Elicitação de Requisitos em Sistemas Críticos de Segurança

Sthéfanie Dal Magro[1] (mestranda), Jaelson Castro (orientador)[1]
[1]Mestrado Acadêmico em Ciência da Computação
Programa de Pós-Graduação em Ciência da Computação
Universidade Federal de Pernambuco (UFPE)
Av. Jornalista Anibal Fernandes, s/n – CEP 50740-560 – Recife – PE – Brasil
Ingresso: 03/2019 – Previsão de Defesa 03/2021
{sdm2, jbc}@cin.ufpe.br;

Resumo. Contexto: *Sistemas Críticos de Segurança (SCSs) são considerados sistemas que caso falhem, podem levar à perda de vida, perdas financeiras e danos ao meio ambiente. A Engenharia de Requisitos é essencial no desenvolvimento destes sistemas, tendo em vista que a utilização de requisitos inadequados ou incompreendidos são reconhecidos como a principal causa de acidentes e catástrofes relacionados com a segurança. Portanto, os requisitos iniciais de segurança dos SCSs devem ser cuidadosamente identificados e adequadamente modelados. No entanto, a literatura apresenta poucas técnicas de elicitação e modelagem de requisitos voltadas para o domínio de SCSs.* ***Objetivo****: Esta pesquisa propõe o desenvolvimento de uma técnica para elicitação de requisitos no contexto de sistemas críticos de segurança que posteriormente serão modelados através da notação iStar4Safety.* ***Método:*** *Inicialmente, será realizado um levantamento bibliográfico com objetivo de investigar as técnicas de elicitação de requisitos existentes no domínio dos SCSs. A partir deste levantamento bibliográfico, será proposta uma nova técnica para descoberta de requisitos para Sistemas Críticos de Segurança. Para validar a técnica proposta será realizado um quase-experimento.* ***Resultados esperados****: Com este trabalho definiremos uma técnica de elicitação de requisitos para SCSs que permitirá a modelagem dos requisitos de segurança através de uma extensão de segurança da linguagem iStar.* ***Conclusão:*** *Os resultados encontrados irão auxiliar no processo de descoberta e modelagem de requisitos no contexto de sistemas críticos de segurança. Com isso, pretendemos contribuir de maneira positiva no desenvolvimento destes sistemas, buscando mitigar perigos e prevenir acidentes.*

Palavras chave: *Engenharia de requisitos, sistemas críticos de segurança, elicitação de requisitos.*

Eventos CBSoft: *SBES*

1. Introdução e Caracterização do Problema

Sistemas críticos de segurança são compostos por um conjunto de hardware, software, processos, dados e pessoas [Du *et al* 2014], que caso falhem, podem resultar em acidentes que provocam danos ao meio ambiente, perdas financeiras, ferimentos e até a perda de vidas [Leveson 2011].

As atividades e o processo da engenharia de requisitos são essenciais no desenvolvimento de SCSs, buscando evitar a introdução de defeitos, além de mal-entendidos entre engenheiros e desenvolvedores [Leveson 2011]. Requisitos iniciais vagos, ambiguidade na especificação de requisitos e confusão entre métodos e ferramentas afetam severamente a qualidade dos sistemas críticos de segurança [Vilela *et al* 2020]. Portanto, é necessário que a engenharia de requisitos caminhe lado a lado com a engenharia de segurança, permitindo que os *stakeholders* possam analisar os potenciais perigos do sistema em questão.

O processo de levantamento de requisitos para Sistemas Críticos de Segurança é bem complexo, uma vez que é necessário capturar os comportamentos de todos os subsistemas envolvidos, bem como integrar diversas restrições [Broomfield and Chung 1997]. Contudo, verificamos que a literatura apresenta poucas técnicas de elicitação de requisitos específicas ao domínio de sistemas críticos de segurança.

De acordo com [Raspoting *et al* 2012] é indispensável a utilização de linguagens de modelagem para o desenvolvimento de sistemas de informação, uma vez que estas linguagens permitem uma melhor visualização e compreensão dos requisitos levantados. É de extrema importância que os requisitos sejam levantados, modelados e especificados corretamente, pois erros na especificação de requisitos podem trazer alguns problemas, como exemplo: atraso na entrega do sistema, falta de confiabilidade no uso do sistema e maior custo no desenvolvimento e posteriormente na manutenção. Ademais, o custo de correção dos erros de requisitos é muito maior do que a correção de erros que aparecem nos estágios posteriores do processo de desenvolvimento [Kotonya and Sommervile 1998].

Diante do cenário apresentado, entende-se como relevante um estudo que possibilite a descoberta de requisitos de segurança o mais completo possível, isento de erros, não ambíguos e que permitam a mitigação dos potenciais perigoso oriundos do SCSs, bem como a especificação destes requisitos em uma linguagem de modelagem apropriada.

Assim, este trabalho tem como objetivo principal desenvolver uma técnica para descoberta de requisitos no domínio de SCSs, baseada em entrevistas, buscando identificar requisitos iniciais de segurança com qualidade, que poderão ser utilizados para mitigar os perigos oriundos dos Sistemas Críticos de Segurança. Ademais, a técnica proposta irá auxiliar na especificação de requisitos através da utilização da iStar4Safety [Ribeiro 2019], uma extensão da popular notação iStar [Yu 1995] que foi estendida para o contexto de SCSs. A fim de avaliar a técnica proposta será realizado um quase-experimento com os alunos da disciplina de Engenharia de Requisitos do Programa de Pós-Graduação em Ciência da Computação na Universidade Federal de Pernambuco.

2. Fundamentação Teórica

2.1. Sistemas Críticos de Segurança

Sistemas críticos de segurança (SCSs), do inglês *Safety Critical Systems*, são aqueles sistemas cuja falha pode resultar em perda de vida, danos significativos à propriedade ou ao meio ambiente, podendo ser encontrados em diversas áreas de aplicação, tais como: dispositivos médicos, controle de voo de aeronaves, armas, sistemas nucleares, sistemas robóticos [Knight 2002].

O software é uma parte importante nos sistemas críticos, no entanto, está se tornando uma fonte de riscos, contribuindo para morte e ferimentos em incidentes e catástrofes ligadas à segurança, pois além de controlar um número crescente de funções tradicionais e inovadoras o software também está lidando com funções que antes eram controladas por seres humanos, tornando-se uma importante fonte de riscos e perigos, tendo em vista que a transmissão de instruções erradas ao hardware, através de atuadores, pode levar à acidentes e lesão de pessoas [Vilela *et al* 2020].

É importante considerar a alteração do modo de desenvolvimento tradicional dos SCSs, buscando começar a considerar as preocupações de segurança no início do processo, através da utilização da Engenharia de Requisitos. Sendo assim, para uma correta especificação dos requisitos de segurança é necessário que previamente seja realizada uma análise de perigos, ou seja, a identificação de todos os perigos que possam ocorrer com o sistema, para que posteriormente sejam definidos os requisitos que visem mitigar e/ou minimizar estes perigos. Portanto, na etapa de especificação de requisitos de segurança em SCSs é importante que fatores potenciais de perigo sejam visualizados e que as medidas de proteção que sejam tomadas [Du *et al* 2014].

Diante do exposto, mostra-se essencial a preocupação com a segurança desde o início do desenvolvimento de sistemas críticos, tendo em vista que é a única possibilidade para alcançar altos níveis de segurança.

2.2. Engenharia de Requisitos

Requisitos são definidos durante os primeiros estágios de desenvolvimento do sistema e são responsáveis por descrever as funcionalidades do sistema, os serviços oferecidos, informações de domínio de aplicativo, restrições de operação do sistema ou especificações de um sistema, podendo variar de acordo com a necessidade dos clientes [Kotonya and Sommervile 1998].

Na literatura podem ser encontradas diversas classificações para o processo de Engenharia de Requisitos, no entanto, neste trabalho, iremos utilizar a classificação de [Kotonya and Sommervile 1998] que inclui várias atividades de alto nível: Elicitação, Análise e Negociação, Documentação, Validação e Gerenciamento dos Requisitos.

2.2.1 Elicitação de Requisitos

A etapa de elicitação consiste na descoberta de requisitos através do trabalho de engenheiros de requisitos e desenvolvedores juntamente com os clientes e usuários finais, a fim de descobrir qual o problema que o software deverá resolver, bem como os serviços do sistema, o desempenho necessário e as restrições [Kotonya and Sommervile 1998]. Para tanto, esta etapa sugere a externalização do conhecimento entre os *stakeholders*, de

modo que os engenheiros consigam levantar os requisitos necessários para o desenvolvimento do software.

Para identificar todas as informações acerca do domínio da aplicação e do problema específico a ser resolvido, os engenheiros de requisitos necessitam utilizar diferentes técnicas para o levantamento dos requisitos, dentre elas: entrevistas, observação em conjunto com análise social, reuso de requisitos, cenários, métodos *soft systems,* dentre outras.

2.2.2 Documentação de Requisitos com iStar4Safety

Técnicas de modelagem de requisitos permitem a compreensão e representação do conhecimento necessário para as fases iniciais da Engenharia de Requisitos. O iStar [Yu 1995] é uma linguagem de modelagem baseada em objetivos utilizada pela Engenharia de Requisitos que permite a representação dos requisitos iniciais do sistema.

[Ribeiro 2019] desenvolveu uma extensão do iStar voltada para a modelagem de requisitos iniciais de segurança, denominada iStar4Safety. Além da representação dos requisitos do sistema através da utilização dos construtores padrões do iStar, a iStar4Safety permite a representação gráfica dos requisitos iniciais de segurança, através da adição de outros construtores gráficos, específicos para o domínio, sendo eles: Objetivo de Segurança, Tarefa de Segurança, Recurso de Segurança, Perigo e o *link* Obstrui.

Para o desenvolvimento desta extensão foram utilizados alguns conceitos relacionados à segurança, sendo eles: acidente, perigo, causa de perigo, condição ambiental, requisitos funcionais de segurança, estratégias de segurança, recursos e nível de impacto do acidente. Assim sendo, o desenvolvimento da técnica de elicitação de requisitos proposta neste trabalho irá se basear nestes conceitos, uma vez que visa permitir o processo de levantamento de requisitos de segurança para posterior documentação utilizando a extensão iStar4Safety, que por sua vez é de fácil entendimento e utilização.

3. Trabalhos Relacionados

Alguns trabalhos relacionados nos auxiliaram na aquisição do conhecimento necessário para o desenvolvimento do nosso projeto de pesquisa, como exemplo, o trabalho de [Vilela *et al* 2017] que define, através de uma revisão sistemática da literatura, aspectos que integram a engenharia de requisitos e a engenharia de segurança. O trabalho busca padronizar os termos utilizados nesta área, e foi de extrema importância para a compreensão dos termos utilizados na engenharia de segurança e que devem ser aplicados na fase inicial da engenharia de requisitos, bem como quais técnicas que podem ser utilizadas para análise de segurança e de risco.

Outro trabalho primordial para a compreensão de termos utilizados do domínio de engenharia de segurança foi o trabalho de [Vilela *et al* 2018], que fornece um meta-modelo de segurança que poderá ser utilizado pelos engenheiros de requisitos no início do processo de desenvolvimento do sistema. Sendo assim, este trabalho nos auxiliou no levantamento de informações necessárias para aquisição de conhecimento e construção da técnica de elicitação de requisitos para o domínio de SCSs.

A literatura apresenta poucas técnicas de elicitação de requisitos no domínio de sistemas críticos de segurança. Pode-se citar três técnicas: [Du *et al* 2014], [Martins e De Oliveira 2014] e [Provenzano *et al* 2017]. A proposta de [Du *et al* 2014] é baseada na utilização de cenários e permite o refinamento da análise de segurança em comportamentos de software através de cenários específicos. Ela utiliza um método de análise de segurança, a *Fault Tree Analysis* (FTA) utilizado para descobrir requisitos de segurança combinado com cenários, de modo que se torne possível que a análise de segurança expresse com precisão os estados perigosos do software.

O trabalho de [Martins e De Oliveira 2014] tem como objetivo derivar requisitos funcionais de segurança a partir da construção de uma FTA. Inicialmente devem ser identificadas as situações de perigo do sistema em análise. A partir de então, deve ser construído a FTA da situação de perigo, para que posteriormente as folhas da árvore de falhas sejam classificadas de acordo com a causa da falha: software, eletrônica ou mecânica. A cada falha identificada devem ser descritos requisitos funcionais de segurança do tipo "*should*" ou "*should not*".

Já [Provenzano *et al* 2017] fornecem uma abordagem heurística para o levantamento de requisitos de segurança baseada em uma ontologia. Inicialmente, devem ser levantados os perigos de um determinado sistema, para que possam ser classificados de acordo com uma ontologia denominada *Hazard Ontology* (HO). A partir da identificação e classificação destes perigos, é iniciada a abordagem heurística para a elicitação dos requisitos de segurança, constituída por três atividades.

O nosso trabalho diferencia-se desses, pois além de propor o desenvolvimento de uma técnica de elicitação de requisitos de segurança, propõe também a integração desta técnica com a linguagem iStar4Safety de modelagem de requisitos orientada à objetivos. Ademais, nossa proposta será constituída por um formulário de perguntas a ser realizado através de uma entrevista estruturada, que buscará entender o ambiente de desenvolvimento do SCSs, os atores envolvidos em sua utilização e os perigos atrelados a estes sistemas.

4. Metodologia

A fim de atingir nosso objetivo, o presente trabalho será conduzido em quatro etapas (fig. 1) sendo elas: Aquisição de conhecimento através de um levantamento bibliográfico, identificação das técnicas de elicitação para SCSs já existentes na literatura, desenvolvimento de uma nova técnica e por fim, a avaliação dela.

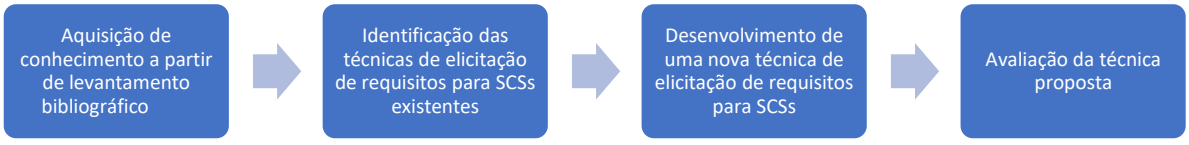

Figura 1. Etapas para Execução do Trabalho

Para aquisição de conhecimento acerca dos temas propostos, foi realizado um levantamento bibliográfico através de bibliotecas digitais, sendo elas: ACM Digital Library, IEEE Xplore Digital Library, ScienceDirect e Springer, buscando encontrar artigos e livros relevantes para a construção da dissertação.

A partir das informações adquiridas no levantamento bibliográfico, foi possível investigar quais técnicas de descoberta de requisitos no contexto de SCSs existem na literatura. Atualmente, está sendo elaborada uma nova técnica de elicitação que visa auxiliar a identificação de requisitos iniciais de segurança e sua posterior especificação através da notação iStar4Safety.

Para avaliar a eficácia da técnica proposta, será conduzido um quase-experimento com estudantes da disciplina de Engenharia de Requisitos no programa de pós-graduação em Ciência da Computação da Universidade Federal de Pernambuco.

O quase-experimento irá analisar a qualidade da elicitação e especificação dos requisitos de segurança na notação iStar4Safety com e sem a utilização da técnica proposta por nós. Para tanto, foram definidas as seguintes hipóteses e variáveis:

Hipótese principal a ser testada (H1): A adoção da técnica proposta melhora a qualidade da especificação de requisitos no contexto de SCSs.

Hipótese Nula (H0): A adoção da técnica proposta não melhora a qualidade da especificação de requisitos no contexto de SCSs.

Variável Independente: Aplicação da técnica para descoberta de requisitos em sistemas críticos de segurança.

Variável Dependente: A qualidade na especificação de requisitos em sistemas críticos de segurança.

5. Estado Atual do Trabalho

As duas primeiras etapas do trabalho que constituíram na aquisição de conhecimento através de um levantamento bibliográfico da literatura e identificação das técnicas de elicitação de requisitos para SCSs já foram finalizadas. O levantamento bibliográfico permitiu a visualização do estado-da-arte da engenharia de requisitos no domínio de sistemas críticos de segurança, a integração de engenharia de segurança e engenharia de requisitos.

Atualmente, estamos trabalhando na terceira etapa da pesquisa, que consiste na criação de uma nova técnica de levantamento de requisitos de segurança. Esta técnica consistirá em um roteiro para realização de entrevistas semiestruturadas, abrangendo conceitos atrelados à segurança. Ainda estamos em uma versão piloto, elaborando as perguntas que serão realizadas e dividindo-as por etapas, sendo elas: definição do perfil do usuário e do cliente, definição do perfil da empresa e dos detalhes da empresa, descoberta dos atores relacionados ao sistema, descoberta e catalogação dos perigos e atrelados ao sistema. Vale ressaltar que este roteiro de entrevista está atrelado à especificação de requisitos da notação iStar4Safety.

Após concluirmos o desenvolvimento do roteiro da entrevista, que será a nossa técnica de elicitação para SCSs, iremos realizar o quase-experimento para avaliar a técnica.

6. Resultados Esperados

Este trabalho tem como objetivo a criação de uma técnica, baseada em entrevistas, que auxiliará no processo de descoberta de requisitos de segurança em sistemas críticos de

segurança e que permitirá a modelagem de requisitos através de uma extensão do iStar. Sendo assim, buscaremos detalhar ao máximo a técnica de elicitação proposta, bem como especificá-los na linguagem de modelagem alvo, que é a iStar4Safety.

Esperamos que a nossa técnica permita uma melhor especificação de requisitos para a notação iStar4Safety, sempre buscando mitigar os perigos oriundos de sistemas críticos de segurança, evitando a ocorrência de acidentes que possam causas perdas de vidas, financeiras e ambientais.

7. Referências

Broomfield, E. J.; Chung, P. W. H. (1997). "Safety assessment and the software requirements specification". In *Reliability Engineering & System Safety*, v. 55, n. 3, p. 295-309, 1997.

Du, J., Wang, J., Feng, X. (2014). A safety requirement elicitation technique of safety-critical system based on scenario. In *Intelligent Computing Theory*, p.127–136.

Knight, J. C. (2002). Safety critical systems. In *Proceedings of the 24th International Conference on Software Engineering - ICSE '02.*

Kotonya, G and Sommervile, I. (1998). Requirements Engineering: Processes and Techniques, John Wiley & Sons, Inc., New York.

Leveson, N. (2011). Engineering a Safer World: Systems Thinking Applied to Safety. Mit Press.

Martins, L.E.G, De Oliveira, T. (2014). A case study using a protocol to derive safety functional requirements from fault tree analysis. In: *2014 IEEE 22nd International Requirements Engineering Conference (RE*). IEEE, p. 412-419.

Provenzano, L. et al. (2017) An Ontological Approach to Elicit Safety Requirements. In: *24th Asia-Pacific Software Engineering Conference (APSEC).* IEEE, p. 713-718.

Raspoting, C., Karpati, P., Katta, V. (2012). A combined process for elicitation and analysis of safety and security requirements. *In: Enterprise, business-process and information systems modeling*. Springer, Berlin, Heidelberg, p. 347-361.

Ribeiro, S. M. S. (2019) Desenvolvimento de uma extensão da linguagem de modelagem iStar para sistemas críticos de segurança – iStar4Safety. Dissertação (Mestrado em Ciência da Computação) – Universidade Federal de Pernambuco, Recife.

Sommervile, l. (2011). Engenharia de Software, Pearson Prentice Hall, São Paulo.

Vilela, J. Castro, J. Martins, L. E. G. and Gorschek, T, (2017). Integration between requirements engineering and safety analysis: A systematic literature review. In *Journal of Systems and Software*, Vol. 125, p. 68-92.

Vilela, J., Castro, J., Martins, L. E. G., & Gorschek, T. (2018). Safe-RE. *In Proceedings of the XXXII Brazilian Symposium on Software Engineering*, p. 196-201.

Vilela, J. et al. (2020) Safety Practices in Requirements Engineering: The Uni-REPM Safety Module. In *IEEE Transactions on Software Engineering*, vol. 46, no. 3, p. 222-250.

Yu, E. (1995) Modelling Strategic Relationships for Process Reengineering, Ph.D. thesis, also Tech. Report DKBS-TR94-6, Dept. of Computer Science, University of Toronto.