MATLAB EXPO 2018
Software modelling and verification for PLC-based automation plants
Alessandro Fantechi, Daniele Menchetti, Maurizio Tommasini
Dip. di Ingegneria dell'Informazione
Università di Firenze - Italy
THE REAL WORLD

Complexity

1400
I/O Signal

40 ms
Scan Rate

40k+
Interconnection
SAFETY LEVEL

People injury

Unavailability of services

Economic losses
PLC: A MULTILANGUAGE LITTLE BIG BRAIN

Ladder Diagram

Structured Text

| U  | %E1.3 |
| FP | %M102.0 |
| U  | %E1.5  |
| S  | %M3.0  |
| R  | %M3.3  |
| U  | %E1.6  |
| FP | %M105.0 |
| U  | %E1.5  |
| S  | %M3.3  |
| R  | %M3.0  |
| U  | %E1.4  |
| FP | %M106.4 |
| U  | %E1.5  |
| S  | %M3.4  |
| U  | %M3.0  |
| FP | %M107.0 |
HOW TO TEST IT?

1. Code porting
2. Model to test
3. Feedback
FIRST APPROACH: using SIMULINK to model the Ladder Diagrams behaviour
SIMULINK DRAWBACKS

High structural complexity of the model

Inaccurate modelling of LD sequential processing

Loss of generality of the approach
SECOND APPROACH: Choice of the Stateflow tool

Better model readability

Optimal model for sequential rungs execution

Higher model generality
CONVERSION TO STATEFLOW LOGICAL MODEL

Ladder Diagram PO

Stateflow Model PO

SA-System Tool
INSIDE A SINGLE STATE BLOCK....

```
Rung1
en: OUT=or(and(not(A),B),C,D);
```
TESTING:
What will happen???

- Semantic and syntactical
- Functionality
- Formal verification

MATLAB EXPO 2018
Example: missed initialization of variable

The data \texttt{LO\_HEATER\_AUTO\_MAN} was read before being written to.
State \texttt{Rung5} in Chart \texttt{’Chart’}: en: if(or(and(HS103\_START,not(LO\_HEATER\_AUTO\_MAN)),and(TSL105,HS101\_AUTO)))==1) \\ ^^^^^^^^^^^^^^^^^^^^^

This error will stop the simulation.
Component: Stateflow | Category: Runtime error
An error occurred while running the simulation and the simulation was terminated
Caused by:
Simulation stopped because of a runtime error.
Component: Simulink | Category: Block error

Focal point: from logical model go back to PLC software to resolve the error
FUNCTIONAL TESTS: FROM REQUIREMENTS.....

Textual requirements

- When IN passes from 0 to 1 then OUT is immediately set to 1 and stays in this state for PT milliseconds;
- When IN passes from 0 to 1 then ET is immediately set to SWEEP and increment of a value equals to SWEEP in each iteration up to ET is equals to PT. In the case which, while OUT is 1, IN passes from 1 to 0 and then from 0 to 1 before that ET is equals to PT, then OUT stays equals to 1 and ET is to 1;
- When ET reaches PT the OUT passes from 1 to 0.

Transformed in test signals using Signal Builder

Graphics requirements
Visual matching

Visual checking

.... TO TEST REPORT!
FORMAL VERIFICATION

Requirements

Observer blocks

High coverage
CONCLUSIONS

- **SA-System** tool with Matlab Stateflow/Simulink permits to obtain a unique testing/porting methods of PLC source code.

- SA-System team is working with industrial partners to optimize the tool.

- Potential application domains: Rail (RAMS Standards), Aerospace, Nuclear, Oil & Gas, Automation.
FUTURE DEVELOPMENTS

**Design Verifier:** formal system verification. DV needs free system input for testing all combinations

**Industrial software:** some system input have mutual links, must follow with attention!!

**Generalize the Front End:** to deal with different languages and dialects
SPECIAL THANKS TO:

- Nuovo Pignone and Sirio Sistemi Elettronici
- A. Bacciottini, F. Contini, G. Giusti (bachelor and master theses)

Thank you for the attention

Software modelling and verification for PLC-based automation plants.

Prof. Alessandro Fantechi, Ing. Daniele Menchetti, Ing. Ph.D Maurizio Tommasini

Dip. di Ingegneria dell'Informazione
Università di Firenze - Italy
email: alessandro.fantechi@unifi.it