Veriﬁcation of Reactive Programs from Industrial Automation

Dimitri Bohlender, Stefan Kowalewski

Programmable Logic Controllers (PLCs)
- Tailored to the domain of industrial automation
- Realise reactive systems, repeatedly executing the same task

PLC Software
- Programming languages standardised (IEC 61131-3)
- Combination of several languages typical
- Typically graphical on higher level but textual on lower level

PDR-based Model Checking
PLCopen Automaton
- Specifies safe observable behaviour of a block

Observations
- Specifications refer to observable state at cycle-end
- Function blocks exhibit mode-semantics

Symbolic Execution
Guided by Mode-Space
- Consider the right-hand program
- Implicit state-machine (state s)
- Fails on input sequence “{}”
- Bad choices hard to identify (cyclicity)

- CFG-based guidance is local, needs bound and degenerates into random search:

Future Work
- Analysis of restart behaviour:
  Variables may retain their value after restart/power cut. Starting from these new states no new behaviour shall be observable.
- Mode-oriented PDR:
  Software-oriented PDR variants partition the transition relation by program locations. An analogous partitioning by modes may help with invariants disjunctive over modes.