# Toward an ontology-based modeling for risk management

Ítalo Oliveira[1,*], Stefano M. Nicoletti[1], Mattia Fumagalli[2], Gal Engelberg[3,4] and Giancarlo Guizzardi[1]

[1]University of Twente, Drienerlolaan 5, 7522 NB, Enschede, The Netherlands
[2]Free University of Bozen-Bolzano - Faculty of Engineering, via Bruno Buozzi 1, 39100, Bozen-Bolzano, Italy
[3]Accenture, The Center of Advanced AI, EMEA
[4]University of Haifa, Abba Khoushy Ave 199, Haifa, Israel

**Abstract**

According to ISO 31000, the risk management process comprises communication, risk assessment, risk treatment, monitoring, and reporting. Numerous techniques address these aspects, particularly risk assessment and treatment, such as attack trees, fault trees, risk matrix, etc. These approaches implicitly or explicitly require a conceptualization of the risk management domain, that is, a reference domain ontology as a background theory. However, because these techniques are not grounded in ontological analyses and well-founded reference ontologies, they suffer from several limitations and semantic confusion, such as ambiguity, little to no modeling guidance, and lack of semantic integration. Existing well-founded reference ontologies of value, risk, security, and related topics, can support a full-fledge ontologically sound risk management framework capable of solving those semantic issues. Nevertheless, such a comprehensive approach to risk management is yet to be seen. To cover this gap, we present a research proposal integrating these ontologies and associated services into a domain-specific modeling language for risk management. First, we establish a risk management ontology network, including value, risk, incident, security, monitoring, trust, and resilience concepts. We will employ them to ground ontological analyses of those important risk management techniques to identify their shortcomings. This analysis will support redesigns of these techniques to overcome the limitations. We will design a domain-specific modeling language interpreted by the ontology network and served by the redesigned versions of those techniques. By doing so, we expect to address semantic interoperability problems among risk management approaches and data sources.

**Keywords**

Ontology-driven conceptual modeling, Risk Management, Semantic Interoperability, Common Ontology of Value and Risk, Reference Ontology for Security Engineering

## 1. Introduction

According to ISO 31000 [1], the risk management process comprises communication and consultation, risk assessment (risk identification, analysis, and evaluation), risk treatment, monitoring and review, and recording and reporting, as shown in Figure 1. Numerous techniques address these aspects, particularly risk assessment and treatment, as listed in the ISO 31010 [2], such as Attack Trees, Fault Trees, Risk Matrix, Failure Mode and Effects Analysis (FMEA), Bow-tie analysis, Bayesian Networks, and many others. These techniques are employed for two important tasks:

1. *Conceptual modeling of risk management scenarios* for human understanding and communication. For example, a qualitative assessment of how attackers can perform attack steps to achieve their goals.

*Proceedings of the 18th International Workshop on Value Modelling and Business Ontologies (VMBO 2025), March 3–4, 2025, University of Twente, Enschede, The Netherlands*
*Corresponding author.
i.j.dasilvaoliveira@utwente.nl (Í. Oliveira); s.m.nicoletti@utwente.nl (S. M. Nicoletti); mattia.fumagalli@unibz.it (M. Fumagalli); gal.engelberg@accenture.com (G. Engelberg); g.guizzardi@utwente.nl (G. Guizzardi)
https://italojsoliveira.github.io (Í. Oliveira); https://stefanonicoletti.com (S. M. Nicoletti); https://www.mattspace.net (M. Fumagalli); https://linkedin.com/in/gal-engelberg (G. Engelberg); https://www.giancarloguizzardi.com (G. Guizzardi)
0000-0002-2384-3081 (Í. Oliveira); 0000-0001-5522-4798 (S. M. Nicoletti); 0000-0003-3385-4769 (M. Fumagalli); 0000-0001-9021-9740 (G. Engelberg); 0000-0002-3452-553X (G. Guizzardi)

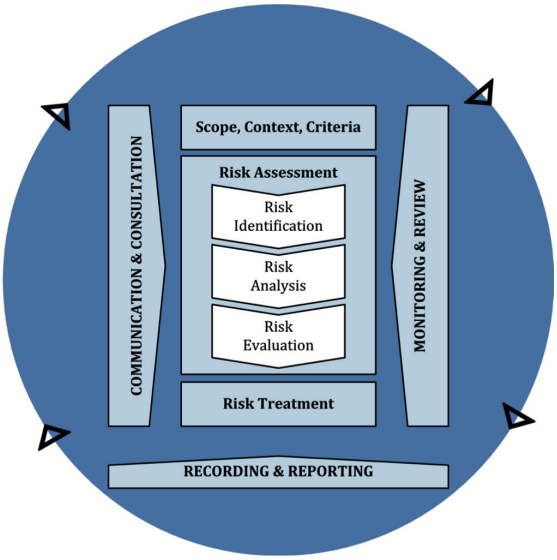


**Figure 1:** Risk management process according to ISO 31000 [1].

2. *The computation of quantitative metrics*, such as the likelihood and impact of risk events, based on that conceptual insight.

The modeling task implicitly or explicitly assumes a conceptualization of the risk management domain. Metrics calculation is only meaningful through the lens of the conceptual model that says how they should be interpreted. This means those techniques require a reference domain ontology as a background theory to assign meaning to their symbols. For example, Bow-tie diagrams assume a theory of causation relating threat events on the diagram's left-hand side to loss events on the right-hand side [3]. The risk matrix supposes the notions of risk likelihood, impact severity, and event types [4]. FMEA, widely used in reliability and safety engineering, includes the concepts of failure, failure effect, detection, mitigation, and others [5].

However, none of these techniques are ontologically grounded in the sense of relying on explicit ontological analyses of the domain. This means they combine an informal domain conceptualization with a degree of mathematical formality to calculate metrics. Consequently, they suffer from several limitations and semantic confusion: (a) *Ambiguous syntactical terms* that can be interpreted in various ways, such as the nodes of attack trees that can be understood as goals, situations, events, event types, or even propositions [6]. (b) *Little to no modeling guidance.* For example, nothing in the attack tree language tells users how to construct an attack tree and find the basic attack steps. And (c) *lack of semantic integration* as each technique is designed to be a stand-alone framework. In real-world cases, this is a problem because we need to apply different methods to obtain different perspectives while relying on the same data or data from various sources. To do that, we need to answer questions such as "How should this data point be interpreted in an attack tree?" and "How should these attack tree elements be interpreted in terms of a Bayesian network?". This is exactly the type of problem addressed by ontological analyses because having explicit ontological commitments helps us connect different worldviews embedded in the datasets and techniques [7].

In recent years, based on the Unified Foundational Ontology [8], researchers have built well-founded reference ontologies of value and risk [9], security [10], trust [11], resilience [12], and related topics. They can support a full-fledge ontologically sound risk management framework capable of solving those semantic issues. Nevertheless, such a comprehensive approach to risk management is yet to be seen. To cover this gap, we present a research proposal integrating these ontologies and associated services into a domain-specific modeling language for risk management. First, we establish a *risk management ontology network*, including value, risk, incident, security, monitoring, trust, and resilience concepts. We will employ them to ground *ontological analyses of those risk management techniques* to identify their

shortcomings. This analysis will support the redesign and integration of these techniques to overcome the limitations. We will design a *domain-specific modeling language* interpreted by the ontology network and served by those techniques. By doing so, we expect to address semantic interoperability problems among risk management approaches and data sources.

In what follows, Section 2 discusses some related works, namely, domain-specific modeling languages for risk management. Section 3 presents an overview of our research proposal. Section 4 discusses the theoretical and practical implications of this research project. Section 5 concludes with final considerations.

## 2. Related work

Diagrammatic representations of scenarios or systems are crucial for risk management since they help with problem-solving, documentation, communication, complexity management, and computation of relevant tasks and metrics (simulation, risk analysis, risk propagation, security effectiveness assessment, etc.). This is why there are many domain-specific language tools for this purpose, commercial or free open-source products, such as securiCAD[1], ThreatModeler[2], IriusRisk[3], OWASP Threat Dragon[4], and Microsoft Threat Modeling Tool[5]. We will discuss three major ontology research-backed modeling approaches: (a) the CORAS language [13]; (b) the ArchiMate's Risk and Security Overlay [14]; and (c) an approach implemented by the open-source Spyderisk project [15].

CORAS[6] is an approach to risk analysis based on ISO 31000 [13]. It consists of a modeling language specification, a tool implementing this specification, and a method for risk and security modeling. The metamodel of the language comprises a domain ontology defining the terminology. The CORAS concrete syntax was designed to facilitate the description of risk models and communication between people of heterogeneous backgrounds.

The ArchiMate's Risk and Security Overlay [14], developed by The Open Group ArchiMate Forum and The Open Group Security Forum, intends to introduce risk and security modeling concepts into ArchiMate language through the customization mechanisms (specialization and stereotypes). This ArchiMate extension has been extensively investigated by ontological analyses of its risk and security layers [16, 17]. Based on the Common Ontology of Value and Risk (COVER) [9] and the Reference Ontology for Security Engineering (ROSE) [10], researchers have found numerous semantic deficiencies, such as ambiguities and underspecification, and proposed a well-founded language redesign [16, 17].

Phillips *et al* [15] describe a modeling approach for automated risk assessment of cyber-physical systems following ISO 27005 ("Information security risk management"). They present an ontology represented through the UML class diagram to define the necessary terminology. The Spyderisk[7] ontology is designed to support a cause-and-effect approach to risk modeling. Spyderisk can compute the threats to a system, ordered by risk level, where the risk level combines the business impact of a consequence and the computed likelihood.

Although these three approaches rely on defining a risk management ontology to assign meaning to their respective domain-specific modeling language, they do not leverage an ontological approach. They do not employ a foundational ontology and well-founded reference domain ontologies to ground their definitions. The problems with this absence have been shown by the studies of ArchiMate's Risk and Security Overlay [16, 17]. In particular, it is harder to integrate different risk management modeling approaches and data from different sources without an explicit heavyweight ontology underneath. Semantic interoperability requires ontologies as *meaning contracts* capturing the conceptualizations represented in information artifacts, backed by Ontology, as a discipline proposing formal methods

[1] https://www.bitcyber.com.sg/foreseeti-securicad
[2] https://www.threatmodeler.com
[3] https://www.iriusrisk.com
[4] https://owasp.org/www-project-threat-dragon
[5] https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling
[6] https://coras.sourceforge.net/index.html
[7] https://github.com/Spyderisk

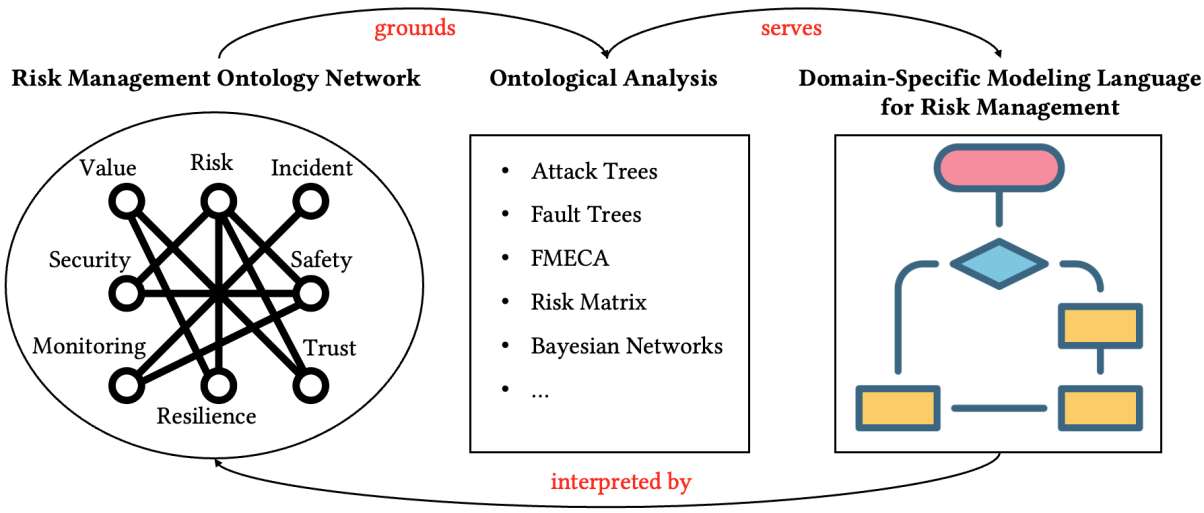


**Figure 2:** Project overview.

and theories for clarifying these conceptualizations and articulating their representations [7]. This is exactly the approach we propose.

## 3. Ontology-based modeling for risk management

Foundational and well-founded reference domain ontologies are information artifacts embodying formal ontological theories of the world. By distinguishing concepts like objects, intrinsic properties, propositions, higher-order types, events, situations, and different types of relations (formal relation, historical dependence, external dependence, generic dependence, etc.), they provide fine-grained conceptual modeling capabilities. Our modeling approach proposal for risk management is "ontology-based" in this sense, instead of merely describing important domain concepts from scratch. We will leverage UFO-based ontologies connected to the risk management domain to build an ontology network that will support ontological analyses and the redesign of several risk management approaches. We will design a domain-specific modeling language whose metamodel will correspond to concepts taken from the ontology network. Moreover, as we carry out the ontological analyses and redesign, we can incrementally provide services around the language ecosystem. The project overview is described in Figure 2. Let us consider each major block of this project.

1. **Risk Management Ontology Network**. The UFO-based Common Ontology of Value and Risk (COVER) [9], the Reference Ontology for Security Engineering (ROSE) [10], the Reference Ontology of Trust (ROT) [11], the Resilience Core Ontology (ResiliOnt) [12] will definitely be part of our ontology network. Still, if needed, we intend to refine them or build novel ontologies, for example for monitoring and detection concepts. They will be the cornerstones of the ontological analysis and modeling language. These ontologies are to be represented in OntoUML modeling language and OWL complying with gUFO [18] (UFO OWL implementation). The goal of establishing this ontology network is to have a complete explicit characterization of the risk management domain. It is a network because it is composed of interconnected individual ontologies about intertwined domains (value, risk, security, etc.).
2. An **Ontological Analysis** denotes a well-known methodology summarized in Figure 3. An ontological analysis is "the evaluation of a modeling grammar, from the viewpoint of a predefined and well-established ontology" [19]. According to Rosemann *et al.* [19], the modeling grammars should be isomorphic to their underlying ontology, that is, the interpretation from the modeling constructs to the ontology concepts should be bijective. This is a desirable characteristic because it prevents the following problems that jeopardize the modeling capability of the language: (a)

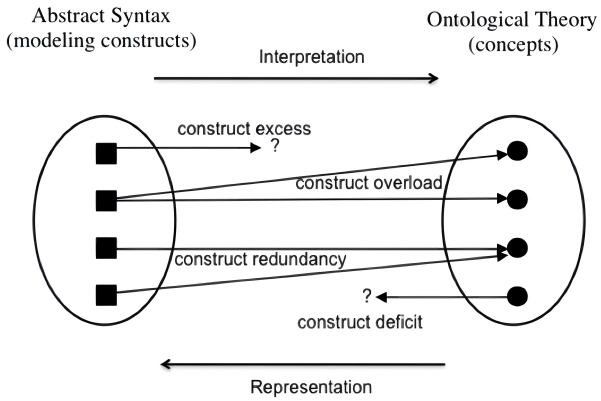


**Figure 3:** The illustration from [20] of the relation between modeling constructs in a language's syntax and ontological concepts.

*ontological incompleteness* (or *construct deficit*), which is the lack of a grammatical construct for an existing ontological concept; (b) *construct overload*, which occurs when one grammatical construct represents more than one ontological construct; (c) *construct redundancy*, which happens when more than one grammatical construct represents the same ontological construct; (d) *construct excess*, when there is a grammatical construct that does not map to any ontological construct [19]. In the context of our project, we will investigate the underlying ontology of attack trees, fault trees, FMECA, Bayesian Networks, risk matrix, and other risk management techniques, to identify their semantic limitations and propose a better version of the respective technique. This approach has been successfully employed throughout the years, such as in the ArchiMate example [16, 17]. An underexplored implication of this sort of ontological analysis is to set up an environment for interoperating those techniques. This happens because explicit ontological commitments allow us to identify corresponding notions crossing techniques and datasets. For example, if a given node in an attack tree denotes an event, we can find the same data point in different datasets or even as a node in a Bayesian network or a fault tree.

3. A **Domain-Specific Modeling Language for Risk Management** will embody the risk management ontology network. It shall allow typical threat modeling activities, representing identified risk sources, and how everything hangs together meaningfully. The resulting models shall have a precise formal specification (say, as OWL serialized in TTL). The language shall be capable of representing types and individuals to distinguish between risk scenarios (possible events) and incidents (past concrete occurrences). This feature is important because it allows the use of databases containing, for instance, cybersecurity incidents to populate the model. The language can be built incrementally and be served by capabilities (automated reasoning, simulation, risk propagation, root cause analysis, etc.) provided by the redesigned version of risk management techniques (attack trees, fault trees, etc.). For example, a model created by this language can specify threats to a given cloud-based system, how risks emerge and propagate from these threats, how risk events affect stakeholders' goals, and this representation can enable computer simulations based on Bayesian networks. We conceive that the language and its services can be integrated with established datasets and knowledge bases, such as CVE[8], CWE[9], CAPEC[10], ATT&CK[11], D3FEND[12], and others. Finally, the language shall support textual and graphical editing.

[8]https://cve.mitre.org
[9]https://cwe.mitre.org
[10]https://capec.mitre.org
[11]https://attack.mitre.org
[12]https://d3fend.mitre.org

## 4. Theoretical and practical implications

This project has major theoretical and practical implications because it involves theoretical and applied research, plus a ready-to-use tool. We summarize the projected implications, as follows:

### Theoretical implications

- Building an ontology network for risk management requires combining different ontologies. This involves a *conceptual clarification* effort toward the very risk management domain. A similar elucidative outcome will follow from constructing some of the related domain ontologies since not all the necessary ones are available (for example, monitoring and detection concepts). This semantic elucidation might have unforeseen consequences for understanding the risk management domain.
- The ontological analyses revealing semantic issues of risk management techniques, such as attack trees and fault trees, will directly impact how these techniques are interpreted today. *New formalisms* might emerge from these *novel interpretations*.

### Practical implications

- The integration of those risk management techniques has the potential to nourish the *rise of new tools*. Our proposed domain-specific language is just one of them.
- Our domain-specific language is expected to improve the modeling practice necessary for risk management tasks because of its domain adequacy. This results from employing a well-founded ontology network as the language metamodel. This *enhanced modeling capability* will leverage a *data-driven approach to compute relevant metrics*. In summary, we expect to contribute to the two important tasks presented in the Introduction.

## 5. Conclusion

We have presented a research proposal to address major semantic interoperability problems among risk management approaches and data sources. Our approach relies on heavyweight ontological foundations going from the UFO upper ontology and UFO-based reference domain ontologies to ontological analyses and a diagrammatic domain-specific modeling language for risk management. The project involves theoretical and practical outcomes and manifold contributions.

## Declaration on Generative AI

The authors have not employed any Generative AI tools.

## References


[1] ISO, ISO 31000:2018 - Risk management – Guidelines, 2018.
[2] ISO/IEC, ISO/IEC 31010:2019 - Risk management – Risk Assessment Techniques, 2019.
[3] A. de Ruijter, F. Guldenmund, The bowtie method: A review, Safety science 88 (2016) 211–218.
[4] L. Anthony (Tony) Cox Jr, What's wrong with risk matrices?, Risk Analysis: An International Journal 28 (2008) 497–512.
[5] R. J. Mikulak, R. McDermott, M. Beauregard, The basics of FMEA, CRC press, 2017.
[6] B. Schneier, Attack trees, Dr. Dobb's journal 24 (1999) 21–29.
[7] G. Guizzardi, Ontology, ontologies and the "I" of FAIR, Data Intelligence 2 (2020) 181–191.
[8] G. Guizzardi, A. Botti Benevides, C. M. Fonseca, D. Porello, J. P. A. Almeida, T. P. Sales, Ufo: Unified foundational ontology, Applied ontology 17 (2022) 1–44.

[9] T. P. Sales, F. Baião, G. Guizzardi, J. P. A. Almeida, N. Guarino, J. Mylopoulos, The common ontology of value and risk, in: Conceptual Modeling. ER 2018, volume 11157, Springer, 2018, pp. 121–135.
[10] Í. Oliveira, T. P. Sales, R. Baratella, M. Fumagalli, G. Guizzardi, An ontology of security from a risk treatment perspective, in: Conceptual Modeling. ER 2022, volume 13607, Springer, Cham, 2022, pp. 365–379. doi:10.1007/978-3-031-17995-2_26.
[11] G. Amaral, T. P. Sales, G. Guizzardi, D. Porello, Towards a reference ontology of trust, in: On the Move to Meaningful Internet Systems: OTM 2019 Conferences: Confederated International Conferences: CoopIS, ODBASE, C&TC 2019, Rhodes, Greece, October 21–25, 2019, Proceedings, Springer, 2019, pp. 3–21.
[12] P. P. F. Barcelos, R. F. Calhau, Í. Oliveira, T. Prince Sales, F. Gailly, G. Poels, G. Guizzardi, Ontological foundations of resilience, in: International Conference on Conceptual Modeling, Springer, 2024, pp. 396–416.
[13] M. Lund, et al., Model-driven risk analysis: the CORAS approach, Springer Science & Business Media, 2010.
[14] I. Band, W. Engelsman, C. Feltus, S. G. Paredes, J. Hietala, H. Jonkers, P. de Koning, S. Massart, How to Model Enterprise Risk Management and Security with the ArchiMate Language, Technical Report W172, The Open Group, 2019.
[15] S. C. Phillips, S. Taylor, M. Boniface, S. Modafferi, M. Surridge, Automated knowledge-based cybersecurity risk assessment of cyber-physical systems, IEEE Access (2024).
[16] T. P. Sales, J. P. A. Almeida, S. Santini, F. Baião, G. Guizzardi, Ontological analysis and redesign of risk modeling in ArchiMate, in: 2018 IEEE 22nd International Enterprise Distributed Object Computing Conference (EDOC), 2018, pp. 154–163. doi:10.1109/EDOC.2018.00028.
[17] Í. Oliveira, T. P. Sales, J. P. A. Almeida, R. Baratella, M. Fumagalli, G. Guizzardi, Ontology-based security modeling in archimate, Software and Systems Modeling (2024) 1–28.
[18] J. P. A. Almeida, G. Guizzardi, T. P. Sales, R. A. Falbo, gUFO: A lightweight implementation of the unified foundational ontology (UFO), 2019. URL: http://purl.org/nemo/doc/gufo.
[19] M. Rosemann, P. Green, M. Indulska, A reference methodology for conducting ontological analyses, in: Conceptual Modeling. ER 2004, volume 3288, Springer, Berlin, Heidelberg, 2004, pp. 110–121.
[20] C. L. Azevedo, M.-E. Iacob, J. P. A. Almeida, M. van Sinderen, L. F. Pires, G. Guizzardi, Modeling resources and capabilities in enterprise architecture: A well-founded ontology-based proposal for archimate, Information systems 54 (2015) 235–262.