Ontological Foundations of Resilience

Pedro Paulo F. Barcelos[1,2,3], Rodrigo F. Calhau[3,4], Ítalo Oliveira[3], Tiago Prince Sales[3], Frederik Gailly[1,2], Geert Poels[1,2], and Giancarlo Guizzardi[3]

[1] Dept. Business Inf. and Operations Management, Ghent University, Belgium
{pedro.favatobarcelos, frederik.gailly, geert.poels}@ugent.be
[2] CVAMO Core Lab, Flanders Make @UGent, Belgium
[3] Semantics, Cybersecurity and Services, University of Twente, The Netherlands
{i.j.dasilvaoliveira, t.princesales, g.guizzardi}@utwente.nl
[4] LEDS, Federal Institute of Espírito Santo, Brazil
calhau@ifes.edu.br

Abstract. Amid rising global challenges, resilience is attracting increased interest across various disciplines. However, significant ambiguities, vagueness, and variations in its definitions present notable obstacles to interdisciplinary communication and practical application. These semantic issues negatively impact not only the applications that rely on these definitions but also undermine the integrity of the conceptual models built from them, rendering them unable to ensure interoperability and clarity for their intended users. Recognizing the need for a robust and clear definition of resilience, this work addresses the complexity inherent in the concept by performing an ontological analysis using the Unified Foundational Ontology (UFO) and creating a sound core ontology model with OntoUML, UFO's related conceptual modeling language. This research unfolds the conceptualization of resilience by investigating its fundamental categories and related concepts. We explore essential aspects of resilience, examining whether it preexists disturbances or is developed in response to them. We also identify its relational dependencies, establish how it is actualized, and determine the circumstances under which it becomes perceptible. Following our analysis of the ontological nature of resilience, the paper establishes an ontologically well-founded definition of this concept. To illustrate the practical application of our theoretical findings, we present a specific case in the field of production management.

Keywords: Resilience · Ontological Analysis · Unified Foundational Ontology · OntoUML · Ontology

1 Introduction

Resilience is an important concept across numerous disciplines, including strategic management, supply chain management, sustainability, disaster management, ecology, engineering, defense, political science, psychology, and sociology [11, 45, 70]. Both scientific and nonscientific literature reflect a rising use of this term, underscoring its broad importance and multidisciplinary roots [1, 34, 36, 45, 47, 70, 71, 79]. However, definitions of resilience vary significantly across disciplines [34, 57, 68, 78], leading to complexities, contradictions, and ambiguities that pose significant challenges in both theoretical and practical domains [38, 57]. Furthermore, the polysemy of resilience leads to contradictory interpretations that undermine its utility in achieving a coherent discourse [57]. These issues hinder the development of operational definitions and generalizable metrics, complicating the application of resilience in normative settings [34, 47].

Conceptual models aiming to represent resilience and their derived knowledge artifacts, such as schemas, data structures, inherit these definitional issues, impacting their clarity and interoperability. The literature presents examples of resilience models in UML and ER, created for diverse fields including small and medium-sized enterprises [72], industrial supply chains [2], maritime systems [41], extreme weather [80], and data ecosystems [26].

The literature underscores the necessity of a clear and general definition of resilience to facilitate interdisciplinary research and enhance empirical testability and operationalization [68, 75, 78]. Despite this recognized need, disambiguating resilience is challenging due to its complex nature and the nuanced interpretations across contexts [68]. Acknowledging that completely neutral perspectives are unachievable when defining resilience, it is evident that existing definitions rely on implicit ontological assumptions. To create a robust and reusable model, researchers must rigorously identify and declare their ontological commitments using a suitable well-founded ontology representation language [28, 29].

This paper addresses the ambiguities surrounding resilience by performing an ontological analysis grounded in the Unified Foundational Ontology (UFO), which provides the necessary ontological foundations for clarifying the fundamental categories of resilience and their related concepts. We formalize this analysis in a sound ontology artifact using UFO's related conceptual modeling language, OntoUML [30] *(contribution I)*. We entitled the generated ontology 'Resilience Core Ontology', or simply **ResiliOnt**.

In our analysis, we explore fundamental aspects of resilience by questioning *(i)* whether resilience is an inherent quality of an object or an outcome observed only after an object has endured a disturbance, *(ii)* what are the necessary and *(iii)* the sufficient conditions for an object to possess resilience, and *(iv)* when resilience can be observed. Addressing these points helps to fill the gaps in the current understanding of resilience. Building upon the results of our analysis, we provide an ontologically well-founded definition of resilience *(contribution II)*.

The remainder of this paper is structured as follows. section 2 presents the foundational ontological theory upon which we build our analysis. Then, section 3 presents the contrasting views on resilience found in different paradigms. Our principal contribution is found in section 4, where we analyze resilience to clarify its semantics. In section 5, we present a case in production management to illustrate the application of the theoretical findings. The discussion in section 6 contextualizes our findings within the existing literature, and section 7 presents our conclusions by synthesizing our contributions, discussing implications, presenting limitations, and outlining future research directions.

2 Ontological Foundations

2.1 The Unified Foundational Ontology

UFO is a well-established foundational ontology that has been used successfully in numerous ontological analyzes in fields as complex as economics, software engineering, treatments, and decision-making processes [30, 37, 54, 76].

Among all the applications of UFO, its role in the design of OntoUML is the most significant. OntoUML is a conceptual modeling language with explicitly defined formal and real-world semantics that reflects the ontological micro-theories of UFO. It serves as an engineering tool for enabling the use of formal ontological theories in the construction of conceptual models and domain ontologies [30, 32]. OntoUML was also used to formalize both the Capabilities [18] and the Common Ontology of Value and Risk (COVER) [60] ontologies, which play a central role in establishing the groundwork for our research, making it the optimal choice for formalizing ResiliOnt.

UFO is organized into three main fragments: UFO-A (ontology of endurants), UFO-B (ontology of perdurants, partially represented in Figure 1), and UFO-C (ontology of social and intentional entities). For our analysis, UFO-A and UFO-B are particularly significant. Extending UFO-A, UFO-B focuses on entities that occur over time, formalizing how Substantials, Situations, and Events relate to each other [10, 31].

Endurants are entities that persist through time while potentially undergoing changes in their properties. Independent Endurants are called Substantials, while those existentially dependent are named Moments. Disposition, a key concept in this work, belongs to the latter category.

Dispositions are properties that a Substantial ("object-like" Endurants) possess and have the potential to produce distinct effects within their context. They come into effect through Situations that provide the necessary conditions for latent qualities to manifest as Events. A classic example of Disposition is a

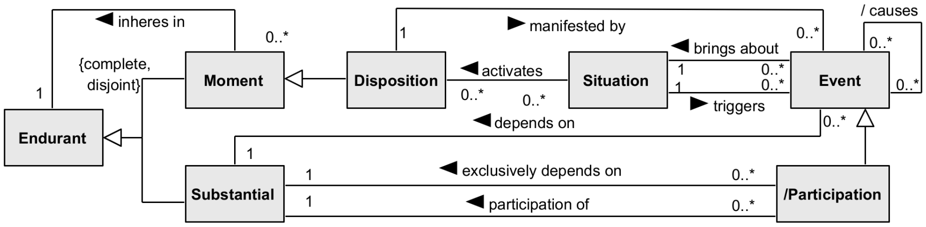

Fig. 1. Representation of UFO-B fragment as a class diagram illustrating the relationships among Substantials, Events, and Dispositions

magnet's ability (object) to attract (event) iron when they are close enough (situation).

Events are the realized outcomes of Dispositions. They represent changes or occurrences that may alter the state of affairs and are inherently linked to Substantials, arising from and acting upon these entities. Events and Situations relate in two distinct forms: an Event can bring about a Situation, making it a fact in the world, or Situations can trigger Events, causing them to occur because the Situations exist [31].

2.2 The Capability Ontology

In a series of recent studies, Calhau et al. [15–18] have expanded on Dispositions in UFO, exploring the relationships among them, with a particular emphasis on Capabilities. Defined as changeable [23] and composable [64] entities, Capabilities represent the ability to achieve specific effects or declared objectives [62]. This "beneficial" aspect is reflected in its definitions across different areas. For instance, it is defined as the "ability to do something useful" in enterprise architecture and systems engineering, and as the "ability to achieve a desired effect" in information systems [48, 63]. In UFO, Dispositions can be characterized as 'Categories' (a rigid mixin, relationally independent type) due to their "neutral" nature regarding their impacts. Capabilities, in contrast, are understood as 'RoleMixins' (an anti-rigid, relationally dependent mixin type), reflecting their conditional and context-dependent nature.

There are numerous ways in which dispositions can be expressed [15], with Enabling and Disabling Dispositions being particularly important in this work. *Enabling Dispositions* lay the groundwork for the activation of other dispositions, such as the foundational IT infrastructure that enables cloud-based services. *Disabling Dispositions*, on the other hand, negate or suppress the function of other dispositions, such as in cybersecurity measures that disable unauthorized access. While Enabled Dispositions can manifest themselves in Events, Disabled Dispositions are unable to manifest.

2.3 COVER: the Common Ontology of Value and Risk

We now turn our attention to COVER, originally presented in [60] and later extended and reinterpreted in [51]. This ontology provides a well-founded conceptualization of value and risk, disentangling three perspectives: experiential, relational, and quantitative. These perspectives are crucial for understanding the nature of risk and its relationship with value. COVER introduces several key concepts that have implications for our analysis of resilience, such as the ones presented in Figure 2.

As seen in Figure 2, the Object at Risk is central to the experience of risk. This specific type of Substantial is a Value Object, the bearer of value—and is consequently susceptible to losing it. In the context of this paper, value is considered binary, i.e., it is either fully preserved or completely lost. An instance of an Object at Risk is a worker in a factory setting, where the possibility of an

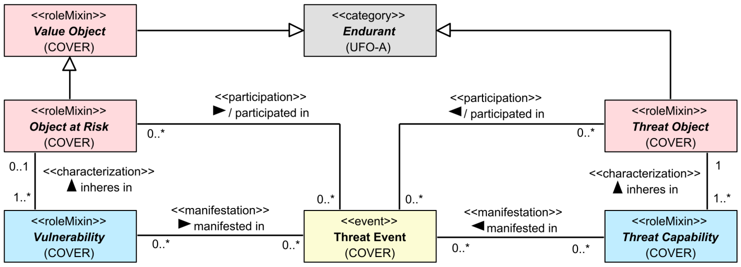

Fig. 2. OntoUML diagram adapted from COVER illustrating the relationships among Objects at Risk, their Vulnerabilities, and their potential participation in Threat Events

accident could result in harm or injury. The occurrence of a threatening situation can activate the vulnerabilities of the Object at Risk, potentially leading to a Threat Event. This event has the potential to cause loss, whether intentional, such as a cyberattack, or accidental, like a spill that damages essential electronics. COVER introduced Threat Object as an important concept, embodying any entity or element that can cause a Threat Event. Examples of Threat Objects include environmental hazards (e.g., toxic chemicals, bacteria, or viruses), cyberattackers, or an aggressive agent (like a bullying peer or an abusive partner).

Objects at Risk are entities characterized by their inherent Vulnerabilities. These Vulnerabilities are Dispositions that predispose an object to potential detrimental events (i.e., they may participate in Threat Events). For example, the flammability of a structure renders a house vulnerable to fire, which, if realized, could result in substantial loss. COVER defines Vulnerabilities as 'RoleMixins', indicating their relation-dependent nature. Finally, in Figure 2, note that the labels used by associations related to events are in the past tense. By incorporating events, the model's semantics transition to a historical perspective, affecting the events and their associated objects [4].

3 Resilience

Resilience, understood as a social construct, is shaped by the beliefs and worldviews of individuals or groups, leading to varied interpretations and applications in different fields [79]. Reghezza-Zitt et al. [57] provide a comprehensive overview of how resilience is defined across different disciplines. In material physics, resilience refers to the capacity of a material to absorb energy and resist breakage, emphasizing its ability to return to its original state after deformation. In psychology, resilience is understood as an individual's ability to adapt and recover from trauma, focusing on the processes and resources that enable overcoming stressors and maintaining well-being. It involves the ability to rebuild after traumatic experiences, leading to new development and strength. In ecology, resilience describes ecosystems' capacity to absorb disturbances and reorganize while maintaining critical functions, emphasizing persistence and adaptation over returning to a pre-disturbance state.

The authors also propose the classification of resilience into two major paradigms that offer distinct perspectives. These paradigms reflect broader differences in understanding resilience as either a static property or a dynamic process. The first is the *technocentric paradigm*, often referred to as *engineering resilience*. It aligns with the traditional view of stability and emphasizes the ability of systems to return to an equilibrium state after a disturbance. Engineering resilience tends to see resilience as a measurable state, often tied to technical and organizational capabilities to withstand and recover from disturbances. This paradigm focuses on resistance to shocks and the speed of recovery, suggesting that a resilient system is one that can bounce back to its pre-disturbance state. The second paradigm, known as *socio-ecological*, views resilience as the capacity of a system to persist through continuous change and adapt to new conditions, highlighting the importance of maintaining essential functions despite transformations. This approach considers resilience as an ongoing capacity to adapt and evolve in response to changing conditions, rather than simply returning to a previous state [57].

4 Ontological Analysis of Resilience

This section undertakes an ontological analysis to provide precise semantics to resilience. By addressing specific guiding questions, we incrementally refine our understanding of what resilience encompasses. Each step of the analysis is crafted to detail the mechanisms and intrinsic properties that define resilience.

Existing studies frequently concentrate on system-level resilience, whereas our approach additionally considers the resilience of individual components and elements not integrated into systems. In the context of this work, we use the term 'Object' to refer to COVER's 'Value Object' concept. Thus, for our purposes, 'Object' encompasses any entity to which resilience can be applied. This choice of terminology is grounded in the system ontology presented in [18] and aligns with the nomenclature used in the COVER ontology.

4.1 Resilience as a Risk-Dependent Capability

After analyzing fundamental characteristics of resilience by examining definitions from diverse disciplines, Daniel [21] argued that Resilience is a Disposition. Using the Basic Formal Ontology (BFO) [6], the study concluded that resilience, like other dispositions in BFO, inherently exists as a potentiality within a system.

Building on the premise that resilience enables an Object to preserve its value—defined in terms of an agent's goals—amidst disturbances, we further classify Resilience as a Capability, a specific type of Disposition. This classification is supported by extensive literature that conceptualizes resilience as a capability. Studies such as [12, 20, 22, 24, 52, 59] corroborate this classification, though without explicit ontological commitment. Additionally, Kochan and Nowicki's supply chain literature review [39] identified resilience as an 'ability' and noted that the analyzed works used this term and 'capability' interchangeably.

Classifying Resilience as a Capability allows us to answer an important question in the resilience literature: “*Is Resilience an inherent quality of an Object, present before impact and revealed at the moment of impact, or is it an outcome observed only after an Object has endured a disturbance?*” Since Capabilities are intrinsic properties of Objects rather than contingent upon Events, we assert that the presence of Resilience in an Object is determined by a specific configuration of Dispositions, and therefore does not depend on experiencing a disturbance (an Event in UFO). Resilience, being a Capability, is a property only manifested in particular situations and that can also fail to be manifested. In other words, Resilience is only observable in certain scenarios and may not always be observable.

Acknowledging Resilience as an intrinsic quality that Objects may have leads us to the subsequent inquiry: *What are the necessary conditions for Objects to possess Resilience?* According to the COVER ontology, there is a clear dependency chain: no goal means no vulnerability, and no vulnerability means no risk. Extending this chain, we argue that there can be no resilience without risk. Since Resilience is proposed as an object’s capability to avoid its loss of value in the face of an adversity, it logically follows that only Objects at Risk—those subjected to potential Threat Events or Loss Events—would be able to possess Resilience. COVER describes Risk as an assessment of potential negative outcomes, fundamentally associated with uncertain future events that could impact valued goals or assets. Objects at Risk have an ascribed value that is deemed worth preserving and that could be under threat from adverse events. Therefore, Resilience is primarily risk-dependent and, ultimately, goal-dependent. However, not all Objects at Risk possess Resilience; for instance, sugar is highly vulnerable to water and dissolves fast upon contact, with irreversible effects.

The relationship between Object at Risk’s Capabilities (capabilities that inheres in Object at Risks, such as a boxer’s capability to fight) and Vulnerabilities, as depicted in Figure 3, is characterized by the state of the latter. Active vulnerabilities expose their related capabilities, making them susceptible to threats. I.e., an active vulnerability is a point of weakness within the Object at Risk that could potentially be exploited. For example, using an outdated cryptographic algorithm (Active Vulnerability) may harm the system’s confidentiality (Vul-

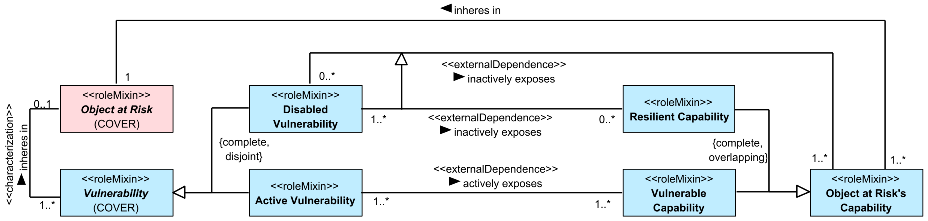

Fig. 3. OntoUML diagram representing the relations between Object at Risk’s Vulnerabilities and Capabilities

nerable Capability), making it susceptible to unauthorized access. Conversely, disabled vulnerabilities, as they are unable to manifest themselves, maintain a neutral stance, neither preserving nor exposing their related capabilities. Disabled vulnerabilities are inactive and cannot be exploited by Threat Capabilities, hence, they are not a source of risk. For instance, updating the cryptographic algorithm to a more secure version (Disabled Vulnerability) preserves the system's confidentiality. In summary, Object at Risk's capabilities can enable or disable related vulnerabilities, altering the Object at Risk's susceptibility to threats.

There is an important distinction between a disabled vulnerability and one that is absent. A disabled vulnerability refers to a condition where the vulnerability still exists, but its potential negative effects are neutralized through specific capabilities. For example, consider the human body's capability to regulate its appendix: a healthy appendix indicates the presence of a capability to counteract potential issues, effectively disabling the vulnerability to appendicitis. In this case, the vulnerability exists but cannot be manifested, and hence, does not lead to losses. The risk only manifests if this disabling capability ceases, potentially leading to appendicitis. Conversely, an 'absent' vulnerability refers to a context where the vulnerability does not exist or has been completely removed, such as in the case of an individual who has undergone an appendectomy and is no longer vulnerable to appendicitis. In this scenario, the vulnerability is not simply disabled but entirely eliminated. Thus, while a disabled vulnerability may become active again if the disabling mechanism ceases to function, a removed vulnerability permanently eliminates the risk.

4.2 Achieving Resilience

Having examined the ontological nature of resilience and its dependency on risk, we now address the question: "*What are the sufficient conditions for Objects to possess Resilience?*"

Considering the relationships between capabilities and vulnerabilities outlined previously, it becomes evident that Resilience does not exist in isolation; it is a capability that exists simultaneously with a given configuration of the capabilities and vulnerabilities of its bearer. Resilience represents the relational dynamics within the Object at Risk where one of its capabilities is affected by one of its vulnerabilities, and this vulnerability is disabled by another capability.

Figure 4 illustrates Resilience within an Object at Risk. It shows that a Disabling Capability becomes a Resilience-Producer Capability when it disables a Vulnerability. This prevents the Disabled Vulnerability from manifesting in a Threat Event, eliminating the opportunity for Threat Capabilities to exploit it, and establishing a Resilient Capability in the Object at Risk. In the OntoUML model shown in Figure 4, three derived associations define the participation of Resilience in an Object at Risk. These associations' derivations can be obtained from a formula that asserts that if an Object at Risk o possesses both a capability c_2 and a vulnerability v, and another capability c_1 disables v that exposes c_2, then logically, Resilience r represents this configuration. This Resilience r inheres in o, is sustained by c_1, and specifically preserves c_2 despite v.

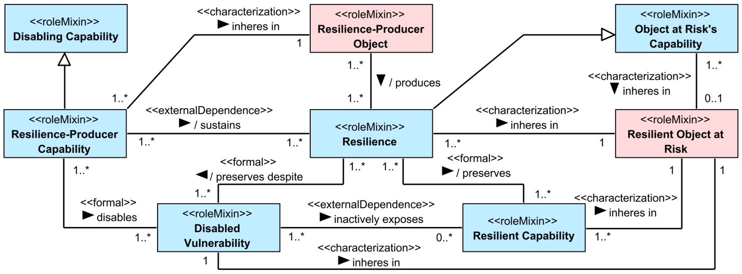

Fig. 4. OntoUML diagram depicting Resilience as the representation of a configuration within an Object at Risk

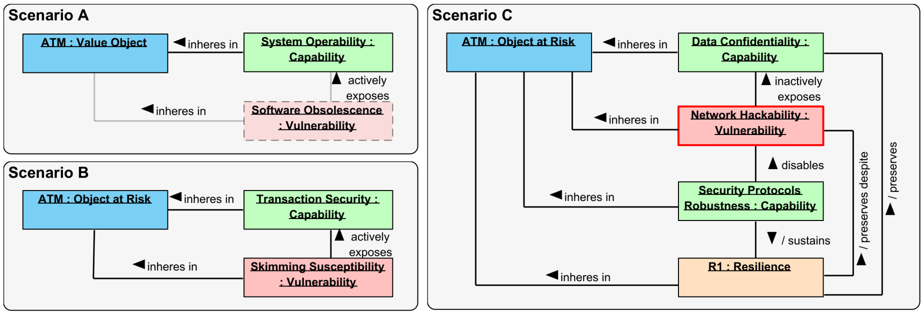

Fig. 5. Comparative analysis of ATM system resilience in three different scenarios: A) non-vulnerable case post-software update, B) vulnerable, non-resilient case subject to skimming, and C) non-vulnerable, resilient case with robust security protocols

To exemplify how Resilience can be achieved in a concrete context, Figure 5 presents three simple practical scenarios within an Automated Teller Machine (ATM) system. We use UML Object Diagrams in all examples in this paper. Blue boxes represent Objects. Capabilities and Vulnerabilities are depicted as green and red rectangles, respectively, with black outlines indicating active dispositions and red outlines indicating inactive ones. Orange boxes denote Resilience instances. Dashed outlines in lighter classes and lighter associations represent past or future possibilities, to be defined in each example.

In Figure 5, Scenario A represents a situation right after a software update nullifies the risk of Software Obsolescence (a change in the Object eliminated the vulnerability). Here, the non-resilient nature of the scenario is evident as the ATM's System Operability currently faces no vulnerabilities. Scenario B also depicts a non-resilient case, however, for a different reason. Here, the ATM's Transaction Security is susceptible to skimming, reflecting an active vulnerability that attackers can exploit, a direct threat to the system's integrity. In contrast, Scenario C exemplifies a resilient configuration; here, the ATM's Data Confidentiality is defended against Network Hackability, a vulnerability that is disabled by the Security Protocols Robustness, thereby achieving Resilience R1.

4.3 Perceiving Resilience

Previously, we described how resilience can be achieved within an Object at Risk. However, possessing resilience is not synonymous with manifesting it. As a capability, resilience only becomes apparent under specific, favorable circumstances during threat events. In this section, we ask "*When can resilience be observed?*" We examine its manifestation in scenarios where resilience prevails over threats and where vulnerabilities lead to loss. This involves a comparative analysis of Threat Events that occur with and without the presence of Resilience, demonstrating the conditions that allow Resilience to be effectively 'visible'.

In this paper, we expand the original idea of Threat Events from COVER to include both successful and unsuccessful outcomes. Understanding the manifestation of resilience begins with recognizing how a Successful Threat Event leads to a Loss Event, presenting the exploitation of an Object's Vulnerability by a Threat Object. Conversely, an Unsuccessful Threat Event occurs when the Object's vulnerabilities are not exploited, preventing the execution of the threat and demonstrating the Object's resilience. This comparative analysis clarifies the nuances of Resilience, emphasizing how it functions as a protective mechanism.

Loss Events represent the concrete realizations of adverse outcomes from risk experiences, such as the actual damages resulting from a cyberattack or an accident. A Loss Event typically occurs when an Object at Risk loses its value as defined by a specific goal of an agent. For instance, in a healthcare setting, a Loss Event might be the accidental exposure of sensitive patient records, where the value is the confidentiality that is critical to patient trust and regulatory compliance. Similarly, in manufacturing, a crucial machine's breakdown due to improper maintenance might constitute a Loss Event, significantly impacting production capacity and hence the company's ability to meet contractual obligations. These events underline the manifestation of loss as historically dependent on a preceding Threat Event. Together, these elements construct the pathway that captures the progression from an Object at Risk's inherent vulnerability through to the occurrence of a Loss Event. This clearly aligns the loss with the decline of valued capabilities or functions critical to the agent's objectives.

Figure 6 presents an OntoUML diagram depicting Successful Threat Events, where a Threat Object with a specific Active Threat Capability exploits an Active Vulnerability in an Object at Risk. This interaction, occurring within a favorable situation, leads to a Successful Threat Event and subsequently to a Loss Event, highlighting the sequence of risk realization that leads to the Object at Risk's loss of value.

While an Object at Risk inherently faces potential threats due to its vulnerabilities, the impact of these Threat Events is primarily determined by the presence or absence of resilience preserving despite vulnerabilities. For instance, a building in a seismic zone, despite being exposed to earthquakes (Threat Events), will not experience structural failures (Loss Events) if it incorporates advanced engineering practices specifically designed for seismic resilience. This underscores that targeted resilience effectively protects against the adverse consequences of specific threats. Conversely, an Object at Risk with exposed vulnerabilities, such

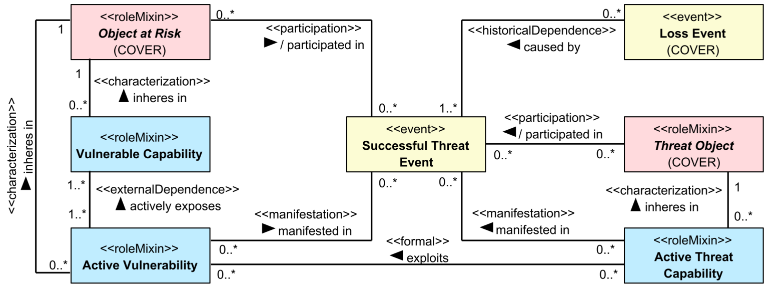

Fig. 6. OntoUML diagram representing a Successful Threat Event and the consequent loss of value of the Object at Risk

as a wooden house in a wildfire-prone area, is almost certain to be destroyed when exposed to fire. This exemplifies how Threat Events result in Loss Events when specific resilience measures are absent. Meanwhile, possessing resilience despite a vulnerability is crucial in preventing corresponding Loss Events. For example, vehicles equipped with advanced safety features, while susceptible to road accidents (Threat Events), can avoid severe damages or injuries (Loss Events) due to their built-in resilience specifically designed for road safety.

Having discussed the dynamics of successful threat events, we now turn to Unsuccessful Threat Events. The OntoUML diagram depicted in Figure 7 shows how a Resilience-Producer Capability plays a crucial role in preventing a Object at Risk from participating in Successful Threat Events. This capability ensures that even when a Threat Object manifests its Threat Capability, the outcome does not lead to a Loss Event. Specifically, the diagram highlights that Resilience-Producer Capabilities are directly related to Unsuccessful Threat Events, which are characterized by their inability to culminate in any Loss Event Types. By preventing the manifestation of vulnerabilities during Threat Events, Resilience-Producer Capabilities ensure that these events do not progress to cause actual losses, thus underscoring the essential function of resilience in safeguarding the Object at Risk against potential damages. Once outlined the dynamics of Threat Events, we next apply these concepts to the example depicted in Figure 8, which examines a submarine's resilience to different pressure levels.

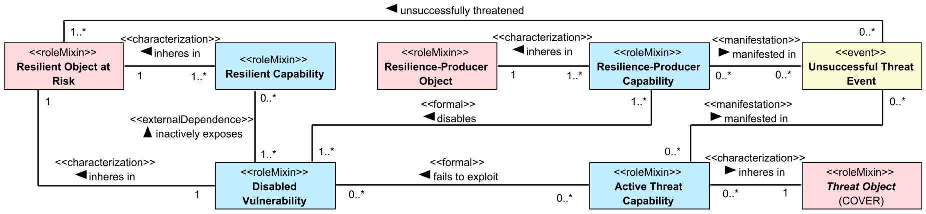

Fig. 7. OntoUML diagram representing the participation of Resilient Capabilities in an Unsuccessful Threat Event, without loss of value of the Object at Risk

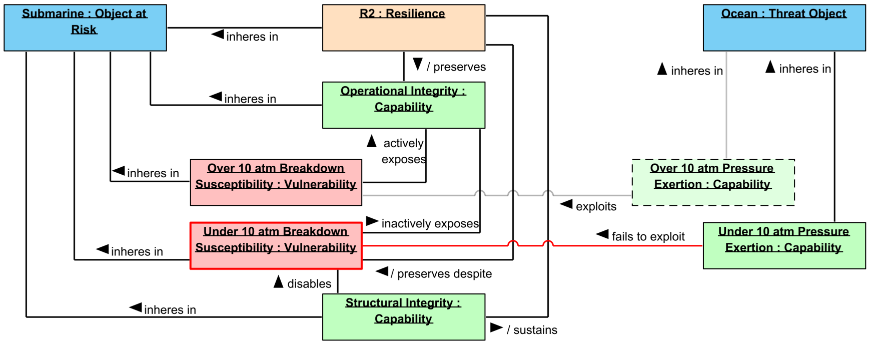
Submarine : Object at Risk
R2 : Resilience
Ocean : Threat Object
inheres in
/ preserves
inheres in
inheres in
Operational Integrity : Capability
inheres in
actively exposes
Over 10 atm Breakdown Susceptibility : Vulnerability
Over 10 atm Pressure Exertion : Capability
exploits
inactively exposes
fails to exploit
inheres in
Under 10 atm Breakdown Susceptibility : Vulnerability
Under 10 atm Pressure Exertion : Capability
/ preserves despite
disables
inheres in
Structural Integrity : Capability
/ sustains

Fig. 8. UML Object Diagram depicting a submarine's pressure response: resilience under 10 atm and loss over 10 atm due to the exploitation of an active vulnerability

In the first possibility, which represents an Unsuccessful Threat Event, the submarine demonstrates its capability to withstand pressures under 10 atmospheres (atm). This resilience is evidenced by the submarine's inherent capabilities, specifically a disabling capability that neutralizes the "Under 10 atm Breakdown Susceptibility." As a result, Resilience R2 is achieved, maintaining the structural integrity of the submarine and preventing the vulnerability from being exploited. Consequently, the operational integrity of the submarine is preserved by the capability that prevents the vulnerability from manifesting.

In the second possibility, we outline a future Successful Threat Event where the submarine lacks resilience against pressures over 10 atm. Here, the "Over 10 atm Breakdown Susceptibility" vulnerability is exploited because of the absence of disabling capabilities, resulting in a failure to maintain structural integrity under high pressure. This results in the submarine's loss as the external ocean's pressure directly affected the operational integrity. The first scenario exemplifies how resilience, through specific protective capabilities, contributes to ensuring the submarine's continued functionality without loss by blocking the potential exploitation of vulnerabilities. In contrast, the second scenario depicts a case where the lack of resilience leads to the successful exploitation of a vulnerability, culminating in a negative outcome for the submarine.

Given the detailed examination of the role of resilience in threat events, we can now revisit this subsection's initial question and answer when resilience can be observed. While objects may inherently possess resilience, it becomes observable only during threat events through the specific capabilities that disable vulnerabilities. These capabilities act decisively to protect the object from loss of value, demonstrating the essential nature of resilience in preventing adverse outcomes under threatening circumstances.

4.4 Defining Resilience

Following our ontological analysis, we propose our own definition of resilience. Moving away from the practice of creating discipline-specific definitions, our definition is universally applicable. It simplifies the understanding of the concept and establishes a domain- and application-independent foundation that enhances its utility and applicability across various fields. Our ontologically well-founded definition of resilience is as follows.

Resilience definition: *A resilience R is a capability that inheres in a value object O when O possesses a vulnerability V that exposes a capacity C_1 of O and is disabled by a capability C_2. As a consequence, R preserves C_1 despite V, prevents the loss of value of O because V cannot be exploited by capabilities of threat objects in threat events, and makes O resilient to these events.*

5 Resilience Modeling: A Production Management Illustration

In this section, we illustrate the application of ResiliOnt by presenting the example of ExCo, a fictitious electronics manufacturer. To manage the risks associated with supplier dependencies, this company has created a structured network consisting of two key suppliers. In a previous state, ExCo used dual suppliers, here named Supplier 1 and Supplier 2, to mitigate the risk associated with single supplier dependence, ensuring operational flexibility and continuous material supply. This section discusses the scenario represented in Figure 9, where Supplier 1 experiences a disruption in its production capability. This scenario presents a complex interplay of capabilities and vulnerabilities, demonstrating that the ontology can be populated with meaningful data.

In the depicted scenario, the production capability of Supplier 1 was disrupted because its 'Political Instability Susceptibility' vulnerability was active, which exposed this capability. Without resilience, the exploitation of this vulnerability led to a loss of value for Supplier 1, resulting in its inoperability. In the original state, Supplier 1's 'Delivery Capability' played a central role in keeping ExCo's 'Single Supplier Dependence' and 'Input Material Shortage' vulnerabilities disabled——in Figure 9, red lines represent the discontinued relations.

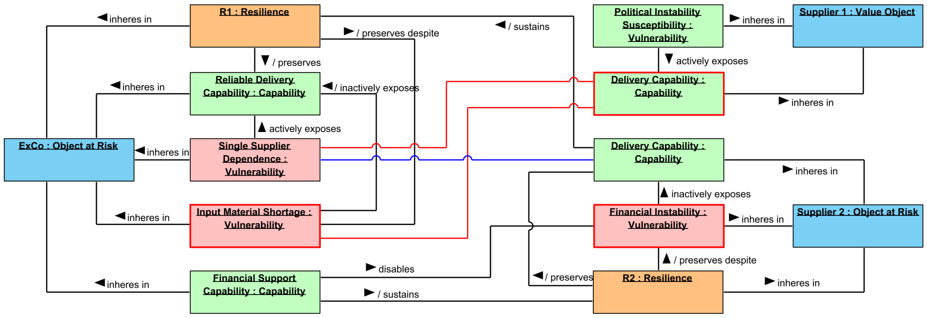
inheres in
R1 : Resilience
/ preserves despite
/ sustains
Political Instability Susceptibility : Vulnerability
inheres in
Supplier 1 : Value Object
/ preserves
actively exposes
inheres in
Reliable Delivery Capability : Capability
/ inactively exposes
Delivery Capability : Capability
inheres in
actively exposes
ExCo : Object at Risk
inheres in
Single Supplier Dependence : Vulnerability
Delivery Capability : Capability
inheres in
inactively exposes
inheres in
Input Material Shortage : Vulnerability
Financial Instability : Vulnerability
inheres in
Supplier 2 : Object at Risk
/ preserves despite
disables
/ preserves
R2 : Resilience
inheres in
inheres in
Financial Support Capability : Capability
/ sustains

Fig. 9. UML Object Diagram illustrating resilience dynamics through the interplay of capabilities and vulnerabilities in a fictitious electronics manufacturer's supply chain

However, once Supplier 1 became non-operational, the absence of its capability affected these vulnerabilities in distinct ways.

The end of Supplier 1's 'Delivery Capability' does not enable ExCo's 'Input Material Shortage' vulnerability, as Supplier 2's 'Delivery Capability' still disables this vulnerability, keeping it inactive. This configuration results in ExCo's Resilience R1, which is supported by Supplier 2's 'Delivery Capability', preserving ExCo's 'Reliable Delivery Capability' despite 'Input Material Shortage'. Regarding ExCo's 'Single Supplier Dependence' vulnerability, the disruption of Supplier 1 means that only Supplier 2's contribution to disabling it is available (represented by the blue line in Figure 9). Since this vulnerability requires contributions from at least two suppliers to be disabled, it becomes active when Supplier 1 is non-operational. An active vulnerability signifies that the 'Reliable Delivery Capability' is exposed and can be exploited. However, this does not mean that exploitation necessarily occurs, as seen in this scenario.

Finally, an operational Supplier 2 bears 'Financial Instability', a vulnerability that, if active, could expose and potentially disrupt its 'Delivery Capability'. Demonstrating proactive management, ExCo addresses this with its 'Financial Support' capability, effectively disabling the 'Financial Instability' vulnerability and ensuring the continuity of Supplier 2's delivery capabilities. This interplay results in Resilience R2 within ExCo's supply chain, preserving Supplier 2's 'Delivery Capability' despite 'Financial Instability'.

6 Related Works

After conducting an extensive, though not systematic, literature review, we observed that several academics have endeavored to explain the meaning of resilience with the aim of deepening the concept's understanding. However, these efforts employ methodologies that differ from ontological analysis. We can divide these efforts into two groups: *(i)* works that offer broad definitions applicable across multiple disciplines [11, 19, 33, 36, 38, 45, 55, 58, 70, 74], and *(ii)* works that provide contributions to particular fields such as sustainability and ecology [14, 27, 50], disaster management [44], politics [5], and to psychology and general health [1, 3, 8, 25, 35, 46, 56, 66, 67, 79].

Particularly illustrative contributions include the explorations of resilience by Haimes [33], Phillips and Chao [55], and Walker [74], which present diverse perspectives that significantly diverge from our ontological analysis. Haimes draws on systems theory and risk analysis to emphasize resilience as a system's reactive capability to specific, identified threats, focusing on recovery and response mechanisms. Similarly, Phillips and Chao argue that resilience lacks inherent meaning and only gains significance within strategic planning contexts, highlighting its dependency on external scenarios; their review of interdisciplinary literature supports this viewpoint. In contrast, Walker critically examines existing definitions in ecological and social areas to propose that resilience is a dynamic capacity for systems to adapt and change in response to disturbances. His work emphasizes the importance of learning and transformation over mere resistance. Our presents resilience as a context-independent characteristic inherent to some Objects, independent of preceding or future disturbances. Unlike these perspectives, we assert that understanding a system's vulnerabilities is sufficient to conclude their potential resilience, thus extending the concept beyond reactive measures.

Regarding the use of foundational ontologies, we could identify two related works. In [53], Ortmann and Daniel propose an ontology design pattern for referential qualities anchored in the DOLCE foundational ontology [13]. Their study employs a generalized definition of resilience from the socio-ecological domain as a case study for the application of the proposed pattern. Although their discussion incorporates DOLCE's meta-properties for resilience, their primary goal was not to define resilience, but merely to model the adopted concept's definition. In a subsequent work, rooted in BFO but still using a resilience definition for the socio-ecological domain, Daniel [21] proposes resilience as a disposition that is realized through processes. We used the author's arguments as one justification for our work to classify resilience as a capability (a subtype of disposition in UFO). Although grounded in a foundational ontology, the analysis of the author takes as its premise the domain-specific definition of resilience and does not address other significant aspects of the concept, as noted by the author.

A major contribution of this paper is ResiliOnt, an OntoUML core ontology built following the ontological analysis presented herein. Ontology artifacts built with this language are ontologically well-founded, as they reflect the ontological principles of UFO. The use of an ontologically well-founded language contrasts with common practices in building resilience ontologies. Our literature review identified that lightweight languages such as OWL—chosen for their ease of implementation rather than their representational fidelity [28]—are typically used for the formalization of these artifacts. Using lightweight ontologies and their related construction methodologies, Van Wassenaer et al. [75] discuss the challenges of creating a resilience ontology due to the impossibility of achieving a unified resilience concept across disciplines, proposing a case-specific approach. Examples of ontologies found using these languages include resilience ontologies for the domains of cybersecurity [7, 9, 69], telecommunications networks [73], supply chains [40, 65], and urban systems [42, 43]. Lastly, Mock [49] used UML Class Diagrams to clarify resilience-related terminology within the engineering domain, rather than applying a foundational ontology. Although Mock's approach brings structured discussion within its scope, it does not create a conceptually sound resilience ontology that can be generalized across different disciplines.

7 Conclusion

In this paper, we addressed the key ambiguity problem associated with the concept of resilience by employing an ontological analysis using UFO and creating ResiliOnt, an OntoUML core ontology for the resilience domain *(contribution I)*. Considering the importance of adopting the FAIR principles (Findability, Accessibility, Interoperability, and Reuse) [77], we made ResiliOnt publicly available with a permissive license (Apache 2.0) in a git repository (https:

//w3id.org/resiliont/git), where the complete ontology can be accessed. Additionally, we added it to the FAIR OntoUML/UFO Catalog [61].

Through our analysis, we clarified that resilience is a capability inherent in objects at risk, defined by their vulnerabilities. Our findings demonstrate that resilience is achieved when an object possesses a vulnerability that is disabled, preventing the exposure of essential capabilities during threat events. We showed that resilience, while existing prior to threat events, can only be observed when such protective mechanisms actively prevent losses during these events. We concluded by developing a sound definition of resilience *(contribution II)*.

Our ontological analysis provides a robust foundation for addressing resilience, which is particularly relevant for managing risks and ensuring continuity in the face of increasing global uncertainties. The developed ResiliOnt ontology allows modelers to represent and analyze the interplay of capabilities and vulnerabilities across various domains, facilitating informed decision-making. Moreover, it extends the applicability of conceptual modeling to pervasive areas, such as resilience engineering, risk management, and system design. When used in the development of other models or systems, it allows for the creation of more precise and interoperable results, thereby enabling these artifacts to effectively incorporate resilience.

Our investigation clarified the conceptual core of resilience, yet it did not address its quantification or gradation, which is useful for many practical implementations. Resilience was viewed as being either present or not——a valid approach when analyzing systems at a granular level. Future studies will address the measurement of resilience, allowing for a spectrum of resilience levels. Once accepting gradation, ResiliOnt must be updated. Additionally, the study did not delve into the complexity of resilience's sub-capabilities, such as resistance and adaptability.

We also acknowledge that some authors argue that the vagueness of resilience may be beneficial, facilitating interdisciplinary connections and acting as a non-controversial 'boundary object' that promotes consensus and multidisciplinary collaboration without forcing a singular definition [47, 68]. They claim that the flexibility of the resilience concept can be seen as advantageous, allowing it to adapt to various disciplinary contexts and expand research possibilities [14, 57]. However, by establishing a clear, ontologically well-founded definition, our work aims to provide a framework that not only supports precise academic discourse, but also enhances the operationalization of resilience in diverse settings.

Finally, as highlighted by Thorén [71], resilience theorists face a central dilemma: to accept a 'thinner' version of resilience that may lack depth but is broadly applicable, or to embrace the substantial ontological implications inherent in more detailed conceptualizations. Our ontological analysis grounded in UFO contributes to the latter approach, providing strong ontological commitments that enhance the conceptual clarity and operational relevance of resilience.

References

1. Aburn, G., Gott, M., et al.: What is resilience? An Integrative Review of the empirical literature. Journal of Advanced Nursing **72**(5), 980–1000 (2016). https://doi.org/https://doi.org/10.1111/jan.12888
2. Ajalli, M.: Conceptual modeling of determining factors in the assessment of sustainability and resilience of the supply chain: a study of rubber industry suppliers in Iran. Journal of Rubber Research (May 2024). https://doi.org/10.1007/s42464-024-00257-3
3. Allen, R.S., Dorman, H.R., et al.: Definition of Resilience, pp. 1–15. Springer International Publishing, Cham (2018). https://doi.org/10.1007/978-3-030-04555-5_1
4. Almeida, J.P.A., Falbo, R.A., et al.: Events as entities in ontology-driven conceptual modeling. In: Conceptual Modeling. pp. 469–483. Springer International Publishing, Cham (2019)
5. Anderson, B.: What Kind of Thing is Resilience? Politics **35**(1), 60–66 (2015). https://doi.org/https://doi.org/10.1111/1467-9256.12079
6. Arp, R., Smith, B., et al.: Building Ontologies with Basic Formal Ontology. The MIT Press (2015)
7. Babiceanu, R.F., Seker, R.: Cyber resilience protection for industrial internet of things: A software-defined networking approach. Computers in Industry **104**, 47–58 (2019). https://doi.org/https://doi.org/10.1016/j.compind.2018.10.004
8. Barasa, E., Mbau, R., et al.: What Is Resilience and How Can It Be Nurtured? A Systematic Review of Empirical Literature on Organizational Resilience. International Journal of Health Policy and Management **7**(6), 491–503 (2018). https://doi.org/10.15171/ijhpm.2018.06
9. Bellini, E., Marrone, S.: Towards a novel conceptualization of Cyber Resilience. In: 2020 IEEE World Congress on Services (SERVICES). pp. 189–196 (2020). https://doi.org/10.1109/SERVICES48979.2020.00048
10. Benevides, A.B., Bourguet, J.R., et al.: Representing a reference foundational ontology of events in SROIQ. Applied Ontology **14**, 293–334 (2019). https://doi.org/10.3233/AO-190214
11. Bhamra, R., Dani, S., et al.: Resilience: the concept, a literature review and future directions. International Journal of Production Research **49**(18), 5375–5393 (2011). https://doi.org/10.1080/00207543.2011.563826
12. Birkie, S.E.: Be lean to be resilient: Setting capabilities for turbulent times. Ph.D. thesis, Politecnico di Milano, Milano (2015)
13. Borgo, S., Ferrario, R., et al.: DOLCE: A descriptive ontology for linguistic and cognitive engineering. Applied Ontology **17**, 45–69 (2022). https://doi.org/10.3233/AO-210259
14. Brand, F.S., Jax, K.: Focusing the Meaning(s) of Resilience: Resilience as a Descriptive Concept and a Boundary Object. Ecology and Society **12**(1) (2007)
15. Calhau, R.F., Almeida, J.a.P.A., et al.: Modeling competences in enterprise architecture: from knowledge, skills, and attitudes to organizational capabilities. Software and Systems Modeling (2024). https://doi.org/10.1007/s10270-024-01151-7
16. Calhau, R.F., Almeida, J.P.A.: Zooming in on Competences in Ontology-Based Enterprise Architecture Modeling. In: Enterprise Design, Operations, and Computing. EDOC 2022 Workshops. pp. 198–213. Springer International Publishing, Cham (2023)
17. Calhau, R.F., Kokkula, S., et al.: Modeling Competence Framework Elements with an Ontology-based Approach. In: 2023 IEEE 25th Conference on Business Informatics (CBI). pp. 1–10 (2023). https://doi.org/10.1109/CBI58679.2023.10187498

18. Calhau, R.F., Sales, T.P., et al.: A System Core Ontology for Capability Emergence Modeling. In: Enterprise Design, Operations, and Computing - 27th International Conference, EDOC 2023, Groningen, The Netherlands, October 30 - November 3, 2023, Proceedings. Lecture Notes in Computer Science, vol. 14367, pp. 3–20. Springer (2023). https://doi.org/10.1007/978-3-031-46587-1_1
19. Carlson, J.L., Haffenden, R.A., et al.: Resilience: Theory and Application. Tech. rep., Argonne National Lab., United States (2012). https://doi.org/10.2172/1044521
20. Chu, Y.H.: Resilience capabilities in the face of environmental turbulence: a case of Hong Kong small to medium enterprises. Ph.D. thesis, RMIT University (2015)
21. Daniel, D.: Resilience as a Disposition. In: Formal Ontology in Information Systems - Proceedings of the Eighth International Conference, FOIS 2014, September, 22-25, 2014, Rio de Janeiro, Brazil. Frontiers in Artificial Intelligence and Applications, vol. 267, pp. 171–182. IOS Press (2014). https://doi.org/10.3233/978-1-61499-438-1-171
22. Davey, J., Krisjanous, J., et al.: Editorial: Service resilience in an increasingly ambiguous, dynamic and complex world – absorb, adapt and transform. Journal of Services Marketing **38**(4), 385–391 (2024). https://doi.org/10.1108/JSM-03-2024-0122
23. Dori, D., Sillitto, H.: What is a System? An Ontological Framework. Syst. Eng. **20**(3), 207–219 (2017). https://doi.org/10.1002/SYS.21383
24. Duchek, S.: Organizational resilience: a capability-based conceptualization. Business Research **13**(1), 215–246 (Apr 2020). https://doi.org/10.1007/s40685-019-0085-7
25. Glantz, M.D., Sloboda, Z.: Analysis and Reconceptualization of Resilience, pp. 109–126. Springer US, Boston, MA (2002). https://doi.org/10.1007/0-306-47167-1_6
26. Grabis, J., Deksne, L., et al.: A Capability-Based Method for Modeling Resilient Data Ecosystems, pp. 339–363. Springer International Publishing, Cham (2022). https://doi.org/10.1007/978-3-030-93547-4_15
27. Gruemm, H.R.: Definitions of Resilience. IIASA Research Report RR-76-005, International Institute for Applied Systems Analysis (IIASA), Laxenburg, Austria (Mar 1976)
28. Guizzardi, G.: On Ontology, ontologies, Conceptualizations, Modeling Languages, and (Meta)Models. In: Proceedings of the 2007 Conference on Databases and Information Systems IV: Selected Papers from the Seventh International Baltic Conference DB&IS'2006. p. 18–39. IOS Press, NLD (2007)
29. Guizzardi, G.: Ontology, Ontologies and the "I" of FAIR. Data Intelligence **2**(1-2), 181–191 (01 2020). https://doi.org/10.1162/dint_a_00040
30. Guizzardi, G., Botti Benevides, A., et al.: UFO: Unified Foundational Ontology. Applied Ontology **17**, 167–210 (2022). https://doi.org/10.3233/AO-210256
31. Guizzardi, G., Wagner, G., et al.: Towards Ontological Foundations for the Conceptual Modeling of Events. In: Conceptual Modeling. pp. 327–341. Springer Berlin Heidelberg, Berlin, Heidelberg (2013)
32. Guizzardi, G., Wagner, G., et al.: Towards ontological foundations for conceptual modeling: The unified foundational ontology (UFO) story. Applied Ontology **10**(3-4), 259–271 (2015). https://doi.org/10.3233/AO-150157
33. Haimes, Y.Y.: On the Definition of Resilience in Systems. Risk Analysis **29**(4), 498–501 (2009). https://doi.org/https://doi.org/10.1111/j.1539-6924.2009.01216.x
34. Herrera, H.: Resilience for Whom? The Problem Structuring Process of the Resilience Analysis. Sustainability **9**(7) (2017). https://doi.org/10.3390/su9071196

35. Herrman, H., Stewart, D.E., et al.: What is Resilience? The Canadian Journal of Psychiatry **56**(5), 258–265 (2011). https://doi.org/10.1177/070674371105600504
36. Hosseini, S., Barker, K., et al.: A review of definitions and measures of system resilience. Reliability Engineering & System Safety **145**, 47–61 (2016). https://doi.org/https://doi.org/10.1016/j.ress.2015.08.006
37. Johannesson, P., Perjons, E.: An Ontological Analysis of the Notion of Treatment. In: Conceptual Modeling. pp. 303–314. Springer International Publishing, Cham (2020)
38. Kaplan, H.B.: Understanding the Concept of Resilience, pp. 39–47. Springer US, Boston, MA (2005). https://doi.org/10.1007/0-306-48572-9_3
39. Kochan, C.G., Nowicki, D.R.: Supply chain resilience: a systematic literature review and typological framework. International Journal of Physical Distribution & Logistics Management **48**(8), 842–865 (Jan 2018). https://doi.org/10.1108/IJPDLM-02-2017-0099
40. Koot, M., Mes, M.R.K., et al.: Building an Ontological Bridge Between Supply Chain Resilience and IoT Applications. In: Enterprise Design, Operations, and Computing. pp. 79–96. Springer Nature Switzerland, Cham (2024)
41. Laun, A., Mazzuchi, T.A., et al.: Conceptual data model for system resilience characterization. Systems Engineering **25**(2), 115–132 (2022). https://doi.org/https://doi.org/10.1002/sys.21605
42. Lestakova, M., Logan, K., et al.: Towards a Common Ontology for Investigating Resilience of Interdependent Urban Systems. In: Proceedings of the Joint International Resilience Conference, JIRC2020, 23.11.2020-27.11.2020. pp. 101–104. University of Twente, Twente (Dec 2020). https://doi.org/https://doi.org/10.3990/1.9789036550956
43. Lombardini, G.: Dealing with Resilience Conceptualisation. Formal Ontologies as a Tool for Implementation of Intelligent Geographic Information Systems. TeMA - Journal of Land Use, Mobility and Environment (May 2014). https://doi.org/10.6092/1970-9870/2540
44. Manyena, S.B.: The concept of resilience revisited. Disasters **30**(4), 434–450 (2006). https://doi.org/https://doi.org/10.1111/j.0361-3666.2006.00331.x
45. Martin-Breen, P., Anderies, J.M.: Resilience: A Literature Review (2011)
46. McCubbin, L.: Challenges to the Definition of Resilience. Information analyses; speeches/meeting papers, ERIC - Institute of Education Sciences (Aug 2001)
47. Meerow, S., Newell, J.P., et al.: Defining urban resilience: A review. Landscape and Urban Planning **147**, 38–49 (2016). https://doi.org/https://doi.org/10.1016/j.landurbplan.2015.11.011
48. Merrell, E., Limbaugh, D., et al.: Capabilities. https://philpapers.org/rec/MERC-14 (2022)
49. Mock, R.G., Leksin, A., et al.: An ontology of risk associated concepts in the context of resilience. In: Proceedings of the 29th European Safety and Reliability Conference. pp. 1320–1327. Research Publishing, Singapore (2019). https://doi.org/10.3850/978-981-11-2724-3_0246-cd
50. Myers-Smith, I., Trefry, S., et al.: Resilience: Easy to use but hard to define. Ideas in Ecology and Evolution **5**, 44–53 (Oct 2012). https://doi.org/10.4033/iee.2012.5.11.c
51. Oliveira, Í., Sales, T.P., et al.: An Ontology of Security from a Risk Treatment Perspective. In: Conceptual Modeling. pp. 365–379. Springer International Publishing, Cham (2022)

52. Oppong Banahene, K., Anvuur, A., et al.: Conceptualising organisational resilience: An investigation into project organising. In: Proceedings of the 30th Annual ARCOM Conference. vol. 2, pp. 795–804. Association of Researchers in Construction Management, Portsmouth, UK (2014)
53. Ortmann, J., Daniel, D.: An Ontology Design Pattern for Referential Qualities. In: The Semantic Web – ISWC 2011. pp. 537–552. Springer Berlin Heidelberg, Berlin, Heidelberg (2011)
54. ao Paulo A. Almeida, J., Guizzardi, G.: An ontological analysis of the notion of community in the RM-ODP enterprise language. Computer Standards & Interfaces **35**(3), 257–268 (2013). https://doi.org/https://doi.org/10.1016/j.csi.2012.01.007
55. Phillips, F.Y., Chao, A.: Rethinking Resilience: Definition, Context, and Measure. IEEE Transactions on Engineering Management pp. 1–8 (2022). https://doi.org/10.1109/TEM.2021.3139051
56. Pooley, J.A., Cohen, L.: Resilience: A Definition in Context. The Australian Community Psychologist **22**(1) (Dec 2010)
57. Reghezza-Zitt, M., Lhomme, S., et al.: Defining Resilience: When the Concept Resists. In: Resilience Imperative, pp. 1–27. Elsevier (2015). https://doi.org/https://doi.org/10.1016/B978-1-78548-051-5.50001-2
58. Reid, R., Botterill, L.C.: The Multiple Meanings of 'Resilience': An Overview of the Literature. Australian Journal of Public Administration **72**(1), 31–40 (2013). https://doi.org/https://doi.org/10.1111/1467-8500.12009
59. Reinmoeller, P., van Baardwijk, N.: The link between diversity and resilience: new research shows that the most resilient companies are those that continually orchestrate a dynamic balance of four innovation strategies. MIT Sloan Management Review **46**, 61+ (May 2005)
60. Sales, T.P., Baião, F., et al.: The Common Ontology of Value and Risk. In: Conceptual Modeling. pp. 121–135. Springer International Publishing, Cham (2018)
61. Sales, T.P., Barcelos, P.P.F., et al.: A FAIR catalog of ontology-driven conceptual models. Data & Knowledge Engineering **147**, 102210 (2023). https://doi.org/https://doi.org/10.1016/j.datak.2023.102210
62. Saxena, M.: Capability Management: Monitoring and Improving Capabilities. Global India Publications, India (2009)
63. SEBoK Editorial Board: The Guide to the Systems Engineering Body of Knowledge (SEBoK), v. 2.9. www.sebokwiki.org (2023)
64. Sillitto, H.G.: 10.2. 1 "Composable Capability"–Principles, strategies and methods for capability systems engineering. INCOSE International Symposium **23**(1), 723–738 (Jun 2013). https://doi.org/10.1002/j.2334-5837.2013.tb03050.x
65. Singh, S., Ghosh, S., et al.: Enhancing supply chain resilience using ontology-based decision support system. International Journal of Computer Integrated Manufacturing **32**(7), 642–657 (2019). https://doi.org/10.1080/0951192X.2019.1599443
66. Southwick, S.M., Bonanno, G.A., et al.: Resilience definitions, theory, and challenges: interdisciplinary perspectives. European Journal of Psychotraumatology **5**(1), 25338 (2014). https://doi.org/10.3402/ejpt.v5.25338
67. Stainton, A., Chisholm, K., et al.: Resilience as a multimodal dynamic process. Early Intervention in Psychiatry **13**(4), 725–732 (2019). https://doi.org/https://doi.org/10.1111/eip.12726
68. Strunz, S.: Is conceptual vagueness an asset? Arguments from philosophy of science applied to the concept of resilience. Ecological Economics **76**, 112–118 (2012). https://doi.org/https://doi.org/10.1016/j.ecolecon.2012.02.012

69. Thinyane, M., Christine, D.: SMART Citizen Cyber Resilience (SC2R) Ontology. In: 13th International Conference on Security of Information and Networks. SIN 2020, Association for Computing Machinery, New York, NY, USA (2021). https://doi.org/10.1145/3433174.3433617
70. Thorén, H.: Resilience as a Unifying Concept. International Studies in the Philosophy of Science **28**(3), 303–324 (2014). https://doi.org/10.1080/02698595.2014.953343
71. Thorén, H., Olsson, L.: Is resilience a normative concept? Resilience **6**(2), 112–128 (2018). https://doi.org/10.1080/21693293.2017.1406842
72. Utami, I.D., Santosa, I., et al.: Conceptual modeling of resilience measurement during natural disasters for SMEs. IOP Conference Series: Materials Science and Engineering **1072**(1), 012050 (Feb 2021). https://doi.org/10.1088/1757-899X/1072/1/012050
73. Vlacheas, P., Stavroulaki, V., et al.: Towards end-to-end network resilience. International Journal of Critical Infrastructure Protection **6**(3), 159–178 (2013). https://doi.org/https://doi.org/10.1016/j.ijcip.2013.08.004
74. Walker, B.H.: Resilience: what it is and is not. Ecology and Society **25**(2) (2020). https://doi.org/10.5751/ES-11647-250211
75. van Wassenaer, L., Oosterkamp, E., et al.: Food system resilience: ontology development and impossible trinities. Agriculture & Food Security **10**(1), 38 (Sep 2021). https://doi.org/10.1186/s40066-021-00332-7
76. Weigand, H., Johannesson, P., et al.: Ontological Analysis of Policy-based Decision Making. In: Proceedings of the 17th International Workshop on Value Modeling and Business Ontologies. University of Twente (2024)
77. Wilkinson, M.D., Dumontier, M., et al.: The FAIR Guiding Principles for scientific data management and stewardship. Scientific Data **3**(1), 160018 (Mar 2016). https://doi.org/10.1038/sdata.2016.18
78. Wilt, B., Long, Suzanna, P., et al.: Defining Resilience: a Preliminary Integrative Literature Review. In: Proceedings of the International Annual Conference of the American Society for Engineering Management. pp. 1–10. American Society for Engineering Management (ASEM), Huntsville, United States (2016)
79. Windle, G.: What is resilience? A review and concept analysis. Reviews in Clinical Gerontology **21**(2), 152–169 (2011). https://doi.org/10.1017/S0959259810000420
80. Zimmerman, R., Zhu, Q., et al.: Conceptual Modeling Framework to Integrate Resilient and Interdependent Infrastructure in Extreme Weather. Journal of Infrastructure Systems **23**(4), 04017034 (2017). https://doi.org/10.1061/(ASCE)IS.1943-555X.0000394