Código: PPGEC-DOUTORADO_2019_1_MLPM2

Universidade de Pernambuco
Programa de Pós-Graduação em Engenharia da Computação (PPGEC)

Proposta de Projeto de Doutorado

Área: Modelagem e Sistemas Computacionais/Engenharia de Requisitos

Título: Sistemas Robóticos Sociais Móveis Seguros

Orientador – Maria Lencastre (mlpm@ecomp.poli.br)

Coorientador – Jaelson Castro (jbc@cin.ufpe.br)

A cada dia aumentam os sistemas de software críticos de segurança que afetam a vida diária das pessoas; em muitas situações, elas passam a depender destes sistemas para facilitar o controle de atividades altamente críticas, como: procedimentos médicos e fisioterápicos, transporte (aviões, trens), sistemas aeroespaciais e de defesa, e manipulação de alta energia.

Nesta pesquisa o foco será a segurança das aplicações que usam plataformas robóticas sociais móveis, tais como o NAO [1] e o TIAgo [2]. Um sistema robótico é uma combinação de algumas peças - hardware para montagem do sistema e software para operações do sistema - que deve ser integrado para permitir que ele funcione conforme esperado. Um Robô Sociável Móvel (RSM) é um tipo de robô autônomo que interage e se comunica com humanos e outros agentes autônomos físicos, seguindo regras e comportamentos sociais que dependem do seu papel. Entre estes robôs, o humanoide NAO [1], de aparência simpática e amigável, é extremamente popular com as crianças e com muitos adultos também, e vem sendo utilizado com sucesso em tratamentos experimentais de crianças com necessidades especiais.

Falhas durante o controle dos sistemas críticos de segurança (do inglês Safety-Critical Systems - SCS) podem causar acidentes com sérios danos ao meio ambiente, à propriedade e às pessoas, provocam impactos nas empresas, no mercado, na qualidade de vida das pessoas e até mesmo a perda de vidas [3]. Essas falhas e situações de perigo – chamadas *hazards* - devem ser detectadas durante o processo de análise de segurança dos sistemas críticos. Entretanto, a segurança desses sistemas não pode ser garantida sem que faça parte do processo de requisitos; sistemas devem ser construídos para serem seguros desde o começo do processo de desenvolvimento. Nesse contexto, uma maior integração das preocupações de engenharia de segurança no processo de requisitos é desejada pela indústria [6, 7, 8, 9, 10, 11]. Portanto, o desenvolvimento de sistemas críticos de segurança exige abordagens sofisticadas de engenharia de requisitos [4] por meio da melhoria da qualidade das especificações e uma análise rigorosa desses sistemas [5]. A especificação e gerenciamento dos requisitos devem ser enfatizados, pois estima-se que 70-90% das decisões relevantes para a segurança são feitas nos estágios iniciais do projeto conceitual de um sistema [3]. A especificação de sistemas críticos de segurança é uma atividade complexa, uma vez que requer muitas informações sejam elicitadas e armazenadas [12] [13]. Uma boa prática é realizar a especificação através de diferentes camadas de abstração. Especificar os requisitos de forma detalhada auxilia na obtenção de documentos completos e consistentes.

Nesse contexto, este projeto de tese de doutorado tem como foco principal a definição de um processo para o desenvolvimento de Sistemas Robóticos que leve em consideração a Engenharia de Requisitos. Será necessário o estudo sobre modelos, indicadores e métricas para melhoria de processos de desenvolvimento de sistemas robóticos críticos de segurança. Em particular, será proposta uma abordagem para Engenharia de Requisitos de Sistemas Robóticos Críticos de Segurança.

Referências

1. SOFTBANK Robotics. Find out more about NAO. https://www.softbankrobotics.com/emea/en/robots/nao/find-out-more-about-nao, 2004. (Online; accessed 10-October-2018.
2. PAL Robotics. Tiago Mobile Manipulator. http://tiago.pal-robotics.com/. 2015 (Online; accessed 10-October-2018)
3. N. G. Leveson An approach to designing safe embedded software. In: Embedded Software. Springer, 2002, pp. 15–29.
4. J. Du, J. Wang, e X. Feng. A safety requirement elicitation technique of safety- critical system based on scenario. In: Intelligent Computing Theory, ser. Lecture Notes in Computer Science, D.-S. Huang, V. Bevilacqua, and P. Premaratne, Eds., vol. 8588. Springer International Publishing, 2014, pp. 127–136.
5. J. Markovski e J. van de Mortel-Fronczak. Modeling for safety in a synthesis-centric systems engineering framework. In: Computer Safety, Reliability, and Security. Springer, 2012, pp. 36–49.
6. LEVESON, Nancy. Engineering a safer world: Systems thinking applied to safety. Mit Press, 2011.
   LUTZ, Robyn R. Software engineering for safety: a roadmap. In: Proceedings of the Conference on The Future of Software Engineering, 2000.
7. SIKORA, Ernst; TENBERGEN, Bastian; POHL, Klaus. Industry needs and research directions in

requirements engineering for embedded systems. In: Requirements Engineering, v. 17, n. 1, 2012, pp. 57-78.
8. HATCLIFF, John et al. Certifiably safe software-dependent systems: challenges and directions. In: Proceedings of the on Future of Software Engineering. ACM, 2014. pp. 182- 200.
9. L. E. G. Martins e T. Gorschek. Requirements engineering for safety-critical systems: A systematic literature review. In: Information and Software Technology, vol. 75, pp. 71–89, 2016.
10. HEIMDAHL, Mats PE. Safety and software intensive systems: Challenges old and new. 2007 Future of Software Engineering. IEEE Computer Society, 2007.
11. M. Glinz e S. A. Fricker. On shared understanding in software engineering: an essay. Computer Science-Research and Development, vol. 30, no. 3-4, pp. 363–376, 2015.
12. J. Vilela, J. Castro, L. E. G. Martins, and T. Gorschek, "Integration between requirements engineering and safety analysis: A systematic literature review," Journal of Systems and Software, vol. 125, pp. 68–92, 2017.
13. J. Vilela, J. Castro, L. E. G. Martins, and T. Gorschek, "Safety practices in requirements engineering: The uni repm safety module," TSE 2018.