# On the Semantics of Risk Propagation

Mattia Fumagalli[1][0000−0003−3385−4769], Gal Engelberg[2][0000−0001−9021−9740], Tiago Prince Sales[3][0000−0002−5385−5761], Ítalo Oliveira[1][0000−0002−2384−3081], Dan Klein[2][0000−0002−8881−1902], Pnina Soffer[4][0000−0003−4659−883X], Riccardo Baratella[1][0000−0002−4387−2912], and Giancarlo Guizzardi[3][0000−0002−3452−553X]

[1] In2Data & Conceptual and Cognitive Modeling Research Group (CORE), Free University of Bozen-Bolzano, Bolzano, Italy
{mattia.fumagalli,idasilvaoliveira,baratellariccardo}@unibz.it
[2] Accenture Israel Cyber R&D Lab, Tel Aviv, Israel
{gal.engelberg,dan.klein}@accenture.com
[3] Semantics, Cybersecurity &Services (SCS), University of Twente, The Netherlands
{g.guizzardi,t.princesales}@utwente.nl
[4] University of Haifa, Haifa, Israel
spnina@is.haifa.ac.il

**Abstract.** *Risk propagation* encompasses a plethora of techniques for analyzing how risk "spreads" in a given system. Albeit commonly used in technical literature, the very notion of risk propagation turns out to be a conceptually imprecise and overloaded one. This might also explain the multitude of modeling solutions that have been proposed in the literature. Having a clear understanding of what exactly risk is, how it be quantified, and in what sense it can be propagated is fundamental for devising high-quality risk assessment and decision-making solutions. In this paper, we exploit a previous well-established work about the nature of risk and related notions with the goal of providing a proper interpretation of the different notions of risk propagation, as well as revealing and harmonizing the alternative semantics for the links used in common risk propagation graphs. Finally, we discuss how these results can be leveraged in practice to model risk propagation scenarios.

**Keywords:** Risk propagation· risk modeling · ontological analysis

## 1 Introduction

Our ability to reason about risk is fundamental in our daily lives. In this regard, the increasing enhancement of statistical methods and analytical applications has opened up promising research directions. An exemplary case is the so-called *Risk Propagation* technique [18].

Typically, in risk management, risk propagation provides a model for analyzing how risk "spreads" in a given system–that is, a model for a sort of cascading effect. Risk propagation addresses questions like:

.i "how does the risk associated with a device in a network 'spreads' through connected devices?";

.ii "how does the risk of my car breaking down affect the risk of me being late for an appointment?";
.iii "how does someone in my office being infected by COVID-19 affect the risk that I get infected as well?".

Risk propagation techniques are often implemented via *probabilistic graphs models* [22], in which a system to be analyzed is encoded as a set of nodes and edges, characterized by correlations and probabilities. Examples include *Bayesian networks* [11,4] and *Fault Trees* [21].

What remains certain is that the work on risk propagation still presents many open challenges from both a theoretical and a technological perspective. For instance, what do people mean when they say that risk propagates? Do they mean that risk propagates physically–like a virus that copies itself and moves through hosts? Is risk something that can be simply encoded as a weight value to be then passed through other nodes in a network? And again, do probabilistic graphs and similar graph models allow us to properly capture all the information about risk and its propagation? Most often what is actually "propagated" are probability values, leveraging some specific measures, like *conditional probability*. So, how should we interpret the notion of risk propagation? Can a further analysis of this notion support current solutions in this domain, and if so, how?

This work stems from the idea that this last question has a positive answer. In particular, we perform what we believe is the first ontological analysis of the notion of risk propagation. Our analysis is guided by the *Common Ontology of Value and Risk (COVER)*, a well-founded ontology of risk from previous research work [24]. As we shall see, our analysis allows us to *.i* explain how the propagation of risk relates to the phenomenon of belief updating; *.ii* explain how talking about the "propagation" of risk can be misleading; and *.iii* identify the concepts and relationships required to capture the cascading effect assumed when talking about risk propagation without incurring in ambiguities and reductions. Our investigation also allows the creation of a unified framework for modeling risk propagation, fostering the clarification of the real-world semantics behind risk propagation graphs, and paving the way for an ontology-based adoption of this technique.

The remainder of this paper is organized as follows. In section 2, we present the research baseline on which we ground our work, namely the ontological foundations provided by COVER. Section 3 illustrates some risk propagation definitions and techniques currently available in the literature. Section 4, provides the core contribution, namely an ontological analysis of the notions of risk propagation and risk propagation graphs. Then, in Section 5, we discuss the implications of our findings. Lastly, Section 6 presents the final considerations and limitations.

## 2 Research Baseline

Before delving into the notion of risk propagation, let us introduce the view on the nature of risk formalized in the *Common Ontology of Value and Risk*

*(COVER)* [24].[5] We will use this ontology as a basis to guide the subsequent analysis of the notion of risk propagation, which, as we shall see, poses entirely new ontological issues w.r.t. the adopted ontology itself. We chose COVER because: *.i* it is based on a foundational ontology; *.ii* it embeds a domain-independent conceptualization of risk; *.iii* it is built upon widespread definitions of risk and shows how the risk is connected to the notion of value. Moreover, COVER has already been connected to different domain ontologies showing its utility in clarifying some related notions (e.g., *trust*, *prevention*, *security*).

### 2.1 Risk Assumptions in COVER

The first assumption in COVER is that risk is **relative**. An event might be seen as a risk by an observer and as an opportunity by another. To exemplify why this assumption holds, consider the case of a potential robbery. The would-be victim perceives such an event as a risk, i.e., as something she does not want to happen and that would hurt some of her goals. From the would-be robber's perspective, the robbery is a desired event that will help her in achieving some of her goals.

The reason why risk is relative constitutes the second assumption about its nature. Risk is perceived according to **impact on goals** as well as the **importance of these goals** to a given agent, i.e. in order to talk about risk, one needs to account for which goals are "at stake". For instance, if one is concerned with the risk of missing a train, it is because missing a train impacts one's goals, such as arriving on time for a meeting.

The third assumption implied by COVER is that risk is **experiential**. This means that we ultimately ascribe risk to events, not objects. This claim may seem counter-intuitive at first, as many theories refer to entities such as "Object at Risk" and "Asset at Risk" [2]. Here the claim is not that such concepts do not exist. Instead, the assumption is that when assessing the risk an object is exposed to, one aggregates risks ascribed to events that can impact the object. For instance, consider the risks your phone is exposed to. In order to identify and assess them, you will probably need to consider: .i which of your goals depend on your phone (e.g. getting in contact with your friends, being responsive to business e-mails); .ii what can happen to your phone such that it would hinder its capability to achieve your goals (e.g. its screen breaking, it being stolen); and .iii which other events could cause these (e.g. you dropping it on the floor or leaving it unattended in a public space). Then the risk your phone is exposed to is the aggregation of the risk of it falling and breaking, the risk of it being stolen, and so on.

The next assumption is that risk is **contextual**. Thus, the magnitude of the risk an object is exposed to may vary even if all its intrinsic properties (e.g., vulnerabilities) stay the same. To exemplify, let us pick one risk event involving

[5] Note that we took COVER as primitive, which was itself subject to validation and proper comparison to the literature of risk in risk analysis and management at large (e.g., [6,16,17]).

your phone, namely that of dropping it and its screen breaking. Naturally, the properties of the phone influence the magnitude of this risk, such as it having a strengthened glass screen. Still, the properties of the surface on which it was dropped (e.g. its hardness) and of the drop itself (e.g. its height) can significantly increase how risky the drop and breaking event is.

Lastly, another assumption that we derive from COVER is that risk is grounded on **uncertainty** about events and their outcomes. This is a very standard position, as proposed in [16] and extensively discussed in [1], which implies that likelihood is positively correlated with how risky an event is. For instance, the risk of a volcano eruption damaging a city is higher for a city that lies by an active volcano than for a city that lies by a dormant one simply because it is more probable.

### 2.2 The Ontology of Risk

Figure 1 represents the concepts in COVER that are germane to the objectives of this paper.

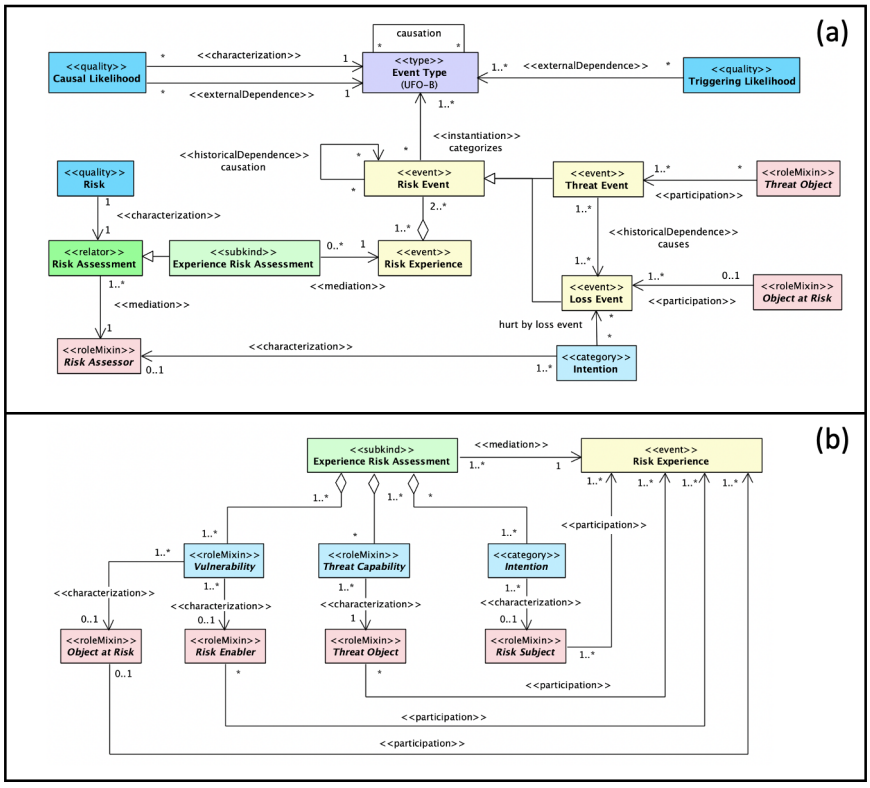


Figure 1: Two views of the *Common Ontology of Value and Risk (COVER)* [24].

Figure 1 provides two views of COVER (i.e., (a) and (b)), by highlighting the concepts that are key for our analysis. (a) allows understanding the notion

of Risk Assessor, namely an agent that makes a Risk Assessment about objects (Object Risk Assessment) and has experiences (Experience Risk Assessment) afforded by these objects. A Risk Experience is a complex event composed of Risk Events, i.e., Threat Events, which may involve the participation of Threat Objects, and Loss Events, which may involve the participation of Objects at Risk. This, as highlighted by view (b), allows us to push the analysis beyond the notions of event and risk assessor's goals, and embed also the concepts of Vulnerability, Threat Capability and Intention, namely *dispositional properties* [3], as aspects that can be involved in risk experiences and propagation.

COVER allows also considering Risk itself as a quantitative measure attributed to a Risk Assessment. The assumption here is that *risk* can be only ascribed to *envisioned experiences* that may (but are not certain to) occur. The ontology addresses this issue by accounting for the existence of future events, as proposed by Guarino [13]. As we will see later on, this aspect will guide us on the analysis and the disambiguation of existing risk propagation models, where event occurrences, event types, and objects are often conflated.

As a final remark, COVER will allow us to further explore how risk is quantified and employed in the propagation process via the concepts of Causal Likelihood and Triggering Likelihood, which are typically expressed by probabilistic measures and, as we will see in the next sections, offers the baseline to understand risk propagation mechanisms. One essential aspect is that considering the ontological grounding of COVER, the likelihood is a quantitative concept that inheres in types of events, not in individuals. Thus, the challenge will be to see how this influences the understanding of current risk propagation approaches and, possibly, the modeling of future ontologically well-founded solutions.

## 3 On Risk Propagation

What we propose here is an ontological analysis of the notion of risk propagation, for which, as far as we know, there is no related work. The goal of this section is to contextualize that notion by reporting some definitions provided in the literature and giving some representative examples of application. The information below is the result of a review of papers found with criterion *[allintitle: "risk propagation"]* on *Google Scholar*, from 2000 to 2021. The selection of approaches and definitions is not complete but aims to offer a representative view of what is available in the current set of still scarcely generalized and standardized works.

### 3.1 Some Definitions

The notion of "risk propagation" refers, often rather vaguely, to phenomena in which one can observe that some events *affect* the probability that some other (desirable or undesirable) events happen. Its semantics varies depending on the application context and actual definitions are given in very few papers. Some representative ones we found state that risk propagation is:

.i "the impact on business value spread across operational assets that results from the occurrence of a disruptive event" [12];
.ii "the sequence of inter-dependent risks in the supply network which may or may not lead to a disruption or ripple effect" [10];
.iii "the process by which certain risk units pass certain elements and/or the consequences of risk to other risk units under the influence of necessary external factors" [7];
.iv "how risks originate at one node of the supply chain and create further risks across the supply chain" [5].

A common aspect of these definitions and different senses is their pragmatic orientation. They are always derived from, or highly dependent on, a specific application context or a complementary implementation, namely, the algorithm adopted to perform inferences and take decisions. As an example, in the context of *cyber-security*, risk propagation can be applied to quantify the risk of connected devices, which can be exposed to and compromised by cyberattacks. In this specific scenario, the risk may *originate* (*.i*, *.iii*, *.iv*) from some intervention actions and *propagate* over connected cyber-assets and, eventually, certain events (e.g., processes connected to the cyber assets, such as "vehicle assembly") via certain types of relationship (e.g., correlation, parthood, or causation). The final outcome of the risk propagation, given a certain threat, is then an *assessment* of the potential vulnerabilities of all the selected elements, i.e., cyber assets and related processes.

### 3.2 Modeling Risk Propagation

Let us consider the following simplified scenario. *"Anna, Bob, and Carl have to make a presentation for a new client. This event is extremely important because it would allow their start-up to gain an important project. On the morning of the presentation, there is heavy traffic congestion on their way to work and the customer only has one 30-minute slot in the early morning. In order to arrive on time and give the presentation, the three must decide whether to take the same means of transportation or each try a different option: subway, car, or bus."*

This example illustrates typical aspects modeled in risk propagation. From it, we can easily understand why the aforementioned risk propagation definitions may arise. As from definition *.i*, we observe how the occurrence of a disruptive event (heavy traffic congestion) impacts business value (potentially losing a customer). Similarly, as from *.ii*, we may talk about a possible *ripple effect* caused by interconnected risk events (e.g., the congestion, the missed presentation, and the loss of a client). As from *.iii*, we may identify multiple risk units, i.e., items for which we may want to calculate the risk, namely the customer, the company, the people involved, and the means of transportation. It is also possible, as from *.iv*, to understand in what sense *risk may originate* at one node (e.g., from the car being stuck in the traffic for a certain amount of minutes). In summary, most of the considerations that emerge from this illustrative scenario suggest a sort of *cascading effect*, which occurs in a network, as if the risk was actually something that could be passed from one node to another.

Risk propagation definitions are often proposed alongside risk propagation techniques, which makes them rather biased by the underlying adopted technology. Figure 2 depicts a risk propagation graph of our scenario, as well as some other techniques proposed in the literature.

Figure 2.a is the example we introduced at the beginning of this section. Each node is a risk unit and risk can be spread over the units through edges connecting them. Here we do not stick to any particular assumption about how the risk value is associated with the nodes and how it is propagated. The whole graph could be taken as a *Labeled Property Graph* in which a risk value is associated with each node and propagated through a simple inference mechanism.

Provided in [25], Figure 2.b was designed to measure how risk spreads over a supply chain. Each node in the graph is taken as a *risk unit*. Besides the source node (the leftmost) and the destination node (the rightmost), other nodes representing different transportation steps are provided. Each node is associated with a risk value which then can affect the value of the other nodes. By analyzing the graph one can discover what are the most critical chains in the transportation process and, eventually, adopt mitigation strategies.

Figure 2.c depicts a technique for propagating risks in a network based on the *Tropos Goal-Risk Framework*, "a goal-oriented framework for modeling and analyzing risks in the requirement phase of software development" [8]. Here the nodes in the graph may represent agents, tasks, activities, and goals, all of which can be combined to model a risk chain.

Figure 2.d also depicts a model for propagating risk over a supply chain [4]. However, differently from Figure 2.b, the model presents the typical structure of a probabilistic network. The nodes being the *target* of an edge are said to be dependent on the corresponding *source* nodes. The nodes that do not present

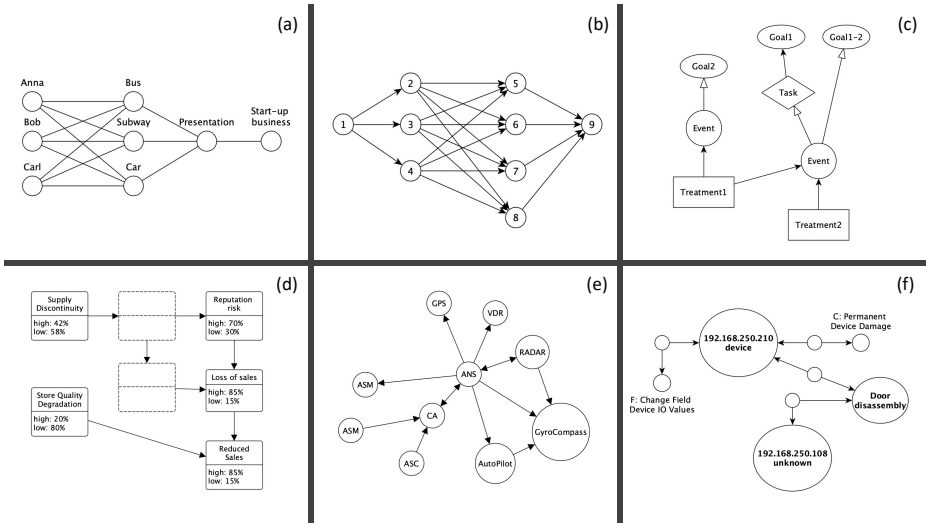


Figure 2: Different risk propagation graphs. (a) Our example; (b) from [25]; (c) from [8]; (d) from [4]; (e) from [19]; and (f) from [9].

dependencies are said to be independent nodes. In this scenario, the risk propagation mechanism consists of "updating" a risk value ascribed to a certain node according to what *happens* to other nodes. Each node, in this context, clearly represents an event associated with a certain probability value. A user can then query the model to calculate the risk for a corresponding node, assuming that some events in the network occur.

Figure 2.e illustrates the technique proposed in [19]. The model is used to perform risk propagation over a cyber-physical system, namely, a cyber-enabled ship. The nodes of the graph represent the different components involved in controlling the navigation of the ship. Similarly to *(b)*, all the edges in the graphs represent a sort of information flow or message-passing mechanism. These edges are then used to calculate how *risk flows* from one node to the others. For instance, the approach allows analyzing how the risk of a radar malfunction can affect other cyber assets (e.g., the collision avoidance system).

Lastly, Figure 2.f is the graph presented in [9], which proposes a knowledge graph-based process-aware risk propagation approach. This work does not provide an ontological analysis of risk propagation but it merely introduces a knowledge graph schema for answering practical queries provided by practitioners. Here risk propagation maps into a kind of *message-passing algorithm* [26]. The nodes in the graph can represent multiple things, such as objects, events, and processes, which are mainly categorized as subclasses of *risk units*. Finally, the edges are used to calculate how the risk values associated with a node affect the values of its neighbor nodes and vice versa.

## 4 Explaining Risk Propagation

The ontological grounding provided by COVER allows us to make explicit the interpretations underlying risk propagation techniques. This involves two major aspects. Firstly, the ontology allows to *unpack* (*unfold*, *explain*) [15] concepts that may be necessary to understand how risk is calculated and propagated. Secondly, we can clarify the rationale behind the risk propagation graphs modeling assumptions, thus paving the way for ontologically well-founded versions of these techniques.

### 4.1 What Does it Mean for Risk to Propagate?

Starting from COVER's assumptions about the nature of Risk, the goal here is to analyze in what sense this *quantitative measure* attributed to a Risk Assessment may *propagate*. Let us first consider the meaning of "propagation". By looking at the definition and the etymology of this term[6] we can identify two main semantic fields.

(a) Firstly, "propagation" concerns *the spreading of something as a belief*, namely an event as a *psychological feature*, a *mental process*.

[6] From https://www.collinsdictionary.com/ and https://www.etymonline.com/

(b) Secondly, the notion concerns a physical process, namely something that can be observed, which can be analogous to *i. biological reproduction* or *ii.* the *gradual change of an object*, in the sense of extension and enlargement.

Given that Risk is a quantitative measure and that Risk Assessment is entangled with the Risk Experience of a Risk Assessor, definition (a) is naturally suited to the *experiential perspective* fostered by COVER. In this sense, the propagation of risk is *an event that concerns the change or update of a judgment of an agent*. This event, as we are going to discuss below, may occur via *observation*, or via *simulation*. Accordingly, it can be said that risk propagates because the beliefs of a given subject, about a certain situation, change. This supplementary consideration highlights the influence of the notion of *belief propagation* [23] in the definition of risk propagation. Furthermore, this explains why current risk propagation models leverage message-passing algorithms, which represent an implementation of belief propagation as a probability inference technique. However, one key observation is that, in belief propagation, the beliefs updating mechanisms concern only how the Likelihoods associated with some given events are quantified and updated. As we have seen, this is not enough to explain the quantification of risk. *Risk*, indeed, *cannot be mapped one-to-one to a probability value*, and risk assessment is not just a probability quantification. Rather, risk, and then risk propagation, always depend on the subjective judgment of a particular agent about *a given probability of having a certain loss, i.e., a certain event that would have an impact on one of its goals, the latter having a certain measure of importance to that agent*. Looking at the available approaches, this last point is often left implicit, and the propagation of risk ends up being identified as the propagation of probabilities.

**Risk propagation via observation**. Let us take the example provided in subsection 3.2. Here risk can be assessed by a Risk Assessor, i.e., Anna, with regard to some possible Loss Events. Consider, for instance, the event of having a car accident. This could mean Anna losing 500 euros to adjust the damaged car. According to Anna's assessment, the risk of having a car accident can be then calculated as (in a simplified manner) $P(A) \cdot 500$, where $P(A)$ stands for *the probability having a car accident* and 500 euros is the *loss value (i.e., impact) related to the damage*. In this setting, the quantitative measure derived through Risk Assessment depends on Anna's judgment, as *"the product of the probability that a given (undesired) event happens and the negative value assigned to that given event"*. Now, how the risk of having a car accident can be propagated? Definition (a) of "propagation" suggests that this has to do with some changes in Anna's *beliefs*. Suppose that the event of having an accident with the car is correlated to the possibility of giving a presentation to an important customer. Suppose that not being able of giving the presentation could be considered by Anna as another possible loss event, because her boss will complain and she will not get a bonus of 1.000 euros at the end of the year. In this sense, if the two events are correlated (Anna uses the car the same morning of the presentation), a higher risk of having an accident has an impact, or, "a cascading effect", using the related work terminology, over the risk of failing the presentation. This cas-

cading effect is related to the notion of *conditional probability*, representing the probability that an event occurs *given the occurrence of another event*, and can be taken as the backbone structure of any graph enabling probability inferences. In this setting, keeping fixed the loss values for two events $A$ and $F$ (e.g., 500 and 1.000 euros respectively), if the probability that $F$ occurs depends on the probability that $A$ occurs (i.e., F, given A as $P(F|A)$), the change of risk for A implies a change of risk for F. This depends on an increase of the probabilities associated to A and then of the probabilities associated to F. Again, the loss values remain unaltered. Following the example, then, the propagation occurs when Anna updates her Risk Assessment according to what happens to some given correlated events composing her Risk Experience (e.g, it is raining and there is a lot of traffic, this may increase the risk of having a car accident, then Anna knows that the risk of being late and failing to deliver the presentation just became higher).

**Risk propagation via simulation**. The propagation of risk can only take place because of an existing chain of events in Anna's experience. These events are associated with a corresponding chain of (possible) events at the type level, which are characterized by Causal Likelihood and Triggering Likelihood, namely the probability an event occurs and the probability an event causes another event, respectively (see Figure 1). The fact that something has occurred has an impact on the event-type chain, thus updating the probability values and, accordingly, Anna's quantification of risk. That being said, in the example above, Anna's experience is updated given a new *evidence*, namely by instantiating an Event Type (e.g., the possibility of having a car accident is realized). The risk related to that event, and other possible correlated loss events, is then updated and such new information is used to update the judgment of the assessor. A different scenario is introduced when the risk is propagated given some simulations run by the assessor. In practice, the new aspect here is that risk propagation is not performed to update the risk assessment *given that something has occurred*, rather it is performed to update the risk assessment *given that something may occur*. Take the presentation example. Anna may want: a) to understand what are the possible transportation actions she can choose when she has to go to the customer; b) to identify possible correlations between those actions (e.g., the probability of arriving on time given the probability of taking the underground); c) to make a ranking of possible loss events (it is better to have a fee for exceeding the speed limits than missing the presentation); given b) and c), d) to select the best option, i.e., the less risky actions in order to not fail the presentation. This involves two main observations. Firstly, the propagation of risk requires the design of an *imaginative risk experience*, which according to COVER naturally maps into a chain of correlated Event Types. In this sense, risk propagation occurs by simulating the occurrence of some of the (loss) event types taken into consideration, and this can be used to discover new information. For instance, the simulations may allow the discovery of new probabilities and then new risk values. Also, adding new possible events in the causal chain of the simulation may lead to discovering some new objects at risk. Secondly,

this simulation could be seen as supplemental to the Risk Assessment itself. In this sense, all the models used to implement risk propagation can be taken as a projection of an *imaginative risk experience* that can support a more accurate risk identification process. Concerning this last point, an analysis of the graphical representations used to run risk propagation in the light of COVER plays a pivotal role, since those can be considered as different ways of modeling the *imaginative risk experience* that is necessary to propagate risk via simulations.

### 4.2 What is in a Risk Propagation Graph?

According to what was discussed in subsection 4.1, a risk propagation graph can be seen as a way of supporting the reasoning abilities of a given Risk Assessor. In this respect, multiple elements are involved. For instance, Threat Events, Loss Events, Threat Objects, Loss Objects, and different possible relationships between them, but also Risk values and the subjects who provide a prior estimation of Risk. In this sense, COVER concepts can be used to discover the multiple interpretations involved in a risk propagation graph.

One first observation is that quite often *types* and *instances* are somehow conflated in these graphs. We may have, indeed, instances of events or event types, where the former is an occurrence of the latter. Similarly, we may have instances of objects or types of objects. This confusion is usually biased by the answering capabilities that should be enabled by the designed graphs. Putting together nodes like "Anna", "Car" and "Failed Presentation", for example, may depend on the queries that the graph should be able to answer. Instance nodes, like "Anna" and "Failed Presentation", usually represent the units that need to be assessed through the propagation process or the things we must decide about (e.g., what is "Anna's risk of losing her job", "given that the presentation failed"). Differently, the nodes representing types are used in the graph to model events having an impact on the final evaluation of risk. That being said, we can straightforwardly divide the types of links in a risk propagation graph as *type-to-type* links and *instance-to-type* links.

**Type-to-type.** When two types are related, this generally means that the source node provides a condition for affecting the risk associated with the target node. We have at least the following kinds of uses for the *type-to-type* link in risk propagation graphs:

(1) *event/event (correlation).* This is one of the most common types of links (it usually occurs when the graph adopted for propagating the risk implements a probabilistic network). In COVER the correlation relation is not explicitly represented but can be somehow related to Event types characterized by (a weaker version of) causal-likelihood. In this setting, when two events are linked in risk propagation graphs, they are said to be correlated. For instance, the event of the *presentation* is correlated to the event of *transportation.*
(2) *event/event (historicalDependence).* The relations of causality between event types are often assumed as being the backbone link on which a risk propagation graph is built. The problem here is that a clear interpretation is often

left implicit by designers, thus leaving open the possibility of mixing correlation links with causality links, or just simply reducing causality to a kind of strong correlation. To understand how causality is different from correlation and how this is important for risk propagation, think that the risk propagated through causality can be deterministically controlled by modifying or un-linking the cause node. If an event type A is the cause of another event type B, controlling A means controlling the effect on B[7]. This is not the case when we have just a correlation relation. For instance, the risk of arriving late may be correlated to the risk that the presentation performs badly, but it might not be the cause of its failure. Notice that this distinction can be of essential importance for querying and using a risk propagation graph (see for instance the choice of mitigation strategies).

(3) *object/event (object participation).* This other link always denotes the dependency between objects of a certain type and the events these are implicitly involved in. This relation can be also used to discover new correlation or causality links between EVENT TYPES. For instance, suppose we have a graph with the link $Device(Object) \rightarrow Computer\ freezes(Event\ Type)$. In a simple risk propagation scenario, this link may be used to 'pass' a risk value from an object to a certain event. Following COVER terminology, "Device" can be taken to represent a THREAT OBJECT (TYPE), implicitly involving a certain EVENT TYPE, e.g., as a shorthand proxy for *"Plugging in Device"*. The "Device" THREAT OBJECT thus hides a PARTICIPATION relationship with that RISK EVENT, which, in turn, represents an occurrence of that given EVENT TYPE. This clarification guided by COVER has multiple implications for modeling. As an example, consider the possibility to identify a set of multiple *threat objects* associated with a single type of event. Similarly, this would imply the possibility of making explicit multiple types of OBJECT AT RISK participating in the same event.

(4) *object/object (parthood).* This case usually occurs in graphs representing the connection between digital objects (see the cybersecurity cases like graphs $e$ and $f$ in Figure 2). But it is also possible to find examples of it in physical contexts, e.g., supply chain scenarios. Here the interpretation is often one of a parthood link between the objects at hand (e.g., hard disk and laptop) such that VULNERABILITIES of an object can be *activate* or enable the VULNERABILITIES of the other (see [3,24]) when they are connected via these links. Notice that, in this case, we have implicit the *Risk events (Types)* connected to the manifestation of these VULNERABILITIES. So, when writing $(A \rightarrow B) \cdot \alpha$, we have $\alpha$ representing a probability value that refers either to: .i the correlation or causality connecting the RISK EVENT (TYPES) that are the manifestation of these VULNERABILITIES; .ii the probability of a manifestation of the VULNERABILITY of my device (of type) A (which, again, is a RISK EVENT) given that A is part of another device (of type) B; .iii the probability of a manifestation of the VULNERABILITY of my device (of type A) given that it has another device (of type) B as part.

[7] [3] advances and ontology-based discussion on causation and event prevention.

**Instance-to-type.** When an instance is related to a type, this generally depends on mixing the semantics of the link in the graph with the possible operations that the link enables.

(1) *individual/event (individual participation)* This possible modeling refers, as in the type-to-type case, to a participation relationship. The different nuance here is that the object in question does not represent a class of objects, but an individual, e.g., a specific IP address, a person like Anna, or a specific product (e.g., "my laptop"). This particular case depends on the need to infer risk values for specific objects in a given system, or the need to identify objects instances that may represent a threat.
(2) *property/event (characterization)* This instance/type relation is less common compared to the previous one. A typical example of this relationship is when one node in the graph is associated with multiple nodes that are considered as "risk characteristics" [20]. For instance, we may have multiple nodes about a delay quantified in minutes (e.g., 15 minutes), associated with a node representing a transportation step - all these ranges of time have a different impact on the final calculation of risk. We may also have nodes like, "low impact", "high impact", and "medium impact" associated with an event. In these cases, the probability value is an abstract particular (an instance) representing a *quality value* [14] characterizing that event type (e.g., the probability of an event of transportation occurring with a 10' delay).

## 5 Implications

According to our analysis Risk Propagation is an event that *leverages the causal relations involved in a risk experience network, to make a (possibly more nuanced) calculation of causal and triggering likelihoods and hence of risk values.* Accordingly, risk propagation always involves bundles of different interconnected concepts, representing events and objects, but also *dispositional properties* as *manifestation of events desired by an agent* [24] (e.g., *intentions*, *vulnerabilities* and *threat capabilities*). Reasoning with the effect of changes in those things can play a key role in the propagation and the analysis of risk. In this respect, we highlight two implications.

**Implications on Expressivity.** Here we map the *expressivity* of a risk propagation model to the *capability to answer queries about a risk experience.* If we consider the analysis we provided, it turns out that the adoption of graphs with no distinctions, for example, between causation and participation, or between objects and events, is restrictive. To emphasize the implication on expressivity, we gathered feedback from 5 domain security expert analysts, in the domain of cyber-security, who have been involved in risk assessment activities and that have been working on the identification of risk causes and risk dependencies via the application of risk propagation approaches. We ran open-ended interviews and the main open questions we asked were about *relevant queries that lack proper support in existing risk propagation approaches.*

We then selected the following examples as the most representative cases of (currently) not addressable requests. These are used *to infer the risk of*:

(1) *"an object, given the event(s) in which it participates"*;
(2) *"an event, given the event(s) to which it is connected"*;
(3) *"an object, given the object(s) to which it is connected"*;
(4) *"an event, sharing an object with other events"*;
(5) *"an object in an event with another object, which is in another event"*;
(6) *"an event, given different properties characterizing the correlated event"*.

These examples cannot be addressed without the support of an ontology. For example, what if the approach relies only on a probabilistic graph where all the nodes are Event Types? What if it does not support any distinction between types of relations, like participation or causation?

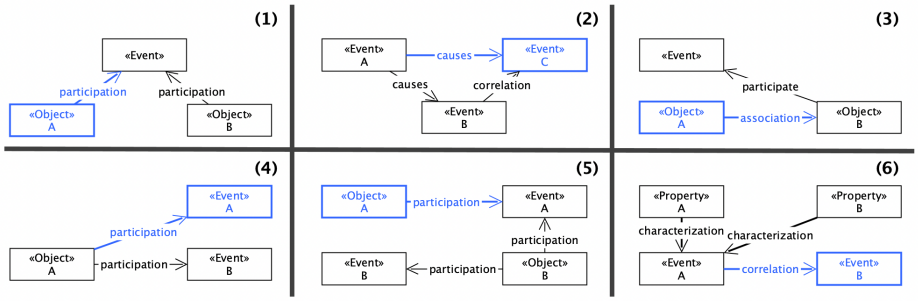


Figure 3: Patterns that can be used to model the example requests (1-6).

Figure 3 shows of how the above-listed requests/queries may be addressed through graph structures. Multiple nodes having different semantics are involved, e.g., objects, events, and different relations (e.g., associations, participation, correlations, and characterization relations). As we have discussed, all these elements composing a Risk Experience can be often conflated and mixed up.

Consider pattern (1). The *mainstream approach* (let us call it MA) is to flatten the structure into a graph where each link can be used to propagate risk values and each node can be associated with a value quantifying risk. In this sense, a person (e.g., Anna) who participates in an event associated with a risk value (e.g., a presentation with a risk of failure), can inherit that risk. Accordingly, all the nodes and relations are involved in the calculation of risk, and no functionality to distinguish objects from events is provided. This is also valid for the semantics of the relations, where no information is provided to understand whether some different links (e.g., "presents" or "look at") are of the same type (e.g., "participation"). Following (MA), all the other patterns highlight similar issues. Consider (2). How can I filter out only chains of events from graphs where I have nodes like "Anna", "Car" and "Presentation", and calculate the risk of one event given only the events to which it is connected? Again, consider (6), given a graph with nodes like "Anna", "Car", "Transportation", "Presentation", "10 mins late", how can we filter out only nodes that are properties characterizing only a specific event?

By leveraging our analysis, instead, we can adopt a new perspective, i.e., an *Ontology-driven Approach (OA)*, where information is represented explicitly. The main suggestion that emerges is that all information regarding the calculation of probability should be represented via a *probabilistic graph* encoding a chain of Risk Event Types. Similarly, the data used to query and assess the given system of events and objects can be modeled via a *knowledge graph* whose structure concerns a completely different scope. This has three main implications. Firstly, the graph for the probabilities assessment can be fully disambiguated, thus involving a clear understanding of the events making the reference scenario, their causal chains, and a better grounding for the modeling and update of probabilities. Secondly, the knowledge graph, by accounting for (types of) Objects (e.g., Objects at Risk), their participation in Risk Events and possible different relations between them, enables users to run queries that go beyond the graph structure built upon probabilities inference mechanisms.

**Implications on Accuracy.** Our analysis can be used also to support the *accuracy* of a risk propagation assessment. Suppose we have a graph including the different concepts we discussed, where nodes and relations may participate in the propagation of risk. This implies a challenge in determining the possible causes of a loss and the possible paths in the graphs that could lead to that loss.

Consider query (3), suppose we have two persons (objects), i.e., A and B, and a loss event that is "presentation" (P). A participates in P, but B does not. Does B inherit the risk of the event by being associated with A, which is involved in P? This depends on *the type of their association*. If B is a "colleague-of" A, B may share the risk of losing the client, if B is just a "friend-of" A, possibly not. Thus, in this case, clarifying the semantics of the graph components allows for discovering critical risk paths. Similarly, suppose that, as from pattern (2) in Figure 3 we have a chain of events, where event C represents a Loss Event, e.g., the *presentation failure*, event A represents the event "studying till late" and the event B represents the event "arriving late". Some key questions in this simple scenario are: *what leads to a change in the presentation performance?*, *what events are likely to improve the probability that the presentation succeeds?*, and *what one should do to improve the final outcome?*. Distinguishing between *causal* and *correlation* relations, in this case, would be of pivotal importance. For instance, by knowing that what is having a causal impact on the presentation performance is "the fact that I rehearsed a lot", I can consider it much "riskier" to not prepare the presentation than arriving late.

As a final key point, the introduction of dispositional properties as first-class citizens allows for connecting risk propagation with *prevention*, but also to explain some other aspects of the propagation between objects. How, for instance, introducing or blocking threat agents and mitigating vulnerabilities may affect the whole risk propagation process? Moreover, what if, for example, Anna's boss is exposed to financial risk and his "risk can propagate to Anna" because of their contract, i.e., because of the commitments and claims (which are again dispositions) in that contract? Our ontological analysis can be used to explain also that kind of propagation.

## 6 Conclusion

In this paper, we leveraged the *(COVER)* ontology to run an analysis of *"risk propagation"*. To the extent of our knowledge, ours is the first attempt to investigate this notion through an ontological investigation. The presented analysis allowed us to: explain *.i* how the propagation of risk is somehow concerned with a phenomenon of belief updating; *.ii* explain how talking about the "propagation" of risk can be misleading; *.iii* identify the concepts and relationships required to capture the cascading effect assumed when talking about risk propagation without incurring in ambiguities and reductions. Moreover, the presented work led us to two new important insights. Firstly, the application of ontology-driven conceptual models may play a key role in the explanation of specific applications and techniques. More concretely, the application of COVER played a central role in the explanation of concepts that are necessary to understand how risk is calculated and propagated in the available approaches. Secondly, the analysis suggests that to fully exploit risk propagation and answer queries about how risk is propagated through different kinds of objects and events, the inference facility provided by probabilistic graphs should be integrated with the representation of several other notions involved in the concept of risk, namely, agent, their goals, the importance of these goals, the impact of certain events on their goals, etc.

We have three main plans for future work based on the presented results. Firstly, we aim to explore further how the phenomenon of risk propagation is related to the quantification of *severity*, the activation of *countermeasures*, and the identification of *vulnerabilities*. In this respect, the idea is to exploit some of the results presented in a companion paper [3] and provide an analysis that goes beyond risk and delves into the connected security domain. Secondly, we aim to compare and assess some of the available technologies that are employed to propagate the risk and see how these may be used to revise, extend or confirm our ontological assumptions (see, for instance, the case of models that are able to update probabilities through a cyclic or acyclic chain of events). Finally, we aim to exploit the explanation proposed in this paper and evaluate it over an ontology-driven risk propagation approach, by using real data and showing how this can improve/extend the current state-of-the-art applications.

## Acknowledgement

This work was done in collaboration with Accenture Labs, Israel. The research conducted by Mattia Fumagalli is also supported by the *"Dense and Deep Geographic Virtual Knowledge Graphs for Visual Analysis - D2G2"* project, funded by the *Autonomous Province of Bolzano*.

## References

1. Aven, T., Renn, O., Rosa, E.A.: On the ontological status of the concept of risk. Saf. Sci. **49**(8), 1074–1079 (2011)

2. Band, I., et al.: Modeling enterprise risk management and security with the archimate language – W172 (2017)
3. Baratella, R., et al.: Understanding and modeling prevention. In: Intl. Conference on Research Challenges in Information Science. pp. 389–405. Springer (2022)
4. Cao, S., Bryceson, K., Hine, D.: An ontology-based bayesian network modelling for supply chain risk propagation. Ind. Manag. Data Syst. (2019)
5. Chaudhuri, A., et al.: Risk propagation and its impact on performance in food processing supply chain: A fuzzy interpretive structural modeling based approach. J. Model. Manag. (2016)
6. Coso, I.: Enterprise risk management-integrated framework. Committee of Sponsoring Organizations of the Treadway Commission **2** (2004)
7. Deng, X., et al.: Formation mechanism and coping strategy of public emergency for urban sustainability: A perspective of risk propagation in the sociotechnical system. Sustainability **10**(2), 386 (2018)
8. Deng, X., et al.: Risk propagation mechanisms and risk management strategies for a sustainable perishable products supply chain. Comput. Ind. Eng. **135** (2019)
9. Engelberg, G., et al.: An ontology-driven approach for process-aware risk propagation. In: 38th ACM/SIGAPP Symposium on Applied Computing (2023)
10. Garvey, M.D., Carnovale, S.: The rippled newsvendor: A new inventory framework for modeling supply chain risk severity in the presence of risk propagation. Int. J. Prod. Econ. **228**, 107752 (2020)
11. Garvey, M.D., et al.: An analytical framework for supply network risk propagation: A bayesian network approach. Eur. J. Oper. Res. **243**(2), 618–627 (2015)
12. González-Rojas, O., et al.: Quantifying risk propagation within a network of business processes and it services. Bus. Inf. Syst. Eng. **63**(2), 129–143 (2021)
13. Guarino, N.: On the semantics of ongoing and future occurrence identifiers. In: Intl. Conf. on Conceptual Modeling. pp. 477–490. Springer (2017)
14. Guizzardi, G.: Ontological foundations for structural conceptual models (2005)
15. Guizzardi, G., et al.: Ontological unpacking as explanation: the case of the viral conceptual model. In: Intl. Conf. on Conceptual Modeling. pp. 356–366 (2021)
16. ISO: Risk Management - Vocabulary, ISO Guide 73:2009 (2009)
17. ISO: ISO 31000:2018 - Risk management – Guidelines (2018)
18. Jiang, J., et al.: Identifying propagation sources in networks: State-of-the-art and comparative studies. IEEE Commun. Surv. Tutor. **19**(1), 465–481 (2016)
19. Kavallieratos, G., et al.: Cyber risk propagation and optimal selection of cybersecurity controls for complex cyberphysical systems. Sensors **21**(5), 1691 (2021)
20. Li, M., et al.: Risk propagation analysis of urban rail transit based on network model. Alex. Eng. J. **59**(3), 1319–1331 (2020)
21. Newman, M.: Networks. Oxford university press (2018)
22. Pearl, J.: Graphical models for probabilistic and causal reasoning. Quantified representation of uncertainty and imprecision pp. 367–389 (1998)
23. Pearl, J.: Reverend bayes on inference engines: A distributed hierarchical approach. In: Probabilistic and Causal Inference: The Works of Judea Pearl, pp. 129–138 (2022)
24. Sales, T.P., et al.: The common ontology of value and risk. In: International Conf. on Conceptual Modeling. pp. 121–135. Springer (2018)
25. Shin, K., et al.: Risk propagation based dynamic transportation route finding mechanism. Ind. Manag. Data Syst. (2012)
26. Sunil, K., et al.: Message passing algorithm: A tutorial review. IOSR J. Comput. Eng. **2**(3), 12–24 (2012)