PLC formal specification

Purpose

Incomplete, ambiguous and wrong specifications are the source of many bugs in every software. The goal of our research is to propose a new specification language that ideally can be also generalized to the development of any PLC program (e.g. safety PLC programs). These specifications should be formal, but easy to understand, specific for the domain; improving the quality of the specified software and the communication between the customers and the developers (process and control engineers) at the same time.

Approach

We are developing a new language called PLCspecif that is a formal, but intuitive behaviour specification language adapted to the needs and knowledge of the PLC domain.

Status

In progress.

Publications


Talks

- D. Darvas: Spécification formelle pour les API (PLCspecif) [in French]. Presented at the CERN-ESTEREL Technical Seminar, 21 January 2016. [Slides]
- D. Darvas: Conformance checking for PLC programs and specifications. Presented at the 11th IEEE International Symposium on Industrial Embedded Systems, 23 May 2016. [Slides]
- D. Darvas: Formal verification of safety PLC based control software. Presented at the 12th International Conference on Integrated Formal Methods, 03 June 2016. [Slides]
- D. Darvas: Practice-oriented formal methods for PLC programs of industrial control systems. Presented at the PhD Symposium at IFM'16 on Formal Methods: Algorithms, Tools and Applications (PhD-IFM'16), 05 June 2016. [Slides]
- D. Darvas: PLC code generation based on a formal specification language. Presented at the 14th IEEE International Conference on Industrial Informatics, 20 July 2016. [Slides]

Contact persons

- Dániel Darvas: daniel.darvas@cern.ch
- Enrique Blanco Viñuela (CERN): enrique.blanco@cern.ch
- István Majzik (Budapest University of Technology and Economics, Hungary): majzik@mit.bme.hu