

Universidade de Pernambuco

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

Proposta de Dissertação de Mestrado

Área: Modelagem e Sistemas Computacionais

Título: Garantia de Segurança de Sistemas Robóticos

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

Uma estreita interação entre humanos e robôs acontece desde a introdução dos robôs industriais no início do ano 1950, quando os robôs se tornaram uma parte natural de vários processos de manufatura [1]. Avanços nos campos da eletrônica, ciência da computação e mecatrônica tornaram essas ferramentas inteligentes, abundantes e robustas. Espera-se que com esses avanços tecnológicos, a robótica contribua cada vez mais com suas contrapartes humanas para o desempenho eficiente e eficaz de todos os tipos de tarefas [2]; mas, essa relação humano-robôs precisa ser prudente e planejada, uma vez que os sistemas robóticos também são Sistemas Críticos de Segurança (SCS). Portanto, caso ocorram falhas ou se comportem de maneira inesperada, os robôs podem levar a acidentes, resultando em danos as pessoas ou propriedades, em grandes prejuízos financeiros, ambientais ou até mesmo perda de vidas [3].

É fundamental que o desenvolvimento de sistema robóticos seja de acordo com os padrões e normas técnicas relevantes. Por exemplo, no caso de Robôs para Cuidados Pessoais há o padrão de segurança ISO 13482 [4] que especifica requisitos e diretrizes para o projeto inerentemente seguro, medidas de proteção e informações para alguns tipos de robôs de cuidados pessoais.

Apesar da evolução constante das normas e dos processos de certificação, pesquisas científicas e de organizações internacionais relatam dificuldade em garantir, de forma eficaz e eficiente, as exigências das normas de segurança nos sistemas críticos de software [5]. Um dos problemas relatado, presente na maioria das normas, é como os objetivos delas podem ser descritos de uma forma clara e rastreável.

Novas abordagens, métodos e ferramentas têm sido sugeridos, dentre elas destaca-se os Casos de Garantia de Segurança (Safety Assurance Case) [6], que visam a construção de argumentos claros, abrangentes e defensáveis em relação às propriedades de segurança e proteção dos sistemas [7]. Para auxiliar sistematicamente na construção desses argumentos, deve-se utilizar as normas existentes que tratam especificamente da construção dos Casos de Garantia de Segurança, tais como a ISO15026-1 [8] e a ISO15026-2 [9].

Os Casos de Garantia de Segurança frequentemente são utilizados para atestar a segurança de vários tipos de sistemas críticos. Neste projeto estamos interessados em investigar como eles têm sido utilizados na área da robótica [10]. Pretendemos estender a linguagem de modelagem iStar4Safety [11] para que ela possa representar os Casos de Garantia de Segurança dos Sistemas Robóticos

Referências Bibliográficas

1. LEVESON, Nancy G. Safeware: system safety and computers. Addison-Wesley, 1995.
2. ANGERER, Andreas; HOFFMANN, Alwin; ORTMEIER, Frank; VISTEIN, Michael; REIF, Wolfgang. Object-Centric Programming: A New Modeling Paradigm for Robotic Applications. In International Conference on Automation and Logistics, (2009), 18-23.
3. LEVESON, Nancy G. Safeware: system safety and computers. Addison-Wesley, 1995.
4. JACOBS, Theo; VIRK, Gurvinder. ISO 13482-The new safety standard for personal care robots. In: ISR/Robotik 2014; 41st International Symposium on Robotics. VDE, 2014. p. 1-6. URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&number=6840202&isnumber=6840100>.
5. PORFÍRIO, E. J. Um metamodelo para casos de garantia de sistemas críticos e intensivos em software baseado em análise do conceito inicial de sistemas teóricos. 122 f. Dissertação (Mestrado em Ciência da Computação) - Universidade Federal de Goiás, Goiânia, 2019.
6. Rushby, J. (2015). The interpretation and evaluation of assurance cases. Comp. Science Laboratory, SRI International, Tech. Rep. SRI-CSL-15-01.

7. SACM, OMG. Structured assurance case Metamodel Specification Version 2.0. 2013. url <https://www.omg.org/spec/SACM/2.0/>
8. ISO/IEC 15026-1:2019 - Systems and software engineering -Systems and software assurance - Part 1: Concepts and vocabulary.
9. ISO/IEC 15026-2:2011- Systems and software engineering -Systems and software assurance - Part 2: Assurance case.
10. Alves Júnior, M. M.; Lencastre, Maria; BRITO, LUCAS FLORÊNCIO DE; Castro, Jaelson; Ribeiro, Moniky. Casos de Garantia de Segurança aplicados a sistemas robóticos: Revisão Sistemática da Literatura. In: 24th WORKSHOP ON REQUIREMENTS ENGINEERING (WER 2021) - 2021, Brasil.
11. Moniky Ribeiro, Jaelson Castro, Jéssyka Vilela, João Pimentel. iStar4Safety: Uma Extensão de iStar para Modelagem de Requisitos de Segurança em Sistemas Críticos. In: 22nd WORKSHOP ON REQUIREMENTS ENGINEERING (WER 2019).