Engineering Process for Safe Autonomous Robots

Vladislav Gribov[1], Holger Voos[2]

***Abstract*—Safety oriented model based SW engineering process and component based robot architecture for autonomous service robots are proposed.**

I. Introduction

Safe service and personal care robots became new exciting research topic over last few years. Physical segregation of the industrial robot and humans works fine [1], but for obvious reasons is not possible if physical human-robot interaction (pHRI) is required. Autonomous robots and untrained humans sharing the operation space and cooperating with each other brings new kind of risks and requirements to robot safety.

The wide deployment of service and personal care robots suggests limited costs for the robot development phase. The existing robots, both industrial and academic, are mostly designed from scratch without providing clear and safety-oriented engineering process for robot design.

II. State of the Art

Safe human robot interaction in a autonomous operation becomes important and unavoidable [2]. The existing standards for industrial robot shall be extended and updated for service robots. The ISO/DIS 13482 is an approach to do that.

A number of *robotics SW* and frameworks was developed in academic field, to name the most successful: Orocos, CLARAty, Orca [3], Player/Stage, ROS.

Almost no accent was made on the issues of *engineering process* for robotics till now. It has been fragmentarily addressed as component based SW engineering in Orca, CLARAty or SmartSoft [4]. BRICS project [5] presents Robot Application Development Process, but without accent on safety.

III. Proposed approach

Confirmed by the study of the sources, the component based multilayer safe SW robot architecture and model based SW engineering process are proposed. The same robot HW can be used in different applications by adopting the SW. That justifies the focus on the robot SW.

A. Safe Robot Architecture

Robot SW performs tasks, which can be classified as "reflexive" (e.g. sensomotoric), "reactive" (e.g. local planning) and "conscious" (e.g. global planning). Those tasks are well decoupled and built layers of control SW, having reasonably different safety or real-time requirements. Cohesive functionality of each layer can be naturally represented as components. At that point, requirements on SW component has also impact on the HW it runs on.

From the safety point of view the components can implement safety relevant features (e.g. obstacle avoidance). The appropriate robot architecture provides sufficient set of safety features, providing corresponding functional safety (SIL) for each of them.

B. Safe Engineering Process

The safety oriented engineering process shall give an answer on the question: "which (safety) requirements are relevant and which components shall be put together to satisfy those requirements?"

Basic safety requirements, relevant for autonomous service robots, are already addressed as risks in ISO/DIS 13482. They can also be extended to a bigger requirement repository with well known methods like FMEA or hazard and risk analysis.

The modeled requirements are matched by the corresponding SW components from the component repository. The development process similar to the V-Model allows to model scenarios from the requirements, building up capabilities from the components. The requirements to the new component are driven, if no match is possible.

IV. Conclusion and Outline

The SysML requirement models can be used for modeling ISO/DIS 13482. The SysML component diagrams fits well for modeling SW components. For the experiment component based safe robot architecture can be implemented based on ROS and can be modeled by component diagrams.

The test case is an assembly assistant robot build from the Schunk LWA arm and equipped with Kinotex sensitive foam and in perspective with computer vision system.

[1]V. Gribov is with the Faculty of Science, Technology and Communication, University of Luxembourg, e-mail: vladislav.gribov@uni.lu

[2]H. Voos is with the Faculty of Science, Technology and Communication, University of Luxembourg, e-mail: holger.voos@uni.lu

References

[1] B. Siciliano and O. Khatib, *Springer Handbook of Robotics*, 1st ed. Springer, Jun. 2008.

[2] C. Harper and G. Virk, "Towards the development of international safety standards for a human robot interaction," *International Journal of Social Robotics*, vol. 2, no. 3, pp. 229–234, Jun. 2010.

[3] A. Brooks, T. Kaupp, A. Makarenko, S. Williams, and A. Orebäck, "Orca: A component model and repository," in *Software Engineering for Experimental Robotics*, D. Brugali, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, vol. 30, pp. 231–251.

[4] C. Schlegel, A. Steck, D. Brugali, and A. Knoll, "Design abstraction and processes in robotics: From Code-Driven to Model-Driven engineering," in *Simulation, Modeling, and Programming for Autonomous Robots*, N. Ando, S. Balakirsky, T. Hemker, M. Reggiani, and O. Stryk, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, vol. 6472, pp. 324–335.

[5] G. K. Kraetzchmar, A. Shakhimardiv, J. Paulus, N. Hochgeschwender, and M. Reckhaus, "Best Practice in Robotics. Deliverable D-2.2: Specifications of Architectures, Modules, Modularity, and Interfaces for the BROCTE Software Platform and Robot Control Architecture Workbench," 2010.