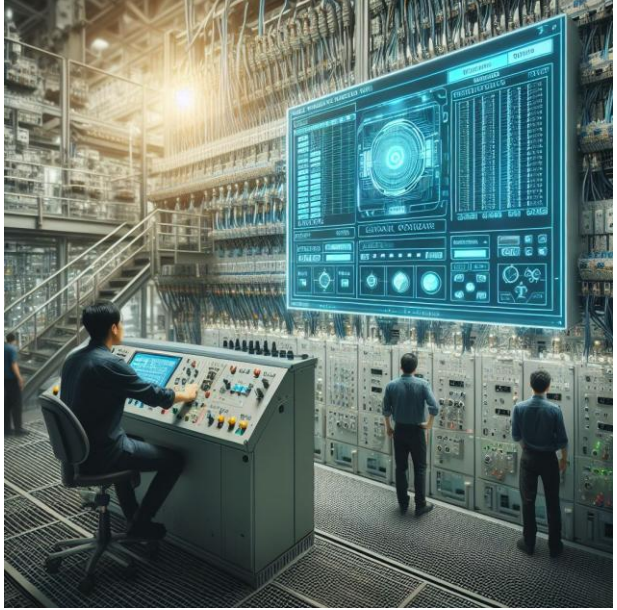
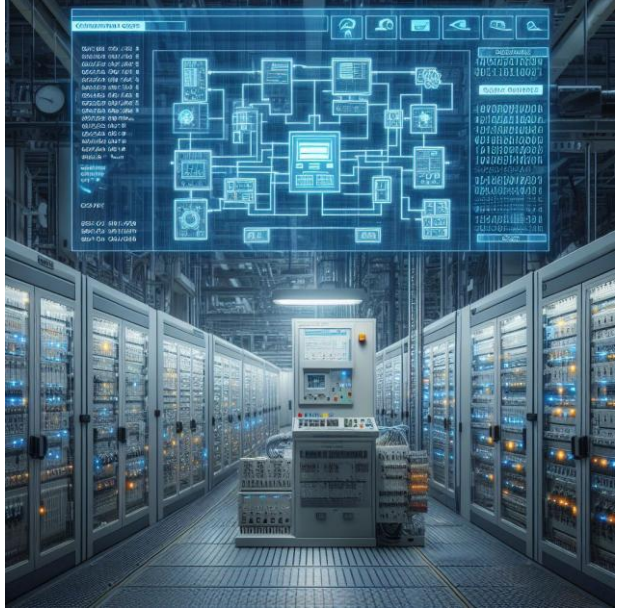




Formal methods for safe PLC programming

Jessica RAVAKAMBININTSOA

March 2025

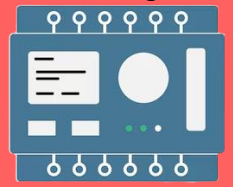
INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES LYON

Ampère

Life Is On Schneider Electric

I. Context

PLC
(Programmable logic controllers)



Programming

IEC 61131-3
- **ST : Structured text**
- **IL : Instruction List**
- **SFC : Sequential Function Chart**
- **FBD : Function Block Diagram**
- **LD : Ladder Diagram**

Critical systems

Safety

Sensitive systems

Reactivity

Checking PLC programs

Conventional Methods:
- Test
- Simulation

Formal Methods :
- Model Checking
- Theorem of proof
- Static Analysis

*

MC : Model Checking
AI : Abstract Interpretation

II. Proposals

Transform PLC programs into mathematical models required for verification

- Automatic translation
- Support for several formal verification approaches (ex : MC, AI*)

Specify a methodological approach

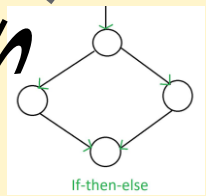
- Identify value-added verification needs for PLC programmers
- Selection of appropriate verification tools and techniques
- Help PLC programmers to improve the quality of PLC programs

III. Steps

PLC program

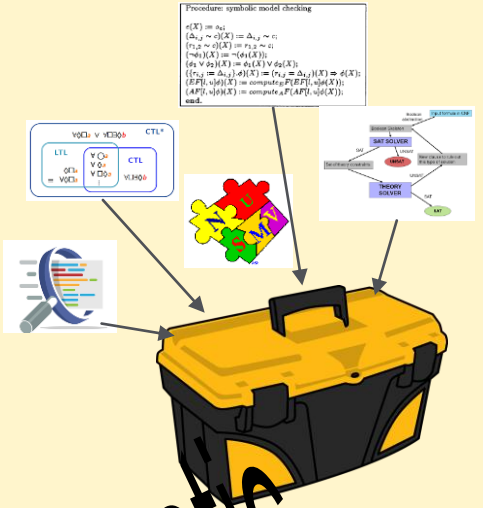
GLIPS

Automatic



*PLC program in GLIPS AST**

Control flow graph (CFG)



verification toolbox

Pillar

Automatic

(*AST : Abstract Syntax Tree
GLIPS : Schneider Electric Tool)

General

Ampère INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES LYON Life Is On Schneider Electric

Thank you for your attention !

Life Is On Schneider Electric

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES LYON