Chapter 4
Model-Based Development and Spatiotemporal Behavior of Cyber-Physical Systems

Peter Herrmann
Norwegian University of Science and Technology, Norway

Jan Olaf Blech
Altran, Germany

Fenglin Han
Norwegian University of Science and Technology, Norway

Heinz Schmidt
RMIT University, Australia

ABSTRACT

Many cyber-physical systems operate together with others and with humans in a joint physical space. Because of their operation in proximity to humans, they have to operate according to very high safety standards. This chapter presents a method for developing the control software of cyber-physical systems. The method is model-based and assists engineers with spatial and real-time property verification. In particular, the authors describe a toolchain consisting of the model-based development toolset Reactive Blocks, the spatial analyzer BeSpaceD in conjunction with the real-time model checkers UPPAAL and PRISM. The combination of these tools makes it possible to create models of the control software and, if necessary, simulators for the actual system behavior with Reactive Blocks. These models can then be checked for various correctness properties using the analysis tools. If all properties are fulfilled, Reactive Blocks transforms the models automatically into executable code.

DOI: 10.4018/978-1-5225-7268-8.ch004

INTRODUCTION

In safety critical domains like aviation, automotive and robotics, autonomous cyber-physical systems interact with each other and with humans in the same physical space. To avoid damage of machine equipment and injuries of humans, the control software of these systems has to guarantee spatiotemporal properties like collision avoidance or the reliable cooperation of several units that carry a heavy workpiece together. A popular way for the creation of functionally correct and safe system software is the application of integrated modeling and verification tools like MATLAB/Simulink (Tyagi, 2012). Our contribution is the combination of such a tool with efficient provers allowing engineers to verify that the coordinated behavior of multiple controlled cyber-physical systems fulfills relevant spatial safety properties. We introduce a toolchain combining the model-based engineering tool-set Reactive Blocks (Kraemer, Slåtten, & Herrmann, 2009) with the verification tool BeSpaceD (Blech & Schmidt, 2013). In particular, we use a development workflow starting with the collection of requirements for a cyber-physical system and its architecture followed by the steps 1 to 7 below:

1. Spatiotemporal properties of components are described in the input language of BeSpaceD.
2. A model of the system controller is created in Reactive Blocks. We compose it with a simulator model of the continuous system parts which is engineered using the BeSpaceD model developed in step 1.
3. The built-in model checker of Reactive Blocks is used to check the combined controller and simulator model for general design errors, (Kraemer, Slåtten, & Herrmann, 2009).
4. If the checks in step 3 are passed, the software model is transformed into the input language of BeSpaceD.
5. Assuming certain maximum reaction times of the discrete controller, the resulting model is now verified with BeSpaceD to check whether it fulfills the required spatiotemporal properties defined in step 1.
6. One of the model checkers UPPAAL (Bengtsson, et al., 1996) and PRISM (Kwiatkowska, Norman, & Parker, 2009) is now applied to prove that the real-time properties assumed in the proofs of step 5 are preserved by the Reactive Blocks model created in step 2 (Han & Herrmann, 2013), (Han, Herrmann, & Le, 2013).
7. By using the code generator from Reactive Blocks (Kraemer & Herrmann, 2007), (Kraemer, Herrmann, & Bræk, 2006), executable Java code of the controller and, if needed, of the simulator of the continuous behavior is created.