Master thesis proposal: Formal modelling and verification of protocols for cyber physical systems kernel

Herman Bruyninckx and Elena Torta

November 2019

1 Project description

KU Leuven with participation from TU/e Eindhoven is developing a kernel for multi-activity integration in cyber-physical systems with relevant use cases in the field of robotics. The kernel is expected to be used and further developed in several ongoing robotics research projects: RobMoSys [5], ROPOD [6], FAST [2] and FlexCraft [3]. The kernel will integrate various software activities (for control, perception, world modelling and monitoring), that interface with each other via wait-free and/or maximal freshness ring buffers. The activities can be deployed inside several threads within one process (with the ring buffers deployed on process-owned shared memory, and the activities deployed on multiple cores), or inside different processes (with the ring buffers deployed on OS-owned shared memory). A remaining technical challenge is to create formal models of the the wait-free buffer access protocols to apply formal verification. The implementation (code and formal models) will be released under industry-friendly open source licenses. The targeted use cases range from distributed real-time robot and machine tool control applications to web-based user interfaces and reactive applications. A non-formal description of the protocol is reported in sections 11.7 and 11.8 of [1]. Formal modelling and verification has been successfully applied to a number of cases [4], in this project we want to follow a similar path by creating formal models of the protocol to verify the correctness of the "ownership transfer" between producer and consumer. In particular, our research questions are:

- Is the shared data at all times owned by one and only one of both?
- Can ownership always be transferred back to the original owner, or are there any deadlock states in the protocol?

The student is welcomed to to further extend and elaborate on the proposed research questions.

2 Supervision

We propose to select a student from the department of mathematics and computer science with interest in formal verification and robotics which can be co-supervised by T. Willemse from the department of computer science and H. Bruyninckx and E. Torta from the department of mechanical engineering (CST group).

References

[1] Herman Bruyninckx. Composable and explainable systems-of-systems. https://robmosys.pages.mech.kuleuven.be/composable-and-explainable-systems-of-systems.pdf, 2019.

[2] FAST. Industrial robots more flexible thanks to soccer and care robots. https://www.tue.nl/en/news/news-overview/15-01-2018-industrial-robots-more-flexible-thanks-to-soccer-and-care-robots/.

[3] FlexCraft. FlexCRAFT – Cognitive Robotics for Flexible Agro-Food Technology. https://flexcraftprogram.com/.

[4] MCRL2ShowCases. Showcases — mCRL2 201908.0 documentation. https://mcrl2.org/web/user_manual/showcases.html.

[5] RobMoSys. RobMoSys Wiki [RobMoSys Wiki]. https://robmosys.eu/wiki/.

[6] ROPOD. http://www.ropod.org/.