UNIVERSIDADE FEDERAL DE PERNAMBUCO

MESTRADO EM CIÊNCIA DA COMPUTAÇÃO
CENTRO DE INFORMÁTICA
2016.2

Engenharia de Requisitos para Sistemas Críticos

Aluna: Sarah Moniky Silva {smsr@cin.ufpe.br}
Orientador: Jaelson Brelaz de Castro {jbc@cin.ufpe.br}

Recife, 30 de Janeiro de 2017

Engenharia de Requisitos para Sistemas Críticos

Sarah Moniky Silva Ribeiro

Monografia desenvolvida junto ao Curso de Mestrado em Ciência da Computação da Universidade Federal de Pernambuco como requisito parcial à obtenção dos créditos referentes à disciplina de Engenharia de Requisitos – IN1020

Professor da disciplina: Jaelson Brelaz de Castro

Recife

2017

“Homens fracos acreditam na sorte. Homens fortes acreditam em causa e efeito”

Ralph Waldo Emerson

RESUMO

A engenharia de requisitos é uma área que objetiva definir especificações para o software, a fim de que sejam criados sistemas mais confiáveis e responsivos. Em se tratando de sistemas críticos, essa fase se torna um ponto crucial devido à necessidade maior de garantia de segurança e confiabilidade. Tendo esses pontos em mente, apresenta-se nesse trabalho alguns conceitos de sistemas críticos e engenharia de requisitos. Apresentamos também a união dessas duas fases e a necessidade de unir as engenharias de requisitos e de segurança a fim de obter sistemas críticos de mais qualidade e confiabilidade.

Palavras-chave: engenharia de requisitos, engenharia de segurança, sistemas críticos

ABSTRACT

Requirements engineering is an area that aims to define specifications for the software in order to create more reliable and responsive systems. When it comes to critical systems, this phase becomes a crucial point due to the greater need for security and reliability assurance. Thus, some concepts of critical systems and requirements engineering are presented in this paper. We also present the union of these two phases and the need to combine requirements and safety engineering in order to obtain critical systems of more quality and reliability.

Keywords: Requirements Engineering, Critical Systems, Security Engineering, Safety-Critical Systems

LISTA DE FIGURAS

SUMÁRIO

1. INTRODUÇÃO

Sistemas de softwares tem sido usados em diversos setores da sociedade. Seja no uso doméstico ou por grandes empresas, um certo nível de segurança é requerido para garantir a disponibilidade, manutenibilidade, segurança e confiabilidade das informações que entram e saem dos sistemas. A sociedade percebe a dimensão das perdas com erros de software somente após os mesmas ocorrerem, e poucos profissionais sabem mensurar os erros e atender às expectativas dos stakeholders quanto à segurança do sistema. [1]

Sistemas críticos são aqueles sistemas que, caso falhem, podem levar à consequências catastróficas, tais como danos ao ambiente, perdas financeiras e até risco de vida. Portanto é desejável um alto nível de segurança e confiabilidade dos mesmos. São muito usados na aviação, setor automobilístico, medicina, indústria em geral, entre outros. Tais sistemas normalmente são sujeitos a uma certificação de segurança, a fim de garantir um nível desejável de segurança, evitando falhas críticas[3]. Esse nível de segurança geralmente é definido por padrões já estabelecidos.

Devido à necessidade de garantir um sistema mais seguro [5] é importante ter uma documentação de requisitos completa e detalhada antes da implementação de tal sistema. É de consenso geral que lidar com a segurança do sistema em seus estágios iniciais é uma boa prática que pode levar a descoberta e prevenção de riscos. Apesar disso, muitas empresas não acreditam que o custo/benefício de uma documentação desse tipo seja favorável aos seus negócios.

Esse trabalho objetiva apresentar conceitos sobre a engenharia de requisitos e sistemas críticos para, então, apresentar a união dessas áreas e os estudos existentes.

Este documento está dividido em 4 tópicos: no primeiro tópico o trabalho é introduzido. Já no segundo tópico é apresentado o conceitos de sistemas críticos, algumas definições pertinentes e algumas técnicas tradicionais de análise de riscos. No próximo tópico apresentamos os conceitos de engenharia de requisitos. No quarto tópico discutimos sobre a engenharia de requisitos para sistemas críticos. No próximo tópico apresentamos alguns trabalhos realizados. Por fim concluímos o trabalho e apresentamos as referências utilizadas.

2. SISTEMAS CRÍTICOS

Sistemas críticos são os sistemas e recursos que são imprescindíveis para a empresa (ou stakeholders). São chamados assim pois deles é exigido um alto grau de confiança e segurança dos quais depende o bom andamento das atividades da empresa [2]. Ainda segundo Moura et al. [7], os sistemas críticos quanto à segurança são aqueles que podem trazer graves consequências caso ocorra alguma falha: perda de vidas humanas, danos ao meio ambiente ou prejuízos econômicos.

Em um sistema crítico a análise da segurança deve estar presente desde o início do projeto e considerar sempre o sistema como um todo e não partes individuais. Quanto maiores as consequências de falhas em um sistema crítico, maior a necessidade de investir na segurança desse sistema. A medida que a complexidade do sistema aumenta, maior a probabilidade de falhas no funcionamento.

Definições Importantes

Alguns conceitos devem ser levados em conta ao consideramos a análise de segurança em sistemas críticos, a saber [10] [11]:

- Segurança: Segurança, Segundo Firesmith [14], é o grau de um risco acidental de acordo com algumas definições. Ex. Prevenido, identificado, etc.
- Risco: Um estado do sistema que pode, caso aconteça algum evento não esperado, levar à acidente. Uma situação potencialmente alarmante.
- Acidente: Um evento não desejado envolvendo perda, danos, dor ou morte
- Requisitos de segurança: Conforme Firesmith [11] requisitos de segurança são requisitos que apresentam o mínimo de segurança exigido de acordo com um nível de qualidade ou métrica associada

A pesquisa acadêmica que objetiva apoiar a integridade e consistência na definição de requisitos não obteve ainda grande sucesso [5]. Em se tratando de sistemas críticos pode ser um ponto bastante preocupante. A falta de uma documentação consistente ocasiona conflitos entre a equipe e os stakeholders e aumenta as probabilidades de falhas.

Considerando todos os pontos apresentados, faz-se necessário a busca por um processo que traga documentos mais assertivos e que atendam às especificações e necessidades de segurança de um sistema crítico.

Técnicas de Análise de Riscos

As técnicas de análise de riscos usadas tradicionalmente são a Análise de Árvore de Falhas(FTA), a análise de árvore de eventos (ETA) e o estudo de perigo e operabilidade (HAZOP). De acordo com os estudos de Martins e Gorschek [10] as abordagens mais utilizadas por profissionais na especificação de requisitos de segurança são FTA, FMEA, HAZOP, FMECA e PHA

Em se tratando da técnica Análise de Árvore de Falhas (FTA), as falhas são representadas por uma árvore. Nela, cada falha principal é uma raiz (raiz) e falhas mais específicas são apresentadas no nível acima de forma hierárquica. Ela é uma representação de como os componentes da falha individual (falhas específicas) irão tornar-se um comportamento indesejável ou catastrófico do sistema [6].

Já a Análise de Árvore de Eventos (ETA) irá atuar mostrando os possíveis resultados (eventos) advindos da inicialização de um evento acidental. Com o ETA pode-se identificar cenários e sequências de acidentes em sistemas complexos.

A técnica de Estudo de Perigo e Operabilidade (HAZOP) é uma das mais utilizadas para avaliação de riscos. Essa técnica qualitativa permite identificar os desvios que podem ocorrer do resultado que era esperado, utilizando-se para isso de uma análise estruturada do processo. As causas e consequências desses desvios também podem ser identificadas [12].

A técnica FMEA (Análise de modos e efeitos de falhas) [15] é uma metodologia específica para avaliar um sistema, desenvolvimento, processo ou serviço sobre as possíveis formas nas quais falhas (problemas, erros, riscos, preocupações) podem ocorrer.

Já a técnica FMECA (Análise do Modo de falha, Efeitos e Criticalidade) objetiva classificar cada falha potencial de acordo com sua gravidade e probabilidade de ocorr Um procedimento realizado após uma falha de análise de efeitos para classificar cada modo de falha potencial efeito de acordo com sua gravidade e probabilidade de ocorrência.

PHA (Análise Preliminar de Riscos) trata-se da primeira análise geralmente realizada. Ela tem a função de identificar fatores de risco ao sistema.

Desafios

O desenvolvimento de sistemas críticos pode ser uma tarefa árdua [1], devido a alguns fatores, como os avanços constantes da tecnologia, aliados à falta de profissionais qualificados. Outro ponto é o aumento da necessidade de integração com outros sistemas e dispositivos e aumento da escalabilidade e complexidade dos sistemas. E por fim, a mudança na forma como os

sistemas são construídos, usando diferentes paradigmas e lidando com times cada vez mais distribuídos geograficamente o que incrementa dificuldade a esse desenvolvimento.

Heimdahl [4] por sua vez, apresenta quatro pontos como desafios ao desenvolvimento de sistemas críticos. Primeiramente a necessidade de um melhor entendimento sobre a natureza da segurança (muitas vezes mal entendida e/ou confundida com o termo confiabilidade) a fim de definir melhor as técnicas a serem usadas, o que pode evitar gastos incorretos de recursos que seriam destinados à segurança. Em segundo lugar o autor cita a diferença que existe entre desenvolver um sistema seguro e certificar que um sistema é de fato seguro. A forma usada para demonstrar que um sistema é seguro ainda é insuficiente. Em terceiro lugar a dúvida quanto ao nível de confiança que pode ser depositada no resultado de processos automatizados. A última questão apresentada é o uso de dados comuns que se usados de forma errônea podem levar a resultados catastróficos, o que torna imprescindível a validação de tais dados.

3. ENGENHARIA DE REQUISITOS

De acordo com Lamsweerde [8] a engenharia de requisitos preocupa-se com a identificação de metas a serem alcançados por um sistema e a sua operacionalização em serviços e restrições e a atribuição dos requisitos que foram alcançados à agentes, sejam humanos, dispositivos ou software.

O custo da fase de engenharia de requisitos gira em torno de 15% do orçamento do projeto.

As atividades principais para qualquer processo de RE, conforme mostrado na figura 1, são [5]:

- Elicitação: Identifica fontes de informações sobre o sistema e descobre os requisitos a partir destes
- Análise: Entende os requisitos, suas combinações e seus conflitos
- Validação: É a atividade que busca saber se os requisitos estão em conformidade com os desejados pelos stakeholders.
- Negociação: Inevitavelmente, a visão dos stakeholders irá divergir e os requisitos propostos poderão conflitar. Na fase de negociação ocorre a tentativa de conciliar visões conflitantes e gerar um conjunto consistente de requisitos.
- Documentação: Os requisitos são escritos de uma forma que seja compreensível tanto para stakeholders quanto para desenvolvedores.
- Gerência: Controla as mudanças que, inevitavelmente aparecerão, nos requisitos.

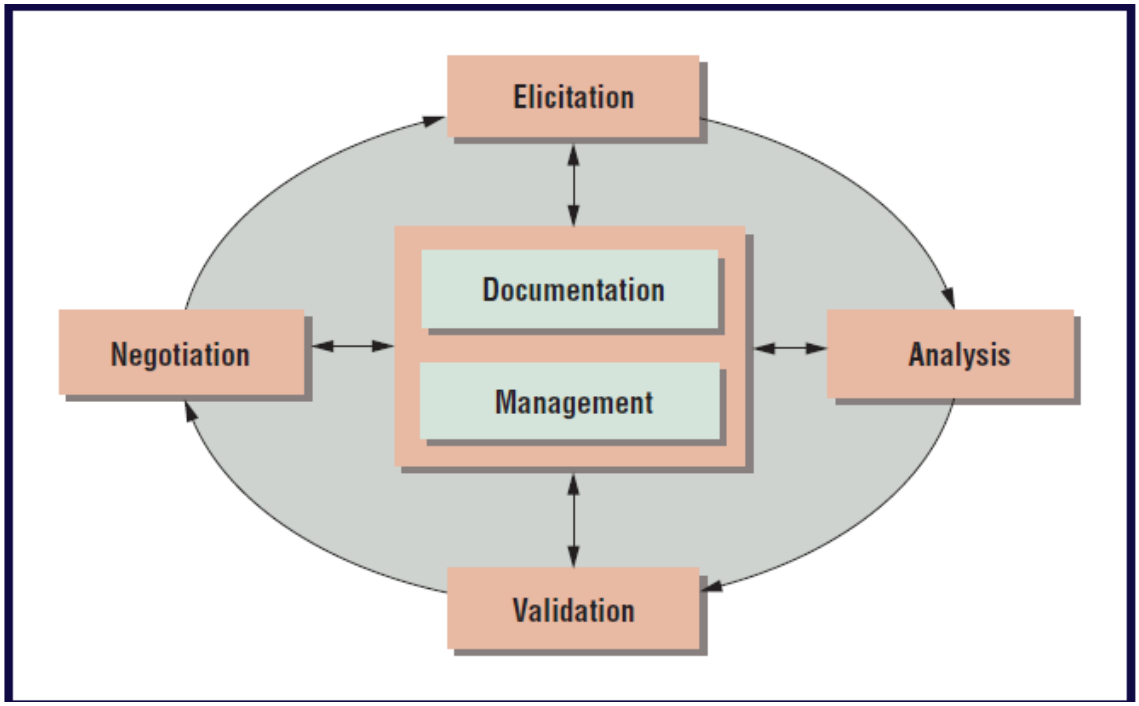

Figura 1 - Fases da Engenharia de Requisitos

A engenharia de requisitos é uma atividade cíclica. As iterações continuam durante a implementação e operação do sistema. O resultado final do processo de RE é um documento de requisitos que definirá o que será implementado.

Os requisitos de um sistema podem ser definidos como:

- Requisitos funcionais: Requisitos que definem as funcionalidades do sistema
- Requisitos não funcionais: São requisitos que tratam de aspectos de desempenho, confiabilidade, segurança, etc.
- Requisitos organizacionais: São requisitos que tratam das metas da empresa.

4. ENGENHARIA DE REQUISITOS PARA SISTEMAS CRÍTICOS

Requisitos inadequados ou mal entendidos podem levar a falhas nos sistemas de software, e se considerarmos sistemas críticos, essas falhas podem tomar dimensões catastróficas, levando a perda de dinheiro, recursos variados e até de vidas. Aliado a isso, estudos mostram que a maior causa dos grandes acidentes e catástrofes no que tange sistemas de informação, está relacionado à requisitos errados, superando até as fases de codificação e implementação, como pode ser visto na figura 2 [9].

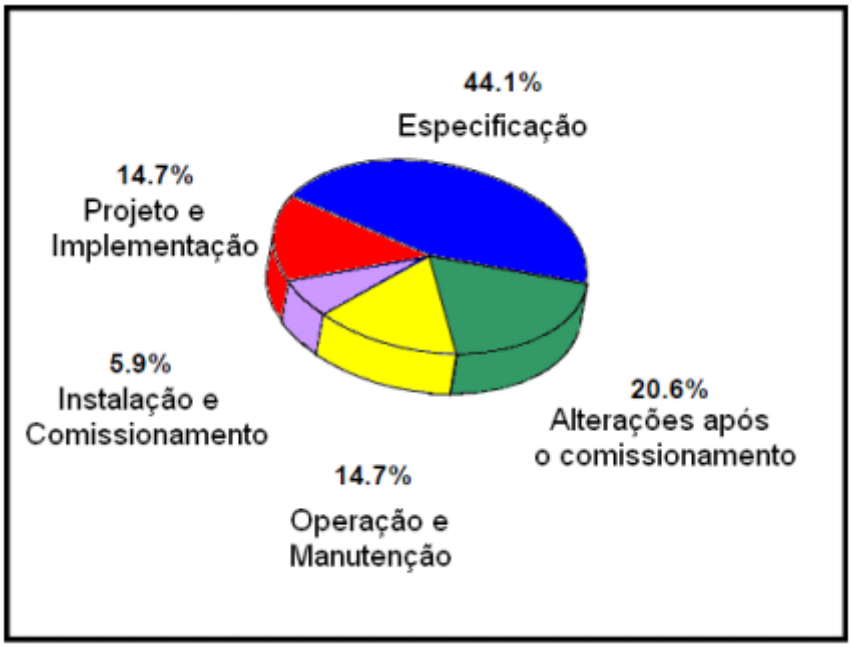

Figura 2 - Responsabilidade de ocorrência de falhas de cada fase [13]

Deve-se unir à fase de engenharia de requisitos a engenharia de segurança. Assim é possível que questões relacionadas à segurança sejam implementadas o mais cedo possível e problemas durantes as fases posteriores do projeto sejam evitados. Além da necessidade de tratar a segurança como ponto chave no desenvolvimento de sistemas críticos.

Apesar da necessidade de unir essas fases, é sabido que essa tarefa não é trivial, visto a complexidade de determinados sistemas e a necessidade de atender à padrões já definidos para segurança de sistemas. Além disso, como cita Vilela et al. [9] existe uma lacuna entre o processo tradicional de desenvolvimento, suas notações, metodologias e ferramentas e àqueles usados na engenharia de segurança.

Vilela et al [9] concluíram alguns pontos em sua revisão sistemática. Primeiro, não há uma padronização de nomenclatura entre a engenharia de requisitos e a engenharia de segurança, o que torna a comunicação e a integração entre as mesmas, algo mais complicado. Os autores também citaram a necessidade de especificação de requisitos de segurança mais completos e a necessidade de melhorar as técnicas usadas para a análise de segurança. A integração de ferramentas é um ponto necessário para que times de requisitos e segurança trabalhem em cooperação. Outro ponto citado pelos autores é a necessidade de rastreabilidade para especificação de requisitos o que facilita o trabalho do time de desenvolvimento. Por fim, o artigo cita a necessidade de integrar a pesquisa com cenários do mundo real, a fim de mensurar o quanto realmente a pesquisa pode afetar/melhorar essa integração entre requisitos e segurança.

Os requisitos de segurança de um sistema são definidos em algumas etapas:

- Identificação e classificação das vulnerabilidades associadas ao sistema;
- Determinação de métodos para tratamento dessas vulnerabilidades;
- Atribuição dos requisitos de confiabilidade e disponibilidade apropriados;
- Determinação de um nível de integridade de segurança apropriado;
- Especificação dos métodos de desenvolvimento exigidos segundo o nível de integridade determinado.

Abordagens usadas na especificação de requisitos de segurança

De acordo com os estudos de Martins e Gorschek [10] as abordagens mais utilizadas para análise de segurança, elicitação de requisitos, especificação e validação e ainda análise de riscos são as FTA, FMEA, HAZOP, FMECA e PHA. Abordagens baseadas nessas linguagens e linguagem natural são as preferidas pelos profissionais para especificação de requisitos de segurança, conforme o estudo.

O estudo[10] revela ainda que o uso acentuado da técnica FTA tanto para a engenharia de requisitos quanto para a análise de segurança mostra a proximidade dessas atividades nos estágios iniciais do desenvolvimento de software o que mostra que as fases podem contribuir entre si, compartilhando artefatos.

A figura 3 apresenta as abordagens utilizadas por processo/atividade da engenharia de requisitos de segurança.

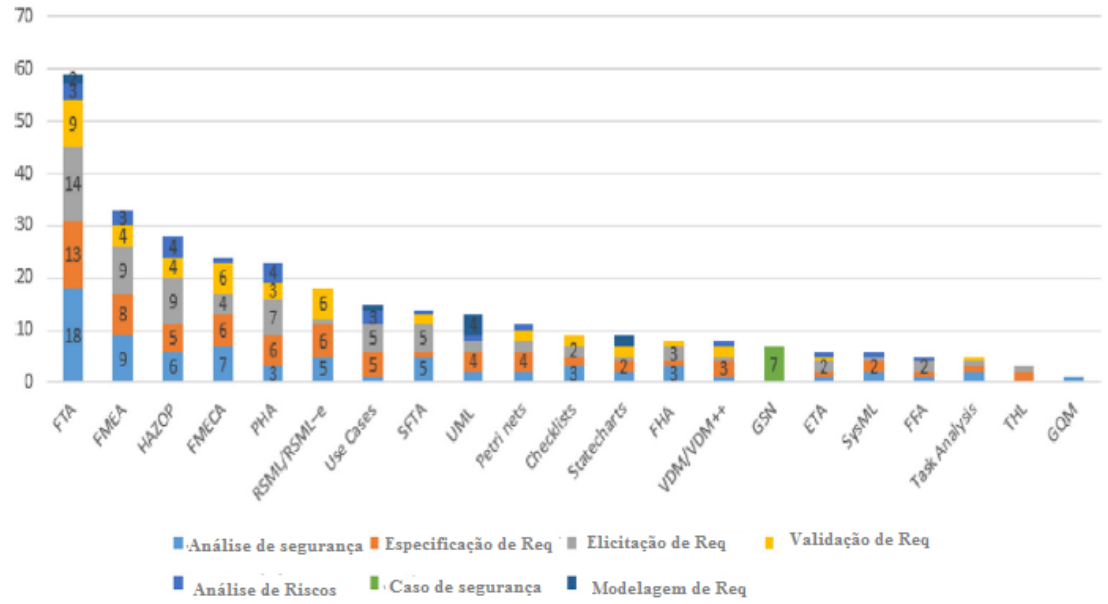

Figura 3 - Distribuição de abordagens por atividade/processo relacionados a requisitos de segurança [10]

Foi concluído também que novas abordagens para especificação de requisitos de segurança tem alta taxa de mortalidade assim que criadas. Segundo o estudo, o motivo tende a ser a falta de cobertura de tópicos relevantes aos sistemas críticos.

É necessário também criar mais validações na indústria [10], além da necessidade do maior uso das novas abordagens pelos profissionais, a fim de validá-las.

5. TRABALHOS REALIZADOS

Nair et al [3] apresenta em seu trabalho algumas práticas usadas para lidar com o gerenciamento de evidências de segurança para sistemas críticos. Um questionário foi aplicado para 52 profissionais de 11 países diferentes divididos ainda em 11 domínios de aplicação. Os autores concluíram que a maior forma de garantir segurança é a técnica V&V[1]. São necessárias mais ferramentas para apoiar a coleta e manipulação de evidências de segurança e as futuras pesquisas em gerenciamento de evidências de segurança precisam ter mais ênfase em aplicações industriais [3].

A integração entre análise de segurança e modelagem funcional é tema do trabalho de Xu e Wang [6]. Os autores sugerem uma novo modelo integrado de especificação funcional e de segurança que mantem a semântica da árvore de falhas com o uso de diagramas de estados. O

[1] Verificação e validação

objetivo é eliminar dificuldades no uso dos dois modelos em separado, além de evitar ambiguidades.

Vilela et al. propõe [11] o método de especificação de requisitos de segurança SaSSRI. Eleé a combinação de duas técnicas: STAMP/STDA e a linguagem i*. O método teve um resultado considerado satisfatório ao ser aplicado em um caso de uso real: uma bomba de infusão de baixo custo.

6. CONCLUSÃO

Sistemas críticos são sistemas que precisam de atenção redobrada para evitar falhas e comportamentos indesejados. Portanto, investir na fase de requisitos, responsável pela maior quantidade de falhas em um sistema, parece ser o caminho mais assertivo na busca por um produto mais seguro. Além disso é necessário unir a engenharia de requisitos com a engenharia de segurança, o que não se trata de algo trivial. As abordagens mais utilizadas para especificar requisitos de segurança continuam sendo as tradicionais, devido a fatores como a falta de utilização/comprovação da eficácia pela indústria, falta de uso de novas abordagens por profissionais. Consequentemente essas novas abordagens tem alta taxa de mortalidade já no início de sua vida útil.

7. REFERÊNCIAS

[1] J. Hatcliff, A. Wassyng, T. Kelly, C. Comar, and P. Jones, “Certifiably safe software-dependent systems: challenges and directions,” in Proceedings of the on Future of Software Engineering. ACM, 2014, pp. 182–200.

[2] S. Neil, Safety Critical Computer Systems. Addison Wesley, 1996.

[3] S. Nair , J.L. de la Vara , M. Sabetzadeh , L. Briand , An extended systematic literature review on provision of evidence for safety certification, Inf. Softw. Tech- nol. 56 (2014) 689–717 .

[4]M. P. E. Heimdahl, “Safety and software intensive systems: Challenges old and new,” in Future of Software ngineering. IEEE Computer Society, 2007, pp. 137–152.

[5]I. Sommerville. Integrated Requirements Engineering: A Tutorial. IEEE Software, January/February 2005, pp. 16-23

[6] O. El Ariss, D. Xu, and W. Wong, “Integrating safety analysis with functional modeling,” Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on, vol. 41, no. 4, pp. 610–624, 2011.

[7] T.A.C, Moura, N. Omar, J. Santellano, "Uma Estratégia de Análise de Segurança de Software para Aplicações Críticas", X Simpósio Brasileiro de Engenharia de Software (Workshop: Pesquisa de Teses em Engenharia de Software); UFSCarIUSP São Carlos, SP, Brasil, Outubro.1996.

[8] A.V. LAMSWEERDE, Requirements Engineering in the Year 00: A Research Perspective. Em Proceedings 22ª International Conference on Software Engineering. Invited paper, ACM Press, Junho, 2000. Limerick, Irlanda.

[9] J. Vilela, J. Castro, L.E. G. Martins, T. Gorschek, “Integration between requirements engineering and safety analysis: A systematic literature review”, Journal of Systems and Software. Elsevier, Março, 2017. RE, Brasil.

[10]L. E. G. Martins, T. Gorschek, Requirements engineering for safety-critical systems: A systematic literature review, Information and Software Technology 75 (2016) 71–89.

[11] J. Vilela, J. Castro,"SaRRSSI: a Safety Requirements Specification Method based on STAMP/STPA and i* language".

[12] J.L.F.Bargues, C.G Gaya, M. C. G Cruz, V. C. Ramírez. “Risk assessment of a compound feed process based on HAZOP analysis and linguistic terms”, em Journal of Loss Prevention in the Process Industries. Vol.44, pp. 44-52, Elsevier, 2016.

[13] R. Bell. Introducion to IEC 61508. ACS Workshop on Tools and Standards, Conference in Research and Practice in Information Technology, V. 55, 2005

[14] D. Firesmith , Engineering safety requirements, safety constraints, and safety–critical requirements, J. Object Technol. 3 (3) (2004) 27–42 march/april .

[15] D.H. Stamatis. Failure mode and effect analysis: FMEA from theory to execution. ASQC Quality Press, 1995.