Modelagem de Requisitos Iniciais de Segurança com Requirements4Safety

Moniky Ribeiro[1] [0000-0002-4834-6647] , Jaelson Castro[1][0000-0002-4635-7297] e Ricardo Argenton[2][0000-0002-9688-719x]

[1] Universidade Federal de Pernambuco, Recife, PE, Brasil
[2] Universidade Federal do Vale do São Francisco, Juazeiro, BA, Brasil
{smsr, jbc}@cin.ufpe.br, {ricardo.aramos}@univasf.edu.br

Resumo. Contexto: Os requisitos de segurança de Sistemas Críticos de Segurança (SCSs) devem refletir as descobertas da fase de análise de segurança inicial. Portanto, é fundamental um alinhamento entre as práticas da Engenharia de Requisitos Orientada à Objetivos e as da Engenharia de Segurança. Observa-se o crescente interesse da comunidade de Engenharia de Segurança na adoção da técnica de análise de perigos *STPA* (*System-Theoretic Process Analysis*). **Objetivo:** Este trabalho tem por objetivo propor uma nova abordagem chamada Requirements4Safety para modelagem dos requisitos iniciais de segurança. Ela possibilitará alinhar os requisitos de segurança modelados na linguagem *iStar4Safety*, aos elementos correlatos identificados através do uso da técnica de análise de perigos *STPA*. **Método:** Serão estudadas as técnicas de modelagem *iStar4Safety* e *STPA*. Depois serão definidos passos para integrá-las, sendo estes definidos através do uso de uma notação adequada (ex. BPMN). Requirements4Safety será aplicada na definição dos requisitos de segurança de alguns sistemas críticos. Por último, espera-se que especialistas das áreas de requisitos e segurança avaliem a abordagem. **Resultado**: Espera-se que Requirements4Safety permita o alinhamento de técnicas conhecidas da comunidade de Engenharia de Requisitos (i.e., *iStar4Safety*) e Engenharia de Segurança (i.e., *STPA*). A abordagem será documentada e ilustrada. Também serão disponibilizados os resultados de *surveys* com a opinião de especialistas de Engenharia de Requisitos e de Segurança. **Conclusão:** Com o uso de Requirements4Safety, os requisitos de segurança dos SCs estarão alinhados aos elementos identificados durante a fase de análise preliminar de segurança. A certificação destes tipos de SCs será facilitada.

Palavras-Chave: Sistemas Críticos de Segurança, IStar4Safety, GORE, STPA, UCM.

Nível: Doutorado
Ano de entrada no programa: 2019.1
Data esperada de conclusão: 2024.1

1 Introdução

Nesta seção, é apresentado o contexto deste trabalho, e as principais motivações para sua realização e a metodologia de pesquisa usada. Então, são elencados os objetivos e questão de pesquisa.

1.1 Contexto

Sistemas Críticos de Segurança (SCSs) são sistemas que, caso falhem ou se comportem de maneira inesperada, podem levar à acidentes que resultarão em danos à pessoas ou propriedades, perdas de vidas ou financeiras, assim como danos ao ambiente [10,11].

Preocupações e inserção de conceitos relacionados à segurança (*safety*) devem acontecer desde o início do processo de desenvolvimento do SCS [11,21] estendendo-se até o fim de sua vida útil, tanto no desenvolvimento, quanto na documentação. Segurança é uma propriedade emergente (assim como confiabilidade, *security* e outras), devendo, portanto, ser pensada à luz da teoria de sistemas, que defende que o inteiro é mais do que a soma de suas partes, referindo-se a ideia de que não basta analisar os componentes do sistema isoladamente, mas sim analisar também as interfaces e inter-relacionamentos complexos [10]. Apesar de clássicas, as abordagens tradicionais de análise de segurança não oferecem uma visão de segurança como uma propriedade emergente. Tais abordagens foram criadas antes de sistemas computacionais sequer existirem.

Para o desenvolvimento de sistemas em geral, algumas fases devem ser necessariamente executadas, sendo a fase de Engenharia de Requisitos uma das primeiras e mais importante delas. Isto se deve ao fato de que requisitos mal definidos e/ou faltosos irão inevitavelmente afetar a qualidade do produto desenvolvido para pior [2,3,10,14].

Quanto à modelagem de requisitos quando na fase inicial, é comum o uso de modelos de objetivos [3,16]. As linguagens do tipo GORE (Engenharia de Requisitos Orientada a Objetivos - *Goal Oriented Requirements Engineering*) têm provado ser bastante úteis pois proveem um melhor meio de organizar e justificar os requisitos de software. Exemplos dessas linguagens são iStar, KAOS, iStar4Safety e GRL.

Nesta proposta de qualificação, tem-se a intenção de alinhar a linguagem iStar4Safety, usada durante a fase inicial de requisitos, à uma técnica de análise preliminar de segurança (ex.: STPA, HAZOP, FTA).

É importante salientar que iStar4Safety é uma extensão da linguagem iStar 2.0. Enquanto iStar 2.0 permite a modelagem de requisitos iniciais gerais, iStar4Safety adiciona à linguagem original construtores de segurança que permitem que sejam modelados também requisitos iniciais de segurança [19]. Portanto, ao usar a linguagem iStar4Safety, é possível modelar requisitos iniciais tanto gerais como aqueles específicos de uma análise de segurança inicial.

Nesse sentido a proposta é utilizar a técnica STPA como parte integrante de Requirements4Safety, atuando como uma técnica de análise de segurança preliminar.

A análise STPA permitirá que sejam encontrados aspectos de segurança com uma visão holística do sistema [11]. Assim, pretende-se usar STPA para a análise de segurança e iStar4Safety como técnica de modelagem desses elementos de segurança encontrados. A escolha de STPA se deu pelo fato da técnica tratar segurança como uma propriedade emergente, em detrimento das outras técnicas usada na área de engenharia de segurança.

Outro ponto importante dessa proposta, é a utilização de uma abordagem que permita integrar as duas técnicas pensadas: iStar4Safety e STPA. Nesse sentido, considerando o uso de UCM na abordagem URN, acredita-se que ela seja uma boa candidata a atuar como linguagem integradora das duas técnicas (iStar4Safety e STPA) devido a seu uso em conjunto com GRL [1].

1.2 Motivação

iStar4Safety é uma extensão de iStar 2.0 (linguagem GORE bastante usada para modelagem de requisitos iniciais) [17,18] que permite modelar requisitos, incluindo aqueles relacionados à segurança. iStar4Safety adiciona conceitos relacionados à Análise Preliminar de Segurança à iStar. Logo, iStar4Safety foi escolhida por nós para ser usada neste trabalho.

Faz-se necessário realizar uma análise de segurança mais abrangente visando encontrar elementos que podem não ter sido encontrados em outras análises [7]. Portanto, é importante conduzir análises preliminares de segurança de forma mais abrangente possível, nas fases iniciais de desenvolvimento, buscando identificar requisitos de segurança o mais cedo possível. A escolha pela técnica STPA vem da necessidade de pensar na propriedade de segurança considerando a soma dos componentes e de suas interações, ou seja, como uma propriedade emergente.

Outra necessidade a ser tratada é a criação de uma interface que permita que, a união das duas abordagens aconteça da melhor forma e possa, se possível, contribuir na tarefa de encontrar mais requisitos de segurança do que em abordagens usadas de forma isolada. Uma possível solução proposta será o uso de uma linguagem de mapeamento de cenários, UCM (Mapa de Casos de Uso - *Use Case Maps*), pela mesma já fazer parte de uma abordagem conjunta com outra linguagem orientada a objetivos, GRL e auxiliar na geração de cenários.

Por esses motivos, nesta qualificação propõe-se a utilização da linguagem de modelagem iStar4Safety (que é orientada a objetivos) associada a uma técnica de análise de perigos, STPA.

1.3 Metodologia de Pesquisa

O presente trabalho será desenvolvido através do uso de métodos empíricos e de engenharia apresentados por [8], conforme a visão apresentada na figura 1 que mostra as fases do método de engenharia e cada ponto que pretende-se atender em tal fase.

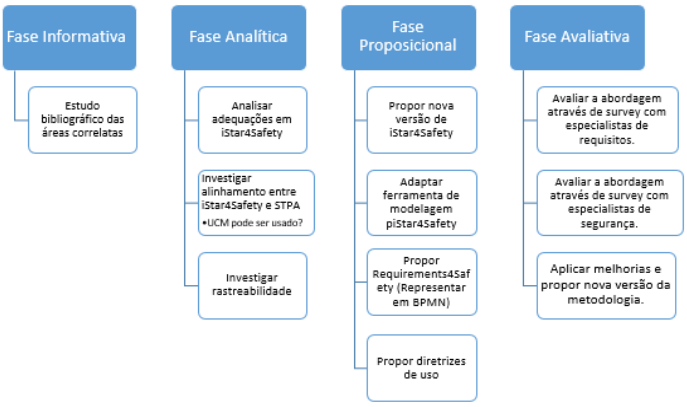

Fig. 1. Fases do método de Engenharia e suas respectivas atividades associadas nesse trabalho. Fonte: (Autora, 2022).

1.4 Objetivos

Baseado no contexto e nas motivações apresentadas, a principal questão de pesquisa, proposta para ser investigada por essa tese é:

> **Questão de Pesquisa:** *Como alinhar os elementos de segurança encontrados em uma análise de segurança preliminar de um sistema à modelagem desenvolvida através de uma linguagem de modelagem de requisitos iniciais orientada a objetivos?*

A fim de responder a essa Questão de Pesquisa, os seguintes objetivos específicos foram definidos:

- O1 - Analisar a necessidade de adequação da linguagem iStar4Safety para a integração com a técnica de análise de perigos STPA.
- O2 - Investigar como pode ser feito o alinhamento entre a linguagem iStar4Safety e a técnica de análise de perigos STPA.
- O3 - Definição dos passos/atividades a serem executados, bem como os artefatos gerados (considerar o uso de BPMN para descrever este processo, já que a linguagem é um padrão definido pela OMG e largamente usada pela indústria [6]).
- O4 - Adaptar uma ferramenta de modelagem para apoiar o uso da nova versão de iStar4Safety, após a definição dos passos/atividades necessários para uso da nova abordagem.
- O5 - Ilustrar o uso da nova abordagem através da modelagem de Sistemas Críticos de Seguranca, tais como Sistema de Bomba de Infusão de Insulina e Robôs Socialmente Assistivos para reabilitação fisioterápica.

– O6 - Avaliar a nova abordagem através de surveys com opiniões de especialistas em Engenharia de Requisitos e engenheiros de segurança.

2 Conceitos Básicos

2.1 STPA

A técnica de análises de perigos STPA (*System-Theoretic Process Analysis*) foi proposta por [11] como parte do modelo STAMP (*System-Theoretic Accident Model and Processes*). STPA apresenta uma nova forma de analisar segurança, pois considera que acidentes podem ser causados pela interação entre os componentes do sistema, mesmo sem ter havido falhas em um componente isoladamente. Os autores chamam a atenção de que cenários onde foram comparados resultados da análise de STPA com outras técnicas como HAZOP [13] ou FTA [10], STPA não só encontrou todos cenários de causas de perigo, como identificou outros novos.

STPA baseia-se na teoria de sistemas [10]. Em STPA, a ideia de propriedade emergente é usada para justificar a necessidade de adicionar a figura do controlador (*controller*) à análise. O controlador irá possibilitar que se avalie ações de controle dos componentes e os respectivos *feedbacks* em relação à segurança do sistema como um todo. O controlador irá garantir restrições no comportamento do sistema [12]. A figura 2 mostra um controlador padrão, conforme usado em STPA.

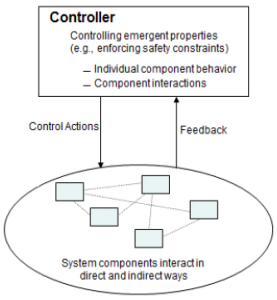

Fig. 2. Modelo padrão de controlador. Fonte: [12].

2.2 iStar4Safety

iStar4Safety é uma linguagem de peso-leve e conservativa [9], portanto mantém todos os construtores e, por consequência, o metamodelo da linguagem original, iStar 2.0. Foi proposta em [17,18,19]. Foram adicionados quatro construtores à linguagem iStar 2.0, um link e uma propriedade, representados pela Figura 3, com a intenção de possibilitar uma modelagem dos diversos aspectos associados a requisitos iniciais de segurança advindos de uma Análise Preliminar de Segurança.

Para mais detalhes sobre a linguagem e exemplos de uso, indica-se o trabalho de dissertação que trata do desenvolvimento da linguagem [17] e os artigos publicados sobre a mesma [18,19].

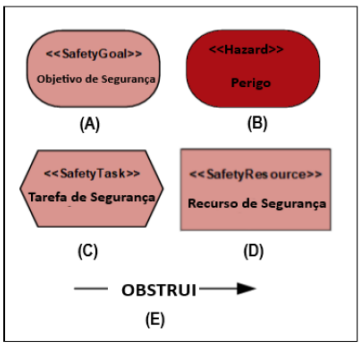

Fig. 3. Construtores adicionados por iStar4Safety à linguagem iStar Fonte: [17].

2.3 UCM

A linguagem UCM (*Use Case Maps*), integra a notação URN que faz parte do padrão ITU-T [15]. Foi proposta por [4] e atualizada em [5]. O foco da linguagem não está em detalhamentos, mas em uma visão geral do sistema. É definida como uma modelagem de caminhos causais que atravessam as estruturas organizacionais [5,1].

UCM vai considerar componentes dos sistemas e seus inter-relacionamentos e comunicações (vide figura 4).

Como pode ser visto na figura 4, um modelo básico de UCM é chamado de mapa. Ele contém três elementos formais, o que classifica a modelagem como peso-leve (*lightweight*): caminhos, caixas de componentes e pontos de responsabilidades. Os caminhos são representados pelas chamadas linhas onduladas (na figura, indicadas pelo dedo indicador), os componentes sendo as caixas retangulares e, por fim, os pontos de responsabilidade são representados pelos marcadores em formato de x's inclusos em toda a extensão das linhas onduladas. As linhas onduladas são marcações indicando a sequência causal de ações e eventos. UCM tem a vantagem de permitir diversos níveis de abstração. Mais detalhe sobre a linguagem pode ser vistos em [1].

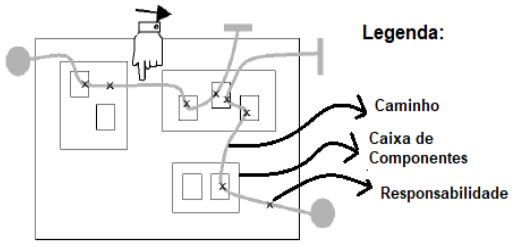

Fig. 4. Mapa de UCM com elementos básicos da linguagem. Fonte: [5].

3 Estado Atual do Trabalho

A primeira fase deste trabalho, relativa ao estudo dos conceitos relacionados, já vendo sendo realizada. A análise da adequação de iStar4Safety para integração com STPA vem sendo feita, a fim de realizar a consolidação dos elementos necessários para a implementação de adaptações, tanto na linguagem como na ferramenta de apoio piStar4Safety. Discussões foram levantadas e uma pesquisa entre trabalhos relacionados foi realizada, o que levou a decisão do uso de UCM como linguagem integradora entre iStar4Safety e UCM. O trabalho passou por seu processo de qualificação e melhorias foram indicadas pelos pesquisadores participantes da banca.

Atualmente tem-se trabalhado em analisar e indicar os pontos necessários a serem realizados para integração entre as linguagens iStar4Safety e STPA de forma mais efetiva, analisando como se fará a interface entre as mesmas.

4 Contribuições Esperadas

O principal objetivo com esse trabalho é propor uma nova abordagem para alinhar os elementos de segurança encontrados em uma análise de segurança preliminar de um sistema, como STPA à modelagem desenvolvida através de uma linguagem de modelagem de requisitos iniciais orientada a objetivos, através da linguagem iStar4Safety.

Além disso, pretende-se contribuir com a realização dos seguintes itens:

- Escolha de uma Técnica de Análise de Perigos apropriada para análise de requisitos de segurança iniciais;
- Atualização da linguagem iStar4Safety;
- Alinhamento entre iStar4Safety e STPA com o uso de UCM;
- Definir os passos/atividades a serem executados para uso de Requirements4Safety, bem como os artefatos gerados;
- Indicar ferramentas que permitam a criação de modelos iStar4Safety e UCM, para uso da nova modelagem;
- Ilustrar o uso da metodologia;
- Avaliar a abordagem Requirements4Safety.

5 Comparação com Trabalhos Relacionados

Em [22], os autores apresentam uma solução para auxiliar a certificação de sistemas FinTech [1], criando um processo de modelagem que pretende unir as vantagens da orientação a objetivos da linguagem GRL com a modelagem de processos da linguagem UCM. Como próximo passo está a expansão do modelo GRL para o modelo UCM. Os

[1] Sistemas Financeiros de Tecnologia

processos de *Use Case Maps* irão modelar os objetivos funcionais descobertos na modelagem GRL, que estão associados aos processos de negócio. Na atual proposta também pretende-se usar modelos intermediários modelados em UCM como ponto para alinhamento com a técnica STPA. É importante salientar que o trabalho de [22] serviu de inspiração também para atender ao objetivo de evoluir os requisitos iniciais (objetivos) fornecidos pela linguagem iStar4Safety. O uso de UCM (*Use Case Maps*) como linguagem de modelagem de processos, em detrimento de outras como BPMN, é também uma proposta inspirada nesse trabalho.

Outra abordagem relacionada a essa proposta, é o trabalho de [20], onde os autores apresentam uma técnica que visa utilizar a linguagem iStar em conjunto com a abordagem de Casos de Uso da UML. Os autores apresentam algumas heurísticas para integrar modelos iStar e Modelos de Caso de Uso, relatando como mapear os elementos entre as linguagens [20].

O trabalho de [23] por sua vez, apresenta a abordagem SARSSi*, que propõe especificar requisitos iniciais de segurança através de seis passos e guias combinando a técnica de análise de perigos STPA, com a técnica de modelagem de requisitos orientada a objetivos iStar, gerando assim uma análise preliminar de segurança. Uma importante diferença dessa abordagem para a técnica Requirements4Safety é que a primeira utiliza iStar na sua versão padrão para modelar elementos de segurança, adicionando tags às descrições dos elementos, enquanto a última usa a versão estendida de iStar 2.0, ou seja, iStar4Safety, que adiciona elementos de forma peso-leve através do uso de cores e estereótipos nos elementos filhos criados. Contudo a abordagem SARSSI* não está detalhada e muitos questionamentos existem. Por exemplo, não está claro como os modelos SD e SR são de fato usados durante a análise de perigos baseada em STPA.

6 Conclusão

Apresenta-se neste trabalho uma proposta de abordagem para modelagem de requisitos de segurança iniciais, chamada Requirements4Safety.

A ideia é alinhar iStar4Safety e STPA, sendo a primeira uma linguagem de modelagem orientada a objetivos que modela requisitos de segurança iniciais relacionados à análise preliminar de segurança e a segunda, uma análise de perigos que tem o objetivo de tratar preocupações sobre a segurança do sistema à luz da teoria de sistemas, gerando uma análise de segurança do sistema.

Foram propostos uma série de objetivos específicos, os quais serão realizados até o período de apresentação da proposta final de tese.

A proposta será avaliada tanto por especialistas da área de Engenharia de Requisitos como de Engenharia de Segurança. Também pretende-se ilustrar o uso da abordagem através da definição de requisitos de segurança de pelo menos dois tipos de Sistemas Críticos.

7 Agradecimentos

Os autores agradecem ao apoio financeiro da Fundação de Amparo à Ciência e Tecnologia do Estado de Pernambuco (FACEPE), da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) e do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq).

Referências

1. Amyot, D., Akhigbea, O., Baslymanc, M., Ghanavatid, S., Ghasemia, M., Hassinec, J., Lessarda, L., Mussbachere, G., Shena, K., Yu, E.: Combining goal modelling with business process modelling two decades of experience with the user requirements notation standard. Enterprise Modelling and Information Systems Architectures 17(2), 1–32 (mar 2022), https://doi.org/10.18417/emisa.17.2.
2. Berry, D.M.: The safety requirements engineering dilemma. In: Proceedings of the 9th International Workshop on Software Specification and Design. pp. 147–. IWSSD '98, IEEE Computer Society, Washington, DC, USA (1998), http://dl.acm.org/citation.cfm?id=857205.858307.
3. Broomfield, E., Chung, P.: Safety assessment and the software requirements specification. Reliability Engineering System Safety 55(3), 295 – 309 (1997). https://doi.org/https://doi.org/10.1016/S0951-8320 (96)00101-9, http:// www.sciencedirect.com/science/article/pii/S0951832096001019.
4. Buhr, R.J.A., Casselman, R.S.: Use case maps for object-oriented systems (1995).
5. Buhr, R.: Use case maps as architectural entities for complex systems. IEEE Transactions on Software Engineering 24(12), 1131–1155 (1998).https://doi.org/10.1109/32.738343.
6. Díaz, E., Panach, J.I., Rueda, S., Vanderdonckt, J.: An empirical study of rules for mapping bpmn models to graphical user interfaces. Multim. Tools Appl. 80, 9813–9848 (2021).
7. Firesmith, D.: Engineering safety requirements, safety constraints, and safetycritical requirements. Journal of object technology 3(3), 27–27 (2004). https://doi.org/10.5381/jot.2004.3.3.c3, http://dx.doi.org/10.5381/jot.2004. 3.3.c3.
8. Glass, R.L.: The software-research crisis. IEEE Softw. 11(6), 42–47 (Nov 1994). https://doi.org/10.1109/52.329400, https://doi.org/10.1109/52.329400.
9. Gonçalves, E., de Oliveira, M.A., Monteiro, I., Castro, J., Araújo, J.: Understanding what is important in istar extension proposals: the viewpoint of researchers. Requirements Engineering (Jul 2018). https://doi.org/10.1007/s00766-018-0302-5, https://doi.org/10.1007/s00766-018-0302-5.
10. Leveson, N.G.: Safeware: System Safety and Computers. ACM, New York, NY, USA (1995).
11. Leveson, N.G.: Engineering a Safer World: Systems Thinking Applied to Safety. Mit Press, Massachusetts, London, England (2011).
12. Leveson, N.G., Thomas, J.P.: STPA Handbook. first edn. (2018).
13. McDermid, J., Nicholson, M., Pumfrey, D., Fenelon, P.: Experience with the application of hazop to computer-based systems. In: COMPASS '95 Proceedings of the Tenth Annual Conference on Computer Assurance Systems Integrity, Software Safety and Process Security'. pp. 37–48 (1995). https://doi.org/10.1109/CMPASS.1995.521885.

14. Medikonda, B.S., Panchumarthy, S.R.: A framework for software safety in safety-critical systems. SIGSOFT Softw. Eng. Notes 34(2), 1–9 (Feb 2009). https://doi.org/10.1145/1507195.1507207, http://doi.acm.org/10.1145/1507195.1507207.
15. Mussbacher, G., Amyot, D., Weiss, M.: Visualizing Early Aspects with Use Case Maps, pp. 105–143. Springer Berlin Heidelberg, Berlin, Heidelberg (2007). https://doi.org/10.1007/978-3-540-75162-55, https://doi.org/10.1007/978-3-540-75162-5_5.
16. Mylopoulos, J., Chung, L., Yu, E.: From object-oriented to goaloriented requirements analysis. Commun. ACM 42(1), 31–37 (Jan 1999). https://doi.org/10.1145/291469.293165, http://doi.acm.org/10.1145/291469.293165.
17. Ribeiro, M.: Desenvolvimento de uma extensão da linguagem de modelagem iStar para Sistemas Críticos de Segurança - iStar4Safety. Master's thesis, Universidade Federal de Pernambuco (feb 2019).
18. Ribeiro, M., Castro, J., Pimentel, J.: istar for safety-critical systems. In: Pimentel, J., Carvallo, J.P., L´opez, L. (eds.) Proceedings of the 12th International i* Workshop co-located with 38th International Conference on Conceptual Modeling (ER 2019), Salvador, Brazil, November 4th, 2019. CEUR Workshop Proceedings, vol. 2490. CEUR-WS.org (2019), http://ceur-ws.org/Vol-2490/paper15.pdf.
19. Ribeiro, M., Castro, J., Vilela, J., Pimentel, J.: istar4safety: Uma extensão de istar para modelagem de requisitos de seguran¸ca em sistemas críticos. In: Lencastre, M., Ridao, M., de Sá Sousa, H.P. (eds.) Anais do WER19 - Workshop em Engenharia de Requisitos, Recife, Brasil, August 13-16, 2019. Editora PUCRio (2019), http://wer.inf.puc-rio.br/WERpapers/artigos/artigos_WER19/WER_2019_paper_22.pdf.
20. Santander, V., Castro, J.: Deriving use cases from organizational modeling. In: Proceedings IEEE Joint International Conference on Requirements Engineering. pp. 32–39 (2002). https://doi.org/10.1109/ICRE.2002.1048503.
21. Scholz, S., Thramboulidis, K.: Integration of model-based engineering with system safety analysis. International Journal of Industrial and Systems Engineering 15(2), 193–215 (2013).
22. Sharifi, S., McLaughlin, P., Amyot, D., Mylopoulos, J.: Goal modeling for fintech certification. In: Guizzardi, R.S.S., Mussbacher, G. (eds.) Proceedings of the Thirteenth International iStar Workshop co-located with 28th IEEE International Requirements Engineering Conference (RE 2020). CEUR Workshop Proceedings, vol. 2641, pp. 73–78. CEUR-WS.org (2020), http://ceur-ws.org/Vol-2641/paper_13.pdf.
23. Vilela, J., Silva, C., Castro, J., Martins, L.E.G., Gorschek, T.: Sarssi*: a safety requirements specification method based on stamp/stpa and i* language. In: Anais do I Brazilian Workshop on Large-scale Critical Systems. pp. 17–24. SBC, Porto Alegre, RS, Brasil (2019). https://doi.org/10.5753/bware.2019.7504, https://sol.sbc.org.br/index.php/bware/article/view/7504.