A domain ontology on cascading effects in critical infrastructures based on a systematic literature review

Beatriz Toscano, André Diegues Fernandes* and Miguel Mira da Silva

Instituto Superior Técnico,
Universidade de Lisboa,
Av. Rovisco Pais 1, 1049-001, Lisboa, Portugal
and
INOV – Instituto de Engenharia de Sistemas e Computadores Inovação,
R. Alves Redol 9, 1000-029, Lisboa, Portugal
Email: beatriz.toscano@tecnico.ulisboa.pt
Email: andre.d.fernandes@ist.utl.pt
Email: mms@tecnico.ulisboa.pt
*Corresponding author

Flávia Maria Santoro

University of the State of Rio de Janeiro,
Rua São Francisco Xavier, 524, Rio de Janeiro, 20550-900, Brazil
Email: flavia@ime.uerj.br

Abstract: Critical infrastructures (CIs) are crucial assets for society and the economy, as they are responsible for providing essential goods and services. The interdependence between CIs makes them vulnerable to large-scale cascading disasters that can significantly impact society. Cascading effects in CIs are thus a worthy area of study and research, with considerable interests in terms of resilience and risk management. In this paper, a domain ontology of cascading effects was developed using the systematic approach to ontology construction (SaBiO) methodology, which provides guidelines for developing domain ontologies. A systematic literature review (SLR) was used to obtain information, an essential part of the first phase of SaBiO. This research identified the main concepts in the domain of cascading effects. Additionally, the relations between the concepts were also identified, which were formalised in the proposed ontology. Besides the proposed ontology, a small analysis of the domain of the cascading effects was also performed. The ontology proposed was also validated using real cases of cascading effects events from an organisation.

Keywords: systematic literature review; interdependencies; ontology; critical infrastructures; SaBiO; cascading effects.

Reference to this paper should be made as follows: Toscano, B., Fernandes, A.D., da Silva, M.M. and Santoro, F.M. (2022) 'A domain ontology on cascading effects in critical infrastructures based on a systematic literature review', *Int. J. Critical Infrastructures*, Vol. 18, No. 1, pp.79–103.

Biographical notes: Beatriz Toscano obtained his Master's in Information Systems and Computer Engineering from the Instituto Superior Técnico of Lisbon – Portugal. She also worked as a researcher in domain ontologies at the INOV Lisbon.

André Diegues Fernandes is currently a PhD student at the Instituto Superior Técnico, University of Lisbon, and researcher in digital resilience at INOV Lisbon. He obtained his Master's in Information Systems and Computer Engineering from the Instituto Superior Técnico of Lisbon – Portugal.

Miguel Mira da Silva is Associate Professor (with habilitation) of Information Systems at the University of Lisbon, Leader of the research group 'Digital Transformation' at INOV, Coordinator of the MISE online Master's degree, and Coordinator of the advanced training programs in the Computing Science Department. His current interests include digital transformation, enterprise architecture and online learning.

Flávia Maria Santoro is the Academic Head of the Institute of Technology and Leadership and Professor at University of the State of Rio de Janeiro. She holds a PhD in Systems and Computer Engineering from the Federal University of Rio de Janeiro (UFRJ), and Bachelor of Electronic Engineering from Polytechnic School of UFRJ. She has been granted the National Council of Technological and Scientific Development (CNPq) Fellowship since 2009. She was on sabbatical at the Université Pierre et Marie Curie – Paris VI, France (2004–2005) and Queensland University of Technology, Australia (2012–2013). She has been working for 20 years as a teacher and researcher in the area of information systems with a focus on business process management, knowledge intensive processes, knowledge management and computer supported cooperative work. She has also worked as a consultant on projects with companies in the area of BPM and software development.

1 Introduction

CIs, which can be either physical or cyber systems, are essential assets for society and economic performance (Schauer et al., 2018a). They are a core part of modern society, supplying essential goods and services for our everyday life (Grafenauer et al., 2018). Examples of CIs in society are the infrastructures of the communication sector (telephone and the internet), the security sector, the financial sector, the health sector, the supply of basic resources (power, gas, or water) and the transportation networks (Abdelgawad and Gonzalez, 2019; Grafenauer et al., 2018).

In the last decade, CIs have become even more interconnected with each other (Van Laere et al., 2017; Schauer et al., 2018b) or more intensively connected (Wang et al., 2018). Research works in the area of CIs' interdependencies categorised them into four different categories: physical, cyber, geographic, and logical (Rinaldi, 2004). The fact that CIs are interdependent makes them vulnerable (Balducelli et al., 2008), meaning that a failure in one CIs can affect the functioning of another one (Abdelgawad et al., 2018). Consequently, a failure in one CIs can trigger more failures and effects in other CIs – an event which is called a cascading effect between CIs (Johansson et al., 2015). A cascading effect is characterised by a 'sequence of events in which each event is the

cause of the following event; all the events can be traced back to the same initial event' (Klaver et al., 2015).

Due to the relevance of this field, we argue that a proper conceptual model would help both the understanding of the domain and the specification of supporting systems. However, to the best of our knowledge, there is a lack of formal definitions to organise and structure this domain knowledge. The main objective of this work is to develop an ontology to represent the domain of cascading effects in CIs to better understand how cascading effects are generated and propagated, how they can be analysed, and how to mitigate their impact on CIs. An ontology is a formal, explicit specification of a shared conceptualisation. It involves concepts and relationships, definitions, properties, and constraints. It is an abstract and simplified view of the world that someone wishes to represent for some purpose (Guarino et al., 2009). A domain ontology is a type of conceptual specification and, consequently, building an ontology is a particular type of conceptual modelling.

For the development of this ontology, we used the SaBiO (De Almeida, 2014), which provides solid guidelines for developing domain ontologies. SaBiO methodology was chosen to construct the cascading effects ontology because it is a proven methodology for developing domain ontologies (Duarte et al., 2018), such as the software process ontology (SPO) (De Almeida and Bertollo, 2009), the software ontology (ROoST) (De Souza et al., 2017), and the ontology of software defects, errors and failures (OSDEF) (Duarte et al., 2018).

In order to support the knowledge acquisition activity in SaBiO, we conducted a SLR (Kitchenham, 2004) to analyse the existing research literature concerning cascading effects in CIs. An SLR, is a widely used methodology for literature reviews (Panichella et al., 2013; Jaramillo-Yánez et al., 2020), intends to identify, evaluate and interpret all the available information concerning a certain research question, topic area or phenomenon of interest. In comparison with traditional literature reviews, the SLR, being a systematic approach, requires a greater effort (Kitchenham, 2004). Our SLR aims to answer two main questions which reflect the purposes of finding the main concepts within the domain of cascading effects in CIs and the relationships among them.

Following the SaBiO methodology and using the information (i.e., concepts, relationships and definitions) from the SM and the SLR, we built the ontology model. The rest of the paper is structured as follows. Section 2 describes the methodology used in this research. In Section 3, the construction of the ontology of cascading effects, following the SabiO methodology, is presented and validated. Section 4 concludes the research work.

2 Structure of the paper

This section presents the two research methodologies used to perform this work: the SaBiO methodology and the SLR.

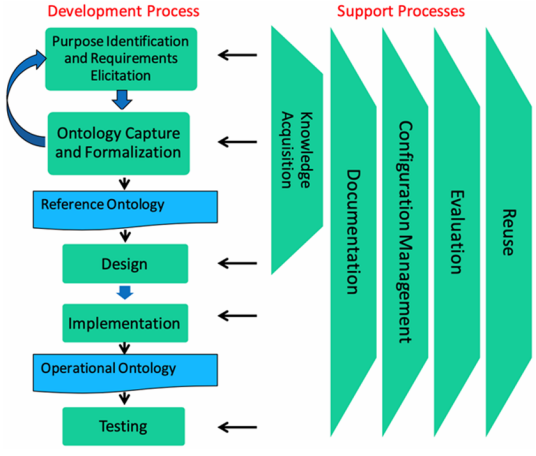
2.1 SaBiO methodology

SABiO focuses on domain ontology developments (De Almeida, 2014) following a process composed of five main phases. The process begins with 'purpose identification and requirements elicitation', followed by 'ontology capture and formalisation' and then

the 'design' phase. After having the ontology formalised and the design completed, the 'Implementation' phase can be performed. Once the ontology has been implemented, the SabiO methodology suggests to end the process with a 'testing' phase.

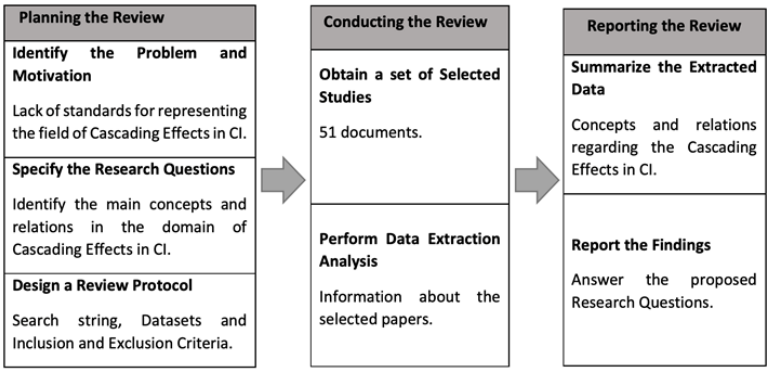
In addition, according to the methodology, some supporting processes should be performed in parallel with the development process. These supporting processes, which include 'knowledge acquisition', 'documentation', 'configuration management', 'evaluation' and 'reuse', are presented in Figure 1. The ontology developed is a domain ontology focusing on cascading effects in CIs. A solution-independent specification (conceptual model) was constructed to best describe this domain without using any reference ontology. Therefore, only the first two phases of the development process were performed (Figure 1).

Figure 1 SaBiO development process (see online version for colours)



Source: Adapted from De Almeida (2014)

Figure 2 Systematic literature review phases



2.2 Systematic literature review

An SLR is a systematic research methodology to perform a literature review. It allows the identification, analysis, interpretation and summary of all available information regarding a specific area, topic or question (Kitchenham, 2004). By applying this methodology, reliable and unbiased results can be obtained.

As mentioned, the SLR used is based on Kitchenham's method (Kitchenham, 2004), which consists of the following phases:

- *Planning:* Exposes the need to perform a systematic review that summarises all information about a particular topic or area in an unbiased manner. The research questions, SLR objectives, exclusion and inclusion criteria are defined, and a review protocol must be written.
- *Conducting:* Applies the review protocol previously defined as a way to obtain studies that contain the information that will be the object of the review.
- *Reporting:* Intends to write and summarise the extracted information from the selected studies.

The three phases of the SLR described above are represented in Figure 2, which specifies the work done in each phase. SLR was selected for this work because it is an acknowledged research methodology, which allowed us to collect and summarise the important concepts of the field of cascading effects in CIs.

3 Cascading effects' ontology construction

This section concerns the construction of the ontology of cascading effects by performing the first two steps of the SabiO methodology, namely 'purpose identification and requirements elicitation' and 'ontology capture and formalisation'. Since the ontology developed was intended to be a reference model and not to be applied in practice, the remaining steps were not required.

3.1 Purpose identification and requirements elicitation

Before starting the ontology construction, it is essential to identify its purpose and intended uses. To define the ontology's scope, a set of competency questions (CQs) was proposed. CQs are questions which the ontology will be able to answer correctly and which can be used later to check its validity (Hippolyte et al., 2018). The defined CQs were obtained using 'middle out strategy', one of the most used strategies when constructing ontologies. The final set of CQ is:

CQ 1 What are the cascading effects composed of?

CQ 2 What initiate cascading effects?

CQ 3 What do the cascading effects generate?

CQ 4 How are cascading effects propagated?

CQ 5 How can cascading effects be analysed?

CQ 6 What types of analysis approaches exist?

CQ 7 How can the impact of cascading effects be assessed?

CQ 8 What types of assets are CIs composed of?

CQ 9 What types of interdependencies exist among CIs?

CQ 10 How can the risks associated with the interdependencies between CIs be minimised?

3.2 Ontology capture and formalisation – systematic literature review

The ontology capture phase is strongly supported by the knowledge acquisition process (De Almeida, 2014). In this research, the extraction of the knowledge for building the ontology was performed through an SLR.

3.2.1 Planning the review

This section corresponds to the first step of the SLR methodology. The motivation for this work was first stated, followed by the objectives and research questions to be answered. Finally, the z presented.

3.2.1.1 Definition of research questions

This research aims to explore the content of the existing primary studies published on cascading effects in CIs. The research questions (RQs), which represent the objectives of this study, are:

RQ 1 What are the main concepts in the domain of cascading effects in CIs?

RQ 2 What are the definitions and relations among the identified concepts?

3.2.1.2 Review protocol

The studies should be collected, according to Peterson et al. (2008), using a search string derived from the defined research questions. A systematic approach to create the search string is to structure it in terms of population, intervention, comparison, and outcome (PICO) as follows:

- population: published studies
- intervention: cascading effects, CIs
- comparison: not applicable
- outcome: published studies on cascading effects in CIs.

Using the PICO approach, the following search string was built: TI (‘critical infrastructure’ OR ‘CIs’) OR AB(‘critical infrastructure’ or ‘CIs’) AND (TI ‘cascading effect’ or ‘cascading effects’) OR AB(‘cascading effect’ or ‘cascading effects’). The defined search string was used to query different data sources. To obtain the set of papers, the string was searched for in the studies’ titles and/or abstracts.

The defined search string was used to query the following five different sources:

- https://www.ebsco.com/products/research-databases EBSCO
- http://www.isiknowledge.com ISI Web of Science
- https://ieeexplore.ieee.org IEEE Digital Library
- http://www.sciencedirect.com Science@Direct
- http://www.scopus.com Scopus
- http://link.springer.com Springer Link

A total of 635 studies were obtain at the end of the database search.

3.2.1.3 Inclusion and exclusion criteria

Several inclusion and exclusion criteria were defined in order to retain only the studies that were relevant to the research.

Inclusion criteria:

- indexed conference or journal
- papers concerning the cascading effects topic
- peer-reviewed papers.

Exclusion criteria:

- a study that was not peer-reviewed;
- a study that was not written in English;
- a study that only concerns cascading effects regarding environmental catastrophes or natural disasters (such as floods, earthquakes, etc.)
- mention of cascading effects in CI in the title/abstract but did not explored them in the content of the paper.

As quality metrics, the following acceptance criteria were defined:

- Article published in journal/conference with H index greater than or equal to 5.

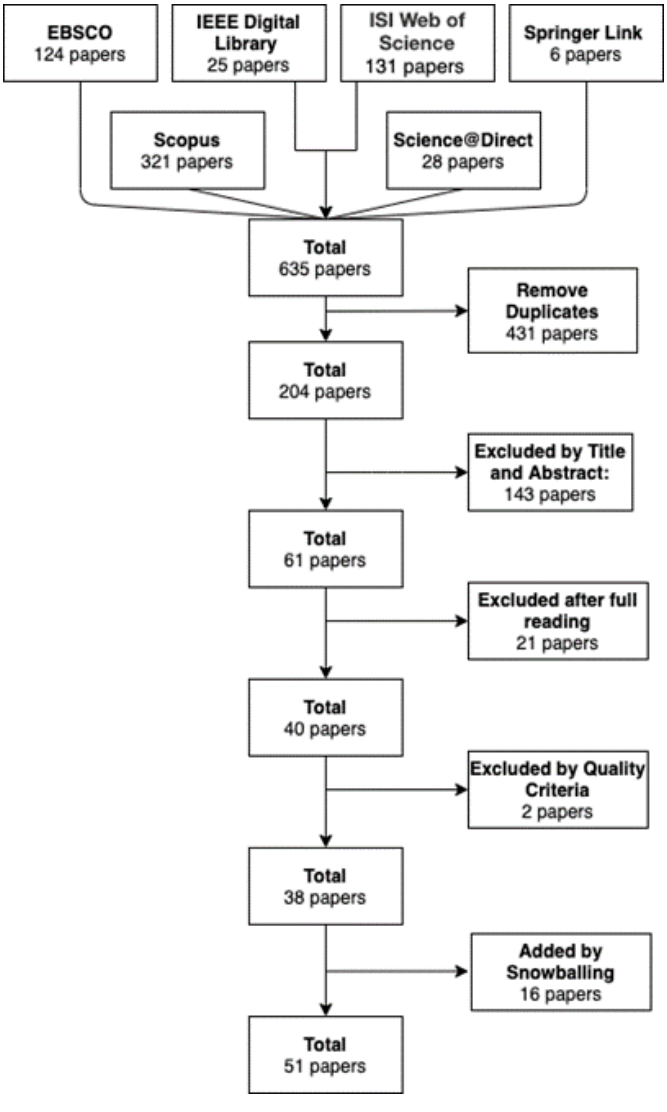
3.2.2 Conducting the review

This section concerns the second phase of the SLR methodology. To obtain the final set of papers, a phased process was executed over the first set of 635 papers collected, as shown in Figure 2.

After the removal of duplicates (431 papers), a total of 204 papers were obtained. The titles and abstracts of these papers were read and the papers were classified into three types: ‘accepted’, ‘rejected’ and ‘undefined’. Eight papers were classified as ‘undefined’ and therefore, they were analysed and discussed by two more researchers to decide whether or not they should be accepted. In total, 143 papers were excluded because they did not comply with the inclusion and exclusion criteria. The remaining 61 papers were fully read and again filtered according to the inclusion and exclusion criteria and the

quality criteria. A final set of 37 papers was obtained (Table 1). The snowballing technique (Wohlin, 2014) was applied on this set of papers to obtain a more complete set, which resulted in an addition of 13 new papers, making a final set of 51 papers.

Figure 3 Selection of papers process



3.2.2.1 Data analysis

After the final set of papers was obtained, they were fully analysed. It was discovered that the year with the most published articles is 2018. As can be seen in Figure 4, the number of publications over the years showed an increasing trend. Figure 5 shows the main publishers in the collected sample. 59% of the publishers had only one associated paper and are not represented in Figure 5.

Figure 4 Number of papers published over the years (see online version for colours)

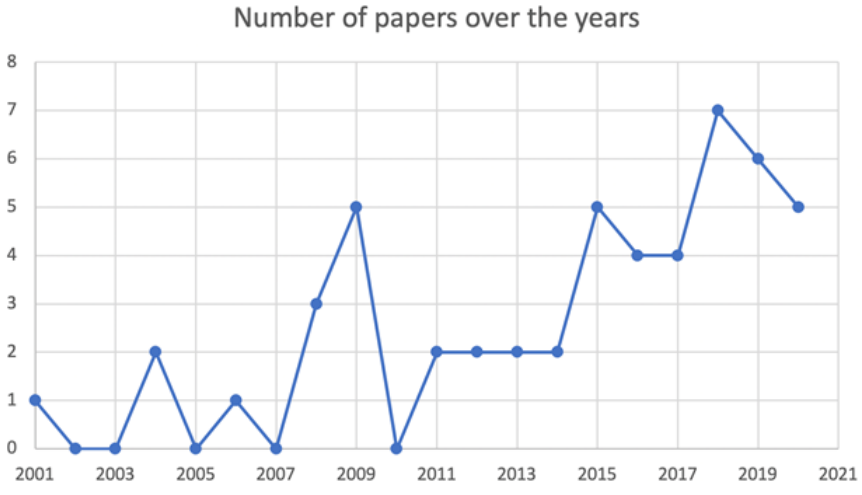
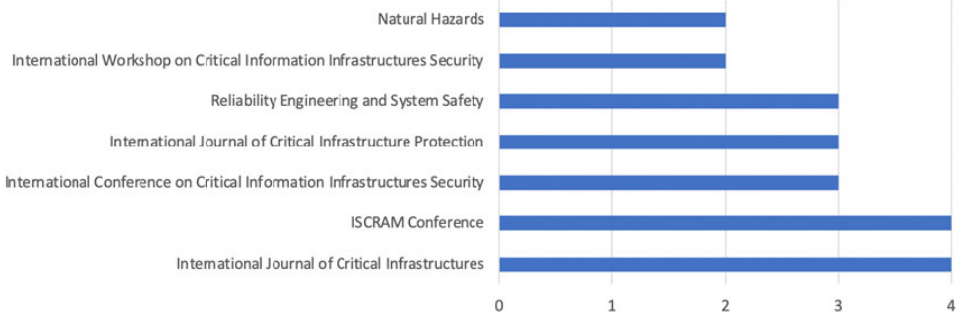


Figure 5 Classification of papers by publisher (see online version for colours)



3.2.3 Reporting the results

This section concerns the last phase of the SLR. The results were divided into two different topics: 'main concepts concerning cascading effects in CIs' and 'definitions and relations among the identified concepts concerning cascading effects in CIs'.

3.2.3.1 Main concepts concerning cascading effects in critical infrastructures

To identify the main concepts concerning cascading effects in CIs, a systematic mapping (Petersen et al., 2008) was performed during the reading phase of the introductions and conclusions of the 50 selected papers. All phrases that included the term 'cascading effect' were extracted and analysed and a word cloud was built, as shown in Figure 7.

In agreement with the keywords found and the topics of research identified in the selected papers, it was noticed that the terms/concepts most strongly related to cascading effects are CIs, dependency, interdependency, impact, risk, simulation, model, propagation and vulnerability.

After this first approach for finding the main terms, a deeper and more detailed reading was carried out on the final set of studies selected in this SLR, taking into account the CQs defined in Section 3.1. The final set of terms was obtained after the mains terms were refined, which is presented in Figure 8.

Table 1 Cascading effect definitions

"A domino effect is a phenomenon in which a primary event at a unit triggers secondary events at nearby units through escalation vectors." (Arief et al., 2020)
"A cascading phenomenon occurs when the failure of one component of the system induces an overload in adjacent components increasing their failure probability. If the overload can be compensated by the strength of the adjacent components, the cascade may be arrested, otherwise the cascade may become an avalanche causing a progressive and rapid disruption of all the system." (Codetta-Raiteri et al., 2012)
"(…) cascading (domino) effect, i.e., the triggering of a series of out of service and cascading disruptions that cause the paralysis of apparently unlinked distinct services." (Franchina et al., 2011)
"Cascading effects in crises refer to a situation where a disruption of one element, such as infrastructure, causes a sequence of disruptive events, which can cause deleterious impacts far beyond the initial impacts of the crisis." (Graham, 2010)
"Cascading effect is a sequence of events in which each individual event is the cause of the following event; all the events can be traced back to one and the same initial event." (Klaver et al., 2015)
"A cascading failure occurs when a disruption in one infrastructure affects one or more components in another infrastructure, which, in turn, leads to the partial or complete unavailability of the second infrastructure." (Kotzanikolaou et al., 2013)
"A cascading failure is defined as a failure in which a disruption in an infrastructure A affects one or more components in another infrastructure, say B, which in turn leads to the partial or total unavailability of B." (Kotzanikolaou et al., 2011)
"In our analysis, we will classify events in cascade initiating events, cascade resulting events and independent events. A cascade initiating event is an event that causes an event in another CI or CI service; a cascade resulting event is an event that results from an event in another CI or CI service, and an independent event is an event that is neither a cascade initiating event, nor a cascade resulting event" (Luiijf et al., 2008)
"A cascading failure occurs when a disruption in one infrastructure causes the failure of a component in a second infrastructure, which subsequently causes a disruption in the second infrastructure (e.g., an electrical power failure could create disruptions in other infrastructures)" (Rehak et al., 2018)
"When a disruption in one infrastructure causes the failure of a component in a second infrastructure, which subsequently causes a disruption in a second infrastructure." (Rinaldi et al., 2001)
"'Cascading effects' is the overall hazard/impact scenario timeline, including the chain of events (cascading events) and damage caused by cascading events on elements at risk assumed in the evaluation (i.e., people, buildings, infrastructures, economy, etc.)." (Zuccaro et al., 2018)
"CIs are essential resources for the performance of society, including its economy and its security, understood as safety of citizens and security of society's assets. They are slightly differently defined in different countries. However, there is general agreement that CIs include government, telecommunication based on ICT (information and communication technology); financial sector; energy supply; water transportation systems; health sector; and security services (first responders, police, military)." (Abdelgawad et al., 2018; Abdelgawad and Gonzalez, 2019)

Table 2 Critical infrastructure definitions

"When we consider CIs, we have to take into account that they are not simply 'physical' plants and networks. In fact, they contain not only a physical layer, but are also made of 'cyber' components and systems, and include human organisations that manage and supervise the daily operations of the infrastructure." (Balducelli et al., 2008)
"CIs are complex system of systems due to the existence of interdependencies that are not readily visible but very often play a central role." (Foglietta et al., 2015)
"CIs are a core part in modern society, supplying essential goods and services for our everyday life. Therefore, any incident compromising the operation of a critical infrastructure can directly affect the social life. (…) CIs represent the backbone of today's society. They implement core functionalities and services of our day to-day life, i.e., supply networks for basic resources (power, gas or water), communication networks (telephone and the internet) or transportation networks (land, air and sea)." (Grafenauer et al., 2018)
"CIs are defined as systems and assets, whether physical or virtual, so vital to the nation that their incapacity or destruction would have a debilitating impact on the nation's existence." (Gueye et al., 2020)
"CIs are large-scale engineered physical structures underpinning every aspect of a modern society. Prominent among them are electric power systems, telecommunication systems, the internet infrastructure, gas and oil production, storage and transportation systems, transportation infrastructure, water-supply systems, and others. These systems are responsible for materials, energy, and information flows that are vital to the security of our homeland and the well-being of our society." (Jiang and Haimes, 2004)
"CIs and societal functions, such as transportation, telecommunications, health care, and energy distribution, constitute the backbone of a modern society." (Johansson et al., 2015)
"Critical infrastructure is an asset, system or part thereof which is 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 as a result of the failure to maintain those functions." (Klaver et al., 2015)
"In particular, CIs can be seen as central elements in a widespread network of risk, because, for the most part, they have physical attributes as well as functional and organisational ones (Penuel et al., 2013). They can be associated with widespread breakdowns, which may cause great harm and may become full-blown transboundary catastrophes." (Ansell et al., 2010; Boin and McConnell, 2007; Pescaroli and Alexander, 2016)
"CIs are assets or systems (or parts thereof) which are essential for the maintenance of vital societal functions" (Schauer et al., 2019)
"CI is the essential physical and virtual systems (or assets) that significantly impact national security, economic security, public health, and public safety, such as electric power distribution system, transportation system and water supply system (Brown et al., 2006; United States, 2013). CIs provide the foundation for human livelihood, social and economic development, and national security." (Wang et al., 2018)

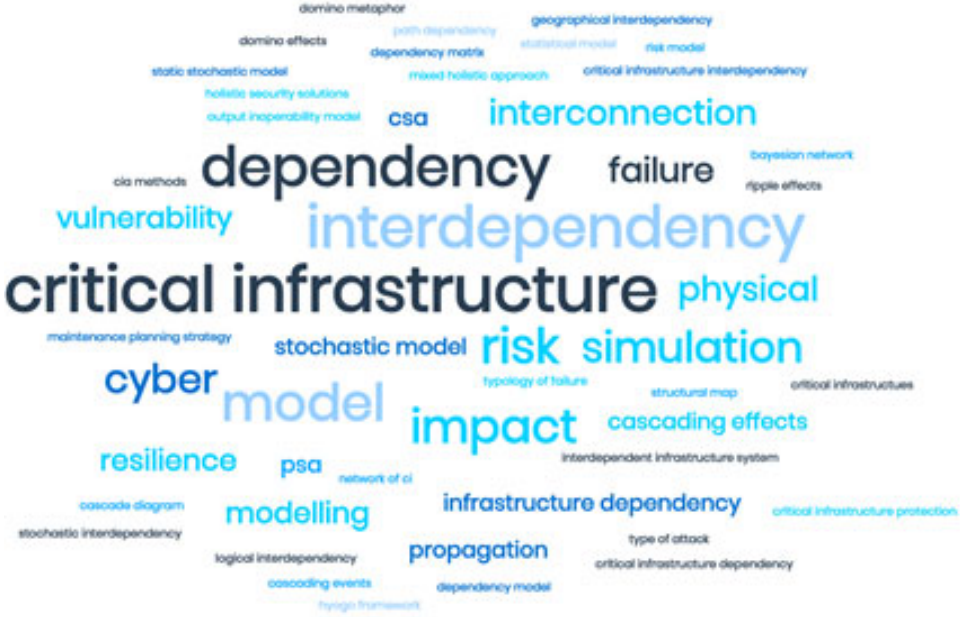
3.2.3.2 Definitions and relations among the identified concepts concerning cascading effects in critical infrastructures

To identify the main concepts concerning cascading effects in CIs and their definitions, an in-depth reading of the selected studies was carried out. The first two concepts identified were the concept of cascading effects, or domino effect, and the concept of CIs. As these concepts were the main terms of our research, for each one of them, several definitions were collected from the different papers, as presented in Tables 1 and 2.

According to the definitions found on the concept of CIs, it was possible to understand that the concept is divided into two types of assets, namely cyber/virtual assets and physical assets (Balducelli et al., 2008; Gueye et al., 2020; König et al., 2019; Wang et al., 2018). Another important concept related to CIs is the concept of Resilience. Resilience can be divided into four dimensions (Bruneau et al., 2003; Gibson and Tarrant, 2010; Zobel, 2011), which are:

- *Technical resilience:* Refers to the ability of the organisation's physical system to perform properly when subjected to a crisis.
- *Organisational resilience:* Refers to the capacity of crisis managers to make decisions and take actions that lead to a crisis being avoided or to a reduction of its impact.
- *Economic resilience:* Refers to the ability of the entity to face the extra costs that arise from a crisis.
- *Social resilience:* Refers to the ability of the society to lessen the impact of a crisis by helping first responders or acting as volunteers.

Figure 6 Cascading effects related terms (see online version for colours)



Source: From systematic mapping

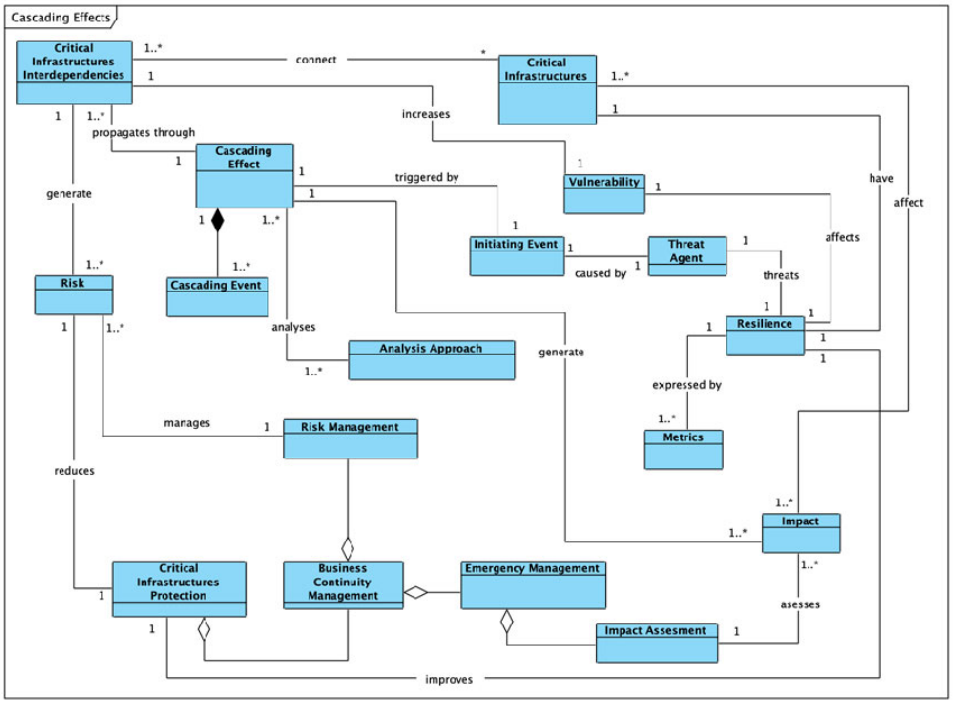
Deriving from the common points of the first two concepts found, cascading effects and CIs, the concept of critical infrastructure interdependencies, which concerns a 'mutual relationship between two or more infrastructures' (Brabcova et al., 2018), was then identified. With the increasing digitalisation and consequent linking of systems of CIs (Grafenauer et al., 2018), they are becoming more and more interconnected among each other (Franchina et al., 2008; Schauer et al., 2018), making them interdependent

(Abdelgawad et al., 2018; Abdelgawad and Gonzalez, 2019; Rahnamay-Naeini and Hayat, 2016).

Figure 7 Cascading effects related terms (see online version for colours)

Source: SLR

Figure 8 Overall cascading effects ontology model (see online version for colours)



Due to the interdependencies among CIs, the effects and the unfolding of a crisis in certain CIs become hard to predict (Hagen et al., 2015). The probability of cascading failures may increase as dependencies and interdependencies among CIs intensify, since, due to critical infrastructure interdependencies, a failure that is seemingly isolated in

one critical infrastructure will be able to cascade to multiple CIs (Setola et al., 2009; Stergiopoulos et al., 2015; Zuccaro et al., 2018), affecting both cyber and physical assets (Kopylec et al., 2007; Schauer et al., 2019).

The interdependency among CIs intensify the probability of a cascading failure (Van Eeten et al., 2011), increasing the vulnerability (Pescaroli and Alexander, 2016; Zimmerman and Restrepo, 2006, 2009) of the CIs and their associated risk (Codetta-Raiteri et al., 2012; Panda and Bower, 2020). Vulnerability can be defined as 'weaknesses or inadequacies in a system that, if exploited by an attacker, could cause harm or damage to the system' (Foglietta et al., 2015).

In the context of CIs, the Risk is related to the consequences of an adverse event (Foglietta et al., 2015). It is essential to have adequate risk management strategies in order to analyse the risks, identify vulnerabilities and emergency preparedness, and prioritise risk-reducing measures (Kjølle et al., 2012). The application of risk management strategies will also contribute to better critical infrastructure protection (Kotzanikolaou et al., 2011) and increase their resilience (Labaka et al., 2016).

Critical infrastructure protection 'embodies the management of risk assessment, risk mitigation, preparedness, response and recovery against serious incidents threatening the critical infrastructure of a region or nation' (Abdelgawad et al., 2018). Thus, the critical infrastructure protection can take advantage of business continuity planning that according to ISO 22301, is defined as the 'strategic and tactical capability of the organisation to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable predefined level'. In combination with both risk management and emergency management, this can increase the resilience of the critical infrastructure (Klaver et al., 2015; Van Eeten et al., 2011).

The process performed for CIs was repeated on the concept of cascading effects and two additional concepts were identified, namely cascading events and initiating event. An initiating event causes direct impacts on infrastructures and could be either a natural event or an internal system failure (Johansson et al., 2015). The cascading effect phenomenon starts with an initiating event and is propagated through cascading events (Codetta-Raiteri et al., 2012). To analyse the cascading effects, the main analysis approaches proposed are modelling interdependencies (among CIs) and simulation approaches (Arief et al., 2020; Chen et al., 2017; Delamare et al., 2009; Foglietta et al., 2015; Franchina et al., 2008; Grafenauer et al., 2018; Guo et al., 2017; Heracleous et al., 2017; König et al., 2019; König and Schauer, 2019; Kotzanikolaou et al., 2013; Peters et al., 2008; Rass and Schauer, 2019; Rehak et al., 2018; Hasan and Foliente, 2015; Ouyang, 2014).

It was also possible to identify the concept of Impact, which is associated with the occurrence of cascading effects in CIs. The Impact 'includes all negative impacts that are deemed relevant and can include the number of casualties and wounded people as well as financial, physical, ecological, mental and intangible damages' (The Netherlands Ministry of Security and Justice, 2014).

3.3 Ontology modelling

To obtain a clearer and more succinct model, the definitions were selected for each of the main concepts which are presented in Table 3.

Table 3 Concepts definition

Concept	*Definition*
Cascading effects	"'Cascading effects' is the overall hazard/impact scenario timeline, including the chain of events (cascading events) and damage caused by cascading events on elements" (Zuccaro et al., 2018). "Each individual event is the cause of the following event; all the events can be traced back to one and the same initial event." (Klaver et al., 2015)
Initiating event	"Initiating event (IE), which, e.g., could be a natural event, such as an earthquake, an accidental event, such as an explosion, or an internal system failure, such as malfunctioning of a technical component. The initiating event gives rise to direct impacts on some systems (societal function or infrastructures)." (Johansson et al., 2015)
Cascade event	"'Cascading events' are a timeline of consecutive events characterised by: cause/effect relationship (i.e. an earthquake that induces a landslide that causes a building collapse that induces casualties), or time interaction among different phenomena independently generated by the same triggering event (i.e. a flood can cause electric failure and interruption roads independently, that can both influence the operation on the same hospital)." (Zuccaro et al., 2018)
Critical infrastructures	"CIs are essential resources for the performance of society, including its economy and its security, understood as safety of citizens and security of society's assets. They are slightly differently defined in different countries. However, there is general agreement that CIs include government, telecommunication based on ICT (information and communication technology); financial sector; energy supply; water transportation systems; health sector; and security services (first responders, police, military)." (Abdelgawad et al., 2018; Abdelgawad and Gonzalez, 2019)
Critical infrastructures protection	"Critical infrastructure protection (CIP) embodies the management of risk assessment, risk mitigation, preparedness, response and recovery against serious incidents threatening the critical infrastructure of a region or nation." (Abdelgawad et al., 2018)
Cascading infrastructures interdependencies	"An interdependency is a bidirectional relationship between infrastructures through which the state of each infrastructure is influenced by or correlated to the state of the other." (Rinaldi, 2004)
Physical interdependencies	"(…) two infrastructures are physically interdependent if the state of each depends upon the material output(s) of the other. Physical interdependencies arise from physical linkages or connections among elements of the infrastructures." (Rinaldi, 2004)
Cyber interdependencies	"(…) an infrastructure has a cyber inter dependency if its state depends on information transmitted through the information infrastructure." (Rinaldi, 2004)
Geographic interdependencies	"(…) infrastructures are geographically interdependent if a local environmental event can create state changes in all of them. This implies close spatial proximity of elements of different infrastructures, such as collocated elements of different infrastructures in a common right-of-way." (Rinaldi, 2004)
Logical interdependencies	"(…) two infrastructures are logically interdependent if the state of each depends upon the state of the other via some mechanism that is not a physical, cyber, or geographic connection." (Rinaldi, 2004)
Analysis approaches	The analysis approaches, include the CIs interdependencies modelling and simulation.

Table 3 Concepts definition (continued)

Concept	*Definition*
Resilience	Resilience is composed by resilience four dimensions technical resilience, social resilience, organisational resilience and economic resilience.
Technical Resilience	"(…) refers to the ability of the organisation's physical system to perform properly when subject to a crisis."
Social	Resilience "(…) refers to the ability of society to lessen the impact of a crisis by helping first responders or acting as volunteers."
Organisational resilience	"(…) refers to the capacity of crisis managers to make decisions and take actions that lead to a crisis being avoided or to at least reducing its impact."
Economic resilience	"(…) refers to the ability of the entity to face the extra costs that arise from a crisis."
Business continuity planning	"Strategic and tactical capability of the organisation to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable predefined level." (Foglietta et al., 2015)
Impact	Impact "includes all negative impacts that are deemed relevant and can include the number of casualties and wounded people as well as financial, physical, ecological, mental and intangible damages." (The Netherlands Ministry of Security and Justice, 2014)
Impact assessment	Impact Assessment consists "of the evaluation process of faults and failures propagation." (Foglietta et al., 2015)
Risk	"Risk is the Cartesian product of all important threats, weaknesses and consequences." (Foglietta et al., 2015)
Risk management	Risk management intends "to identify and control all possible risks before they occur" Pasha et al. (2018) and it can be divided, according to ISO 31000, into "a process including setting the scope, context, and criteria, risk assessment, and risk treatment, in addition to the cross-cutting functions of communication and consultation and monitoring and review through all of the steps." (Rød et al., 2020)
Emergency management	"Emergency management is the overall approach preventing and managing emergencies that might occur." (Klaver et al., 2015)

Figure 9 Critical infrastructures model (see online version for colours)

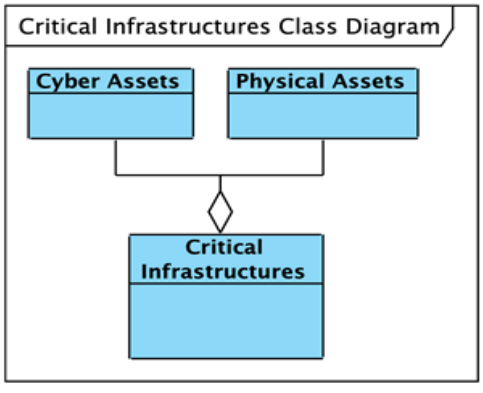


Figure 10 Analysis approach model (see online version for colours)

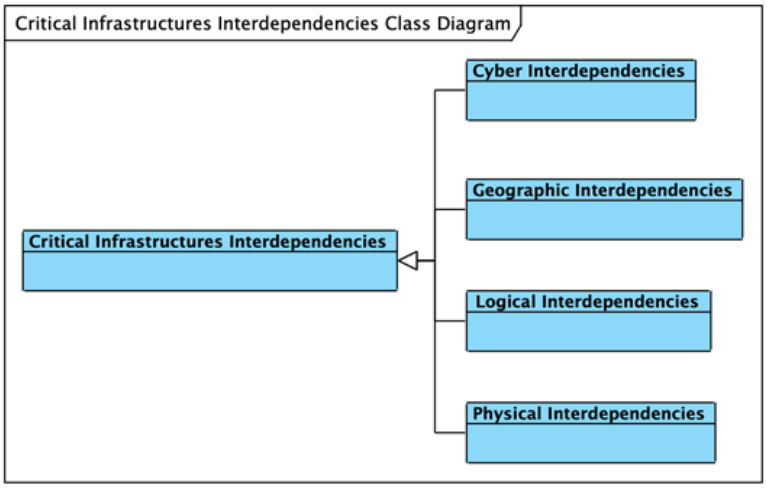
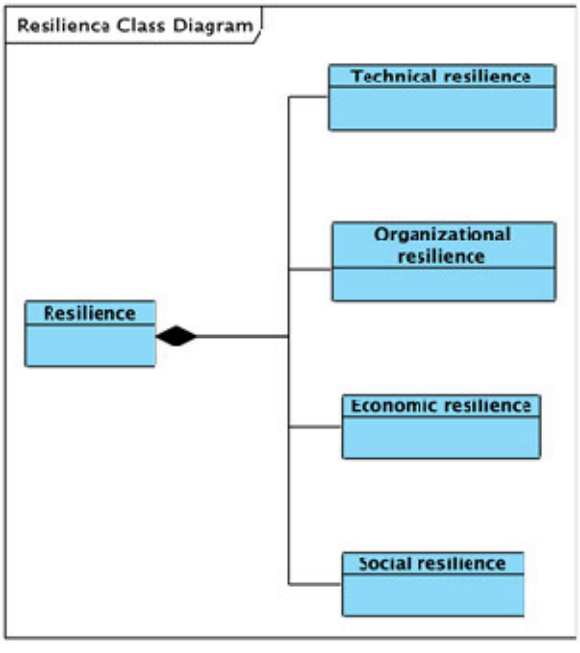


Figure 11 Resilience model (see online version for colours)

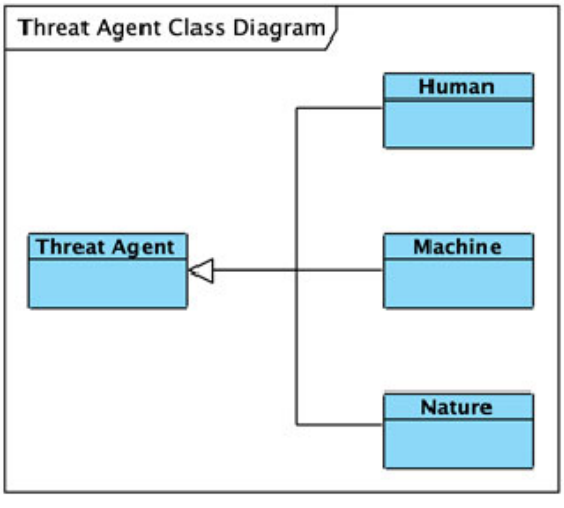


The concept of analysis approach was created to cover the concepts of interdependencies modelling and simulation, which often come together. Modelling interdependencies is about modelling networks of CIs that are interdependent. This modelling can serve as a basis for simulating (Foglietta et al., 2015) the behaviour of these interdependent infrastructures in the event of a disaster. So, interdependencies modelling and simulation are often referred to together (Hasan and Foliente, 2015; Ouyang, 2014).

It is also important to mention that other ontologies that covered the same domain as the one proposed in this article were sought, for reusing purposes. In Vlacheas et al. (2011), an ontology referring to resilience was found, which led to the inclusion of the concepts of 'metrics' and 'threat agent' in the domain of this work. However, the partial integration of this ontology into our model has gone through a process of refinement, since we considered some of the relations rather rudimentary and needs a better representation.

To model the ontology, the 'visual paradigm' tool was used. The model was built in UML, which helps to avoid inconsistencies and allows the relationships between the concepts to be easy to interpret. After modelling the identified concepts, represented in agreement with the relations obtained through the SLR, they were refined and integrated as part of the resilience ontology. The final model of the cascading effects ontology is present in Figure 9, Figure 10, Figure 11 and Figure 12.

Figure 12 Threat agent model (see online version for colours)



3.4 Validation

In order to check the ontology validity, we used the defined QC.

To complement the validation process over the cascading effects ontology, we interviewed the cyber security and data protection officer of one of the largest retailers in Europe (with a turnover of more than 5 billion euros) in order to obtain real-world situations of cascading effects, which affected the organisation. During the interview, two different cases were discussed (case A and case B), which the details are presented.

3.4.1 Case A

- Context: This retailer, besides physical stores (physical infrastructure), has a coupon service and discounts associated with a card. This discount service is composed of a web portal (cyber infrastructure), outsourced, and a physical card. Users can use the

web portal to check the accumulated balance and discount coupons available for use in physical stores (infrastructure interdependency).

- Event: A hacker (human threat agent), through a vulnerability (vulnerability) of the discount portal, managed to break the security protocols associated with user authentication (initiating event). In this way, he obtained access not only to the discount card code but also to its balance and discount coupons associated, allowing it to misuse the balance and discounts of other users (impact), compromising the security of the portal (affecting the resilience of infrastructure).
- Response of the organisation: This risk was already identified (risk management) and the organisation, when facing this threat, followed the internal protocols (infrastructure protection) and created a task force (emergency management) consisting of elements from various departments (IT, IT security, network, legal, public relations). They began by shutting down the web portal (impact management) while trying to solve the fragility of the system, preventing any type of access to the card account through the internet and keeping possible the use of the physical card in stores (business continuity management). Within 48 hours, the fragility was resolved, and the system became available again.
- After the resolution: The organisation rethought the whole process of customer authentication, starting by transferring the web portal system to the internal development and maintenance teams. To improve the security of the portal, the protocols for generating codes for physical cards were changed, and the option of having a validation system using a personal PIN was implemented.
- Conclusion: This was a case in which a rapid solution prevented the spread of unwanted effects to other business infrastructures. If the weakness had not been resolved, it could initiate a cascading effect, since, through this deficient security in the portal, it would allow the hacker to use the balance and discount coupons of other customers in the physical stores (cascading event) which would cause both financial and reputational impact.

3.4.2 Case B

- Context: This retailer is supplied by a telecommunications network of a specific operator (critical infrastructure). For the physical stores (critical infrastructure) to provide payments through ATM terminals, the connection to the telecommunication network is required (CIs interdependency). This telecommunication operator also provides internet and mobile network to the company's employees. This telecommunication operator, in turn, is supplied (CIs interdependency) by an electricity company (critical infrastructure).
- Event: Due to an electrical network failure (initiating event), the operator was unable to provide its telecommunications service (cascade event) to the retail company. As such, the International Journal of CIs 17 physical stores were unable to allow their customers to pay for their purchases via an ATM (cascading event) terminal. This shortage led many of the customers who were shopping in the physical store to give up doing so, leaving the store (cascade event). In addition to the financial impact of

drop-in sales (impact), the fact that the store was without payment services via ATM also showed a negative image of the company (impact).

The lack of a telecommunications network in the organisation also made the company's employees unable to work (cascade event) since they ran out of internet on their computers and cell phones, causing an operational impact (impact).

Response from the organisation: In order to mitigate the impact of the unavailability of ATMs, the company warned customers that they were not working so they would have to pay in cash, and it was possible to withdraw cash at an ATM within the store (business continuity management).

- After the resolution: The company, to mitigate situations like this, adhered to the redundancy of operators, so that there was always one possible for network supply.

Table 4 Answers obtained from the literature

Question	*Answer*
What are the cascading effects composed by?	Cascading effects are composed by one or more cascading events
What initiate cascading effects?	Cascading effects are triggered by an initiating event
What do the cascading effects generate?	Cascading effects generate impact that affects CIs
How are propagated cascading effects?	Cascading effects propagate through CIs interdependencies
How can cascading effects be analysed?	The cascading effects are analysed through analysis approaches, such as interdependencies modelling and simulation approaches
What types of analysis approaches exist?	The analysis approaches can be empirical approach type, agent-based approach type, system dynamics-based approach type or economic theory-based approach type
How can the impact of cascading effects be assessed?	The impact can be assessed with impact assessment
For which types of assets are critical infrastructures composed of?	CIs are composed by cyber assets and physical assets
What types of interdependencies among critical infrastructures exist?	CIs interdependency can be physical interdependencies, cyber interdependencies, logical interdependencies or geographic interdependencies
How can be minimised the critical infrastructures interdependencies associated risk?	The risk is reduced by CIs protection.

4 Conclusions

In this paper, we presented an ontology that represents the domain of cascading effects in CIs providing a better understanding of how cascading effects are generated and propagated, how they can be analysed and how their impact can be minimised. This model aims to represent the cascading effects in CIs, how it is possible to reduce their impact, and identify their causes, namely the interdependencies between them. With this

knowledge in mind, we believe our model can help improve the resilience of CIs, recognising the interdependencies between them and how to minimise the damage of possible cascading effects.

For the development of this ontology, we used the SaBiO (De Almeida, 2014). In order to support Knowledge Acquisition activity, we implemented another methodology, a SLR (Kitchenham, 2004). The SLR analysed the existing research literature concerning the cascading effects in CIs, and provided us the essential information (concepts, relationships and definitions) to build the ontology model. It was possible to identify some limitations in the proposed model, namely the lack of a deeper analysis about the concepts of risk and their management.

The ontology was validated in a two-step process. Firstly, the model was validated according to the CQs defined at the beginning of its development to verify if the ontology met the objectives and the defined scope. It was concluded that the ontology was able to respond correctly to the CQs.

Secondly, we instantiated the ontology to validate if it was in accordance with real world situations. For this purpose, an interview with the cyber security and data protection officer of one of the largest retailers in Europe was done, who reported two real cases of cascading effects, one affecting critical infrastructure and another affecting non-critical infrastructure. The two cases were instantiated, in which the ontology was validated, managing to cover its domain.

Although the validation process was based on two approaches, consisting of CQ and the instantiation of the model, it had limitations. The instantiation covers only one professional area, namely the retail area, and it may occur that the model is not applicable to other areas.

Acknowledgements

The research work presented in this paper was undertaken in the scope of project ENSURESEC, which has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No. 883242.

References

Abdelgawad, A., Saleh, M. and Gonzalez, J. (2018) 'Analysing cascading effects in interdependent critical infrastructures', in *International Conference on Information Technology in Disaster Risk Reduction*, *International Journal of Critical Infrastructures*, Vol. 19, pp.50–65, Springer.

Abdelgawad, A.A. and Gonzalez, J.J. (2019) 'Reliability of expert estimates of cascading failures in critical infrastructure', in *ISCRAM*.

Ansell, C., Boin, A. and Keller, A. (2010) 'Managing transboundary crises: Identifying the building blocks of an effective response system', *Journal of Contingencies and Crisis Management*, Vol. 18, No. 4, pp.195–207.

Arief, R., Khakzad, N. and Pieters, W. (2020) 'Mitigating cyberattack related domino effects in process plants via ICS segmentation', *Journal of Information Security and Applications*, Vol. 51, p.102450.

Balducelli, C., Di Pietro, A., Lavalle, L. and Vicoli, G. (2008) 'A middleware improved technology (MIT) to mitigate interdependencies between critical infrastructures', in *Architecting Dependable Systems*, Vol. 5, pp.28–51, Springer.

Boin, A. and McConnell, A. (2007) 'Preparing for critical infrastructure breakdowns: the limits of crisis management and the need for resilience', *Journal of Contingencies and Crisis Management*, Vol. 15, No. 1, pp.50–59.

Brabcova, V., Slivkova, S., Rehak, D., Toseroni, F. and Havko, J. (2018) 'Assessing the cascading effect of energy and transport critical infrastructure elements: case study', *Communications-Scientific Letters of the University of Zilina*, Vol. 20, No. 2, pp.8–15.

Brown, G., Carlyle, M., Salmerón, J. and Wood, K. (2006) 'Defending critical infrastructure', *Interfaces*, Vol. 36, No. 6, pp.530–544.

Bruneau, M., Chang, S.E., Eguchi, R.T., Lee, G.C., O'Rourke, T.D., Reinhorn, A.M., Shinozuka, M., Tierney, K., Wallace, W.A. and VonWinterfeldt, D. (2003) 'A framework to quantitatively assess and enhance the seismic resilience of communities', *Earthquake Spectra*, Vol. 19, No. 4, pp.733–752.

Chen, Y. and Milanovi´c, Jovica J.V. (2017) 'Critical appraisal of tools and methodologies for studies of cascading failures in coupled critical infrastructure systems', in *IEEE EUROCON 2017-17th International Conference on Smart Technologies*, IEEE, pp.599–604.

Codetta-Raiteri, D., Bobbio, A., Montani, S. and Portinale, L. (2012) 'A dynamic Bayesian network based framework to evaluate cascading effects in a power grid', *Engineering Applications of Artificial Intelligence*, Vol. 25, No. 4, pp.683–697.

De Almeida, F.R. (2014) 'Sabio: systematic approach for building ontologies', in *Onto. Com/odise@ Fois*.

De Almeida, F.R. and Bertollo, G. (2009) 'A software process ontology as a common vocabulary about software processes', *International Journal of Business Process Integration and Management*, Vol. 4, No. 4, pp.239–250.

De Souza, É.F., de Almeida Falbo, R. and Vijaykumar, N.L. (2017) 'Roost: reference ontology on software testing', *Applied Ontology*, Vol. 12, No. 1, pp.59–90.

Delamare, S., Diallo, A-A. and Chaudet, C. (2009) 'High-level modelling of critical infrastructures' interdependencies', *International Journal of Critical Infrastructures*, Vol. 5, Nos.1–2, pp.100–119.

Duarte, B.B., Falbo, R.A., Guizzardi, G., Guizzardi, R.S.S. and Souza, V.E.S. (2018) 'Towards an ontology of software defects, errors and failures', in *International Conference on Conceptual Modeling*, pp.349–362, Springer.

Foglietta, C., Panzieri, S. and Pascucci, F. (2015) 'Algorithms and tools for risk/impact evaluation in critical infrastructures', in *Intelligent Monitoring, Control, and Security of Critical Infrastructure Systems*, Springer, pp.227–238.

Franchina, L., Carbonelli, M., Gratta, L., Crisci, M. and Perucchini, D. (2011) 'An impact-based approach for the analysis of cascading effects in critical infrastructures', *International Journal of Critical Infrastructures*, Vol. 7, No. 1, pp.73–90.

Franchina, L., Carbonelli, M., Gratta, L., Petricca, C. and Perucchini, D. (2008) 'An effective approach for cascading effects prevision in critical infrastructures', in *International Workshop on Critical Information Infrastructures Security*, Springer, pp.386–393.

Gibson, C.A. and Tarrant, M. (2010) 'A'conceptual models' approach to organisational resilience', *Australian Journal of Emergency Management*, Vol. 25, No. 2, pp.6–12.

Grafenauer, T., König, S., Rass, S. and Schauer, S. (2018) 'A simulation tool for cascading effects in interdependent critical infrastructures', in *Proceedings of the 13th International Conference on Availability, Reliability and Security*, pp.1–8.

Graham, S. (2010) *Disrupted Cities: When Infrastructure Fails*, Routledge.

Guarino, N., Oberle, D. and Staab, S. (2009) 'What is an ontology?', in Staab, S. and Studer, R. (Eds.): *Handbook on Ontologies, International Handbooks on Information Systems*, pp.1–17, Springer.

Gueye, A., Mbaye, B., Fall, D., Diop, A. and Kashihara, S. (2020) 'A matrix model to analyse cascading failure in critical infrastructures', in *International Conference on Innovations and Interdisciplinary Solutions for Underserved Areas*, Springer, pp.211–223.

Guo, H., Zheng, C., Ho-Ching, H.I. and Fernando, T. (2017) 'A critical review of cascading failure analysis and modeling of power system', *Renewable and Sustainable Energy Reviews*, Vol. 80, pp.9–22.

Hagen, K., Tzanetakis, M. and Watson, H. (2015) 'Cascading effects in crises: categorisation and analysis of triggers', in *ISCRAM*.

Hasan, S. and Foliente, G. (2015) 'Modeling infrastructure system interdependencies and socioeconomic impacts of failure in extreme events: emerging R&D challenges', *Natural Hazards*, Vol. 78, No. 3, pp.2143–2168.

Heracleous, C., Kolios, P., Panayiotou, C.G., Ellinas, G. and Polycarpou, M.M. (2017) 'Hybrid systems modeling for critical infrastructures interdependency analysis', *Reliability Engineering and System Safety*, Vol. 165, pp.89–101.

Hippolyte, J-L., Rezgui, Y., Li, H., Jayan, B. and Howell, S. (2018) 'Ontology driven development of web services to support district energy applications', *Automation in Construction*, Vol. 86, pp.210–225.

Jaramillo-Yánez, A., Benalcázar, M.E. and Mena-Maldonado, E. (2020) 'Real-time hand gesture recognition using surface electromyography and machine learning: a systematic literature review', *Sensors*, Vol. 20, No. 9.

Jiang, P. and Haimes, Y.Y. (2004) 'Risk management for leontief-based interdependent systems', *Risk Analysis: An International Journal*, Vol. 24, No. 5, pp.1215–1229.

Johansson, J., Hassel, H., Cedergren, A., Svegrup, L. and Arvidsson, B. (2015) 'Method for describing and analysing cascading effects in past events: initial conclusions and findings', in *European Safety and Reliability Conference (ESREL2015)*.

Kitchenham, B. (2004) *Procedures for Performing Systematic Reviews*, Vol. 33, No. 2004, pp.1–26, Keele University, Keele, UK.

Kjølle, G.H., Utne, I.B. and Gjerde, O. (2012) 'Risk analysis of critical infrastructures emphasizing electricity supply and interdependencies', *Reliability Engineering and System Safety*, Vol. 105, pp.80–89.

Klaver, M.H.A., Luiijf, H.A.M., Nieuwenhuijs, A.N., van Os, N. and Oskam, V. (2015) 'Critical infrastructure assessment by emergency management', in *International Conference on Critical Information Infrastructures Security*, Springer, pp.79–90.

König, S. and Schauer, S. (2019) 'Cascading threats in critical infrastructures with control systems', in *ISCRAM*.

König, S., Rass, S., Rainer, B. and Schauer, S. (2019) 'Hybrid dependencies between cyber and physical systems', in *Intelligent Computing Proceedings of the Computing Conference*, Springer, pp.550–565.

Kopylec, J., D'Amico, A. and Goodall, J. (2007) 'Visualizing cascading failures in critical cyber infrastructures', in *International Conference on Critical Infrastructure Protection*, Springer, pp.351–364.

Kotzanikolaou, P., Theoharidou, M. and Gritzalis, D. (2011) 'Interdependencies between critical infrastructures: analysing the risk of cascading effects', in *International Workshop on Critical Information Infrastructures Security*, Springer, pp.104–115.

Kotzanikolaou, P., Theoharidou, M. and Gritzalis, D. (2013) 'Cascading effects of common-cause failures in critical infrastructures', in *International Conference on Critical Infrastructure Protection*, Springer, pp.171–182.

Labaka, L., Hernantes, J. and Sarriegi, J.M. (2016) 'A holistic framework for building critical infrastructure resilience', *Technological Forecasting and Social Change*, Vol. 103, pp.21–33.

Luiijf, E., Nieuwenhuijs, A., Klaver, M., van Eeten, M. and Cruz, E. (2008) 'Empirical findings on critical infrastructure dependencies in Europe', in *International Workshop on Critical Information Infrastructures Security*, Springer, pp.302–310.

Ouyang, M. (2014) 'Review on modeling and simulation of interdependent critical infrastructure systems', *Reliability Engineering and System Safety*, Vol. 121, pp.43–60.

Panda, A. and Bower, A. (2020) 'Cyber security and the disaster resilience framework', *International Journal of Disaster Resilience in the Built Environment*.

Panichella, A., Dit, B., Oliveto, R., Di Penta, M., Poshynanyk, D. and De Lucia, A. (2013) 'How to effectively use topic models for software engineering tasks? An approach based on genetic algorithms', in *2013 35th International Conference on Software Engineering* (ICSE), pp.522–531.

Pasha, M., Qaiser, G. and Pasha, U. (2018) 'A critical analysis of software risk management techniques in large scale systems', *IEEE Access*, Vol. 6, pp.12412–12424.

Penuel, K.B., Statler, M. and Hagen, R. (2013) *Encyclopedia of Crisis Management*, Sage Publications.

Pescaroli, G. and Alexander, D. (2016) 'Critical infrastructure, panarchies and the vulnerability paths of cascading disasters', *Natural Hazards*, Vol. 82, No. 1, pp.175–192.

Peters, K., Buzna, L. and Helbing, D. (2008) 'Modelling of cascading effects and efficient response to disaster spreading in complex networks', *International Journal of Critical Infrastructures*, Vol. 4, Nos. 1–2, pp.46–62.

Petersen, K., Feldt, R., Mujtaba, S. and Mattsson, M. (2008) 'Systematic mapping studies in software engineering', in *12th International Conference on Evaluation and Assessment in Software Engineering (EASE)*, Vol. 12, pp.1–10.

Rahnamay-Naeini, M. and Hayat, M.M. (2016) 'Cascading failures in interdependent infrastructures: an interdependent Markov-chain approach', *IEEE Transactions on Smart Grid*, Vol. 7, No. 4, pp.1997–2006.

Rass, S. and Schauer, S. (2019) 'Refining stochastic models of critical infrastructures by observation', *Reliability: Theory and Applications*, Vol. 14, No. 3.

Rehak, D., Senovsky, P., Hromada, M., Lovecek, T. and Novotny, P. (2018) 'Cascading impact assessment in a critical infrastructure system', *International Journal of Critical Infrastructure Protection*, Vol. 22, pp.125–138.

Rinaldi, S.M. (2004) 'Modelling and simulating critical infrastructures and their interdependencies', in *37th Annual Hawaii International Conference on System Sciences, Proceedings of the IEEE 2004*, p.8.

Rinaldi, S.M., Peerenboom, J.P. and Kelly, T.K. (2001) 'Identifying, understanding, and analysing critical infrastructure interdependencies', *IEEE Control Systems Magazine*, Vol. 21, No. 6, pp.11–25.

Rød, B., Lange, D., Theocharidou, M. and Pursiainen, C. (2020) 'From risk management to resilience management in critical infrastructure', *Journal of Management in Engineering*, Vol. 36, No. 4, p.4020039.

Schauer, S., Grafenauer, T., König, S., Warum, M. and Rass, S. (2019) 'Estimating cascading effects in cyber-physical critical infrastructures', in *International Conference on Critical Information Infrastructures Security*, Springer, pp.43–56.

Schauer, S., König, S., Latzenhofer, M., Rass, S. and Grafenauer, T. (2018b) 'Analysing cascading effects among critical infrastructures: the Cerberus approach', in *Proceedings of the 15th ISCRAM Conference–Rochester*, NY, USA, May 2018, pp.428–437.

Schauer, S., Rainer, B., Museux, N., Faure, D., Hingant, J., Rodrigo, F.J.C., Beyer, S., Lopez, S.Z. et al. (2018a) 'Conceptual framework for hybrid situational awareness in critical port infrastructures', in *International Conference on Critical Information Infrastructures Security*, Springer, pp.191–203.

Setola, R., De Porcellinis, S. and Sforna, M. (2009) 'Critical infrastructure dependency assessment using the input–output inoperability model', *International Journal of Critical Infrastructure Protection*, Vol. 2, No. 4, pp.170–178.

Stergiopoulos, G., Kotzanikolaou, P., Theocharidou, M. and Gritzalis, D. (2015) 'Risk mitigation strategies for critical infrastructures based on graph centrality analysis', *International Journal of Critical Infrastructure Protection*, Vol. 10, pp.34–44.

The Netherlands Ministry of Security and Justice (2014) *Working With Scenarios, Risk Assessment and Capabilities in the National Safety and Security Strategy of the Netherlands,* October.

United States (2013) 'Department of Homeland Security. NIPP 2013: partnering for critical infrastructure security and resilience', *Homeland Security*.

Van Eeten, M., Nieuwenhuijs, A., Luiijf, E., Klaver, M. and Cruz, E. (2011) 'The state and the threat of cascading failure across critical infrastructures: the implications of empirical evidence from media incident reports', *Public Administration*, Vol. 89, No. 2, pp.381–400.

Van Laere, J., Berggren, P., Gustavsson, P., Ibrahim, O., Johansson, B., Larsson, A., Lindqwister, T., Olsson, L. and Wiberg, C. (2017) 'Challenges for critical infrastructure resilience: cascading effects of payment system disruptions', in *14th International Conference on Information Systems for Crisis Response and Management (ISCRAM2017)*, ISCRAM, Albi, France, 21–24 May, Vol. 14, pp.281–292.

Vlacheas, P.T.V., Demestichas, S.P., Cadzowm, S., Gorniak, S. and Ikonomou, D. (2011) 'Ontology and taxonomies of resilience', *ENISA Report.*

Wang, W., Yang, S., Hu, F., Stanley, H.E., He, S. and Shi, M. (2018) 'An approach for cascading effects within critical infrastructure systems', *Physica A: Statistical Mechanics and its Applications*, Vol. 510, pp.164–177.

Wohlin, C. (2014) 'Guidelines for snowballing in systematic literature studies and a replication in software engineering', in *Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering*, pp.1–10.

Zimmerman, R. and Restrepo, C.E. (2006) 'The next step: quantifying infrastructure interdependencies to improve security', *International Journal of Critical Infrastructures*, Vol. 2, Nos. 2–3, pp.215–230.

Zimmerman, R. and Restrepo, C.E. (2009) 'Analyzing cascading effects within infrastructure sectors for consequence reduction', in *2009 IEEE Conference on Technologies for Homeland Security*, IEEE, pp.165–170.

Zobel, C.W. (2011) 'Representing perceived tradeoffs in defining disaster resilience', *Decision Support Systems*, Vol. 50, No. 2, pp.394–403.

Zuccaro, G., De Gregorio, D. and Leone, M.F. (2018) 'Theoretical model for cascading effects analyses', *International Journal of Disaster Risk Reduction*, Vol. 30, pp.199–215.