Dániel Darvas (CERN / TU Budapest)
daniel.darvas@cern.ch | darvas@mit.bme.hu

Formal verification of industrial control systems at CERN

VTSA 2014 Student Session
30/10/2014

Contains joint work of B. Fernández, E. Blanco, S. Bliudze, J.O. Blech, J-C. Tournier, T. Bartha, A. Vörös, I. Majzik

http://go.cern.ch/DGj7
Context – CERN

- European Organization for Nuclear Research
- laboratory and accelerator complex for particle physics research
- PLCs for controlling vacuum, cryogenics, HVAC, etc. systems
Context – PLCs at CERN

- Programmable Logic Controllers
  robust industrial computers

- 1000+ PLCs at CERN

- Common framework (UNICOS)
  → Common library of base modules
Motivation for formal verification

- Human lives are not depending on PLCs
- but
- expensive equipment
- long-term consequences
- common library
- update is difficult
- long life-time of PLC programs
Goal

- To **improve the quality** by eliminating bugs
  - Complementing automated and manual testing
- Applying **model checking** to find “**high quality**” bugs

**but**

- CERN is not a CS research institute
- Building on **off-the-shelf solutions**
Challenges and answers

- How to get models?
  - Automated generation

- Which model checker should be used?
  - Multiple (general method, intermediate model)

- How to formalize requirements?
  - Requirement patterns

- How to make it efficient?
  - Reductions

- Counterexample

- And it should be integrated to the development process.
The PLCverif tool

Eclipse-based editor for PLC programs
The PLCverif tool

Defining verification cases (requirement, fine-tuning, etc.)

*No model checker-related things or temporal logic expressions*
The PLCverif tool

PLCverif — Verification report

Generated at: Mon Jul 07 15:19:22 CEST 2014 | PLCverif v2.0.1 | (C) CERN EN-ICE-PLC | Show/hide expert details

ID: Demo001
Name: If A is false, C cannot be true.
Description: If A is false, C cannot be true. As this function block models an AND-gate, if any of the inputs (A or B) is false, the output should be false too.

The requirement is based on the documentation of the function block and the following Jira case: https://icecontrols.its.cern.ch/jira/browse/UCPC-1111

Source file: DemoSource.scl
Requirement: 3. A = false & C = true is impossible at the end of the PLC cycle.
Result: Not satisfied

Tool: nusmv
Total runtime (until getting the verification results): 212 ms
Total runtime (incl. visualization): 361 ms

Counterexample

<table>
<thead>
<tr>
<th>Variable</th>
<th>End of Cycle 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input a</td>
<td>FALSE</td>
</tr>
<tr>
<td>Input b</td>
<td>TRUE</td>
</tr>
<tr>
<td>Output c</td>
<td>TRUE</td>
</tr>
</tbody>
</table>

Click-button verification, verification report with the analysed counterexample
Still to improve

- **Big programs**
  - Works fine for 100-1000 LoC ($10^{200}$ states before reduction)
  - What about 100 kLoC ($10^{100,000}$ states before reduction)?
    (many reused modules and a bit of code to connect them)

- **Integers and time**
  - Works fine for mostly Boolean programs (with few integers/timers)
  - What about having 10-100-1000-… integers?
  - BDD-based NuSMV fails. What about other model checkers?

- And a blocker problem…
The Blocker Problem

“We can check if the program behave as it is supposed to behave. **But how should it behave?**”

- **The code is the authoritative specification**
  - Already long evolution (10+ years)
  - Complex code

- Big need for a **specification** method that …
  - … is **unambiguous, formal**.
  - … has a **semantics** adjusted to the PLC domain.
  - … can be **easily used by automation engineers** and by the “internal customers” without long training.
  - Ongoing research: 2014 – 2017
Summary

− First steps are made to apply FV to industrial control systems of CERN
  • Many interesting bugs were found (with joint effort of automation engineers and formal methods people)

− Still long way to go
  • Improving the performance
  • Formal specification

http://go.cern.ch/DGj7
References


Visit https://cern.ch/enice/PLC+formal+verification for contacts and more information.