Ontological Analysis and Redesign of Risk Modeling in ArchiMate

Tiago Prince Sales[1], João Paulo A. Almeida[2], Sebastiano Santini[3], Fernanda Baião[4] and Giancarlo Guizzardi[3]
[1] *Department of Information Engineering and Computer Science (DISI), University of Trento, Italy*
[2] *Ontology & Conceptual Modeling Research Group (NEMO), Federal University of Espírito Santo, Vitória, Brazil*
[3] *Conceptual and Cognitive Modeling Research Group (CORE), Free University of Bozen-Bolzano, Italy*
[4] *Department of Applied Informatics, Federal University of the State of Rio de Janeiro (UNIRIO), Brazil*
tiago.princesales@unitn.it, jpalmeida@ieee.org, sebastiano.santini@stud-inf.unibz.it,
fernanda.baiao@uniriotec.br, giancarlo.guizzardi@unibz.it

***Abstract*—Risk analysis is a complex and critical activity in various contexts, ranging from strategic planning to IT systems operation. Given its complexity, several Enterprise Architecture (EA) frameworks and modeling languages have been developed to help analysts in representing and analyzing risks. Yet, the notion of risk remains overloaded and conceptually unclear in most of them. In this paper, we investigate the real-world semantics underlying risk-related constructs in one of such approaches, namely ArchiMate's Risk and Security Overlay (RSO). We perform this investigation by means of ontological analysis to reveal semantic limitations in the overlay, such as ambiguity and missing constructs. Building on the results of this analysis, we propose a well-founded redesign of the risk modeling aspects of the RSO.**

***Index Terms*—Risk Modeling, Enterprise Architecture, ArchiMate, Ontological Analysis, Unified Foundational Ontology**

1. Introduction

Risk is an inherent aspect of many human endeavors. Since risks often threaten an enterprise's ability to achieve its goals, risks are frequently subject to scrutiny and mitigation in enterprises, under the banner of risk management. Risk management involves a complex number of activities that include identifying, understanding, assessing and addressing potentially unfavorable prospects. It is widely accepted as a business-critical activity in various contexts, ranging from strategic planning to IT systems operation.

Given the importance of risk management to business success, it is no surprise that risk-related concepts have made their way in to Enterprise Architecture (EA) frameworks and modeling languages in an effort to assist architects in representing and analyzing risks in their business contexts. One of such frameworks is ArchiMate, particularly its Risk and Security Overlay (RSO) [5]. The RSO establishes means for representing important aspects of risk-related phenomena in ArchiMate including threats, vulnerabilities, losses, assets at risk, and associated control strategies.

Despite the advances in the representation of risk-related phenomena, we have observed that there are still some limitations in the clarity and expressiveness concerning certain aspects of risk. We trace some of these shortcomings to the difficulty in characterizing the central notion of risk itself, which has been the subject of systematic investigations for over 50 years [17]. The notion of risk remains elusive, as evidenced by the plethora of definitions in the literature [2], the number of standardization efforts (e.g. ISO 73:2009 [12], IRM [11], COSO [7]) and the notable variability among risk modeling languages with respect to the concepts and relations they adopt (e.g. CORAS [14], RiskML [22], the Goal-Risk Framework [1], and the RSO [5]).

In this paper, we address some challenges in conceptualizing and modeling risk with a systematic ontology-based approach. We investigate the concept of risk and related notions and propose an ontology of risk as a semantic foundation for the representation of risks in Enterprise Architecture. This ontology is the result of a thorough analysis of the notion of risk in the literature and is aligned with the Unified Foundation Ontology (UFO) [9]. We use the proposed risk ontology to perform an ontological analysis of ArchiMate's Risk and Security Overlay (RSO). We have selected ArchiMate and the RSO as they form the most comprehensive Enterprise Architecture approach with support for the representation of risks (other languages and frameworks for risks have not been fully-integrated into EA solutions). We focus on the risk modeling fragment of the RSO, not addressing here in depth the security elements. Building on the results of the analysis, we propose an ontologically well-founded redesign of the RSO, which clearly distinguishes between different perspectives on risk and is more expressive to represent risk-related phenomena.

The remainder of this paper is structured as follows. In Section 2, we provide an overview of the Risk and Security Overlay (RSO). In Section 3, we introduce an ontology of risk, which serves as conceptual foundation for the analysis in Section 4. The results of the analysis are used to redesign the RSO in Section 5. We conclude with a discussion on related work and final remarks in Sections 6 and 7.

TABLE 1. SUMMARY OF RISK MODELING ELEMENTS IN ARCHIMATE'S RISK AND SECURITY OVERLAY (RSO)

RSO Element	ArchiMate Element	Definition
THREAT AGENT	Active Structure Element	Anything that is capable of acting against an asset in a manner that can result in harm.
THREAT EVENT	Business Event	Event with the potential to adversely impact an asset (including attacks).
LOSS EVENT	Business Event	Any circumstance that causes a loss or damage to an asset.
VULNERABILITY	Assessment	D1: The probability that an asset will be unable to resist the actions of a threat agent. D2: A weakness which allows an attacker to threaten the value of an asset.
RISK	Assessment	D1: The probable frequency and probable magnitude of future loss. D2: The potential of loss resulting from an action, activity or inaction, foreseen or not.
ASSET AT RISK	Resource, Core Element	D1: Anything tangible or intangible that can be owned or controlled to produce value. D2: Any data, device or environmental component that supports information-related activities.

2. ArchiMate's Risk and Security Overlay

The Risk and Security Overlay (RSO) for ArchiMate is the result of a collaboration between The Open Group's ArchiMate and Security Forums, which aimed to support the systematic identification, representation and analysis of risks in organizations. The overlay was developed based on an extensive review of several risk frameworks (e.g. the Open FAIR Risk Taxonomy [23], the TOGAF security guide [24], and the SABSA framework [21]) and a consolidation of risk-related concepts, which were then mapped to ArchiMate constructs. The overlay was proposed in compliance with ArchiMate 2.0, but it has been recently revisited to accommodate the improvements of ArchiMate 3.0.1 in [5].

The overlay proposes a representation strategy for risk and security modeling, following the scheme depicted in Figure 1, specializing existing ArchiMate constructs. The overlay supports the representation of THREAT AGENTS as those responsible for THREAT EVENTS, which are events that trigger LOSS EVENTS. Both THREAT and LOSS EVENTS are associated with VULNERABILITIES, which in turn are associated with RESOURCES. LOSS EVENTS influence RISK assessments, which can motivate CONTROL OBJECTIVES. These are then realized in SECURITY REQUIREMENTS and CONTROL MEASURES, which are in turn realized in IMPLEMENTED CONTROL MEASURES. Table 1 lists the elements that form the RSO risk modeling fragment, including their mapping into basic ArchiMate elements and their respective definitions (from [5]).

The RSO defines a THREAT as "a possible danger that might exploit a vulnerability to breach security and thus cause possible harm". Recognizing that the term is inherently ambiguous, the authors distinguish between the events that have the potential of harming the organization, which they call THREAT EVENTS, from the entities responsible for intentionally or unintentionally causing them, which are labeled THREAT AGENTS. Note that, even though the term "agent" is used, this element is applicable to groups and objects as well. Thus, either a machine or an organization can be classified as a THREAT AGENT, and thus THREAT AGENT may be represented by any ACTIVE STRUCTURE ELEMENT. A THREAT EVENT is represented by a specialized BUSINESS EVENT.

A LOSS EVENT is defined as "any circumstance that causes a loss or damage to an asset" and is triggered by a THREAT EVENT. The concept is mapped to a BUSINESS EVENT in ArchiMate.

VULNERABILITY is given two definitions. In one definition, extracted from [23], a VULNERABILITY is "the probability that an asset will be unable to resist the actions of a threat agent". The second, which seems to be consolidated from the literature, defines a VULNERABILITY as "a weakness which allows an attacker to threaten the value of an asset". VULNERABILITIES are mapped as ArchiMate ASSESSMENTS, which "represents the result of an analysis of the state of affairs of the enterprise with respect to some driver." [25]. A VULNERABILITY can be associated with both THREAT EVENTS and LOSS EVENTS as well as with resources and other core elements.

Different definitions for RISK are provided in [5], which is symptomatic of the difficulty in characterizing its semantics. On the one hand, risk is defined as "the probable frequency and probable magnitude of future loss", following the definition proposed in the Open FAIR Risk Taxonomy [23]. On the other hand, it is defined as "the potential of loss (an undesirable outcome; however, not necessarily so) resulting from a given action, activity, and/or inaction, foreseen or unforeseen". A third definition, namely that "a risk is a quantification of a threat" is invoked to justify the representation of RISK using a specialization of the ASSESSMENT construct in ArchiMate.

In the overlay, risks are usually represented focusing on a particular entity the organization wants to protect. Such an entity is labeled an ASSET AT RISK. This notion of asset accounts for any kind of object, tangible or intangible,

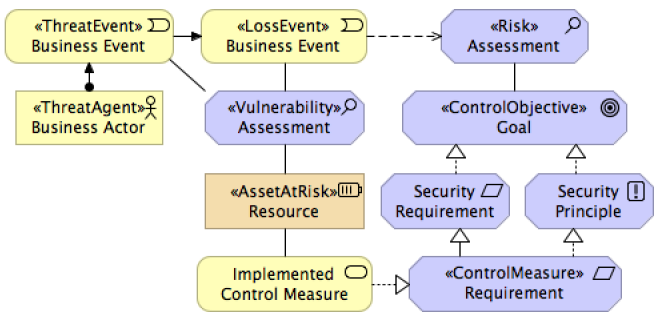

Figure 1. ArchiMate's Risk and Security Overlay (extracted from [5]).

that can be owned or controlled by the organization to create value. Given its general nature, it can be applied to a RESOURCE or any CORE ELEMENT in ArchiMate (including BUSINESS ACTORS and BUSINESS PROCESSES)

The RSO proposes five elements in the Security domain, namely CONTROL OBJECTIVE, SECURITY REQUIREMENT, SECURITY PRINCIPLE, CONTROL MEASURE and IMPLEMENTED CONTROL MEASURE. Given our scope, we focus here on CONTROL OBJECTIVE, which is associated with the risk modeling fragment through RISK assessments. These are addressed by CONTROL OBJECTIVES, a sort of high level goal that defines what the organization intends to do about an identified risk. For instance, if the RISK of employees getting injured in work-related accidents is considered unacceptable, the organization might decide to reduce it (e.g. by changing safety procedures) or to transfer it (e.g. by purchasing a broader insurance policy). In any case, the result of this decision is captured by a CONTROL OBJECTIVE, which is mapped as an ArchiMate GOAL.

To briefly exemplify how the RSO can be used, we now present three examples from [5], all of which pertain to risks in the Coldhard Steel company. Figure 2 depicts an RSO model concerning the risk of losing production due to machine failure. In the example, a *Power supply assembly* is an ASSET AT RISK that fails when power fluctuates (this failure is represented as a THREAT EVENT). When the power assembly fails, some machines also fail, characterizing a loss for the organization (represented as a LOSS EVENT). In this scenario a risk is identified, namely the RISK of a *Production loss due to machine failure*. Then, the CONTROL OBJECTIVE *Adequate peak capacity of power supply* implies that the organization seeks to reduce this risk, which is done by *replacing the power supply assembly*.

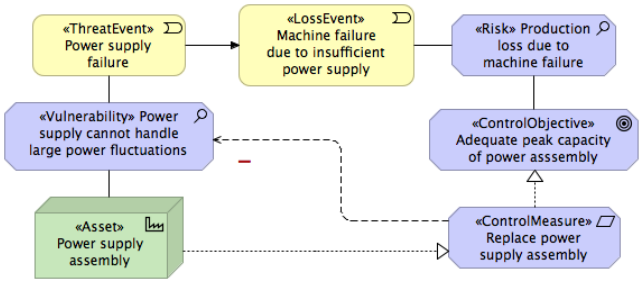

Figure 2. Modeling the risk of losing production (from [5]).

Although this model provides valuable information for stakeholders of the Coldhard Steel company, it leaves some relevant questions unanswered, such as "why is the *Power supply assembly* an ASSET AT RISK if it does not seem to be in any danger?", and "why is a *Machine failure* considered a LOSS EVENT if the loss actually occurs when production is compromised?". Concerning the root cause of the events, one might add "what causes power fluctuations?"

Figure 3 depicts another risk scenario present in the RSO paper [5]. In this case, the THREAT EVENT is a *work-related incident*, in which an employee gets injured. Such an incident triggers the *submission of a compensation claim*, an event represented as a loss to the organization. Associated to this LOSS EVENT, there is an assessment (represented as a RISK) that the total cost of such claims is not acceptable to someone in the organization (maybe the business owner?). Thus, a plan to reduce this risk is represented, which will be implemented by extending the currently inadequate safety procedures.

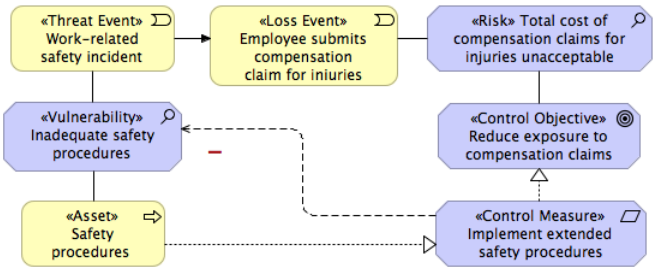

Figure 3. Modeling the risk of paying compensation claims (from [5]).

The classification of the various events in these examples raises some interesting semantic questions. For instance, "Shouldn't an incident where an employee gets hurt be considered a loss?". From the perspective of an employee, it is most likely an unwanted event. This suggests that the classification of events is somewhat contextual in nature, and that stakeholders may classify events differently according to their own goals. A further question is "Why is a submission of a claim already considered a loss?". If the loss regards financial reasons, should not the loss be the compensation claim payment? This suggests that anchoring losses somehow in the motivations of the various stakeholders may be required to clarify the modeler's intent.

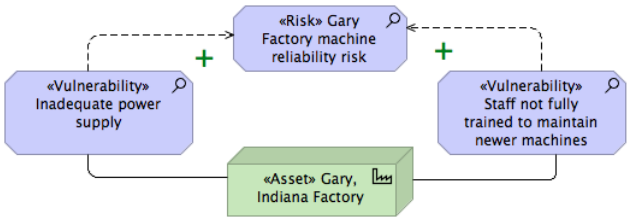

Figure 4. Modeling the overall risk that a factory is exposed to (from [5]).

Note that the two risk assessments in the examples discussed thus far differ in their nature. In Figure 2, the risk assessment concerns consequences of the loss event (*Production loss due to machine failure*), whilst in Figure 3, the risk assessment concerns a decision regarding how the organization intends to address the perceived risk (*the risk is unacceptable)*. A third example in the proposal [5] (see Figure 4) includes an assessment in which no particular statement about the risk is included, and a RISK element is defined with the rather neutral label *Gary Factory reliability risk*. This noteworthy variability in the usage of the RISK element in the proposal indicates that it currently lacks a clear semantics. As a consequence, we argue that the RSO lacks guidance for the modeler concerning the adequate representation of risk-related phenomena.

3. Ontological Foundations

In order to systematically address the representation of risks and risk-related phenomena, we propose to first grasp the ontological foundations of risks. This is done here with a fragment of the Common Ontology of Value and Risk [19], which is a reference ontology aiming to unify and clarify conceptualizations about these two phenomena. It was designed as an extension of the Unified Foundational Ontology (UFO) [9] and was built on top of an ontological analysis of value presented in [20]. In this section, we provide an overview of this reference ontology, focusing exclusively on its risk fragment. We clarify our assumptions on the nature of risk and then introduce its formalization in OntoUML [9], reusing foundational ontological distinctions from UFO (those concerning events, objects, dispositions, situations, relationships, their types, etc.)

3.1. Assumptions on the Nature of Risk

Our first assumption on risk is that it is **relative**. This means that an event might be simultaneously considered as a risk by one agent and not as a risk by another (it may even be considered as an opportunity by such an agent). To exemplify why this assumption holds, consider a potential terrorist attack. Most people would view such an event as a risk, i.e., as something they do not want to happen and that would "hurt" them in some way. Now, consider a terrorist organization who plans such an attack. For them, the attack itself is not a risk, as it is a way to achieve their goals.

The reason why risk is relative constitutes our second assumption on its nature. A risk is perceived according to its **impact on goals**, 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, this is because missing a train has an impact on one's goals, such as arriving on time at a meeting or saving money.

Our third assumption is that risk is **experiential**. This means that we ultimately ascribe risk to events, not objects. This claim may seem counterintuitive at first, as many conceptualizations assume entities such as "Object at Risk" [6] and "Asset at Risk" [5]. Our claim is not that such concepts do not exist. Our assumption is that if a risk assessment is made towards an object, the overall identified risk will be derived from the risks ascribed to events that can impact such an 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.

Our next assumption is that risk is **contextual**. Thus, the risk an object is exposed to may vary even if all its intrinsic properties (e.g. its vulnerabilities) are the same. To exemplify this position, consider the risk of a car accident. Naturally, the properties of a car have some influence on this risk, such as having or not an anti-lock braking system (ABS). Still, the properties of the road (e.g. the asphalt's adherence) and the weather (e.g. a snow storm) can significantly increase (or enable) risks.

Lastly, we assume that risk is grounded on **uncertainty** about events and their outcomes. This is very standard position, as proposed in [12] and extensively discussed in [2], which implies that likelihood is positively correlated with how risky an event is. For instance, the risk of a smoker having lung cancer is higher than that for a non-smoker simply because it is more probable.

3.2. The Ontology of Risk

The ontology of risk [19] formally captures our conceptualization of risk following the assumptions discussed in the previous section. Given the polysemic nature of the term "risk" [8], [13], we aim to disentangle three perspectives on risk: (i) a perspective of risk centered on (unwanted) events and their causes, which constitute an overall RISK EXPERIENCE, (ii) a relational perspective which identifies the subjective nature of risks by establishing a relationship (a RISK ASSESSMENT) between those assessing risks and a risk experience, and (iii) a perspective of RISK as a (quantifiable) quality inherent to a RISK ASSESSMENT. The core part of the ontology is presented in figures 5 and 6. In the diagrams, we adopt the following color coding: events are represented in yellow, objects in pink, objectified intrinsic properties (tropes) in blue, objectified relationships (relators) in green, and situations in orange.

Figure 5 presents risk centered on the event perspective. A RISK EXPERIENCE is composed by events of two types, namely threat and loss events. A THREAT EVENT is one with the potential of causing a loss. It might be the manifestation of: (i) a VULNERABILITY, such as the flammability of a house which is manifested in a fire; or (ii) a THREAT CAPABILITY, such as the dexterity of a pick-pocketer to grab a wallet without alerting the owner. A THREAT EVENT might be intentional, such as a hacker attack, or unintentional, such as an accidental liquid spill on a computer. In any case, one can identify a THREAT OBJECT[1] as the entity "responsible" for causing the threat.

The second mandatory component of a RISK EXPERIENCE is a LOSS EVENT, which is defined by its impact on GOALS. This can either be: (i) a direct impact, captured by the HURTS relation between LOSS EVENT and INTENTION (e.g. the event of being robbed directly hurts the goal of feeling safe); or (ii) an indirect impact, i.e., a LOSS EVENT bringing about a LOSS SITUATION, which in turn hurts an INTENTION (e.g. having my phone stolen puts me in a

1. In this context, we use the term object in a very general sense, which includes agents, groups and organizations.

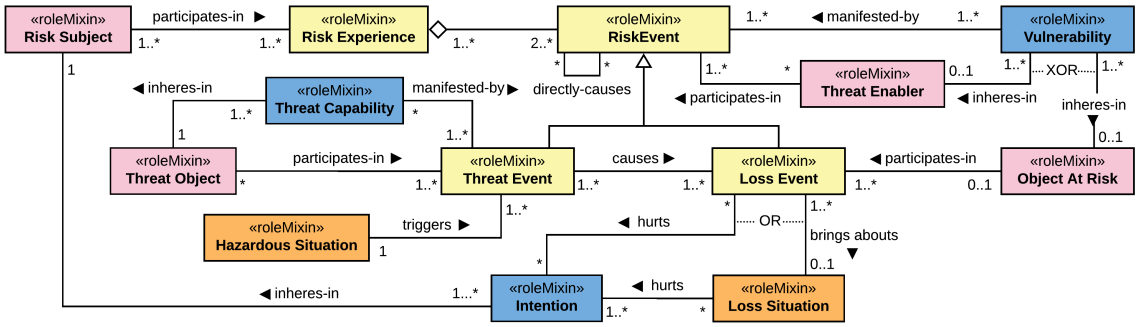

Figure 5. Modeling risk as an event composed by threats and losses (aka. RISK EXPERIENCE).

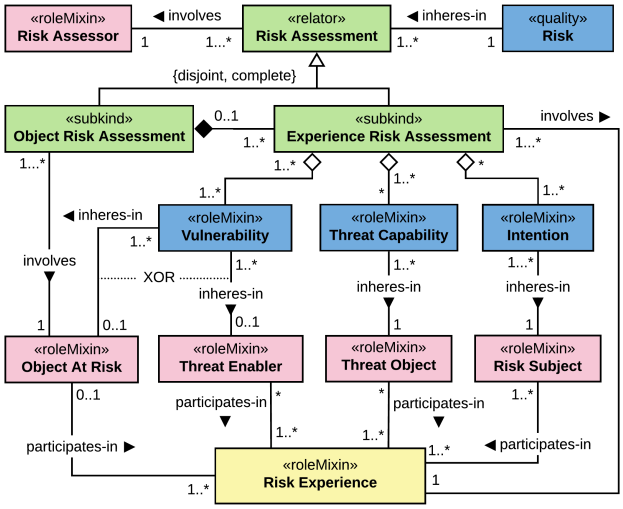

Figure 6. Modeling risk as an assessment relationship and as a quality.

phone-less situation, which hurts my goals of calling my family, closing business deals, etc.).

To capture the relative nature of risks, every RISK EXPERIENCE involves at least one RISK SUBJECT, the agent whose INTENTIONS would be affected by a potential loss.

The ontology also introduces an important role in LOSS and THREAT EVENTS, namely that of THREAT ENABLER. This role accounts for objects whose VULNERABILITIES enable threats and losses to happen, but do not cause or are harmed by them. Take for instance a factory accident caused by a worker, who ended up injured. In this case, the worker is both the THREAT OBJECT, as he caused the accident, and the OBJECT AT RISK, as he was injured by it. Still, if the reason he actually got hurt was because his safety equipment was not safe enough, the equipment would have played the role of a THREAT ENABLER.

Note that, with the exception of INTENTION, the concepts presented in Figure 5 are modeled as roles. This means that the very same event might be a threat to one agent, a loss to another, and neither for a third. The same goes for vulnerabilities and threat capabilities.

The relational perspective of risk is depicted in Figure 6. We formalize it as an objectified relationship labeled RISK ASSESSMENT, which involves an agent as the assessor of risk, deemed the RISK ASSESSOR, and the target of the assessment, either an object or an event. Risk assessments on objects are labeled OBJECT RISK ASSESSMENTS and involve exactly one OBJECT AT RISK. Risk assessments on events are deemed EXPERIENCE RISK ASSESSMENTS and involve exactly one RISK EXPERIENCE. Note that, given our assumption that risk is experiential, assessing the risk an object is exposed to means assessing the risk of all the envisioned events (experiences) that may potentially harm the OBJECT AT RISK. This assumption is formalized by the composition between OBJECT- and EXPERIENCE RISK ASSESSMENTS.

The quantitative perspective of risk is also depicted in Figure 6. It is captured by the RISK quality inhering in a RISK ASSESSMENT. In UFO, a quality is an objectification of a property that can be directly evaluated (projected) into certain value spaces [9]. Common examples include the weight of a person, which can be measured in kilograms or pounds, and the color of a flower, which can be specified in RGB or HSV. Representing risk as a quality means that it can also be measured according to some scales, such as an easy discrete scale like $< Low, Medium, High >$ or a more precise continuous scale (e.g. from 0.00 to 100.00).

4. Ontological Analysis

Rosemann et al. [18] define an ontological analysis as *"the evaluation of a modeling grammar, from the viewpoint of a pre-defined and well-established ontology"*. The authors argue that modeling grammars should be isomorphic to their underlying ontology, i.e. there should be a one-to-one mapping between the constructs of a language and the concepts of its ontology. This is a desirable characteristic because it prevents issues such as **construct overload** and **construct deficit**. The former is characterized by the presence of a grammatical construct that represents more than one ontological concept, which would lead to ontological inaccuracy. The latter is characterized by the absence of a grammatical construct for an existing ontological concept, which would result into ontological incompleteness. In the following section we describe the ontological analysis we conducted to assess the risk-related constructs of RSO, in light of the risk ontology we have just discussed.

4.1. Analysis of Vulnerabilities

The RSO defines a VULNERABILITY as: (i) "a weakness which allows an attacker to threaten the value of an asset"; and (ii) "the probability that an asset will be unable to resist the actions of a threat agent" [23]. These definitions suggest that a vulnerability may be two very different things. Nonetheless, by analyzing the other constructs that compose the RSO and the uses of the VULNERABILITY element in [5], it is clear that the first definition prevails. An example is the claim that "a vulnerability of an asset can lead to a loss event" and the representation of "Lack of access control" as a VULNERABILITY that enables an "Identity theft". Thus, we shall assume that a vulnerability is understood in the RSO as a weakness that enables threats and losses.

The concept is mapped as an ArchiMate ASSESSMENT, as the creators of the RSO argue that it "is the result of analyzing the weaknesses of elements in the architecture". We observe that this mapping collapses the entity itself (the vulnerability) with the assessment that results in identifying and possibly qualifying the entity. We interpret a vulnerability as a disposition of a special type. A disposition is a property that endows its bearer with the potential of exhibiting some behavior or bringing about certain effects under certain conditions [10]. The difference of a vulnerability from dispositions in general is that the former assumes a negative connotation, i.e., the manifestation of a vulnerability constitutes a loss or can potentially cause a loss from the perspective of a stakeholder. In fact, this is why we represent vulnerabilities as roles played by dispositions in the risk ontology discussed in Section 3.

An advantage of distinguishing between a vulnerability from an assessment about it made by a stakeholder is the possibility of representing multiple assessments for the same vulnerability. This may capture disagreements between stakeholders on the probability of it being manifested, as well as different assessments concerning how to address it (e.g., that it is too expensive to be removed). We refer to the semantic overload of the VULNERABILITY construct, which collapses actual vulnerabilities with assessments about them, as *Limitation L1*.

4.2. Analysis of Threat Events and Threat Agents

In an effort to consolidate existing risk terminology, the authors of the RSO admit the existence of a general concept of threat, informally defined as "a possible danger that might exploit a vulnerability [...] and thus cause possible harm". They recognize, however, that the term is inherently ambiguous, as it may refer to: (i) *an entity capable of causing harm*, such as a hacker who seeks to steal data from a company or a truck filled with flammable liquids; (ii) *an actual event that may cause harm*, such as a hacker attack, which can lead to the leak of sensitive data or a misuse of a machine, which can cause an employee getting hurt; and (iii) *a threatening circumstance*, such as a blizzard during a snowboarding session that increases the likelihood of an accident, or having untrained workers operating a machine which increases their chance of hurting themselves;

A threat in the first sense, that of a *harm-causing entity*, was introduced in the RSO as a THREAT AGENT. Given that things of various natures can play this role, it was mapped as an ACTIVE STRUCTURE ELEMENT in ArchiMate, which generalizes elements like BUSINESS ACTOR, BUSINESS ROLE, FACILITY, EQUIPMENT and so on. In the ontology we discussed in Section 3, this element is interpreted as the THREAT OBJECT. Note that this role can be played not just by agents, but also by objects (including those that would be represented as *Passive Structure Elements*). An example is a poisonous gas used in a production process that poses a threat to workers that have manipulated it. Thus, we argue that by ignoring its application to *Passive Structure Elements*, the current mapping is overly restrictive. We label this issue *Limitation L2*.

A threat in the second sense, that of a potentially *harm-causing event*, was introduced in the RSO as a specialization of BUSINESS EVENT labeled THREAT EVENT. In the RSO, a THREAT EVENT: (i) is associated to a VULNERABILITY, (ii) is assigned from a THREAT AGENT, and (iii) triggers a LOSS EVENT. We interpret this element as the homonymous class in our ontology. By only focusing on vulnerabilities, the RSO fails to account for the capabilities of the THREAT AGENTS that enables them to make threats, which we formalized in the ontology as a THREAT CAPABILITY[2]. As an example, consider a hacker launching a Distributed Denial-of-Service (DDoS) attack against the online platform of an e-commerce company. Such an attack only occurred due to a capability of the attacker to launch such attack. We label this construct deficit as *Limitation L3*.

Lastly, threats in the third sense, that of a *threatening circumstance*, are actually neglected in the RSO. These regard particular configurations of the world that allow or increase the probability of the occurrence of a threat event. We interpret these circumstances as HAZARDOUS SITUATIONS in our ontology and define them as situations which activate vulnerabilities and threat capabilities, which in turn will be manifested as threat events. Explicitly accounting for hazardous situations allow the representation of how several environmental factors increase the likelihood of threat events or empower threat agents, thus providing more information for devising mitigation strategies. We deem this construct deficit as *Limitation L4*.

4.3. Analysis of Assets at Risk

An ASSET AT RISK is defined in the RSO both as "anything tangible or intangible that can be owned or controlled to produce value" and as "any data, device or environmental component that supports information-related activities". Still neither definition actually describes what an asset *at risk* is, but what an asset is in general. In fact, the first definition resembles that of a RESOURCE in ArchiMate 3.0.1: "an asset owned or controlled by an individual or organization" [25].

2. This particular term is also used with a similar meaning in The Open Group Risk Taxonomy Standard [23]

In this paper, we assume the ontological interpretation of resources discussed in [4], which explains resources as tangible or intangible things needed to make progress towards a goal. Thus, if something is considered a resource to an organization, it has some value to it. This interpretation of a resource, roughly equivalent to those provided for an asset, shows that introducing an ASSET element in the RSO would be borderline redundant. Still, we argue that the distinction between a RESOURCE (or an ASSET) and an ASSET AT RISK should not be omitted, as it clearly identifies to the organization what assets are considered to be exposed to risks.

In the risk ontology, we distinguished two roles played by objects in a RISK EXPERIENCE, namely the OBJECT AT RISK and the THREAT ENABLER. In both cases, the dispositions of these objects enable the occurrence of threat and loss events. The difference between them is that the former is the thing at stake (i.e., the thing that may be harmed or damaged in a LOSS EVENT), whilst the latter is simply a risk-enabling thing, as it is not exposed to any potential damage. To exemplify this distinction, consider that a machine failed and caused a production loss. It was the machine's vulnerability that caused it to fail. Still, the integrity of the machine might not be affected by the failure at all. In this case, the machine is playing the role of a threat enabler. We label this lack of distinction between an OBJECT AT RISK and THREAT ENABLER as *Limitation L5*.

4.4. Analysis of Loss Events

The RSO defines a LOSS EVENT as "any circumstance that causes a loss or damage to an asset" [5]. This highlights that there could be two different emphases in the formulation of a loss event. One of them concerns an event that frustrates one's objectives ("a loss") and the other concerns the negative impact ("damage") to an asset. We consider that the negative impact on an asset should be accounted for by an underlying goal of protecting that asset, as it is considered a resource in a strategy to realize some goal [3].

By inspecting the RSO metamodel, we find that a LOSS EVENT: (i) is triggered by THREAT EVENTS, (ii) is associated to VULNERABILITIES, and (iii) influences a RISK assessment. None of these relational properties, however, captures a key aspect that constitutes a "loss" – namely that there is a stakeholder whose goal is compromised by such an event. The absence of a relation between loss events and goals prevents a modeler from explaining why there is a risk in the first place. For example, in Figure 2, we find a machine failure represented as a LOSS EVENT. Account for the impact on goals would clarify: Is a machine failure a loss because it delays production? Or it is a loss because a machine failure will result in defective products that might end up being shipped to customers? Without precisely representing specifically which events impact particular objectives, such questions cannot be properly addressed in the models. We refer to this construct deficit as *Limitation L6*.

The RSO also lacks a direct relation between LOSS EVENTS and ASSETS AT RISK. There is instead an association with a VULNERABILITY, which in turn is associated with an ASSET AT RISK. However, some events might be a manifestation of a vulnerability of one object that in turn damages another. In this case, the RSO would be unable to distinguish between objects whose vulnerabilities are manifested in the loss event from those that are compromised by the loss event. Suppose, for instance, that we want to represent that work incidents are caused by a vulnerability in the safety procedures, but that the assets at risk are actually the machines that can be damaged in an accident. We label this deficit as *Limitation L7*.

4.5. Analysis of Risks

The risk element is arguably the most complex to analyze, as it embodies a classical scenario of systematic polysemy. Evidences for this claim are the two very different definitions proposed in the RSO. On one hand, risk is defined as "the potential of loss resulting from an action, activity or inaction, foreseen or not", which emphasizes its nature as a causal chain of events that potentially leads to a loss. On the other hand, it is defined as "the probable frequency and probable magnitude of a future loss", which highlights its quantitative nature, mostly popularized by the famous equation, in which $risk = probability \times impact$.

Another evidence of the polysemic nature of risk is found in the examples presented in Section 2. In these examples, risk is used to represent the following elements: R1: "*Production loss due to machine failure*"; R2: "*Total costs of compensation claims for injuries unacceptable*"; and R3: "*Gary Factory machine reliability risk*"

In the examples, R1 and R2 are directly connected to their respective loss events, while R3 is connected only to vulnerabilities – in the sense that the vulnerabilities increase the risk. Note that, by analyzing the description of these risks, one can clearly see that they refer to entities of different ontological natures. R1 refers to a complex event composed by a particular loss (the production loss) that was caused by particular threat (the machine failure). R2 refers to a risk assessment, which captures: (i) a perception that compensation claims are a risk, and (ii) a judgment that this risk is unacceptable to the organization (or at least to some hidden stakeholder). Lastly, R3 refers to the aggregated risk a particular asset (the machines in the Gary Factory) is exposed to, which does not directly refer to any particular threat or event.

The nature of these different concepts represented by the same construct can be unveiled by means of the risk ontology discussed in Section 3. We interpret that cases like R1 refer to RISK EXPERIENCES, thus capturing the perspective of risk as an unwanted event. Cases like R2 refer to relationships of RISK ASSESSMENT. Such relationships represent that a stakeholder, the RISK ASSESSOR, interprets an event as a RISK EXPERIENCE according to someone's perspective, the RISK SUBJECT[3]. Lastly, R3 refers to the

3. Note that in context of a RISK ASSESSMENT, the roles of RISK ASSESSOR and RISK SUBJECT might be played by the same agent or by different ones.

RISK quality, which inheres in a RISK ASSESSMENT. In sum, by offering modelers a single construct to represent three different concepts, the RSO suffers from another problem of construct overload. We label this *Limitation L8*.

The identified limitations are summarized in Table 2.

TABLE 2. SUMMARY OF ONTOLOGICAL LIMITATIONS.

Ontological limitation
L1. A *construct overload* on the VULNERABILITY construct, which collapses actual vulnerabilities with assessments about them.
L2. A *construct deficit* to capture THREAT OBJECTS that are not active structure elements.
L3. A *construct deficit* to represent THREAT CAPABILITIES.
L4. A *construct deficit* to model a HAZARDOUS SITUATION, that activates vulnerabilities or increases the likelihood of threat events.
L5. A *construct overload* on the ASSET AT RISK construct, which collapses assets that are exposed to potential damages and those whose vulnerabilities enable threats and losses.
L6. A *construct deficit* to model a core property of a LOSS EVENT: its negative impact on goals of an affected stakeholder (the RISK SUBJECT).
L7. A *construct deficit* to model a LOSS EVENT's damage to an asset.
L8. A *construct overload* on the RISK construct, which collapses: (i) a complex event, (ii) the overall risk an asset is exposed to, and (iii) an assessment regarding what to do about an identified risk.

5. Redesigning the Risk and Security Overlay

In order to address the identified shortcomings, we now propose a redesign of the risk-related portion of the RSO, which also follows its original strategy of only using existing ArchiMate constructs. Addressing *Limitations L1, L2 and L3* is fairly straightforward. Concerning *L1*, we propose to map the VULNERABILITY concept as a CAPABILITY in ArchiMate instead of an ASSESSMENT. Then, as many assessments as necessary can be represented about a vulnerability, such as the beliefs of individual stakeholders about its relevance. This mapping is consistent with the interpretation of the ArchiMate CAPABILITY construct as a disposition in [4], albeit a disposition with negative connotation in the case of a vulnerability. Concerning *L2*, we propose it be addressed by also allowing RESOURCES to be qualified as THREAT AGENTS. This opens up the possibility for passive structure elements to play the role of THREAT OBJECTS in threat events. *Limitation L3* can be addressed simply by representing CAPABILITIES of THREAT AGENTS explicitly.

To address *Limitation L4*, we would need to add a HAZARDOUS SITUATION element to the RSO. However, since ArchiMate does not provide a native construct for modeling situations in general, we propose to model assessments of hazardous situations associated to threat events. This way, one can represent, for instance, that employees working overtime increase the probability of safety incidents.

To address *Limitation L5*, we propose to distinguish the two roles played by bearers of vulnerabilities, namely ASSET AT RISK and THREAT ENABLER. Both of these elements are associated to vulnerabilities, as their bearers, and to threat and loss events, as their participants. We propose to explicitly stereotype ASSETS AT RISK. Any other ArchiMate STRUCTURE ELEMENTS involved in threat and loss events and not considered ASSET AT RISK nor THREAT AGENTS represents THREAT ENABLERS. These changes are illustrated in Figure 7. A "Power supply failure" is a THREAT EVENT that is the manifestation of a vulnerability from a "Power supply assembly", which plays the role of a THREAT ENABLER. Additionally, this threat leads to a "Machine failure", a LOSS EVENT that damages a "Machine", which is then playing the role of an ASSET AT RISK. To illustrate all the roles played by assets (or other objects) in the risk experiences, we represented a root cause event that caused the power supply failure, namely the power fluctuation. In this event, the power grid is causing the threat, and thus, playing the role of a THREAT AGENT.

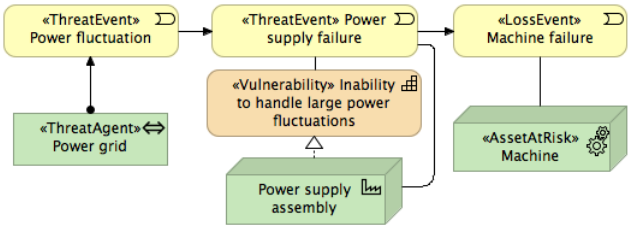

Figure 7. Modeling the different roles played by assets and other objects.

In order to address *Limitation L6*, we propose the representation of a negative INFLUENCES association between a LOSS EVENT and a GOAL, which captures why an event is considered a loss. To address *L7*, we propose the representation of an association between a LOSS EVENT and an ASSET AT RISK, in order to represent that some events are considered losses because they harm or damage an asset. We illustrate the impact of these changes in Figure 8, which redesigns part of the examples discussed in Section 2.

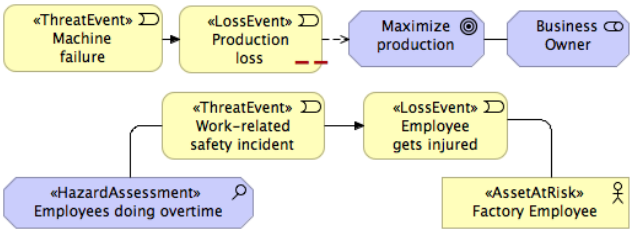

Figure 8. Modeling LOSS EVENTS with their core properties.

On the top part of the figure, we separated the event of a "Machine failure" from the actual event of "Production loss". Note, however, that the loss event is properly characterized by its negative impact on the goal of "Maximizing production". Additionally, note that we also represented the stakeholder who wants to maximize production: the Business Owner. In the context of this example, he is playing the role of the RISK SUBJECT, i.e., that to whom the event constitutes a loss. On the bottom part of the example, we represent a loss named "Employee gets injured", which is characterized by a damage to an asset, the "Factory

employee". For the sake of conciseness of the figure, we omitted the goal compromised by an employee getting injured, which could belong to the employee himself, a business owner or a worker's union.

Finally, we address *Limitation L8* by splitting the original RISK element into three. The first captures the risk experience. We map this concept as a type of GROUPING, stereotyped as a RISK EXPERIENCE, which aggregates the elements and the relations in the experience. The second represents risk from a quantitative perspective, commonly described as $probability \times impact$. We map this concept as a DRIVER stereotyped as RISK, as drivers represent "conditions that motivate an organization to define its goals and implement the changes necessary to achieve them" [25]. Since a risk quantification is about some event, we propose to represent RISK in association with a RISK EXPERIENCE. The third element is a RISK ASSESSMENT, which naturally maps as an ASSESSMENT in ArchiMate, as this concept represents "the result of an analysis of the state of affairs of the enterprise with respect to some driver" [25]. In this case, the drivers are risk drivers. Additionally, we propose to represent the associated RISK ASSESSORS, to capture which stakeholders analyzed an identified risk. The application of this last proposal is depicted in Figure 9. In the example, we represent a RISK EXPERIENCE named "Production loss due to machine failure", defined by its threat and loss events. Associated to this experience, there is RISK simply labeled "Production loss", which reflects the likelihood that all the parts of the experience occur and cause each other, as well as on the quantitative impact of the potential losses. Lastly, the RISK ASSESSMENT "Risk of production loss is unacceptable" concerns the production loss RISK.

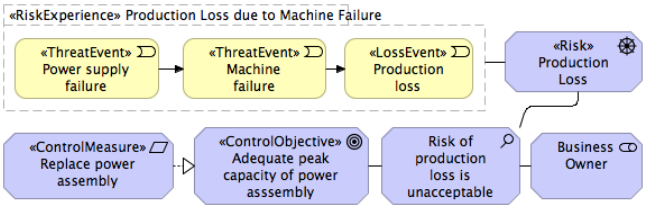

Figure 9. Modeling the three perspectives of risk.

The resulting representation scheme which aggregates all of the discussed modifications is shown in Figure 10. The elements we added or modified are represented with bold labels and thicker lines. Note that the resulting scheme clearly separates (but links) the motivation elements employed (to the right-hand side), and the risk experience elements (to the left-hand side). In case the risk experience grouping is omitted (due to abstraction), a derived negative influence relation between the risk driver and the affected goal enables the motivation elements to be used on their own. We consider this a benefit of this scheme, as it enables risk to be integrated into an overall motivational analysis, even if specific details of events are omitted. The mapping between the ontological risk-related concepts and their representation in ArchiMate are listed in Table 3.

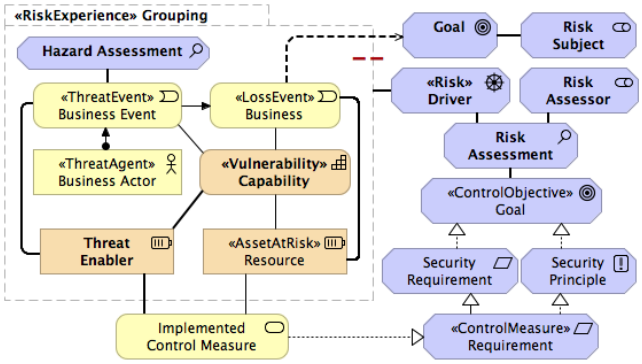

Figure 10. Proposal for evolving the Risk and Security Overlay.

TABLE 3. REPRESENTATION OF RISK CONCEPTS IN ARCHIMATE.

Ont. Concept	Representation in ArchiMate
VULNERABILITY	Capability stereotyped with «Vulnerability»
THREAT OBJECT	Structure Element stereotyped with «ThreatAgent»
THREAT EVENT	Event stereotyped with «ThreatEvent»
HAZARD ASSMT.	Assessment stereotyped with «HazardAssessment»
LOSS EVENT	Event stereotyped with «LossEvent»
INTENTION	Goal
RISK SUBJECT	Stakeholder associated with a Goal that is negatively impacted by a «LossEvent»
OBJECT AT RISK	Structure Element stereotyped with «AssetAtRisk»
THREAT ENABLER	Structure Element associated with a «ThreatEvent» or a «LossEvent»
RISK EXP.	Grouping stereotyped with «RiskExperience»
RISK	Driver stereotyped with «Risk»
RISK ASSMT.	Assessment associated with a «Risk»
RISK ASSESSOR	Stakeholder associated with a Risk Assessment

6. Related Work

Recently, Mayer and colleagues proposed two applications of the Information System Security Risk Management (ISSRM) domain model: (i) integrated with plain ArchiMate to model and analyze risks related to information systems security [15], and (ii) to evaluate the expressiveness of the RSO w.r.t to the risk domain [16]. The ISSRM domain model, however, suffers from some similar deficiencies as the RSO, as it does not untangle the various dimensions of risk, focusing on the risk experience perspective.

Besides the efforts to model risk in an Enterprise Architecture context, a number of risk modeling frameworks have been proposed in other domains. One of them is **CORAS** [14], a visual modeling language designed to be a "common tongue" among those involved in risk management activities, from risk analysts to stakeholders. Its distinguishing feature is a comprehensive series of methodological guidelines on how to systematically identify, analyze and treat risks. Still, it suffers from ontological deficiencies similar to those we discussed in Section 4, such as an ambiguity regarding the risk construct. Moreover, it has not been properly integrated with Enterprise Architecture approaches, so to leverage ex-

isting architectural model of organizations.

Another modeling framework is **RiskML** [22], an i*-based approach designed specifically for assessing risks related to the adoption of open source components in software projects. In comparison with the other approaches we discussed so far, RiskML is extremely concise. It does not distinguish, for instance, threat events from loss events, relying mostly on relations to represent these concepts. It is, however, the only one that explicitly represents the negative impact on a stakeholder's objectives.

7. Final Remarks

In this paper, we presented an ontological analysis of the risk modeling fragment of ArchiMate's Risk and Security Overlay (RSO). This analysis, which was grounded on the well-founded Common Ontology of Value and Risk [19], allowed us to clarify the real-world semantics underlying the risk-related constructs of the overlay, as well as to unveil several ontological deficiencies in it. We then addressed these deficiencies by redesigning the risk modeling fragment of the RSO, making it more precise and expressive.

The redesigned risk modeling fragment proposes a number of solutions for the representation of notions that were not present in the original RSO. These include threat capabilities, vulnerabilities of threat enablers and assets at risk (as opposed to assessments about vulnerabilities), threat objects beyond active structure elements and hazardous situations. Risk experiences (and more specifically) losses are explicitly characterized as such by their relations to the goals of an affected risk subject. Finally, the redesigned fragment distinguishes between the three perspectives on risk: (i) the risk experience grouping captures threat and loss events along with their causality relations as well as the capabilities and vulnerabilities that are manifested in the risk experience; (ii) the risk driver captures the qualitative aspect of risks, opening up the possibility for quantification, and introducing risk as a concern that motivates mitigation efforts; (iii) risk assessment is separated from risk driver, enabling different evaluations of risk to emerge and coexist. The latter can be attributed to different stakeholders which perceive risk differently, emphasizing risk's subjective nature.

Since our analysis focused on the risk elements of the RSO, a natural direction of future work is conducting a similar analysis of the security elements (e.g. control measure, security principle). Moreover, since the reference ontology we used in this paper unifies the phenomena of risk and value, it could also be used to revisit *value modeling* in ArchiMate, a domain that is significantly less developed in the current version of the language. Lastly, we would like to further develop the risk ontology, especially regarding the representation of types of expected events and how these can impact the conceptualization of risk.

Acknowledgment

This work is partly supported by CNPq (407235/2017-5 and 312123/2017-5) and CAPES (23038.028816/2016-41).

References

[1] Y. Asnar, P. Giorgini, and J. Mylopoulos, "Goal-driven risk assessment in requirements engineering," *Requirements Engineering*, vol. 16, no. 2, pp. 101–116, 2011.

[2] T. Aven, O. Renn, and E. A. Rosa, "On the ontological status of the concept of risk," *Safety Science*, vol. 49, no. 8, pp. 1074–1079, 2011.

[3] C. L. B. Azevedo, J. P. A. Almeida, M. van Sinderen, and L. F. Pires, "Towards Capturing Strategic Planning in EA," in *19th Int. Enterprise Distributed Object Computing Conf.*, 2015, pp. 159–168.

[4] C. L. B. Azevedo, M. E. Iacob, J. P. A. Almeida, M. van Sinderen, L. F. Pires, and G. Guizzardi, "Modeling resources and capabilities in enterprise architecture: A well-founded ontology-based proposal for archimate," *Information systems*, vol. 54, pp. 235–262, 2015.

[5] I. Band, W. Engelsman, C. Feltus, S. G. Paredes, J. Hietala, H. Jonkers, P. d. Koning, and S. Massart, "Modeling enterprise risk management and security with the archimate language – W172," The Open Group, 2017.

[6] Å. Boholm and H. Corvellec, "A relational theory of risk," *Journal of Risk Research*, vol. 14, no. 2, pp. 175–190, 2011.

[7] Committee of Sponsoring Organizations of the Treadway Commission, "Enterprise Risk Management - Integrated Framework," 2004.

[8] C. J. Fillmore and B. T. Atkins, "Toward a frame-based lexicon: The semantics of RISK and its neighbors," *Frames, fields, and contrasts: New essays in semantic and lexical organization*, pp. 75–102, 1992.

[9] G. Guizzardi, *Ontological foundations for structural conceptual models*. University of Twente, 2005.

[10] G. Guizzardi, G. Wagner, R. de Almeida Falbo, R. S. Guizzardi, and J. P. A. Almeida, "Towards ontological foundations for the conceptual modeling of events," in *Int. Conf. on Conceptual Modeling (ER)*. Springer, 2013, pp. 327–341.

[11] Institute of Risk Management, "A Risk Management Standard," 2002.

[12] ISO, "Risk Management - Vocabulary, ISO Guide 73:2009," 2009.

[13] G. Kjellmer, "On the awkward polysemy of the verb 'risk'," *Nordic Journal of English Studies*, vol. 6, no. 1, 2007.

[14] M. S. Lund, B. Solhaug, and K. Stølen, *Model-driven risk analysis: the CORAS approach*. Springer Science & Business Media, 2010.

[15] N. Mayer, J. Aubert, E. Grandry, C. Feltus, E. Goettelmann, and R. Wieringa, "An integrated conceptual model for information system security risk management supported by enterprise architecture management," *Software & Systems Modeling*, pp. 1–28, 2018.

[16] N. Mayer and C. Feltus, "Evaluation of the risk and security overlay of archimate to model information system security risks," in *9th Int. Workshop on Vocabularies, Ontologies and Rules for the Enterprise (VORTE)*. IEEE, 2017, pp. 106–116.

[17] O. Renn, "Three decades of risk research: accomplishments and new challenges," *Journal of risk research*, vol. 1, no. 1, pp. 49–71, 1998.

[18] M. Rosemann, P. Green, and M. Indulska, "A reference methodology for conducting ontological analyses," in *23rd Int. Conf. on Conceptual Modeling (ER)*. Springer, 2004, pp. 110–121.

[19] T. P. Sales, F. Baião, G. Guizzardi, N. Guarino, and J. Mylopoulos, "The common ontology of value and risk," in *37th Int. Conf. on Conceptual Modeling (ER)*, 2018.

[20] T. P. Sales, N. Guarino, G. Guizzardi, and J. Mylopoulos, "An ontological analysis of value propositions," in *IEEE Int. Enterprise Distributed Object Computing Conf. (EDOC)*, 2017, pp. 184–193.

[21] N. A. Sherwood, A. Clark, and D. Lynas, *Enterprise security architecture: a business-driven approach*. CRC Press, 2005.

[22] A. Siena, M. Morandini, and A. Susi, "Modelling risks in open source software component selection," in *33rd Int. Conf. on Conceptual Modeling (ER)*. Springer, 2014, pp. 335–348.

[23] The Open Group, "Risk Taxonomy (O-RT). Standard C13K," 2013.

[24] ——, "Integrating Risk and Security within a TOGAF Enterprise Architecture - G152," 2016.

[25] ——, "ArchiMate 3.0.1 Specification. Standard C179," 2017.