Requirements4Safety – Construindo uma Técnica para Modelagem de Requisitos Iniciais de Segurança

Moniky Ribeiro[1] [0000-0002-4834-6647] , Jaelson Castro[1][0000-0002-4635-7297], Ricardo Argenton[2][0000-0002-9688-719x], Maria Lencastre[3][0000-0002-8032-8801], Abimael Santos[1][0009-0003-7555-6927]

[1] Universidade Federal de Pernambuco, Recife, PE, Brasil
[2] Universidade Federal do Vale do São Francisco, Juazeiro, BA, Brasil
[3] Universidade de Pernambuco, Recife, PE, Brasil

{smsr, jbc}@cin.ufpe.br, ricardo.aramos@univasf.edu.br, mlpm@ecomp.poli.br, ajfs@cin.ufpe.br

Resumo. Os requisitos de segurança de Sistemas Críticos de Segurança devem refletir as descobertas da fase de Análise de Segurança Inicial. Portanto, é fundamental um alinhamento entre as práticas da Engenharia de Requisitos Orientada a Objetivos e as da Engenharia de Segurança. Observa-se também o crescente interesse da comunidade de Engenharia de Segurança na adoção de técnicas modernas de análise, tais como a técnica de análise *System-Theoretic Process Analysis - STPA*. Este trabalho tem por objetivo apresentar uma proposta de pesquisa de uma nova abordagem para modelagem de requisitos iniciais de segurança chamada **Requirements4Safety**. 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*. Portanto, os requisitos de segurança estarão integrados aos elementos identificados durante a fase de análise preliminar de segurança, o que facilitará a certificação de sistemas críticos por órgãos de regulação. **Requirements4Safety** será aplicada na definição dos requisitos de segurança de alguns Sistemas Críticos, tais como uma bomba de infusão de insulina. Entre as formas de avaliação da proposta está a condução de surveys, envolvendo especialistas das áreas de requisitos e segurança.

Palavras-Chave: Sistemas Críticos de Segurança, iStar4Safety, STPA

1 Introdução

Nesta seção, é apresentado o contexto para realização deste trabalho, a metodologia de pesquisa usada, bem como os objetivos específicos.

Proceedings of the 26th Workshop on Requirements Engineering (WER23), August 15-17, 2023, Porto Alegre, RS, Brazil.
DOI: 10.29327/1298356.26-10

1.1 Contexto

Sistemas Críticos de Segurança (Safety Critical Systems - SCSs) são sistemas que, caso falhem ou se comportem de maneira inesperada, podem levar a acidentes que resultarão em danos às pessoas ou propriedades, perdas de vidas ou financeiras, assim como danos ao ambiente [10,11]. Observa-se que em inglês existem os termos *Safety* e *Security*, enquanto em português ambos os temos são traduzidos para Segurança.

O foco desta pesquisa são os requisitos de segurança do tipo *Safety*. Preocupações e inserção de conceitos relacionados à segurança (*safety*) devem acontecer desde o início do processo de desenvolvimento de SCSs [11,21], estendendo-se até o fim de sua vida útil. Segurança (safety) é uma propriedade emergente (assim como confiabilidade, *security* e outras). As abordagens tradicionais/clássicas de análise de segurança (tais como HAZOP, FTA, FMEA, etc.), não oferecem uma visão de segurança como uma propriedade emergente. Tais abordagens foram criadas antes de sistemas computacionais sequer existirem [10]. Contudo, *safety* pode 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].

A técnica STPA foi proposta recentemente e trata segurança como uma propriedade emergente [12]. É intenção dos proponentes conduzir análises preliminares de segurança da forma mais abrangente possível, já nas fases iniciais de desenvolvimento, buscando identificar requisitos de segurança o mais cedo possível [7]. Portanto, será adotada a técnica STPA, já que neste trabalho considera-se a segurança como sendo uma propriedade emergente, que pode ser definida considerando a soma dos componentes do sistema em questão e das interações entre tais componentes.

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 negativamente a qualidade do produto desenvolvido [2,3,10,14]. O uso de modelos de objetivos tem sido amplamente adotado para a fase inicial de requisitos [3,16]. As linguagens do tipo GORE (*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 orientadas a objetivos incluem *iStar*, *KAOS*, e *GRL*. Percebe-se que a linguagem iStar tem atraído muito interesse na comunidade de requisitos, com mais de uma centena de extensões tendo sido proposta. Em particular, a extensão da linguagem iStar 2.0 chamada iStar4Safety adiciona conceitos relacionados à Análise Preliminar de Segurança [17,18].

Neste trabalho apresenta-se uma proposta de pesquisa que aponta caminhos de pesquisa preliminarmente identificados para o desenvolvimento da abordagem Requirements4Safety**.** Tem-se a intenção de alinhar a linguagem iStar4Safety, que é usada durante a fase inicial de requisitos, à técnica de análise preliminar de segurança STPA. A integração de iStar4Safety e STPA possibilitará encontrar mais requisitos de segurança do que em abordagens usadas de forma isolada. Nesse sentido, considera-se o uso de UCM, que é parte da notação URN [1], para definir os cenários de alinhamento.

1.2 Metodologia de Pesquisa utilizada

O presente trabalho está sendo 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 que seja atendido em tal fase.

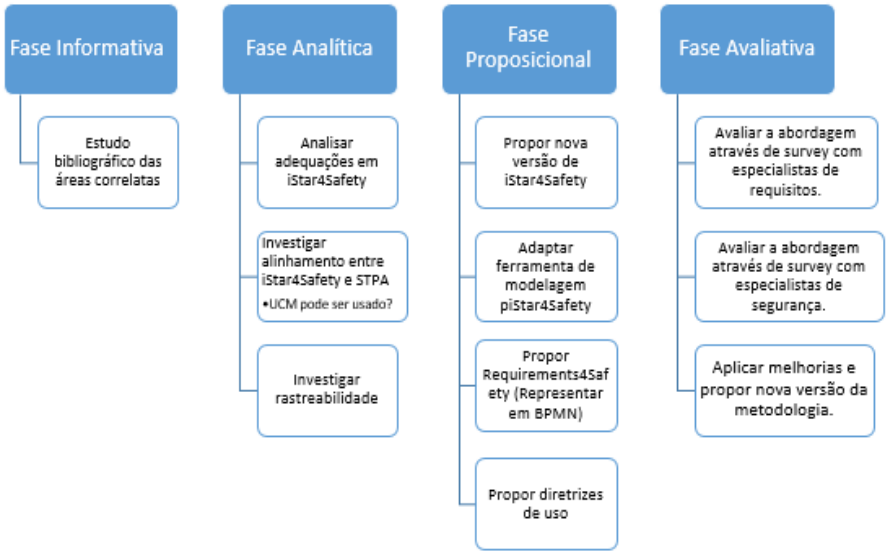

Fig. 1. Fases do método de Engenharia e suas respectivas atividades associadas nesse trabalho. Fonte: (Autores, 2022).

1.3 Objetivos

Baseado no contexto e nas motivações apresentadas, descreve-se a principal questão de pesquisa, proposta para a construção da abordagem Requirements4Safety:

> **Questão de Pesquisa (QP):** *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 esta **QP**, os seguintes objetivos específicos foram definidos:

- O1 - Analisar a necessidade de adequação da linguagem iStar4Safety para a integração com a técnica STPA.
- O2 - Investigar como pode ser feito o alinhamento entre a linguagem iStar4Safety e a técnica de análise de perigos STPA.

- O3 - Definir os 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 - Indicar ferramentas que permitam a criação de modelos iStar4Safety e UCM, para uso da nova modelagem.
- O5 - Ilustrar o uso da nova abordagem através da modelagem de Sistemas Críticos de Segurança, 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

Nesta seção, são apresentadas as técnicas iStar4Safety, STPA e UCM, que serão utilizadas respectivamente para modelagem de requisitos, análise de segurança e descrição de caminhos causais dos cenários possíveis.

2.1 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 2, com a intenção de possibilitar a 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].

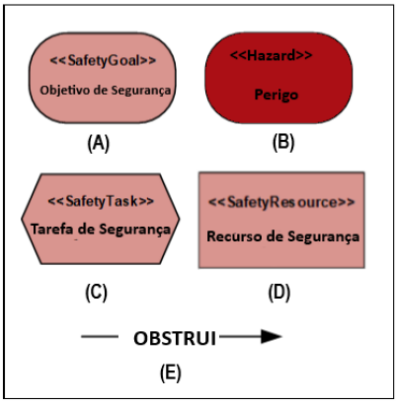

Fig. 2. Construtores adicionados por iStar4Safety à linguagem iStar Fonte: [17].

2.2 STPA

A técnica de análise 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 foram encontrados todos os cenários de causas de perigo, como foram identificados 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 3 mostra um controlador padrão, conforme usado em STPA.

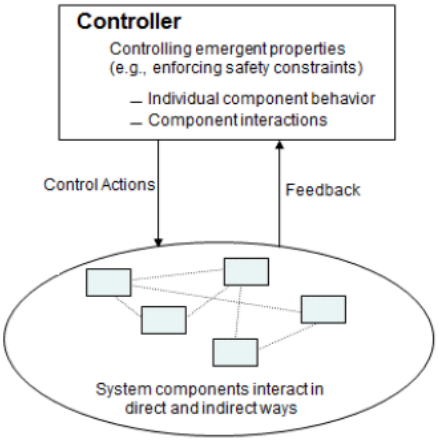

Fig. 3. Modelo padrão de controlador, Fonte: [12].

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 do sistema[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 somente 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].

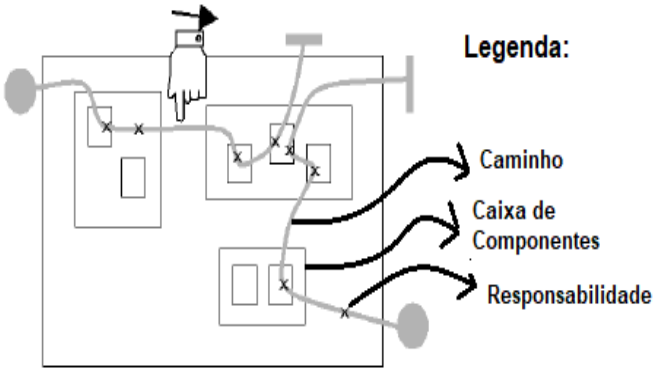

Fig. 2. Mapa de UCM com elementos básicos da linguagem. Fonte: [5].

3 Contribuições Esperadas

O principal objetivo deste trabalho foi apresentar o processo de criação de uma nova abordagem para alinhar os elementos de segurança encontrados em uma Análise Preliminar de Segurança de um sistema, como STPA, com a modelagem desenvolvida através de uma linguagem de modelagem de requisitos iniciais orientada a objetivos, através da linguagem iStar4Safety.

Adicionalmente, tem-se a intenção de colaborar para a concretização dos seguintes itens:

- Escolha de uma Técnica de Análise de Perigos apropriada para Análise de Requisitos de Segurança iniciais;
- Atualização da linguagem iStar4Safety, caso necessário;
- 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.

No próximo sessão, serão detalhadas cada contribuição que espera-se oferecer com a nova abordagem.

4 Construindo a Abordagem Requirements4Safety

Descreve-se a seguir os caminhos preliminarmente identificados para a elaboração da abordagem Requirements4Safety. Vale ressaltar que algumas das etapas propostas ainda necessitarão de trabalhos futuros.

4.1 Escolha de uma Técnica de Análise de Perigos apropriada para análise de requisitos de segurança iniciais:

Visando a construção de Requirements4Safety, foi realizada a revisão do estado da arte relacionado aos temas de Engenharia de Segurança, em particular, investigou-se quais as técnicas de análise de perigos existentes, identificando suas vantagens e limitações. Entre as existentes, escolheu-se a técnica STPA como candidata a alinhamento aos requisitos de segurança modelados em iStar4Safety. A técnica escolhida foi a STPA por ser considerada como tão poderosa como as demais e adotar uma visão holística, ou sistêmica, de segurança. Com o objetivo de desenvolver um trabalho que utilize uma base sólida de conceitos e esteja em alinhamento com pesquisas que já foram e vem sendo desenvolvidas, temas relacionados à segurança foram estudados. Pesquisas relacionadas às técnicas de análises de perigos foram feitas para que fosse encontrada a que mais se adequaria e traria vantagens quando associada a uma técnica de modelagem orientada a objetivos. Além disso, nessa escolha foi considerado também o quanto a análise poderia cobrir com a visão sistêmica de segurança, o que levou os proponentes a optarem por STPA.

4.2 Atualização da linguagem iStar4Safety

iStar4Safety é uma linguagem Orientada a Objetivos proposta com o intuito de modelar requisitos de segurança iniciais em conjunto com os demais requisitos do sistema, adicionando então à modelagem orientada a objetivos, a visão de segurança oriunda da Análise Preliminar de Segurança. Porém, observa-se que é necessário realizar adequações em iStar4Safety, tanto para atender demandas encontradas durante o estudo de avaliação apresentado em [18] e outros feedbacks, como para permitir um alinhamento com as demais técnicas utilizadas na nossa abordagem, tais como UCM e STPA.

Um dos pontos a ser melhorado, é a necessidade de pontuar condições ambientais de forma mais clara. É sabido que, a ocorrência de um perigo deve estar associada a condições ambientais desfavoráveis que complementam os requisitos para a ocorrência de um acidente. Por exemplo, [12] dizem que deve haver um ambiente de pior caso em que necessariamente perigos levem a um acidente. Deve-se porém, atentar ao fato de que apesar de muitas informações sobre o ambiente que circunda o sistema poderem ser identificadas no início do desenvolvimento, algumas informações somente estarão

claras após detalhadas decisões de desenvolvimento e análise de segurança, ou seja, elas emergem posteriormente. Atualmente em iStar4Safety, condições ambientais são consideradas perigos, sendo inclusive representadas pelo elemento "*hazard*". Essa forma de modelagem poderia dificultar a análise, já que não diferencia os dois elementos. Sendo assim, pretendemos analisar a necessidade de mudança e, caso seja necessário, definir uma melhor forma de diferenciar perigos de condições ambientais, levando em conta as especificidades de uma modelagem inicial.

Outro ponto a ser analisado e consequentemente refinado, é a granularidade do perigo. Apesar de não ter sido definido em iStar4Safety, perigos associados diretamente a objetivos de segurança (*Safety Goals*), ou seja, perigos da mais alta granularidade, devem se referir ao sistema em geral e a estados do sistema. A justificativa para isso vem da metodologia STPA que trata assim também do elemento perigo, com o objetivo de não correr o risco de modelar elementos relacionados aos componentes isolados, não tratando segurança como uma propriedade emergente.

As causas de perigo por sua vez, podem sim se referir a componentes e serem de mais baixo nível. Além disso, deve-se atentar ao fato de que perigos devem ser elementos que podem ser controlados/gerenciados pelos projetistas do sistema. Carece de sentido modelar situações que não poderão ser tratadas pela abordagem [12]. Uma forma de solucionar essas questões, seria alterar ou criar uma versão de diretrizes no uso da técnica, pontuando as melhores formas de uso e descrição dos elementos.

Deve-se analisar a necessidade real, e caso necessário, como inserir em iStar4Safety o elemento "restrição" (*constraint*), que não está presente na versão inicial, devido à necessidade de maiores análises [17,18]. Conforme [7] argumenta, restrições dizem respeito a qualquer decisão de engenharia que tenha sido imposta como um requisito. Restrições de segurança, por sua vez, seriam qualquer restrição que especifique uma salvaguarda específica (ex.: mecanismo de segurança na arquitetura, funcionalidade de segurança no projeto, técnica de implementação de segurança). Somado a isso, [24] inseriram o conceito de restrição de segurança como um dos conceitos que deveriam compor a Análise Preliminar de Segurança. Na primeira versão de iStar4Safety tal elemento não foi inserido devido a necessidade de mais estudos sobre a diferenciação entre restrições e sua especialização, restrições de segurança, sendo apontado como trabalho futuro.

Outra possibilidade de melhoria seria a realização de uma análise sobre se a definição do conceito de "Nível de Impacto do Acidente", tratada na versão atual de iStar4Safety como uma propriedade do elemento "*Safety Goal*", deveria ser modelado de outra forma. Essa análise se faz necessária devido aos sujeitos que participaram da avaliação da linguagem terem indicado, em sua maioria, certa insatisfação quanto a forma de modelagem desse conceito [18]. No experimento realizado observou-se uma quantidade significativa de erros quanto ao seu uso. De fato, o nível de impacto do acidente foi omitido por grande parte dos participantes do experimento. Outra questão a ser melhor analisada seria se qualidades (softgoals) poderiam ser usadas para tratar de aspectos de segurança do tipo *safety*. Portanto é necessário avaliar melhor se alguma modificação se faz necessária na linguagem iStar4Safety.

4.3 Alinhamento entre iStar4Safety e STPA com o uso de UCM

STPA é uma abordagem que utiliza a teoria de sistemas na busca por requisitos de segurança, considerando a propriedade segurança como emergente [12]. Através do uso do modelo de loop de controle, STPA pode explicar e antecipar interações complexas entre sistemas e humanos que podem levar a acidentes. Segundo [12,25,26], STPA permite encontrar a mesma quantidade ou até mais elementos de segurança do que as técnicas de análise de perigos clássicas, como FTA e HAZOP. Por ser uma abordagem iterativa, STPA permite uma evolução da modelagem dos perigos (e demais elementos) de acordo com o momento do desenvolvimento. Neste trabalho pretende-se utilizá-la ainda na fase inicial do processo de desenvolvimento. Apesar desta fase inicial, em geral, não dispor ainda de muita documentação e informações detalhadas sobre o sistema a ser desenvolvido, pode-se tomar exemplos de sistemas já existentes para a definição da arquitetura inicial [7]. Desta forma pode-se definir a estrutura de controle do sistema, possibilitando o uso de STPA já em fases iniciais do desenvolvimento. Isso permite e abre portas para a ideia de alinhar iStar4Safety e STPA, pois permite que as abordagens sejam usadas em níveis de detalhamento de acordo com a necessidade do *stakeholder*.

Para um melhor alinhamento entre iStar4Safety e STPA, será considerado o uso de uma etapa intermediária que permita uma melhor transição entre as duas abordagens. As investigações conduzidas nos levam a proposta de utilização de Use Case Maps (UCM) como o elo entre iStar4SAfety e STPA. Isso se dá devido à possibilidade de criação de cenários em UCM e a utilização de componentes. Esse ponto será mais esmiuçado para uma melhor definição de se UCM será realmente usado ou outra abordagem poderia ser mais adequada.

4.4 Definir os passos/atividades a serem executados para uso de Requirements4Safety, bem como os artefatos gerados

Deve-se definir o processo para uso da nova abordagem, incluindo os passos a serem tomados e atividades necessárias para uma modelagem de requisitos de segurança que atenda às demandas da abordagem criada. Pretende-se modelar tais diagramas em uma linguagem de modelagem de processos tal como BPMN.

4.5 Indicar ferramentas que permitam a criação de modelos iStar4Safety e UCM, para uso da nova modelagem

Faz-se importante a busca pela indicação de ferramentas de modelagem que permita a criação semi-automatizada ou automatizada dos modelos de iStar4Safety, STPA e UCM. É sabido que o uso de uma ferramenta pode facilitar e incentivar o uso de uma linguagem [9].

Sabe-se que apesar de piStar4Safety já ser a ferramenta de apoio a modelagem da versão atual de iStar4Safety, devido às alterações que deseja-se fazer na linguagem de modelagem (possibilidade de uma versão 2.0 de iStar4Safety), pode ser necessário

adaptar a ferramenta existente para apoiar as mudanças realizadas. Porém, não será escopo deste trabalho tais alterações.

Por sua vez, as ferramentas disponíveis para modelagem de UCM (jUCMNav) e STPA (Ex.. Cairis, RM Studio) devem ser analisadas e avaliadas para definir se as mesmas podem ser usadas como são atualmente para a modelagem de Requirements4Safety, ou se indicações de modificações precisam ser feitas.

Não está no escopo deste trabalho integrar as ferramentas existentes, mas sim indicar as modificações necessárias.

4.6 Ilustrar o uso da metodologia

A fim de proporcionar um melhor entendimento da abordagem e ilustrar sua utilidade e usabilidade, Requirements4Safety será aplicada na definição de requisitos de segurança de alguns Sistemas Críticos tais como Sistema de Infusão de Bomba de Insulina e um Sistema Robótico Socialmente Assistivo.

4.7 Avaliar a abordagem Requirements4Safety

A abordagem Requirements4Safety será avaliada. Os resultados dessas avaliações serão usados para melhorias/adaptações e/ou definições de trabalhos futuros.

5 Comparação com Trabalhos Relacionados

Em [22], os autores apresentam uma solução para auxiliar a certificação de sistemas FinTech (Sistemas Financeiros de Tecnologia), 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 do trabalho, está a expansão do modelo GRL para o modelo UCM. Os processos de *Use Case Maps* irão modelar os objetivos funcionais descobertos na modelagem GRL, que estão associados aos processos de negócio. Na atual proposta 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, criando uma extensão peso-leve, através do uso de diferentes cores e também de 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

De acordo com a recente literatura, é necessário que os Engenheiros de Requisitos e os Engenheiros de Segurança sejam capazes de unir esforços para melhorar a segurança dos Sistemas Críticos [27]. Este trabalho descreveu os caminhos identificados para a elaboração de uma nova proposta para modelagem de requisitos de segurança iniciais, chamada Requirements4Safety. O trabalho está sendo desenvolvido através do uso de métodos empíricos e de engenharia que incluem 4 fases: Informativa, Analítica, Proposicional e Avaliativa.

A ideia é alinhar duas técnicas existentes, iStar4Safety e STPA, através de uma abordagem que trata de sequências causais de ações e eventos. A linguagem de modelagem orientada a objetivos iStar4Safety será utilizada para modelar requisitos de segurança iniciais relacionados à Análise Preliminar de Segurança que será por sua vez conduzida com a técnica STPA, que trata de preocupações sobre a segurança do sistema à luz da teoria de sistemas. Enquanto os mapas descritos em UCM, descreverão as sequencias causais de ações e eventos.

Foram propostos uma série de objetivos específicos, os quais vem sendo realizados para a construção da abordagem. No momento vem sendo trabalhada a fase de ilustração do uso da abordagem através da definição de requisitos de segurança de um Sistema Crítico.

Uma das limitações da abordagem é que o uso da análise STPA requer uma descrição arquitetural do sistema, o que pode ser difícil de obter nos estágios iniciais do desenvolvimento de Sistemas Críticos. Será examinado o reuso de arquiteturas similares de outros Sistemas Críticos no mesmo domínio, porém isto poderá restringir a aplicabilidade da proposta.

No futuro, a efetividade da abordagem será avaliada, tanto por especialistas da área de Engenharia de Requisitos como de Engenharia de Segurança.

7 Agradecimentos

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

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 goal oriented 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.
24. Vilela, J., Castro, J., Martins, L.E.G., Gorschek, T.: Integration between requirements engineering and safety analysis. J. Syst. Softw. 125(C), 68–92 (Mar 2017). https://doi.org/10.1016/j.jss.2016.11.031, https://doi.org/10.1016/j.jss.2016.11.031
25. Robertson, J.: Systems Theoretic Process Analysis Applied To Manned-Unmanned Teaming. Master's thesis, Massachusetts Institute of Technology, https://dspace.mit.edu/bitstream/handle/1721.1/122516/1121277240MIT.pdf?sequence=1&isAllowed=y (feb 2019)
26. Fugivara, S., Merladet, A., Lahoz, C.: Stpa analysis of brazilian sounding rockets launching operations. Microgravity Sci. Technol. 33(43) (jun 2021), https://doi.org/10.1007/s12217-021-09871-x.
27. Martins, L. E. G, Gorschek, T. Requirements Engineering for Safety-Critical Systems, River Publishers Series in Software Engineering, Denmark (2021).