PLC formal verification

Formal methods applied to PLC programs

Purpose

Developing safe and robust PLC (Programmable Logic Controller) control systems is a common goal for control engineers. Traditionally, testing techniques have been applied for that purpose, but some obvious problems remain unsolved as typically the exhaustive testing of a non-trivial system is not possible.

The goal of this project is to provide a methodology which guaranties that a PLC program is compliant with the required specification. This methodology is based on applying automated formal verification methods to PLC programs, hiding the complexity from the control engineers whenever possible. For that purpose, the methodology is supported by a specialized tool which creates the formal models automatically and helps the user to formalize the project specifications.

Approach

The formal models are generated automatically out of the PLC programs to verify. Currently ST (Structured Text), IL (Instruction List) and SFC (Sequential Function Chart) languages are included in the methodology, as they are widely used at CERN. In addition, the methodology is meant to be general and open to any verification tool. For that reason the methodology is based on an Intermediate Model (IM) which is the central point of the methodology, which have 5 steps:

1. Formalization of the requirements.
2. Transformation from PLC code to the IM.
3. Reduction of the state space of the IM.
4. Transformation from the IM to the input language of the verification tools (Currently nuXmv, UPPAAL and BIP and included).
5. Verification and analysis of the results.

All these steps are hidden from the control engineer and the methodology is integrated in the traditional development of PLC programs as it is shown in the following figure.
Status

First experiments on UNICOS CPC-based PLC programs have been performed and outstanding results have been already achieved. The project is still in its development phase.

We are developing a proof-of-concept tool named PLCverif.

Selected publications


Publications

Related Presentations

- B. Fernández Adiego: **Formal verification in Industrial Control Systems.** Presented at the ICE Tea, 14 February 2014. [Slides]
- D. Darvas: **Domain-specific languages – What, how and when?** Presented at the ICE Tea, 21 February 2014. [Slides]
- B. Fernández Adiego: **Formal methods applied to PLC code verification.** Presented at the Advanced Control Engineering: Academia - Industry workshop, 2-3 June 2014. [Slides on Indico]
- D. Darvas: **Formal verification of industrial control systems... at CERN.** Presented at the 1st Developers@CERN Forum on Software Quality, Reliability and Testing, 28-29 September 2015. [Slides on Indico]
- B. Fernández Adiego: **Automated Formal Verification of PLC Programs.** Presented at the CERN-ESTEREL Technical Seminar, 21 January 2016. [Slides on Indico]
- D. Darvas: **Formal verification of industrial control systems.** Presented at the 3th Workshop on PLC/COTS-based Interlock and Protection Systems, 01-02 February 2016. [Slides on Indico]
- D. Darvas: **Practice-oriented formal methods to support the software development of industrial control systems.** Presented on the PhD Thesis defense, 15 May 2017. [Slides]
- G. Sallai: **Exploring the possible uses of translating PLC code to C (and more).** Presented at CERN, 29 August 2017. [Slides]
- D. Darvas: **Finding bugs in the LHC: Verification methods for PLC programs.** Presented at the Alpine Verification Meeting 2017, 18 September 2017. [Slides]

Contact persons

- Borja Fernández Adiego: borja.fernandez.adiego@cern.ch
- Daniel Darvas: daniel.darvas@cern.ch
- Enrique Blanco Viñuela: enrique.blanco@cern.ch