Development of a PLC code analyzer

November 2014

candidate	Altin Qeriqi
supervisors	Martin Steffen (UiO), Ingrid Chieh Yu (UiO), Jingyue Li (DNV-GL)
group	PMA, in collaboration with *DNV-GL*
type	60 ECTS
recommended background	program analysis, parsing, compilation
study program	computer science

Short description

The task is to design and implement a translation from a PLC language to an analyzer back-end such as NuSVM.

Background and motivation

Programmable logic controllers (PLCs) are industrial digital computer control systems used e.g., to automate production processes or execute process control. In many cases, the applications involve real-time requirements and are, in addition, safety-critical. To program those controller systems, domain-specific languages have been developed and standardized (in the international IEC 61131-3 standard [3]). Since those systems are often used for safety-critical functions, for instance for oil & gas production and transport systems in this context of the master thesis, the code needs to undergo rigorous scrutiny to ensure its functioning.

Problem setting

One approach to verify PLC programs is *model checking* [2][1] i.e., to exhaustively and automatically check whether a model of the given program or system meets a given specification and thus is free of defects. Currently, the PLC code for examples used in DNV-GL is manually converted into a model (which then can be model-checked). Obviously, that process is laborious, and error-prone in itself. Therefore, in this project, the task is to develop a *compiler* to read in PLC code and compile it then into a model that can be analyzed using model checking tools.

In this project, the task is to develop a compiler to read in PLC code and compile it then into a model that can be analyzed using model checking tools. The task includes the following:

1. understand and work out the intended meaning of the PLC input language (i.e., its semantics)
2. develop a parser/compiler that translates PLC programs to the input language of a model checker (NuSMV, Maude)
3. model check a *case study* provided by DNV-GL.

Keywords: program analysis, model checking, PLCs

References

[1] C. Baier and J.-P. Katoen. *Principles of Model Checking*. MIT Press, May 2008.

[2] E. M. Clarke, O. Grumberg, and D. Peled. *Model Checking*. MIT Press, 1999.

[3] IEC 61131. Programmable controllers – part 3: Programming languages (version 3), Feb. 2013.