning) ->

(?new_warning rdf:type isid:Warning), (?new_warning ipm:hasCause ?incident),

(?new_warning ipm:attachedTo ?asset), (?asset ipm:hasWarning ?new_warning)]

The premise of this rule instantiates all the assets having a place, the warnings triggered in this place and the incidents causing these warnings. The conclusion attaches warnings to all assets located in the same place. An application of this rule may be a fire detection incident on a server room that could affect all the materials inside this room.

Figure 10: Architecture of the IPM Prototype



14 https://jena.apache.org/documentation/inference/

This first prototype will, of course, evolve as the project progresses. More complex real-world threat scenarios will be considered to enrich the knowledge base and the IPM rules database.

3.3 Central database – IPM interconnexion

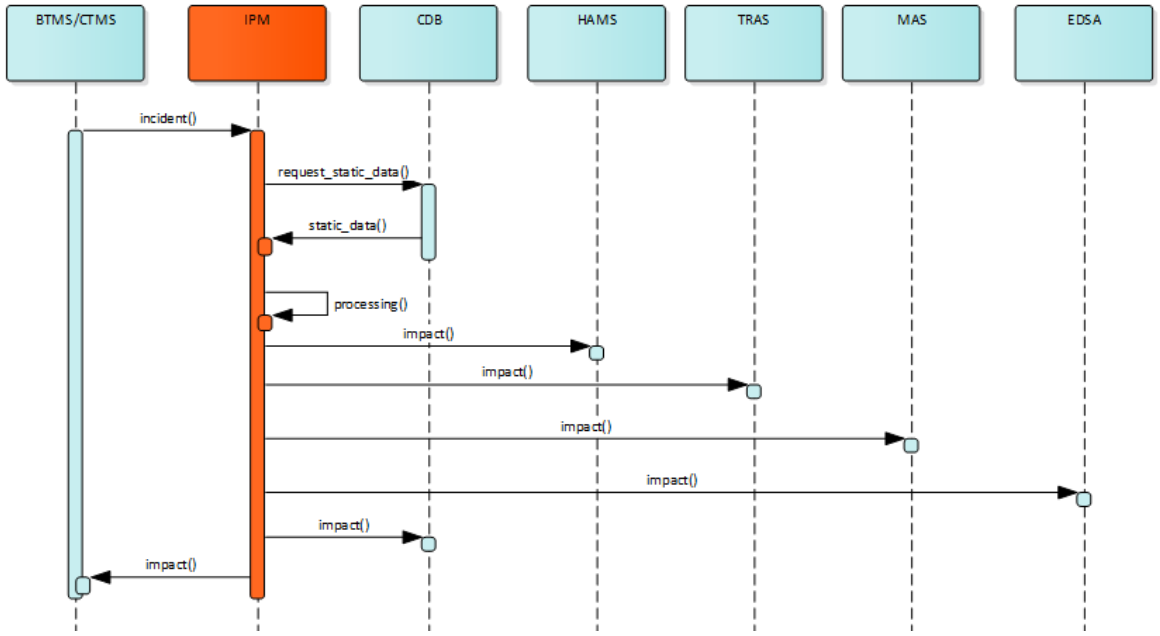
The main objectives of the impact propagation and decision support model are: (i) combine physical and cyber incidents that occur on assets; (ii) infer cascading effects as impacts that could potentially affect the same or related assets, and (iii) alert other modules about the potential impacts and severity. To do so, the impact propagation and decision support models (IPDSM) operates in 2 modes, a static mode for knowledge capitalization about assets and, a dynamic mode for decision support. For both modes, to communicate with the different components of the SAFECARE global architecture, the IPDSM goes through the DXL. It retrieves the information concerning the assets (static mode) of the CDB, and then as soon as an incident arrives, it operates to generate the assets that may be impacted with a degree of severity.

In this section, we present the overall interconnection flow, following the arrival of an incident. Then we detail the two modes of static and dynamic data exchange.

3.3.1 The overall interconnection flow

The interconnection between the central database and the IPDSM goes through the data exchange layer. The IPDSM is a decisional module that generates a response according to the incident. BTMS's and CTMS's role is to elaborate local "events" and "alerts" to determine which of them could be considered as "incident", thus they send incidents to the DXL. Once the incident has been sent to the DXL, the latter publish it and IPDSM receives the incident, then requires static data from CDB, and elaborates an impact that is sent to all other components and stored in CDB. In fact, CDB contains all the static data about health facilities and assets and receives and stores all the dynamic data passing through the DXL. It keeps a historical trace of the happening and makes them available for the other components. Impacts generated by IPDSM and sent to CDB inform about which assets are threatened by the incident and with which degree of severity. The information flow between BTMS/CTMS, IPM and CDB is described in the sequence diagram shown in Figure 11. All the data exchanged among the different modules shown in this diagram go through the DXL.

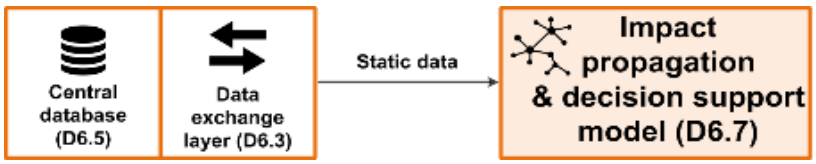
Figure 11: Sequence diagram of data flow relating to IPM



3.3.2 Static data interchange

To be able to reason about incidents and their potential impacts, the impact propagation model needs to hold knowledge about physical and cyber assets that are prone to attacks. To do so, it relies on ontology-based formalization to represent the knowledge about the assets. As sketched in Figure 12: IPM - static data interchange, information about assets is sent by the healthcare facilities, such as hospitals and health services, to the central database to inform the system about changes affecting the assets they hold (new assets or updates on existing ones). The impact propagation model queries regularly the central database, throughout the DXL to get knowledge about the assets and this is done in a static way. Moreover, the impact propagation model acquires extra knowledge about the assets from other sources such as manufacturers and vulnerabilities open databases. These inputs will increasingly enrich the knowledge graph about the assets of the system.

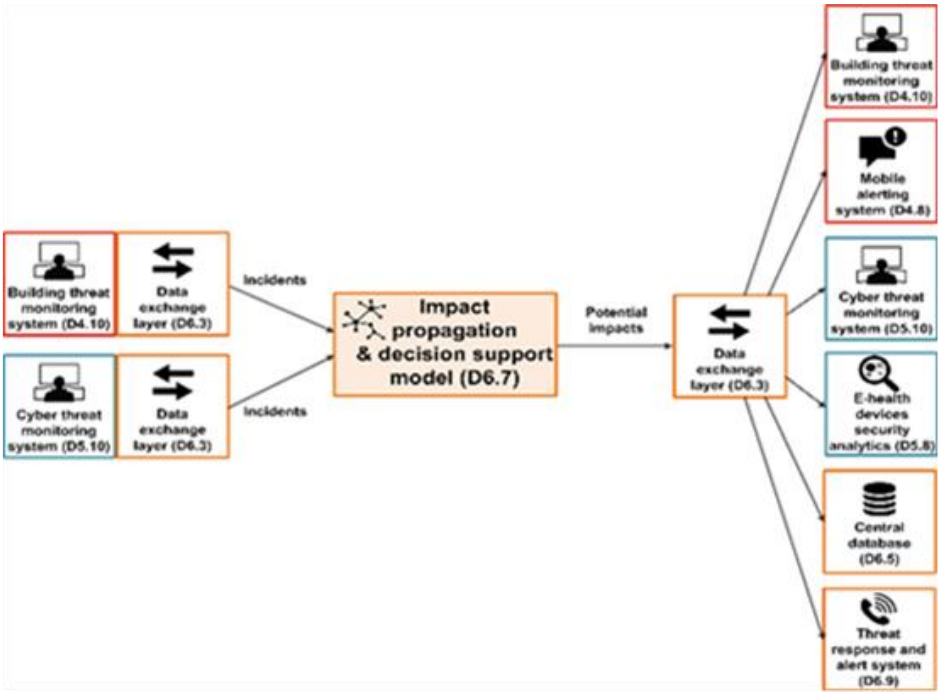
Figure 12: IPM - static data interchange



3.3.3 Dynamic data interchange

The reaction to incidents, even relying partly on static data, need first to be triggered timely by the incident occurrence notification and the related data. This is referred to dynamic data.

Figure 13: IPM - dynamic data interchange



As depicted Figure 13, incidents are pushed dynamically to the IPM through the DXL. The incidents' description includes information about the attacked assets by providing their identification information, the nature and severity of the incident. Based on the knowledge hold about the concerned assets such as known vulnerabilities and relationships with other assets, the state of the related assets resulting from previous incidents, and the propagation rules, the IPM will compute a set of potential impacts on assets. The inferred impacts are qualified by a likelihood value that considers the context of the incident and the impact score induced on the assets by previous incidents. Once the impacts computed, they are sent to the other modules through the DXL.

```
{
	"impact_id":"XXXXXXX",
	"incident_id":"YYYYYYY",
	"assets":[
		{
			"asset_id":"AAAAAAA",
			"risk_type":"Fire",
			"impact_score":1
		},
		{
			"asset_id":"AAAAAAB",
			"risk_type":"Fire",
			"impact_score":0.8
		},
		{
			"asset_id":"AAAAAAC",
			"risk_type":"Data leak",
			"impact_score":0.6
		}]
}
```

An impact consists of a list of assets threatened by a single incident. The list is compiled by the IPM every time that it receives an incident from the DXL. As an output of the decisional algorithm it sends back a ".json" file called "impact". In the example below, it is reported the ID of the incident that generated the impact and the list of assets that will probably impacted, for each of them is specified the risk type (chosen from a list of possible types) and an impact score.

4 Impact propagation issues: lessons learned on top of scenarios

As a support for the specification of the IPM model and SafecareOnto, different scenarios of threat have been identified as the most relevant against critical health infrastructures. These scenarios have been refined in Task 3.4. They have been described with respect to the EBIOS RM methodology using a multistage threat model, frequently referred to as a "cyber kill chain" (see D3.6 deliverable). For each scenario, the involved assets have been identified.

We detail hereby some lessons learned for which the objective is to improve the process of ontology construction and refinement.

4.1 Lesson 1: Details make perfection, and perfection is not a detail

The scenarios are used, in the project, as vectors for entry or exploitation or as a propagation relay for the modelled attacks. Once we started working on this basis, it rapidly appeared that their description is not enough for the development of a successful IPM engine. Indeed, impact propagation requires a detailed and precise information on compromised assets, the way they interact and influence each other, the impact of previous incidents on their state etc. Without this knowledge, propagation is either irrelevant or, even worse, impossible.

However, this kind of knowledge, should essentially be provided by hospitals. Gathering this information on the whole assets in a hospital or even in a service has appeared as unreachable objective due to the volume and the variety of assets, plus the amount of detail required. We thus decided to limit our investigation to the scope of the studied threat scenarios. These extracts will contribute to the validation/refinement/enrichment of SafecareOnto and of the set of propagation rules.

4.2 Lesson 2: The devil is in the detail

For each scenario, we projected to conduct a brainstorming with security experts in order to define, for each cyber or physical supporting asset a description that includes, its role, some of its technical characteristics, the relations it has with other supporting asset of the target, the description of the business process it serves and some of vulnerabilities to which it is exposed. This activity is in progress since, till now, we have collected knowledge about assets of one scenario. These knowledge acquisition allows us to enrich the IPM ontology by other kind of assets. This collaborative work highlighted three issues:

i. The need to revise the classification of assets provided in deliverable D3.3: The classification appeared to be too high level and not enough refined. A more precise classification will lead to an economy of rules as they could be specified on categories of assets instead on specifying them on individual assets.
ii. The lack of likelihood of the defined scenarios: One of the interesting exercises we conducted with hospital partners was to play on the site an attack scenario. This experience showed the lack of likelihood that led to corrective attacks. It also showed the need to define variants to take into account the context of each potential attack scenario such as the mitigation controls currently implemented.
iii. The need to a normalized labelling of assets. Finally, the conducted activity has highlighted the need to characterize more finely both the assets and their relationships.

4.3 Lesson3: Structure is not semantics

It appeared very early that capturing the semantics of interdependencies is crucial for propagation rules expression. We initially tried to solve this issue by refining the categories of interdependencies. We finally reached the conclusion that the semantics problem could not be complete solved through a structural solution of categories of links but through the rules and by relying on combining both structural solution and expressiveness of rules.

5 Conclusion

Based on both the state of the art on existing propagation mechanisms and risks assessment methods, and the description of the assets and scenarios, we have proposed a first version of the ontology. Furthermore, we have instantiated this ontology simulated the propagation rules according to some attack scenarios provided by the partners.

As the assets, their risks and vulnerabilities evolve over time, the ontology needs to be an evolutionary model with an impact on the storage structure of the central database. On the other hand, the quality and the precision of the propagation rules and the computed impacts rely on a fine characterization of the assets' dependencies. Therefore, for next step, it will be essential to integrate the semantics of dependencies and the propagation rules need to formalize the usage of this semantics.

6 References

[1] S. Kaplan and B. J. Garrick, "On the quantitative definition of risk," *Risk Analysis,* vol. 1, pp. 11--27, 1981.

[2] M. Ouyang, "Review on modeling and simulation of interdependent critical infrastructure systems," *Reliability engineering & System safety,* vol. 121, pp. 43-60, 2014.

[3] S. M. Rinaldi, J. P. Peerenboom and T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *IEEE control systems magazine,* vol. 21, no. 6, pp. 11--25, 2001.

[4] D. Laefer, A. Koss and A. Pradhan, "The need for baseline data characteristics for GIS-based disaster management systems," *Journal of urban planning and development,* pp. 115--119, 2006.

[5] C. Chou and S. Tseng, "Collection and analysis of critical infrastructure interdependency relationships," *Journal of computing in civil engineering,* vol. 24, no. 6, pp. 539-547, 2010.

[6] D. Mendonça and W. Wallace, "Impacts of the 2001 world trade center attack on New York City critical infrastructures," *Journal of Infrastructure Systems,* vol. 12, no. 4, pp. 260-270, 2006.

[7] P. Kotzanikolaou, M. Theoharidou and D. Gritzalis, "Cascading effects of common-cause failures in critical infrastructures," in *International Conference on Critical Infrastructure Protection*, 2018.

[8] C. Barrett, R. Beckman, K. Channakeshava, H. F, V. Kumar, A. Martha, M. Marathe and G. Pei, "Cascading failures in multiple infrastructures: From transportation to communication network," in *5th International Conference on Critical Infrastructure (CRIS)*, 2010.

[9] C. Gómez, M. Sènchez-Silvia and L. Buenãs-Osorio, "An applied complex systems framework for risk-based decision-making in infrastructure engineering," *Structural Safety,* vol. 50, pp. 66-77, 2014.

[10] S. Shah and R. Babiceanu, "Resilience modeling and analysis of interdependent infrastructure systems," in *systems and information engineering design symposium*, IEEE, 2015, pp. 154-158.

[11] P. a. M. T. a. G. T. a. S. K. Cichonski, "Computer security incident handling guide," *NIST Special Publication,* vol. 800, no. 61, pp. 1--147, 2012.

[12] ANSSI, "EBIOS Risk Manager – The method," The French National Cybersecurity Agency (ANSSI), 18 November 2019. [Online]. Available: https://www.ssi.gouv.fr/uploads/2019/11/anssi-guide-ebios_risk_manager-en-v1.0.pdf.

[13] R. David, M. Jiri, M. Hromada and K. Barcova, "Quantitative evaluation of the synergistic effects of failures in a critical infrastructure system," *International journal of critical infrastructure protection,* vol. 14, pp. 3--17, 2016.

[14] D. Rehak, P. Senovsky, M. Hromada, T. Lovecek and P. Novotny, "Cascading impact assessment in a critical infrastructure system," *International Journal of Critical Infrastructure Protection,* vol. 22, pp. 125--138, 2018.

[15] ENISA, "Methodologies for the identification of Critical Information Infrastructure assets and services," The European Union Agency for Cybersecurity, 23 February 2015. [Online]. Available: https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis.

[16] 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," 2015.

[17] W. Schmitz, F. Flentge, H. Dellwing and C. Schwaegerl, "Interdependency Taxonomy and Interdependency Approaches," IRRIS Project (Integrated Risk Reduction of Information-based Infrastructure Systems), Deliverable D 2.2.1, 2007.

[18] 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," *Journal of systemics, Cybernetics and Informatics,* vol. 6, no. 5, pp. 21--27, 2008.

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

[20] D. D. Dudenhoeffer, M. R. Permann and M. Manic, "CIMS: A framework for infrastructure interdependency modeling and analysis," in *Proceedings of the 38th conference on Winter simulation*, 2006.

[21] D. Clemente, Cyber security and global interdependence: what is critical?, Chatham House, Royal Institute of International Affairs, 2013.

[22] A. O. Adetoye, M. Goldsmith and S. Creese, "Analysis of dependencies in critical infrastructures," in *International Workshop on Critical Information Infrastructures Security*, 2011.

[23] F. Silva and P. Jacob, "Mission-Centric Risk Assessment to Improve Cyber Situational Awareness," in *Proceedings of the 13th International Conference on Availability, Reliability and Security*, 2018.

[24] 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," vol. 15, no. 3, pp. 246--274, 2014.

[25] AXELOS, ITIL Foundation, ITIL 4 edition, The Stationery Office, 2019.

[26] P. Bernard, COBIT 5 - A Management Guide, Van Haren Publishing, 2012.

[27] G. Jakobson, "Mission cyber security situation assessment using impact dependency graphs," in *14th International Conference on Information Fusion*, 2011.

[28] X. a. B. X. Tong, "A hierarchical information system risk evaluation method based on asset dependence chain," *International Journal of Security and Its Applications,* vol. 8, no. 6, pp. 81--88, 2014.

[29] J. Breier and F. Schindler, "Assets dependencies model in information security risk management," in *Information and Communication Technology-EurAsia Conference*, 2014.

[30] M. Amutio, J. Candau and J. Mañas, "Magerit-version 3, methodology for information systems risk analysis and management, book I-the method," *Ministerio de administraciones pùblicas,* 2014.

[31] PM/SGG/DISIC, "Cadre Commun d'Urbanisation du Système d'Information de l'Etat," Secrétariat général du Gouvernement - Direction interministérielle des systèmes d'information et de communication, 26 October 2012. [Online]. Available: https://references.modernisation.gouv.fr/sites/default/files/Cadre%20Commun%20d%27Urbanisation%20du%20SI%20de%20l%27Etat%20v1.0_0.pdf.

[32] P. Katina, C. A. Pinto, J. Bradley and P. Hester, "Interdependency-Induced Risk with Applications to Healthcare," *International Journal of Critical Infrastructure Protection,* 2014.

[33] R. Studer, V. R. Benjamins and D. Fensel, "Knowledge engineering: principles and methods," *Data & knowledge engineering,* vol. 25, no. 1-2, pp. 161--197, 1998.

[34] B. Chandrasekaran, J. R. Josephson and V. R. Benjamins, "What are ontologies, and why do we need them?," *IEEE Intelligent systems,* vol. 1, pp. 20--26, 1999.

[35] M. C. Suárez-Figueroa, A. Gómez-Pérez and M. Fernández-López, "The NeOn methodology for ontology engineering," *Ontology engineering in a networked world,* pp. 9--34, 2012.

[36] MITRE, "Medical Device Cybersecurity. Regional Incident Preparedness and Response Playbook," October 2018. [Online]. Available: https://www.mitre.org/sites/default/files/publications/pr-18-1550-Medical-Device-Cybersecurity-Playbook.pdf.

[37] K. a. F. J. a. S. K. Stouffer, "Guide to industrial control systems (ICS) security," *NIST special publication,* vol. 800, no. 82, pp. 1-255, 2011.

[38] S. Bhne, G. Halmans and K. Pohl, "Modelling Dependencies between Variation Points in Use Case Diagrams," 2003.

[39] J. D. Thompson, "ORGANIZATIONS IN ACTION: SOCIAL SCIENCE BASES OF ADMINISTRATIVE THEORY," *McGraw-Hill,* 1967.