A Verifiable and Correct-by-Construction Controller for Robots in Human Environments

Lavindra de Silva
Inst. for Advanced Manufacturing, University of Nottingham, UK, *ezzlpd@nottingham.ac.uk*

Rongjie Yan
State Key Lab. of Computer Science, Chinese Academy of Sciences, China, *yrj@ios.ac.cn*

Félix Ingrand, Rachid Alami
LAAS/CNRS, University of Toulouse, France, {*felix,rachid*}*@laas.fr*

Saddek Bensalem
Verimag/CNRS, Grenoble I University, France, *saddek.bensalem@imag.fr*

Abstract

With the increasing use of domestic and service robots alongside humans, it is now becoming crucial to be able to verify whether robot-software is safe, dependable, and correct. Indeed, in the near future it may well be necessary for robot-software developers to provide safety certifications guaranteeing, e.g. that a hospital nursebot will not move too fast while a person is leaning on it, that the arm of a service robot will not unexpectedly open its gripper while holding a glass, or that there will never be a software deadlock while a robot is navigating in an office. To this end, we have provided a framework and software engineering methodology for developing safe and dependable real-world robotic architectures [4], with a focus on the *functional* level—the lowest level of a typical layered robotic architecture—which has all the basic action and perception capabilities such as image processing, obstacle avoidance, and motion control. Unlike past work we address the formal verification of the functional level, which allows providing guarantees that it will not do steps leading to undesirable/disastrous outcomes.

Our solution involves integrating two state-of-the-art technologies: GenoM, a tool in the LAAS architecture [1] for designing and implementing the functional level of robots; and BIP [2], a framework for formally modeling and executing complex, real-time component-based systems, with supporting toolsets for verifying such systems. Our combined framework has allowed the synthesis of a correct-by-construction model of a complete BIP functional level for "Dala"—an iRobot ATRV rover. The model, equivalent to the GenoM one, can be checked *offline* for properties such as deadlock-freedom using associated verification tools, and user-supplied "safety constraints" defining what behaviour is unsafe, can be included in the BIP model and enforced *online* by the resulting BIP controller. This "protects" the functional level, e.g. from any bugs in plans executed by the robot's decisional level—the OpenPRS executive [1] in our case—which may request the execution of unsafe steps. The BIP model is created using our following methodology: *(i)* design and implement the functional level using the conventional GenoM tool; *(ii)* automatically translate the functional level into an equivalent BIP model; *(iii)* manually include in it any necessary safety constraints; and *(iv)* verify the resulting model with the D-Finder [3] tool in the BIP toolkit.

We demonstrate our framework using a scenario where Dala works fully autonomously with humans to assist them with construction site inspections. Dala's main mission is to explore a set of waypoints supplied by a human inspector, by first navigating to each waypoint, taking pictures via two high resolution cameras mounted on a pan-tilt unit at the front, and then returning to the initial location. However, while navigating, Dala uses a panoramic camera mounted on its mast to monitor its surroundings for relevant objects such as potentially hazardous piles of bricks, which are detected by analysing images for a specific hue of red. On spotting a relevant object, Dala stops moving, directs its pan-tilt unit toward the object, and takes high resolution pictures of it. All images and their coordinates are wirelessly sent to the PDA of the human inspector.

We show how Dala stays clear of obstacles and humans, and we inject faults into the BIP controller via OpenPRS to show how the user's safety constraints are enforced. Some of these are: navigation should not take place unless the "speed" attribute has been initialized; the pan-tilt unit (supporting stereo cameras) should not move while navigating via stereo vision; and during this navigation mode the laser navigation mode should not be used, and vice versa. A constraint is enforced by either rejecting an OpenPRS request to do an (unsafe) step, or aborting a step being executed.

HRI'15 Extended Abstracts, March 2–5, 2015, Portland, OR, USA.
ACM 978-1-4503-3318-4/15/03.
http://dx.doi.org/10.1145/2701973.2702098.

Acknowledgements

This work has partly been supported by the European Commission under contract FP7-ICT-600877 (SPENCER).

1. REFERENCES

[1] R. Alami, R. Chatila, S. Fleury, M. Ghallab, and F. Ingrand. An architecture for autonomy. *IJRR*, 17(4):315–337, 1998.

[2] A. Basu, M. Bozga, and J. Sifakis. Modeling heterogeneous real-time components in BIP. In *SEFM*, pages 3–12, 2006.

[3] S. Bensalem, M. Bozga, T.-H. Nguyen, and J. Sifakis. Compositional verification for component-based systems and application. In *ATVA*, pages 64–79, 2008.

[4] S. Bensalem, L. de Silva, F. Ingrand, and R. Yan. A verifiable and correct-by-construction controller for robot functional levels. *JOSER*, 1(2):1–19, 2011.