Model checking cyber-physical workflows*

Barnabás Králik

Department of Programming Languages and Compilers, Faculty of Informatics
Eötvös Loránd University
`kralikba@elte.hu`

Abstract

Cyber-physical systems (CPSes) - complex networks of computational nodes, sensors and actuators - take a significant role in our everyday lives. Most of them are directly responsible for human lives; thus, guaranteeing their adherence to strict safety and security specifications is of utmost importance.

On one hand, the job of the implementor can be made less error-prone by programming these systems in a domain-specific language tailored for such applications. On the other hand, the completed software can be automatically checked whether it is correct with respect to its aforementioned specification.

A novel approach is the use of cyber-physical workflows; workflows that not only have a discrete nature (as business workflows have), but also a continous nature (as physical processes have).

P$\acute{\varepsilon}\alpha$ is a language that supports this paradigm. The basic building block is the "task": units of work that run for some time and give a result, but, while running, might also have an externally observable "unstable value". Primitive tasks can then be used to construct complex ones through combinators - which simply are parametric tasks.

In this paper, we propose a method to model check cyber-physical workflows written in P$\acute{\varepsilon}\alpha$.

At the core of our solution lies software transformation: the aim is to translate P$\acute{\varepsilon}\alpha$ code to the PROcess MEta LAnguage (PROMELA), which, in turn, can automatically be checked using proven 3rd party software. To accomplish this, we specify the precise meaning of P$\acute{\varepsilon}\alpha$'s language elements in terms of the primitive constructs used for describing generic concurrent software in PROMELA.

Keywords: cyber-physical programming, task-oriented programming, workflow, model extraction, software transformation

MSC: 68Q60, 68N15

*The research is carried out as part of the EITKIC_12-1-2012-0001 project, which is supported by the Hungarian Government, managed by the National Development Agency, financed by the Research and Technology Innovation Fund and was performed in cooperation with the EIT ICT Labs Budapest Associate Partner Group.