An Automated Verification Process for Industrial Safety Applications

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

*Saarland University, Saarbrücken, Germany, °University of Patras, Greece

Abstract— **Legacy systems that do not conform to the norms and regulations imposed by recent safety standards have to be upgraded to meet safety requirements. In this paper, we describe a methodology to upgrade legacy industrial applications based on the IEC61131 function block model without the need to redesign the whole application. We then describe an approach for automating the verification process of safety applications that is based on the use of the UPPAAL simulation and verification platform for embedded real-time systems. The meta-models of the source and target domains are presented and a transformation process of the PLCopen XML design specification to UPPAAL XML specification is described. A laboratory system is used as a case study to demonstrate the applicability of the proposed verification process.**

I. Introduction

International standard organizations, such as ISO and IEC have defined various standards on safety due to social and environmental demands. These standards, as for example the IEC61508 [9] and the IEC61511 [10], impose manufacturing industries to develop new industrial automation systems and upgrade legacy ones to conform to various norms and regulations and also certify that their systems are safe for the human life and the environment. The alternative to throw away the legacy system and develop a new one from scratch to meet the requirements specification, if such a specification exists, is very expensive. More specifically, the main reason for upgrading, instead of redesigning, the legacy industrial systems to be compliant with safety standards is the high value of the software part of these systems.

Among the challenges that the engineer phases for upgrading legacy systems are: the definition of safety requirements for the upgraded system, the definition of the requirements of the safety system, the design of the safety system, the verification of the safety application, its integration with the legacy system and the verification of the upgraded system. This makes the upgrade process significantly different from the development of a new system where an integration of the traditional development process with safety engineering is also required [1].

A methodology to systematically address the above challenges and upgrade legacy industrial systems to meet safety regulations is briefly presented in this paper. This methodology has been applied to a laboratory system to demonstrate its feasibility. During this work it was found that one of the most challenging parts of this process is the verification of the safety application. There are several works to this direction [13]-[16] and it seems that there is an increasing interest for automating the verification process of FBD based safety applications. However, all the published verification approaches are based on proprietary tools and notations and none of them can be generalized since no common intermediate platform is shared by PLC tools vendors.

In this paper we propose an automatic verification process for safety applications developed using the FBD language of the IEC61131-3 [11]. More specifically, we will focus on the automatic transformation of the safety application design models expressed in PLCopen XML, to UPPAAL models to automate the verification process. The source and target domains meta-models have been defined as well as the required mapping rules from one domain to the other. XML is used as a notation for expressing both domain models. Safety properties formalized from safety functions which are derived from safety requirements are verified using the transformed safety application. Depending on model checking results, the implemented safety application is iteratively modified to meet all safety requirements. The transformation process is demonstrated developing a real safety application for a laboratory system using MultiProg from KW software. The so generated UPPAAL TA models are also presented. For the development of the safety application the PLCopen Safety Function Blocks (SFBs) library [5], [6] was used. This library was developed by the technical committee TC5 of the PLCopen to facilitate the development of safety applications. Its main objective is not only to reduce the certification time and costs but also to contribute to the understanding of safety aspects in the IEC61131 domain. The main contribution of this paper is the description of a process to upgrade a legacy system to conform to safety regulations and the definition of an approach to automatically verify a safety application based on IEC61131-3, safety standards IEC61508/IEC61511 and PLCopen. The proposed verification approach can be applied using many IEC61131 compliant tools due to the fact that the PLCopen XML scheme, which is adopted as interface platform to allow automatic verification in this work, is widely accepted by many companies inside and