Contribution ID: **4**   Type: **not specified**

Formal verification of PLC programs with PLCVerif

Friday 15 October 2021 16:40 (20 minutes)

Formal verification techniques, in particular Model Checking, are powerful methods that can be used to guarantee that a PLC program is compliant with its specifications.

They are a good complement to the traditional testing techniques and they are recommended by the Functional Safety standards (e.g. IEC 61508 and IEC 61511).

The main advantage of Model Checking is that it checks all combinations in the PLC program trying to find a violation of the requirement specification.

The main disadvantages are 2: (1) using formal methods is a complex and time consuming task; (2) the so-called "state space explosion" problem, when the number of combinations to be checked is huge.

PLCverif hides the complexity of using formal methods from the user of the tool. In addition, it uses advanced model checking algorithms to deal with the "state space explosion" to a certain extend.

Presenter: FERNANDEZ ADIEGO, Borja (CERN)

Session Classification: Testing & verification

Track Classification: (3) Testing and verification