Methodology and Toolset for Testing Highly Reconfigurable Programmable Logic Controllers

Miriam Ugarte Querejeta, Miren Illarramendi Rezabal, Goiuria Sagardui Mendieta

Mondragon Unibertsitatea - Faculty of Engineering
Goiru Kalea 2, 20500 Arrasate-Mondragon, Gipuzkoa, Spain

INTRODUCTION

At the core of the production system, the Programmable Logic Controller (PLC) orchestrates all necessary resources to initiate new processes, including modifications to the PLC program. For this reason, PLC software must be thoroughly tested to ensure operational safety.

At present, testing is conducted during commissioning, which typically takes place at the end of the development process, resulting in a significant impact in time and cost. In addition, the manual nature of testing practices requires considerable effort, and leaves the PLC open to errors. All these issues are further compounded in frequently changing and adaptive environments, hence the **need** to adopt new practices. In this regard, some authors have focused on automating the testing process of these programs by generating automated test cases. However, the cost-effectiveness of these tests is yet to be optimised, and their transfer to industrial PLCs remains a significant challenge.

OBJECTIVES

To address these gaps, the main goal of this research work is to provide a methodology to cost-effectively test and commission highly reconfigurable industrial PLC programs. Our approach focuses on the following objectives:

- **Objective 1**: to develop a tool to automatically generate and evaluate test cases for a wide range of IEC 61131-3 standardised FBD program
- **Objective 2**: to develop and evaluate test case selection metrics and algorithms for highly reconfigurable PLCs.
- **Objective 3:** to develop and evaluate a methodology to automatically perform SiL-based commissioning on industrial PLCs.

METHODOLOGY

We present a methodology to cost-effectively test the software of highly reconfigurable PLCs in industry. The methodology was implemented in the Siemens TIA Portal environment, which is designed to program, simulate, and test PLC programs. A SiL approach is proposed to validate the changes before commissioning and deploying the new PLC code into operations.

1. As the developed solution is designed for PLCopen XML programs, Siemens PLC programs should first be converted to PLCopen XML standards.
2. Next, the test generation tools parse the PLCopen XML code to define IEC 61131-3 Functions and Function Blocls, constant values, and input and output signals. This information is used to define the data paths and data path conditions for the FBD.
3. The test generation tool generates test cases based on structural coverage and mutation criteria.
4. The cost-effective metrics (including coverage, calculation, execution time and fault detection capability) of the generated test cases are evaluated then in the FBDTester 3.0. These measures are used as fitness metrics to select the optimal subset of the test suite for error detection.
5. The execution results of the selected test cases are employed as oracles to define test output assertions. With this information, TIA Test Suite application tests are generated.
6. Finally, the PLC code is executed with given input data in the simulation environment.TIA Portal establishes a connection with PLCSim Advanced simulation environment and compares the obtained results with the expected behaviour. In this way, the newly modified PLC code is validated through the imported application test cases in TIA Portal Test Suite.

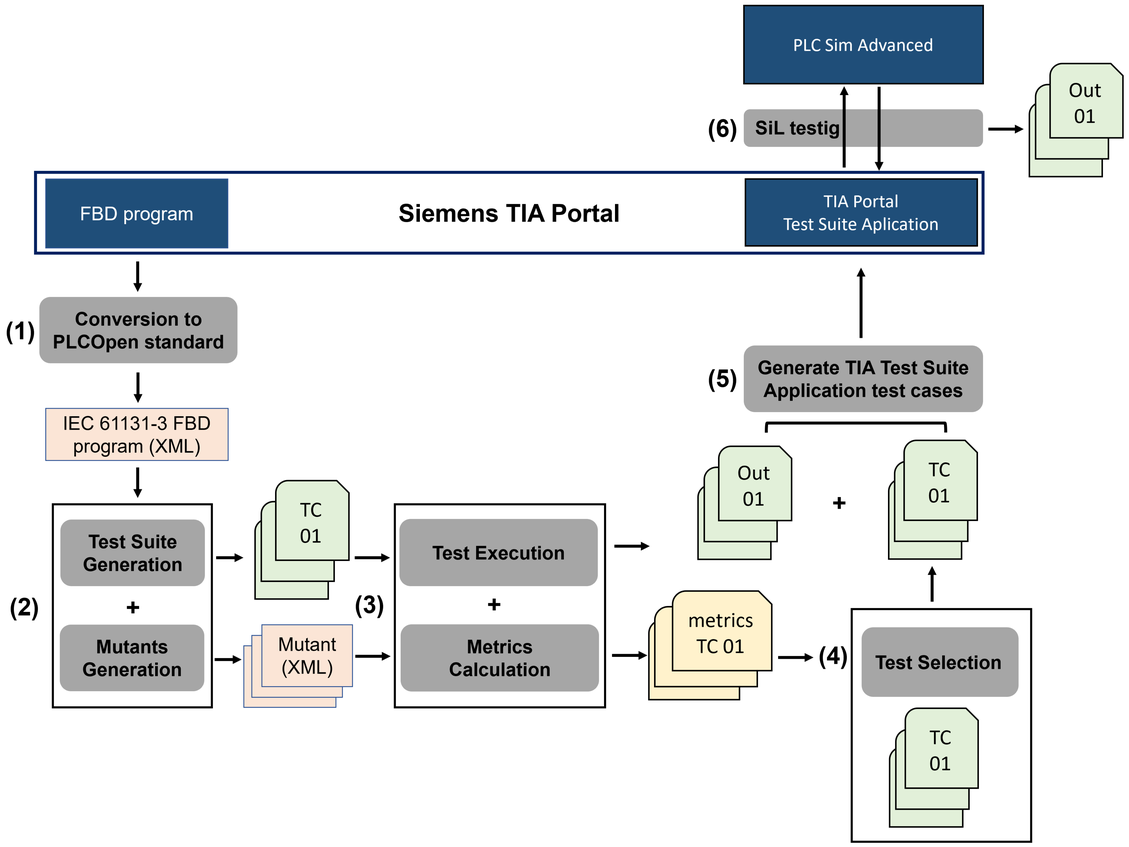

Figure 1: Overview of the methodology

EVALUATION

The methodology was developed under the framework of the DiManD ITN programme. The DiManD project supports the development of a holistic framework for future highly intelligent, adaptable, and responsive manufacturing infrastructure. In this context, the main objective of this body of research was to build an agile and robust testing methodology to validate systems undergoing frequent changes. Two industrial case studies were defined to validate the proposed methodology:

1. Omnifactory, which is the future automated aerospace assembly demonstrator at the University of Nottingham, and is envisaged to showcase the DiManD integrated project as one of the main beneficiaries of the project.
2. A CNC machine tool solution at Danobatgroup, which is an industrial partner of the DiManD project.

In addition, four use cases from the Korea Nuclear Instrumentation and Control System (KNICS) reactor protection system were employed to validate the developed test generation and test the optimisation techniques.

RESULTS

1. Our findings demonstrate that coverage-based and mutation-based testing can be used to automatically generate test cases for most of the IEC 61131-3 function groups, including complex and non-linear arithmetic functions. This is attributed to the integration of the new Yices 2 SMT2 solver into the test generation process.
2. Our findings demonstrate that search-based test selection algorithms optimise the selection of the generated test cases in a cost-effective manner, in which the search-based NSGA-II algorithm outperformed RS in 95.24% of the experimental scenarios. Specifically, the NSGA-II algorithm in combination with the CCC_T ET metric showed the most optimal solutions in 83.33% of the experimental scenarios.
3. The results validate that the presented PLC testing methodology can successfully test Siemens PLC programs for non-time dependent FBD programs. However, the methodology was not found to be valid for testing time related FBD programs.

CONCLUSIONS

In this study, we present a methodology to cost-effectively test industrial PLC programs with the aim of reducing commissioning time, while ensuring a high level of reliability. To this end, our study leverages advances in CPS testing techniques and employs regression testing solutions to cost-effectively test the PLC code. This helps maximise existing manufacturing resources by promoting the continuous integration of PLCs. To this end, we introduced a simulation-based approach to automatically tests PLCs by applying software engineering techniques to commercially available automation solutions.

By automating conventional practices our methodology can effectively test real industrial PLC programs, which ultimately reduces costs and time, and ensures the reuse of available resources.

The proposed methodology is based on PLCopen XML format IEC 61131-3 projects, hence the methodology promotes interoperability by supporting open standards. However, at present most PLC vendors do not fully follow the IEC 61131 specifications, which limits the ability to exchange PLC programs between different devices

As future lines, we envisage transferring this knowledge into industry in two ways: 1) showcasing our technology on the Omnifactory platform, which will be used to demonstrate the future assembly platform for the aerospace industry, and 2) working with Danobatgroup to enhance the PLC acceptance process of their machining solutions,

REFERENCES

- Miriam Ugarte Querejeta, Leire Etxeberria, Goiuria Sagardui, Gorka Unamuno, and Iñigo Bediaga. ``**Virtual commissioning in machine tool manufacturing: a survey from industry**" in DYNA Ingeniería e Industria (2021), 96 (6), pp. 612-619.
- Miriam Ugarte Querejeta, Miren Illarramendi Rezabal, Gorka Unamuno, Jose Luis Bellanco, Eneko Ugalde, and Antonio Valor Valor. ``**Implementation of a holistic digital twin solution for design prototyping and virtual commissioning**". IET Collaborative Intelligent Manufacturing (2022), vol. 4 (4), pp. 326-335.
- Fan Mo, Miriam Ugarte Querejeta, Joseph Hellewell, Hamood Ur Rehman, Miren Illarramendi Rezabal, Jack C. Chaplin, David Sanderson, Svetan Ratchev. ``**PLC Orchestration Automation to enhance Human-Machine Integration in Adaptive Manufacturing Systems**''. Journal of Manufacturing Systems (2023), 71, pp, 172-187,
- Miriam Ugarte Querejeta}, Leire Etxeberria, and Goiuria Sagardui. ``**Towards a DevOps Approach in Cyber Physical Production Systems Using Digital Twins'' at the International Conference on Computer Safety, Reliability, and Security** " (2020), pp. 205–216.
- Miriam Ugarte, Leire Etxeberria, Gorka Unamuno, Jose Luis Bellanco, and Eneko Ugalde. ``**Implementation of Digital Twin-based Virtual Commissioning in Machine Tool Manufacturing**" in Procedia Computer Science (2022), 200, pp.527-536.
- Itziar Ricondo, Alain Porto, Miriam Ugarte. ``**A digital twin framework for the simulation and optimisation of production systems**" in Procedia CIRP (2021), vol. 104, pp. 762-767.
- Miriam Ugarte Querejeta}, Pablo Valle, Aitor Arrieta, Eunkyoung Jee, Lingjun Liu, Miren Illarramendi Rezabal. `` **Search-based test case selection for PLC systems using functional block diagram programs**." 2023 IEEE 34th International Symposium on Software Reliability Engineering (2023).

ACKNOWLEDGEMENTS

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 814078

mugarte@mondragon.edu