Function Block Diagram to UPPAAL Timed Automata Transformation Based on Formal Models

Doaa Soliman*, Kleanthis Thramboulidis, Georg Frey***

*Saarland University, Saarbrücken, Germany
(e-mail: {doaa.soliman,georg.frey}@aut.unisaarland.de)
**University of Patras, Greece
(e-mail: thrambo@ece.upatras.qr)

Abstract: Verification of IEC61131-3 based safety applications is a challenge in the development process of industrial systems. In this paper, we formally describe the set of transformation rules we have defined for the automatic transformation of IEC61131-3 function block based safety applications to UPPAAL timed automata models. These models are used for the verification of the safety application. Both the source and the target domain models have been formally defined and these definitions are used for the formal definition of the transformation rules. We adopted as format of the source models the PLCopen XML specification that is widely accepted by industry. Based on this format and the defined transformation rules a prototype model transformer was developed using Java. The transformer was used on several safety applications to check its functionality and the efficiency of the transformation process.

Keywords: IEC61131-3, UPPAAL, Function Block Diagram, Safety Applications, PLCopen.

1. INTRODUCTION

The IEC61131-3 (2003) set of programming languages is widely adopted by industry and the majority of industrial automation systems are based on these languages. Many of these systems are safety critical and should conform to various safety standards defined by international standard organizations, such as ISO and IEC. This is why safety issues of IEC61131 have already been examined by the research community. Moreover, PLCopen (http://plcopen.org) has developed a library of safety function blocks (SFBs) that can be used for the development of safety applications. Among the challenges that engineers face during the development process of safety applications is the verification of the safety application before implementing it. UPPAAL (http://www.uppaal.org) was selected, in this work, to be used for the verification process of function block diagram (FBD) safety application. The FBD design models of the safety application are transformed to UPPAAL models, which are next imported to the UPPAAL model checker. UPPAAL is a good choice for formal verification of systems that can be modelled as a collection of non-deterministic processes with real valued clocks. This makes the tool suitable for the verification of FBD safety applications built from function blocks (FBs) triggered by timers.

Soliman, Thramboulidis, and Frey (2011) have defined the set of mapping rules for the transformation process based on the meta-models of the source and target domains. Soliman and Frey (2009, 2011) have presented the validation via simulation and verification via model checking based on these models. In this paper, we proceed with the formal definition of the models of the two domains and express the transformation rules based on these formal models. Based on this, we have developed a prototype model transformer using the Java language and we have checked its behaviour on several safety applications. We adopted the PLCopen XML as format of the IEC61131-3 FBD safety applications. This allows the approach to be used by many IEC61131-3 commercial development tools that support the PLCopen XML specification, defined by PLCopen (2009). An example safety application is used through the paper to illustrate the proposed modelling and transformation process.

The remainder of this paper is organized as follows: In Section 2, related work is discussed. Section 3 presents the formal definitions of FBD programs defined by IEC6113-3. UPPAAL timed automata (TA) models are presented in section 4. The transformation rules are formally defined in Section 5. Conclusions are given in the last section.

2. RELATED WORK

Nowadays, there is an increasing interest of automating the verification process of applications in industrial automation. Several research groups have already published the results of their work to this direction. These works are mainly based on the transformation of the FBD models of the safety application to formal models, which are next used for verification purposes with the help of a model checking tool.

Pavovic and Ehrich (2010), present a method for the automated formal verification of PLC software written in FBD using the NUSMV model checker. The FBD should be constructed from basic FBs such as bit operations, comparators and jumps. Moreover, the IL representation of the FB body, which is generated from the corresponding FBD