Transformation of Function Block Diagrams to UPPAAL timed automata

for the verification of safety applications

Doaa Soliman a , Kleanthis Thramboulidis b, Georg Frey a

1. Introduction

The IEC 61131-3 (IEC, 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. For example, the IEC 61508 (IEC, 1998) and its implementation

for the machinery sector, i.e., the IEC 62061 (IEC, 2000), impose

manufacturing industries to certify that their systems are safe for

the human life and the environment. This is why safety issues of

IEC 61131 have already been examined by the research community,

e.g., Toon (2002) and Lewis (2002). Moreover, PLCopen

(http://plcopen.org) has developed a library of Safety Function

Blocks (SFBs) to facilitate the development of safety applications.

Safety applications that are developed using verified libraries, such

as the one of PLCopen, are suitable to meet the requirements of the

second upper Safety Integrity Level, i.e., SIL 3, as defined by IEC

61508 (IEC, 1998).

Among the challenges that engineers face, during the development

process of safety critical industrial systems, is the verification

of the safety application before implementing it. Over recent years

the complexity of safety applications has increased dramatically.

This makes the formalization of safety applications a very difficult

task. Formalization is important in order to verify that the design

meets the specified safety requirements. There are several research

works that try to facilitate the transformation of PLC code into formal

models supported by available model checker tools. UPPAAL

(Larsen et al., 1997; Behrmann et al., 2004) was selected, in this

work, to be used for the verification process of safety applications

based on Function Block Diagrams (FBDs). UPPAAL is a good choice

for formal verification of systems that can be modeled as a collection

of non-deterministic processes with real valued clocks. This

makes the tool suitable for the verification of safety applications

built from Function Blocks (FBs) triggered by timers.

In this paper, we have adopted as format of the IEC 61131-3 FBD

the PLCopen XML one, defined by PLCopen (2009). This allows our

approach to be used by any IEC 61131-3 commercial development

tool that supports the PLCopen XML specification. The FBD design

models of the safety application are transformed to UPPAAL models,

which are next imported into the UPPAAL model checker. In

Soliman and Frey (2009, 2011) the validation via simulation and

the verification via model checking based on these models, is presented.

In this paper, we formally define the models of the two domains.

A set of formal definitions for the IEC 61131-3 FBD and the

UPPAAL system are given. Then, based on these models we formally

define the set of transformation rules. A set of mapping rules

for the transformation process based on the meta-models of the

source and target domains have been informally defined in

Thramboulidis et al. (2011). A prototype model transformer was

developed using the Java language and its behavior was checked

1367-5788/$ - see front matter \_ 2012 Elsevier Ltd. All rights reserved.

http://dx.doi.org/10.1016/j.arcontrol.2012.09.015