Trustworthiness Requirements: The Pix Case Study

Glenda Amaral[1(✉)], Renata Guizzardi[2], Giancarlo Guizzardi[1,2], and John Mylopoulos[3]

[1] CORE/KRDB, Free University of Bozen-Bolzano, Bolzano, Italy
{gmouraamaral,giancarlo.guizzardi}@unibz.it
[2] University of Twente, Enschede, The Netherlands
r.guizzardi@utwente.nl
[3] University of Toronto, Toronto, Canada
jm@cs.toronto.edu

Abstract. The advent of socio-technical, cyber-physical and artificial intelligence systems has broadened the scope of requirements engineering, which must now deal with new classes of requirements, concerning ethics, privacy and trust. This brings new challenges to Requirements Engineering, in particular regarding the understanding of the non-functional requirements behind these new types of systems. To address this issue, we propose the Ontology-based Requirements Engineering (ObRE) method, which aims to systematize the elicitation and analysis of requirements, by using an ontology to conceptually clarify the meaning of a class of requirements, such as privacy, ethicality and trustworthiness. We illustrate the working of ObRE by applying it to a real case study concerning trustworthiness requirements.

Keywords: Trustworthiness requirements · Requirements elicitation and analysis · Unified Foundational Ontology

1 Introduction

Requirements Engineering (RE) is a critical system development activity that makes or breaks many software development projects [12]. A myriad of RE methods, following different paradigms, have been around for at least four decades. Early methods focused on 'what' stakeholders need, resulting in a list of system functionalities directly indicated by stakeholders or inferred by requirements analysts. In the early nineties, goal-oriented RE (GORE) inaugurated a new paradigm that focused on 'why' a system was needed and 'how' needs of stakeholders can be addressed [14]. Also around this time, the realization that not only functionalities but also *qualities* are important to shape the system-to-be led to newfound attention on non-functional requirements (e.g., privacy, security, etc.) [6]. In the 2000s, the agile software engineering paradigm emerged, leading to new RE methods focusing on incremental software delivery and teamwork

A. Ghose et al. (Eds.): ER 2021, LNCS 13011, pp. 257–267, 2021.
https://doi.org/10.1007/978-3-030-89022-3_21

(e.g., capturing requirements via user stories [7])[1]. Generally, RE has evolved in response to an ever-increasing system complexity that today spans not only system concerns, but also social (e.g., security, privacy), physical (as in cyber-physical systems), and personal (e.g., ethical concerns for artificial intelligence systems) ones. A major challenge for RE today is to propose concepts, tools and techniques that support requirements engineering activities for incorporating high-level societal concerns and goals, such as privacy, fairness ands trustworthiness, into the software development processes as explicit requirements.

This paper is intended to address this challenge with a novel method named Ontology-based Requirements Engineering (ObRE). The method aims to systematize the elicitation and analysis of requirements, by using an ontological account for a class of requirements, such as privacy, fairness and trustworthiness. ObRE is intended to help by "semantically unpacking" concepts such as trustworthiness or fairness where the analysts may struggle in understanding, for example, which requirements can make the system under development trustworthy or fair. Ontological analysis provides a foundation for ObRE as it enables a deep account of the meaning of a particular domain. The notions of *ontology* and *ontological analysis* adopted here are akin to their interpretations in philosophy [4]. In this view, the goals of *ontological analysis* are: (i) characterize what kinds of entities are assumed to exist by a given conceptualization of a domain; (ii) the metaphysical nature of these kinds of entities. An *ontology*, in turn, is a collection of concepts and relationships that together address questions (i) and (ii).

The paper presents in detail the ObRE and illustrates its use with a case study, focused on a recently released real system, named Pix. Pix is an instant payment solution, created and managed by the Central Bank of Brazil (BCB), which enables its users to send or receive payment transfers in few seconds at any time. The success achieved by Pix has led us to consider it an appropriate case study for our approach.

The remainder of the paper is structured as follows. First, in Sect. 2 we explain the ontological account of trustworthiness requirements adopted in this work. Then, in Sect. 3 we present the ObRE method. In Sect. 4 we present the Pix case study and in Sect. 5 we use ObRE to analyse the trustworthiness requirements of Pix. In Sect. 6 we make some final remarks on the implications of our proposal to the requirements engineering practice, and we describe our future research agenda.

2 The Reference Ontology of Trustworthiness Requirements

Trustworthiness requirements are a class of requirements where the objective is to get user stakeholders to adopt an attitude of trust towards the system-to-be. We

[1] This is a brief historical account intended to highlight the evolution of ideas and methods in RE. This account is not meant to be exhaustive; we acknowledge the existence of many other high impact RE methods, such as feature-based RE, recent methods based on CANVAS.

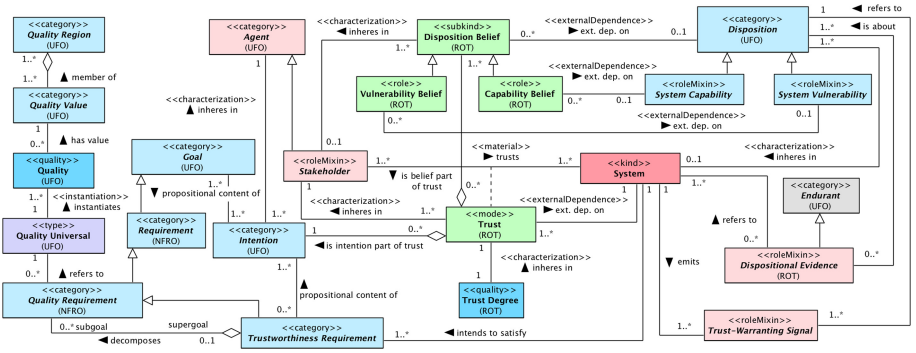

Fig. 1. The reference ontology of trustworthiness requirements

propose to first unpack the concept of trust. This is done here with a fragment of the Reference Ontology of Trustworthiness Requirements[2] (ROTwR) [1], which is a reference ontology grounded on UFO [9], and based on the trust-related concepts defined in the Reference Ontology of Trust[3] (ROT) [2,3] and on the ontological interpretation of non-functional requirements presented in [11]. Some of the main ontological commitments of ROTwR on the nature of trust and trustworthiness requirements are: (i) trust is relative to intentions [5]; (ii) trust is grounded on beliefs [5]; (iii) trustworthiness requirement is related to an intention that is part of a trust relation between a stakeholder and the system-to-be [1]; (iv) trustworthiness requirements are quality requirements [11]; and (v) the system can emit trust-warranting signals to ensure trustworthy behavior [13].

Figure 1 presents an excerpt of ROTwR, represented in OntoUML (an ontology-driven conceptual modeling language based in UFO [9]). In ROTwR, Requirement is modeled as a Goal, which is the propositional content of a Stakeholder's Intention. Quality Requirement is a type of Requirement, and Trustworthy Requirement is a type of Quality Requirement. All Quality Requirements are such that they restrict the value of the qualities at hand to a particular set of values of the corresponding Quality Region. For example, "being trustworthy" is a constraint on the mental state of the trustor to be in the trustworthiness region of a space that also includes an untrustworthiness region. Stakeholders are represented as Agents that play the role of trustor, while the System is an existentially independent object that plays the role of trustee. The System intends to satisfy the Trustworthiness Requirements. As for Trust, it is represented as a complex mode composed of a Stakeholder's Intention and a set of Beliefs that inhere in the Stakeholder and are externally dependent on the dispositions [10] that

[2] The complete version of ROTwR in OntoUML and its implementation in OWL is available at https://purl.org/krdb-core/trustworthiness-requirements-ontology.

[3] The complete version of ROT in OntoUML and its implementation in OWL are available at http://purl.org/krdb-core/trust-ontology.

inhere in the System. These beliefs include: (i) the Belief that the System has the Capability to perform the desired action (Capability Belief); and (ii) the Belief that the System's Vulnerabilities will not prevent it from exhibiting the desired behavior (Vulnerability Belief). The System's Vulnerabilities and Capabilities are dispositions that inhere in the System, which are manifested in particular situations, through the occurrence of events [10]. The System can emit Trust-Warranting Signals to indicate that it is capable of successfully realizing the capabilities and prevent the manifestation of the vulnerabilities. Another important aspect is the role played by pieces of evidence that indicate that a trustee (System) is trustworthy, named here Dispositional Evidence. Examples of dispositional evidences are certifications by trusted third parties, history of performance, recommendations, past successful experiences, among others. Ontologically speaking, Dispositional Evidences are social entities, typically social relators (e.g., a relator binding the certifying entity, the certified entity and referring to a capability, vulnerability, etc.), but also documents (social objects themselves) that represent these social entities (e.g., in the way a marriage certificate documents a marriage as a social relator). They are modeled as roles played by endurants (objects, relators, etc.) related to a Disposition of the System.

3 Ontology-Based Requirements Engineering

In ObRE, we address the challenge of dealing with non-functional requirements, such as trustworthiness, by relying on ontological analysis. Ontological analysis provides a foundation for our proposal as it enables a deep account of the meaning of a particular domain, thus allowing to "semantically unpack" the requirements concepts at-hand, thereby facilitating requirements activities. Figure 2 illustrates the process of the ObRE method, showing the three activities that compose it, which are described below.

1. Adopt or develop an ontology for conceptualizing a class of requirements: In this step, requirements analysts and ontology engineers can choose between reusing an existing ontology or performing ontological analysis for the particular class of requirement. Having the requirements explicitly defined and understood, the analyst may proceed to the next step.
2. Instantiate the ontology for a system-to-be, resulting in a domain model: In this step, key concepts of the ontology can be used as a guide to define the right questions to be asked to the stakeholders during requirements elicitation (e.g., Table 1). The answers can be used as input to instantiate elements of the ontology. This is intended to serve as a domain model for conducting requirements analysis.
3. Analyze requirements based on the domain model: In this step, the analyst uses the domain model to define and analyze system requirements. For instance, she may simply define a requirements table, listing the requirements instantiated with the help of the ontology. Or if she prefers a more sophisticated analysis methodology, she may use goal modeling, defining the contribution of

different choices to accomplish a particular goal (i.e., requirement), and specifying how goals relate to each other, as well as to relevant stakeholders' resources and tasks. Or yet, she may create user stories based on the identified ontological instances. From this point on, the requirements analysis may progress as the chosen method prescribes, however, with the benefit of having the ontology and ontological instances as guides.

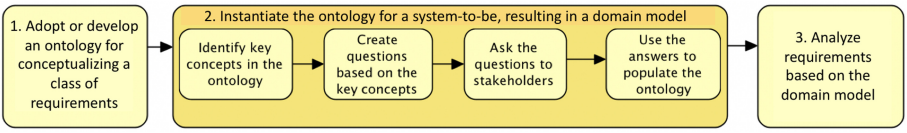

Fig. 2. Ontology-based requirements engineering method

4 Case Study

4.1 Research Method

To evaluate and demonstrate the contribution of our ontology-based method for the analysis of trustworthiness requirements, we conducted a case study in the Central Bank of Brazil (BCB), in the context of the Brazilian Instant Payments Ecosystem.

The research procedure was adapted from [15]. The initial stage involved the planning and designing of the case study. We defined the purpose of the case study - *evaluate the feasibility of the application of ObRE for the analysis and elicitation of Pix's trustworthiness requirements* - and held a planning meeting to identify different areas of interest and select the interviewees.

In the collect stage, we gathered information from documentation and interviews. Firstly, documents describing and documenting the project were collected from the BCB's website[4] to deepen the knowledge about Pix. Then, we conducted interviews with the stakeholders responsible for the areas of interest, namely communication, instant payment systems, communication interfaces, transaction accounts identifier directory, security and infrastructure. The questions in the interviews were based on the notions of trust and trustworthiness requirements described in the adopted ontology (Sect. 2) (step 1 of ObRE method, in Fig. 2). The interviews were recorded and transcribed to facilitate and improve the analysis. In the analyze stage, the interviewers examined the transcripts and searched for the elements to instantiate the ontology of trustworthiness requirements (step 2 of ObRE method, in Fig. 2). Then, we used the ontology instantiation as a domain model to define and analyze trustworthiness requirements (step 3 of ObRE method, in Fig. 2).

[4] https://www.bcb.gov.br/en/financialstability/pix_en.

4.2 The Brazilian Instant Payments Ecosystem (Pix)

The Central Bank of Brazil is a special nature agency, characterized by the absence of ties or hierarchical subordination to any Ministry. Among the main tasks of the BCB are the regulation and supervision of the National Financial System and the administration of the payments system.

Pix is the instant payment solution, created and managed by the BCB, having two kinds of stakeholders: *financial institutions* that want to offer this instant payment service, and *end users*, i.e. the clients of the financial institutions, aiming at exchanging money through such service. A Pix transaction will typically be initiated through the usage of a predefined Pix Key or a QR code associated with the beneficiary's transactional account. The Pix key is a 'nickname' used to identify the user account, which can be a cell phone number, an email, a taxpayer number or a random key. The key links one of these basic items of information to the complete information that identifies the customer's transactional account. Once started, Pix transactions are irrevocable and processed individually in a few seconds. Pix can be processed between: Person-to-Person (P2P), Person-to-Business (P2B), Business-to-Business (B2B), Person-to-Government (P2G), or Business-to-Government (B2G).

Pix operates through a centralized framework comprising messaging communication among the various participants and BCB. All transactions take place through digitally signed messages exchanged, in encrypted form, through a private network apart from the Internet. In order to promote public awareness, BCB created the Pix's brand, whose principles—Design, Sonority, Governance—aim at promoting an easily identifiable brand that should be displayed by all participating financial institutions.

5 Using ObRE to Analyze Pix's Requirements

This section presents the results of the case study. As aforementioned, our findings are based in the analysis of the documentation and the interviews conducted with stakeholders responsible for Pix key areas. Our analysis took into account the whole ecosystem in which the system is included, whose main stakeholders are the *Pix ecosystem participants* (financial and payment institutions that offer transaction accounts) and *end users* (individuals and organizations).

5.1 Domain Ontology Development or Adoption

We reused our previous Reference Ontology on Trustworthiness Requirements [1] (Sect. 2) to unpack the notions of trust and trustworthiness requirements (step 1 of ObRE method, in Fig. 2). Then, we defined the initial questions that would guide the interviews with the stakeholders (Table 1). The ontology served as guidance for our work from the beginning of the case study, helping us focus on the domain being investigated and supporting the creation of the interview questions. As can be seen on Table 1, these questions are actually formulated based on the concepts from ROTwR (see column 2).

Table 1. Questions related to key ontology concepts

Question	ROTwR concept
Stakeholders trust the system to...	Intention
Stakeholders trust the system because they believe that it is capable of...	Capability Belief System Capability
Stakeholders trust the system because they believe that it has mechanisms to prevent...	Vulnerability Belief System Vulnerability
How can the system indicate that it is trustworthy?	Trust-warranting Signal
What pieces of evidence show that the system is trustworthy?	Dispositional Evidence

5.2 Domain Ontology Instantiation

We adopt the following coding to refer to instances of key ROTwR concepts hereafter: (i) INT for intentions; (ii) BEL for disposition beliefs; (iii) TS for trust-warranting signals; (iv) DE for dispositional evidences; and (v) TR for trustworthiness requirements.

The interviews showed that, in general, *end users trust Pix to send or receive payment transfers safely and easily, in few seconds on a 24/7 basis* (INT1). According to an interviewee, "users want to be sure that the system will access their money only when they want, and in the way they want". In other words, users who trust the system believe that *it is safe* (BEL1) and that *it will be available when they need* (BEL2). Interviewees also expressed that it is important that Pix participants feel safe to perform transactions in the ecosystem. It was a consensus among the interviewees that *security* (TR1), *availability* (TR2) and *instantaneity* (TR3) are essential to build sustainable trust in the system.

As stated by the Pix project team and explained in the documentation, *security* has been a part of Pix design since its inception, and it is prioritized in all aspects of the ecosystem, including transactions, personal information and the fight against fraud and money laundering. The requirements for the *availability*, *confidentiality* (TR4), *integrity* (TR5) and *authenticity* (TR6) of the information were carefully studied and several controls were implemented to ensure a high level of security. All transactions take place through digitally signed messages that travel in encrypted form, over a protected network, apart from the Internet. In addition, user information is also encrypted and protected by mechanisms that prevent scans of personal information in the sole and centralized proxy database, an addressing database that will store Pix keys information. There are also *indicators that assist the ecosystem participants in the process of prevention against fraud and money laundering* (TS1). Another important aspect related to security is *traceability* (TR7). All Pix operations are fully traceable, which means that the Central Bank and the institutions involved can, at the request of the competent authorities, identify the origin and destination account holders of any and all payment transactions in Pix. Thus, in a situation of kidnapping or other means of unlawful coercion, the recipient of a financial transfer is fully identified.

In addition, *all participants must comply with basic regulation on operational and liquidity risk management framework* (DE1); *cybersecurity policy* (DE2); a *service level agreement that establishes high availability parameters and processing time limits* (DE3); among others.

Another aspect that emerged from the interviews is the importance of providing a simple experience for end users. Interviewees mentioned that "people are more likely to trust in something they understand" and "simplicity leads to trust". Simply put, users who trust the system believe that *it is simple and easy to use* (BEL3). The general consensus is that *usability* (TR8) is of paramount importance for effectively promoting trust in the system. *Visual identity* (TS2) was mentioned by interviewees as an important attribute to facilitate the understanding and adoption of the functionality. According to them, the establishment of a universal brand was essential for users to identify the new way of making/receiving payments and transfers, in a clear and unambiguous way. Equally important was the definition of a *manual with minimum usability requirements* (DE4), which must be followed by all participants of the Pix ecosystem.

Still in this direction, actions focusing on *explainability* (TR9) have been taken since the beginning of the project. Some examples mentioned during the interviews are: *advertising campaigns in the media and social networks using everyday examples* (TS3); *documentation available on the BCB website* (See footnote 4) (TS4); *dissemination events* (held in virtual mode, due to the COVID-19 pandemic) *for different market sectors* (TS5); (iv) partnership with the press and digital influencers for advertising, as well as for monitoring and preventing the spread of fake news about the system.

Finally, *transparency* (TR10) was another attribute mentioned by a number of interviewees. One of the reasons for the prioritization of *transparency*, as explained by several interviewees, is that "if the participants are involved in the discussions from the beginning, *they believe that their needs will be considered and that they will not be taken by surprise, consequently, they feel safe and trust the system*" (BEL4). Interviewees also mentioned that "participants' trust in the Pix ecosystem contributed to foster end users' trust". In this direction, the Pix operational framework development has been an open and transparent process, with intense participation from market agents and potential users. In order to foster a collaborative implementation process, BCB created a specific forum, named *'Pix Forum'* (DE5), which has about 200 participating institutions. Lastly, as previously mentioned, an extensive documentation about the Pix project and the Pix ecosystem is available at the BCB website (See footnote 4), providing information such as a Pix regulations, Frequently Asked Questions, and Pix statistics[5], which contribute to *transparency* at different levels. Pix statistics include indicators, such as number of registered Pix keys, number of Pix transactions, number of users transacting Pix, among others. We identified that, in general, *these indicators* positively exceeded the initial expectations, thus demonstrating the success of the project. In this case, they can be seen as pieces of evidence (DE6) that indicate that the Pix ecosystem is trustworthy.

[5] https://www.bcb.gov.br/en/financialstability/pixstatistics.

5.3 Requirements Analysis Method Execution

We exemplify the step 3 of ObRE method (Fig. 2) by analyzing the requirements of Pix. In particular, we present both a requirements table and a goal model for this case.

We start by presenting Table 2, showing how a requirements table may be enriched with the inclusion of columns representing some of ROTwR concepts. All words highlighted in boldface in Table 2 refer to ontological concepts analyzed in Sect. 2, while the ontological instances are written as non-emphasized text. Due to space limitations, we focused only on security. To build a requirements table such as Table 2, we first capture the elements that compose the trust of stakeholders in Pix, namely their intentions and beliefs about Pix dispositions, and then we come up with particular requirements for the system-to-be to fulfill these goals and beliefs. In particular, these are requirements for the developing capabilities (i.e. system's functionalities) needed to accomplish the desired requirements.

Table 2. Requirements table of the Pix Ecosystem focusing on security

Stakeholder	**Intention**	**Capability belief**	**Trustworthiness requirement**	**Capability**
End Users, Participants	Send and receive payment transfers safely	Pix is Safe (BEL1)	Security (TR1)	Has security mechanisms
			Confidentiality (TR4)	Make info traffic in protected network
				Encrypt info and messages
			Integrity (TR5)	Encrypt info and messages
			Authenticity (TR6)	Digitally sign messages
			Traceability (TR7)	Use traceability mechanisms

As an alternative, consider a requirements analysis for the Pix case using goal modeling. Given the limited space available, we only present, in Fig. 3, a fragment of goal model for this case using the i^* framework [8]. The model shows the goals that the stakeholders referred to in Table 2 delegate to the Pix Ecosystem (through the i^* dependency relation). Besides dependencies, the goal model depicts the internal perspective of Pix, assisting in the analysis of the system's requirements. Note that security (TR1), availability (TR2), instantaneity (TR3), confidentiality (TR4), integrity (TR5), authenticity (TR6), traceability (TR7), usability (TR8), explainability (TR9), transparency (TR10) were represented as qualities and goals that contribute to (help) the ultimate goal of being trustworthy. Then, for each of them, more specific goals and qualities were identified and related to them by contribution links. For instance, the *protecting information confidentiality* goal helps the achievement of *being secure*.

The goal model also allows the requirements analyst to progressively identify more concrete requirements and solutions and the resources needed to accomplish them. For example, *making the information traffic in a protected network* contributes to the *protecting information confidentiality* goal, and the *protected*

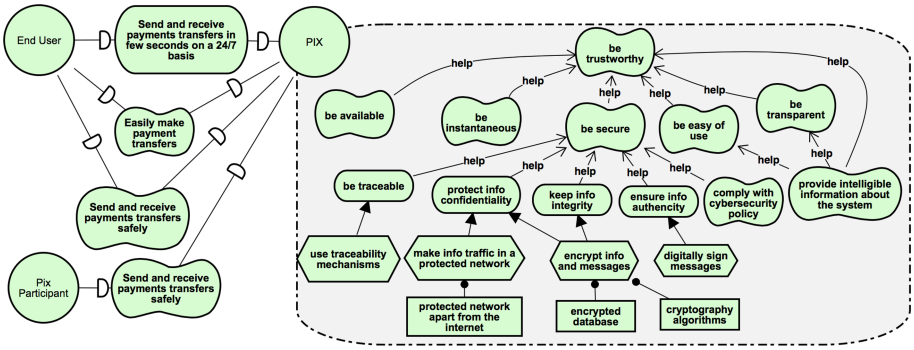

Fig. 3. A fragment of the goal model of the pix ecosystem focusing on security

network itself is a resource needed in this task. To accomplish the higher level of *being secure*, other tasks, qualities and goals are involved. The complete diagrams presenting the case study can be found at https://purl.org/krdb-core/obre. We emphasize that ObRE does not subscribe to a specific RE method, leaving this choice for the requirements analyst, based on their particular preference or skill.

6 Final Remarks

In this paper, we proposed the ObRE method to support requirements elicitation and analysis for challenging requirements, such as trustworthiness, fairness and privacy. The ObRE method has important implications for RE research and practice. For RE research, it suggests first and foremost that for a host of requirements families, including security, privacy, ethicality, trustworthiness and fairness, we need ontologies that capture relevant concepts. Many such ontologies have been proposed for security and privacy. For other families that only recently became prominent because of advent of AI systems, such ontologies are currently being developed. Secondly, we need tools for domain building by instantiating relevant ontologies for a particular system-to-be. Thirdly, for RE practice such tools need to be made available to practitioners who can't be expected to be knowledgeable in these fancy requirements in order to conduct requirements analysis for their next project.

The case study experience confirmed that the ontology-based method proposed here can have a positive impact in the requirements engineering activities of requirements related to high-level societal concerns and goals, such as trustworthiness, and suggests that this approach could be used to systematize the elicitation of other abstract requirements, such as privacy, fairness and ethical requirements. We acknowledge that our case study has some limitations in terms of evaluating the use of ObRE. First, the interviews and analysis were made by the developers of the method. Moreover, only members of the Pix project team were interviewed, and not Pix's stakeholders. However, for the latter, the results shown by the Pix statistics confirm the team's perception regarding Pix's trustworthiness and indicate that they are going in the right direction.

Our research agenda for the future includes a full-fledged evaluation of the method, including surveys and other empirical studies. Moreover, we aim at applying ObRE for other classes of requirements, such as fairness, privacy, and ethical requirements.

Acknowledgments. This work is partially supported by CAPES (PhD grant# 88881.173022/2018-01) and NeXON project (UNIBZ). The authors would like to thank the Central Bank of Brazil for sharing their experience with the Pix project.

References

1. Amaral, G., Guizzardi, R., Guizzardi, G., Mylopoulos, J.: Ontology-based modeling and analysis of trustworthiness requirements: preliminary results. In: Dobbie, G., Frank, U., Kappel, G., Liddle, S.W., Mayr, H.C. (eds.) ER 2020. LNCS, vol. 12400, pp. 342–352. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-62522-1_25
2. Amaral, G., Sales, T.P., Guizzardi, G., Porello, D.: Towards a reference ontology of trust. In: Panetto, H., Debruyne, C., Hepp, M., Lewis, D., Ardagna, C.A., Meersman, R. (eds.) OTM 2019. LNCS, vol. 11877, pp. 3–21. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-33246-4_1
3. Amaral, G., Sales, T.P., Guizzardi, G., Porello, D.: Ontological foundations for trust management: extending the reference ontology of trust. In: 15th International Workshop on Value Modelling and Business Ontologies (2021)
4. Berto, F., Plebani, M.: Ontology and Metaontology: A Contemporary Guide. Bloomsbury Publishing, London (2015)
5. Castelfranchi, C., Falcone, R.: Trust Theory: A Socio-cognitive and Computational Model, vol. 18. Wiley, Hoboken (2010)
6. Chung, L., Nixon, B., Yu, E., Mylopoulos, J.: Non-Functional Requirements in Software Engineering. International Series in Software Engineering, vol. 5. Springer, Heidelberg (2000). https://doi.org/10.1007/978-1-4615-5269-7
7. Cohn, M.: User Stories Applied: For Agile Software Development. Addison Wesley Longman Publishing Co., Inc., Boston (2004)
8. Dalpiaz, F., Franch, X., Horkoff, J.: iStar 2.0 language guide. arXiv:1605.07767 [cs.SE] (2016). dalp-fran-hork-16-istar.pdf
9. Guizzardi, G.: Ontological foundations for structural conceptual models. Telematica Instituut/CTIT (2005)
10. Guizzardi, G., Wagner, G., de Almeida Falbo, R., Guizzardi, R.S.S., Almeida, J.P.A.: Towards ontological foundations for the conceptual modeling of events. In: Ng, W., Storey, V.C., Trujillo, J.C. (eds.) ER 2013. LNCS, vol. 8217, pp. 327–341. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-41924-9_27
11. Guizzardi, R., et al.: An ontological interpretation of non-functional requirements. In: 8th International Conference on Formal Ontology in Information Systems, vol. 14, pp. 344–357 (2014)
12. Hussain, A., Mkpojiogu, E., Kamal, F.: The role of requirements in the success or failure of software projects. EJ Econjournals **6**, 6–7 (2016)
13. Riegelsberger, J., et al.: The mechanics of trust: a framework for research and design. Int. J. Human-Comput. Stud. **62**(3), 381–422 (2005)
14. Van Lamsweerde, A.: Requirements Engineering - From System Goals to UML Models to Software Specifications. Wiley, Chichester (2009)
15. Yin, R.K.: Case Study Research: Design and Methods (Applied Social Research Methods). Sage Publications, Thousand Oaks (2008)