2nd IFAC Workshop on Automatic Control in Offshore Oil and Gas Production,
May 27-29, 2015, Florianópolis, Brazil

Automatic test of safety specifications for PLC programs in the Oil and Gas Industry ⋆

T. J. Prati, J. M. Farines, M. H. de Queiroz

Departamento de Automação e Sistemas,
Universidade Federal de Santa Catarina, Florianópolis, Brazil
(thiagojprati@gmail.com, j.m.farines@ufsc.br, max.queiroz@ufsc.br)

Abstract: The software of Programmable Logic Controllers (PLC) for Safety Instrumented Systems in the oil and gas industry is designed based on safety specifications that must be validated prior to deployment. This paper proposes a method for the automatic test of the Cause and Effect Matrix specifications on PLC systems. For such testing, the specifications are represented as a set of Petri net models that observe the controlled system behavior. The use of a formal model allows to systematically compose and translate the Petri Nets into a program that commands the PLC inputs and observes when the PLC outputs fail the safety specifications. A prototype tool has been developed to automatically perform the test of the Cause and Effect Matrix on a given PLC. A furnace project has been used to ascertain that the proposed method is easy to use and viable.

Keywords: Programmable Logic Controllers; Automatic Testing; Validation; Petri Nets

1. INTRODUCTION

The complexity of industrial control problems can reach large scales. In the Oil and Gas Industry, specific control systems may be used to perform such automation tasks that require a high degree of reliability, since faults can lead to serious and costly equipment damage, environmental damage and even loss of human life, as seen on Skogdalen and Smogeli (2011). Specially for Safety Instrumented Systems, the software development of Programmable Logic Controllers (PLC) requires great attention since it deals with strict requirements, which may include time constraints, safety and reliability. For the development of such automation projects, companies often use standards that have as an objective the construction of an automation software that meets the project requirements.

The methodology for development of automation systems currently adopted by oil and gas companies consists of a sequence of steps starting from basic specifications of the plant to be automated and ends with the development of a software used in a PLC for automation. This methodology uses a set of general and mostly internal standards, as the Petrobras standards N-1883 and N-2595. According to these standards, a range of documents containing relevant information along the project is created. The cause and effect matrix ($C\&E$ Matrix), for example, is a document that defines the relation of field signals which indicate critical situations to the proper safety actions. The Factory Acceptance Test (FAT) document describes how to test the final automation program in order to validate the PLC program, from the plant equipment interaction and signals as described on the project documents.

In order to create and validate a PLC program, techniques based on the correct construction of a program or techniques based on testing programs can be used, as, for example, the methods in Biallas et al. (2012), Farines et al. (2011) and Squillante (2011). Petri Nets, timed automata and other formal methods have been widely used for validation in the research field because they offer a mathematical way to assure that the program performs the expected behavior. More information on the subject of Petri nets can be found on Murata (1989).

Bel Mokadem et al. (2010), Soliman and Frey (2011) and Zoubek et al. (2003) deal with formal verification of safety and time restriction properties by modeling a PLC and plant with Timed Automata and model-checking with the tool named UPPAAL [1] The approach presented in Rossi and Schnoebelen (2000) is based on automata as formal semantics of PLC programs and symbolic model checking of temporal properties. Farines et al. (2011) propose a model-driven engineering (MDE) approach to model and verify PLC programs written in Ladder Diagram. PLC and plant are modeled in an intermediate language named Fiacre [2], according to transformation models. A verification toolchain is built around Fiacre, in order to guarantee the satisfaction of generic properties of the PLC as race-condition (constant alternation of PLC outputs), deadlock (point in which the program is locked on the same state indefinitely) and application-oriented properties as safety and reachability.

⋆ We would like to thank the CAPES organization for providing financial support during this work and Petrobras engineers for providing documents and discussions about the test methodology.

[1] http://uppaal.org/
[2] http://projects.laas.fr/fiacre/

Squillante et al. (2010) propose a methodology for generating programs for safety instrumented systems based on Bayesian network and Petri Net. In this work, the documents of the project are used to create Bayesian networks responsible for diagnostics of the field while Petri nets are defined as the functions that should be executed given some positive diagnostic (safety function). The Bayesian networks are later translated to Petri nets, fused with the corresponding safety functions (also Petri nets) and finally transformed into Ladder code.

In Oliveira et al. (2012), a methodology for testing PLC programs through class equivalence is proposed. In this work, four steps are defined in order to test a PLC program. The project specification is transformed in timed automata, this automata is used to generate test cases, these cases are executed in a PLC trough Open Platform Communications (OPC) and finally, a veredict is given by comparing these test cases with the expected output from the model generated. The decision about test case to be generated, is based on equivalence classes because it only selects the minimum number of cases to activate each output at least once.

The objective of this paper is to present a new method for systematically testing safety specifications in PLC programs. This method can be used as an auxiliary tool to support the FAT, so that it can be automated in order to save time of project commissioning and to enhance the coverage of tests. For the proposed methodology, the information contained in the $C\&E$ Matrix is used to generate an observer based on Petri nets. The same document is used to determine a series of inputs for the PLC. These inputs characterize the tests to be conducted. The information acquired during these tests (inputs and outputs of the PLC) are then compared with the observer results to determine whether the system has met the requirements stated on the cause and effect matrix or not.

We present in section 2 the current methodology development and testing adopted by Oil and Gas Companies, and, in section 3, the new methodology for automatic PLC program testing. Finally, in section 4, we show and discuss the usability and feasibility of methodology and its associated tool from the application to a furnace test case.

2. AUTOMATION PROGRAM DEVELOPMENT METHODOLOGY

The currently adopted methodology for automation systems development in Oil and Gas includes the creation of many documents in a particular order, each document providing important information for the development of project. For example, among the documents defined by the Petrobras internal standard 1883, some are directly connected with the final PLC program used for the plant automation:

- Piping and instrumentation diagram($P\&I$ Diagram): it contains representation of the control loops, variables, functions, localization, and also control, safety and relief valves.
- Cause and effect matrix ($C\&E$ Matrix): it shows the inter-relationship between the abnormal events likely to occur during normal operation of the plant or equipment and in particular the actions to be taken by the safety system. The matrix lines represent the signals from the field while the columns, the signals to control equipment on the field. If a line is related with a column, this means that, if a field signal is active, the related equipment should be activated or deactivated according to what is specified. Besides the relation between a sensor signal and an equipment signal, the matrix also contains specific notes that can modify the action that must be taken or determine different treatments for the arriving signals. These notes may contain information on signal voting, command sequencing or timing.
- Descriptive memorial: it contains basic information to allow complete specification of equipment and instruments for the various instrumentation systems and also the sequencing which exists in the plant.
- Logic Diagram: it is based on the descriptive memorial of the protection systems, interlocking and signaling alarm and also, is built using boolean algebra. This document is intended to represent all the interlocking logic in the project and can be thought as a preview of the final PLC program.
- Factory Acceptance Test document (FAT Document): a textual document containing all the test cases that should be executed in order to validate a given PLC program.

The generation of the Descriptive Memorial and the $C\&E$ Matrix is based on information from $P\&I$ Diagram plus the knowledge from experts and SIS standards. Combined information from $C\&E$ Matrix and Descriptive Memorial allows the creation of the Logical Diagram, which specifies the PLC program in detail, and the FAT Document, that is used as a guide for manual tests during the system commissioning.

Once the programmed PLC is delivered for commissioning, the period reserved for its approval, by using the FAT Document, is relatively short. This results in the need to perform multiple tests in a short space of time. Likewise, not all test cases that an expert can conceive are inserted in the document. Besides, time spent testing is a variable of great importance, and each extra test requires more time for validating the PLC program.

3. AUTOMATIC TEST BASED ON $C\&E$ MATRIX

The purpose of the methodology to be presented in this section is the integration into the existing design methodology used internally by Petrobras. It offers the possibility of automating the test procedure and exploring more test cases due to its systematic approach. The proposed methodology consists in using the $C\&E$ matrix, part of the requirements of the PLC program, as a starting point. The $C\&E$ matrix has been chosen because it contains the safety properties the system must obey and it leads to an easy translation into a formal model.

As discussed before, the $C\&E$ matrix specifies safety actuation based on relations between field sensors and also field equipments. Besides assigning signals detecting an abnormal condition (cause) to the equipment to be put into a safe state (effect), each relation in the $C\&E$ matrix may contain a note with additional requirements

on sequencing or timing of safety actions. These notes can also specify the way multiple signals must be combined to activate a given cause, for example, by a voting rule. Fig. 1 shows a note in the *C&E* matrix of a furnace project. In this case, the safety action of closing and opening valves must follow a specified timed sequence after detection of high pressure in pilot.

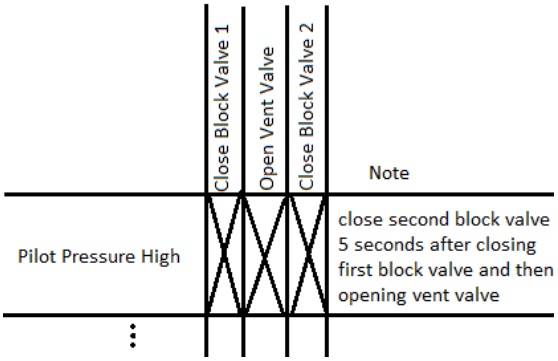

Fig. 1. Example of a *C&E* matrix row with note forcing a timed sequence

The information contained in the *C&E* matrix allows the specification of test cases and also the creation of Petri net models that represent the expected PLC software behavior. The test cases generation results in a sequence of PLC inputs related to the lines of the *C&E* matrix. The PLC is executed to command a simulation of the real plant via an industrial protocol like OPC, with its inputs being forced according to the test sequence. The PLC output data is stored for later use. Models of Petri nets previously created are then used as observers for the comparison; they are fed with the outputs recorded previously and then, according to the final state each model reaches, it is possible to determine whether there is an error or not.

Fig. 2 presents the proposed automatic test inserted in the current software development methodology (Section 2). The test of general specifications from the Descriptive Memorial is still documented by FAT and manually executed on the implemented automation system. On the other hand, a Test Generation tool automatically translates the safety specifications of the *C&E* matrix into test cases and formal observers that are used by a Test Execution tool to automatically force PLC inputs and read PLC outputs, indicating the observed errors in the Test Result.

3.1 Generation of Petri net observers

Based on each type of relations found in the *C&E* Matrix, a class of Petri Net observer is defined . Each observer instance must detect when the outputs from a PLC program under the presence of some field signal follows the expected behavior or not. A *C&E* Matrix may include the following classes of relations between field signals and actions:

Single boolean input The simplest case is the direct relationship between an input and an output in the *C&E* matrix. The Petri net model that represents this class of relation is shown in Fig. 3. Places "PLC input" and "PLC output" indicate respectively the arrival and the sending of a field signal. In this observer, once a signal arrives

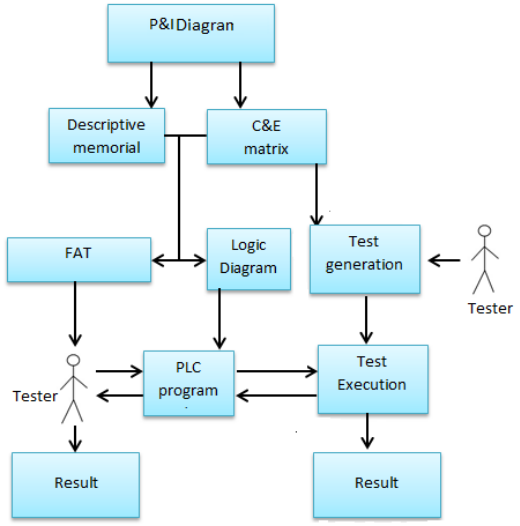

Fig. 2. New proposed project methodology where a tester only has to command the start of the procedure.

from the field, the PLC has "t" seconds to produce the respective output. When it happens, the place "Ok" will be reached, if not, the place "NOk" will be reached.

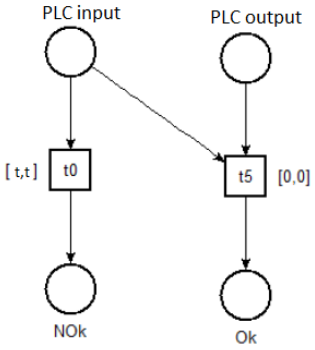

Fig. 3. Observer for a simple boolean input

Multiple boolean input This observer represents that the PLC output must be activated when at least **n** signals from the PLC input group are active at the same time; the arc weight **n** in the Petri Net model expresses this condition. The behavior regarding time is the same as described for the simple boolean input. The only difference between both observers is the mandatory presence of n signals simultaneously from the field. The structure of the Petri net would be the same as in Fig.3, except that the place representing PLC input would now represent a group of PLC inputs and its output arcs have weight n.

Voting Another *C&E* Matrix construction regards the combination of boolean inputs according to voting logic, like one one out of two of two (1oo2) and two out of three (2oo3). These rules are used when the logical signal has more than one physical signal on the field. In 1oo2 voting, there are two redundant signals arriving from the field and, if one of them is active, then the resulting vote should be considered active. In 2oo3 voting, it is necessary that at least two of three signals are coherent (and active) for the vote to be considered. Fig. 4 and

5 present the corresponding observers. Even though the voting observer could be represented as a multiple boolean input observer, it was chosen to create different models for these signal treatments due to its wide spread utilization and to represent a clean view of its structure.

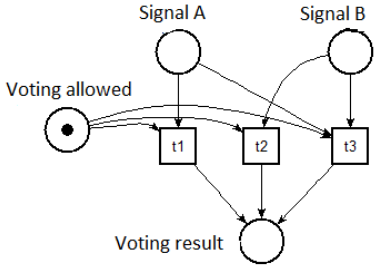

Fig. 4. Observer for a 1oo2 voting

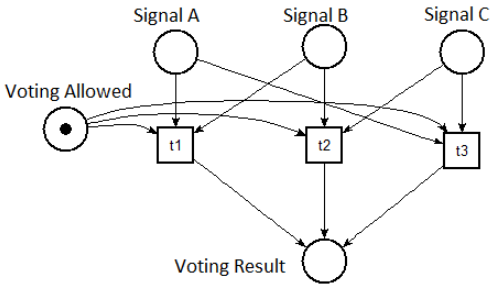

Fig. 5. Observer for a 2oo3 voting

Outputs with timed sequence Another common case found in *C&E* Matrix notes is the existence of sequencing within the safety actions triggered by an input signal. To illustrate one possible sequence, the note presented in Fig. 1 is used as basis for the observer making, which can be seen in Fig. 6. Three steps must be orderly performed when very high pressure is detected in the pilot: firstly, it is necessary to close the first block valve, then to close the vent valve, and after 5 seconds, to close the second valve block. The Petri net model in Fig. 6 has three places representing PLC output signals ("Close valv. 1", "open vent valv." and "Close valv. 2") and one place, representing a PLC input signal ("pilot pressure high"). In this model the path composed of the transitions t1, t4, t6 and t10 represents the expected path for proper operation. Transitions t0, t2, t5, t7, t9 and t12 lead a token to the places that identify every possible execution error. Note that such an observer can be systematically designed for any given timed sequence.

Observer composition Each specification in the *C&E* Matrix may be represented as an instance or as the combination of multiple instances of relation classes. For example, the "pilot very high pressure" signal that triggers the sequence in Fig. 1 could be the result of a 1oo2 voting or 2oo3 voting. The composition of observers can be computed according to a Petri Net formal operation named place fusion (Murata (1989)). Fig. 7 exemplifies the place fusion between 1oo2 voting observer (with dashed outline in the figure) and the observer for a simple boolean input (continuous outline in the figure).

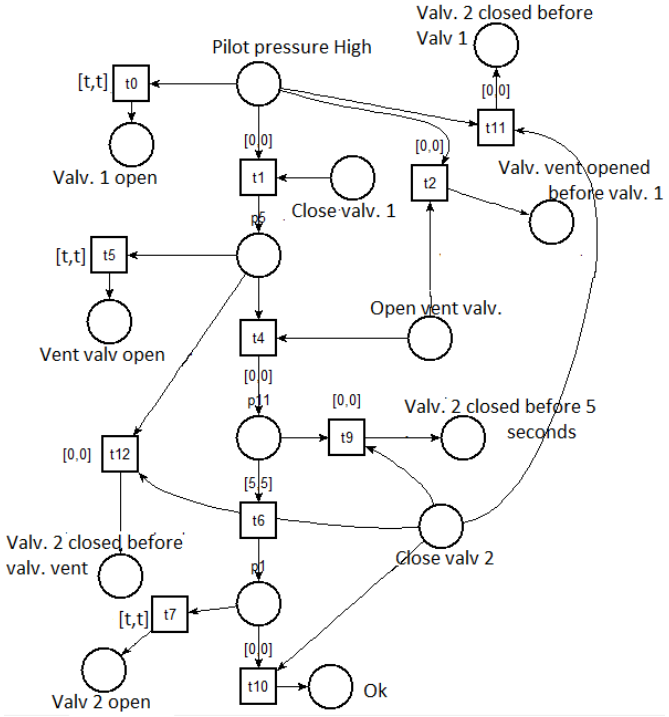

Fig. 6. Example of observer for timed effects

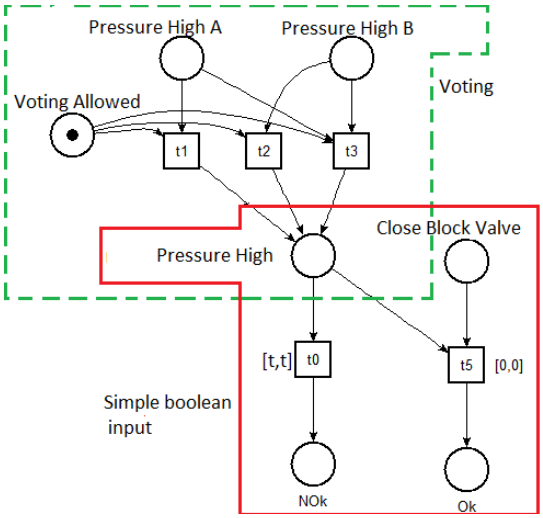

Fig. 7. Example of fusion between observers

3.2 Generation of Test Cases

The test list includes inputs to be forced on the PLC. Each test case should have at least one row and one correspondent column of the *C&E* Matrix, i.e., a field signal and all the related actuators.

Three types of tests are defined: tests for single boolean input, tests that require voting and tests for multiple boolean input. The single boolean input test forces the corresponding input of the *C&E* Matrix. For a test with voting, a combination of tests must be generated in order to include all the voting possibilities. For multiple boolean inputs, each test must force active the minimum amount of signals in order to activate the corresponding logical signal.

3.3 Execution of Tests

The generated tests are stored in the form of a list that indicates, for each test case, which entry should be enabled. During test execution, the following is done:

- Activating or deactivating a specified entry in the list of tests;
- Storing variables and time, relative to the start of the test;
- Awaiting the end of the test case;
- Beginning the next test case.

3.4 Evaluation of Test results

At the end of the testing phase, the inputs and outputs of the PLC are stored. This data is used in this phase to execute the observers and evaluate the success of the test. For each test case performed in the last phase, an equivalent observer is selected and by using the stored values, the observer is executed until it reaches a final state. The final state of the observer is then used to assert whether the test is successful or not.

4. APPLICATION OF THE PROPOSED METHODOLOGY

In order to check the feasibility of the proposed methodology, a case study based on a furnace is presented. The documents of this furnace are provided by Petrobras and represent a real project developed by this company.

4.1 Development of a test tool

An automatic tool based on the proposed methodology has been built. As input for the tool, the information of the *C&E* Matrix is translated into an ASCII text file, where the relations between signals and equipments are written on lines and the possible specifications are added on the end of each line. From this text file, the tool generates automatically both the test cases and the observers. On a simulated plant, the tool executes the test cases and stores the PLC input and output values and time stamps during the test. For the communication between the simulation and the tool, we choose the OPC for its great acceptance and ease of use. With the stored information (PLC IOs) and the already generated observers, the tool can then execute each observer using this information as input for the execution. Based on the final state achieved by the observer, it is possible to indicate if there is an error or not. Finally, with the conclusion of the occurrence of an error, the tool outputs a log informing the user. Fig. 8 presents the tool internal structure and the described information flow.

4.2 Application to a Furnace test case

A furnace is a heat exchanger. It burns a fuel, which releases hot gases; the ones in contact with a coil inside the furnace provide heat to a fluid. A complete furnace description is presented in Silva (2009). Based on *P&I* Diagram and Descriptive Memorial of a Furnace Automation case provided by Petrobras, a simple simulation has been developed in Matlab to perform the tests.

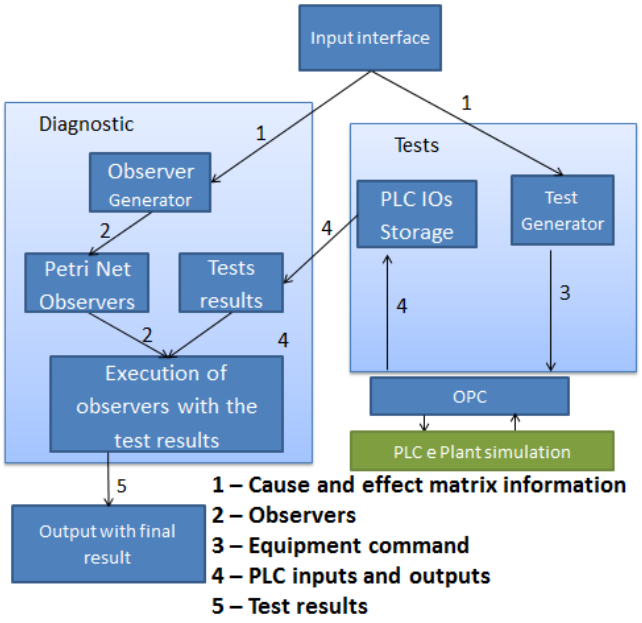

Fig. 8. Tool internal structure

The specifications of the SIS for this furnace is given on a *C&E* Matrix with 26 lines, 33 columns and 17 notes. Based on this document, a Siemens S7-1200 PLC has been manually programmed in order to control the Matlab simulation via OPC. The *C&E* Matrix provided by Petrobras has been written in a text file with the notes translated from natural language to standard formulas.

The proposed methodology is then applied to these formulas, following the same steps of the methodology already explained. For the *C&E* matrix used for the test, a total of 105 observers have been generated and the corresponding tests have been systematically executed. When errors were inserted in the PLC program, the tool was able to determine their existence, showing the information provided by the observer for the corresponding failing specification. One case is going to be explained in detail to clarify the test case and how to possibly locate an error.

For illustration, we choose as an example the following scenario: in the specific PLC program, there is a function for 2oo3 voting. Signal A, B and C are the inputs and Result is the output of this block. We insert an error in order to test whether the tool would be able to detect it. Fig. 9 presents the error (in the third rung, Signal B in place of Signal A).

After the complete execution, the tool generates the output presented in Fig. 10. Each test sequence is used for executing one observer and is presented as one simulation on the Log. Each simulation handles one input signal and the respective output signals as dictated by the *C&E* matrix. Each simulation presents the variables used on the test case, inputs and outputs, as well as a short sentence relative to the error that occurred. On Fig. 10, "PSHH" is an input signal and means high pressure while "XY" are valves that should be closed or opened upon the arrival of a "PSHH" signal. The signals PSHH-014A, PSHH-014B and PSHH-014C are respectively the inputs Signal A, Signal B and Signal C for the 2oo3 voting block described above.

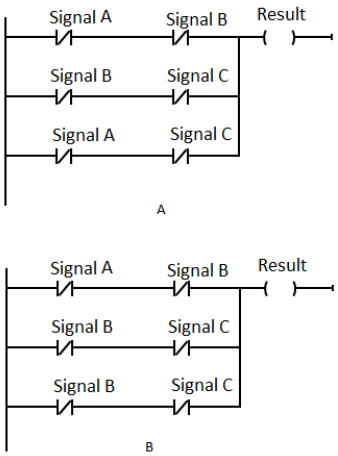

Fig. 9. Program correct (Part A), with error (Part B)

The result presents an error message that the ventilation valve opened before the block valve and this message is also present on the other tests. As a user, these messages indicate possible locations of the error on the code. If there is an error message only on some messages, this means the error must be on a section responsible for handling only the signals corresponding to those messages. Since the same error message is present on all the tests regarding 2oo3 voting, it must mean the error is present on a section common to all of those signals, that is, the voting itself.

```
Log:
Total generated observers: 140
Total tests executed: 49

Possible error encountered
Signals involved: PSHH014A, PSHH-014B, PSHH-014C
Equipment involved: xy-015V, XY-015B, XY-018
Ventilation valve opened before block valve

Possible error encountered
Signals involved: PSHH014A, PSHH-014B, PSHH-014C
Equipment involved: xy-026V, XY-026B, XY-029
Ventilation valve opened before block valve
                    .
                    .
                    .
```

Fig. 10. Output generated by the developed tool

5. CONCLUSION

A complementary test methodology for the development of automation projects in the oil and gas industry has been presented. This methodology allows to automatically test safety specifications in the implemented PLC as an auxiliary tool to the FAT, reducing the deployment time and the possibility of human error in test. For such testing, the safety specifications of *C&E* matrix are represented as a set of Petri net models that observe the controlled system behavior. The use of a formal model allows to systematically compose and translate the Petri Nets into a program that commands the PLC inputs and observes when the PLC outputs fail the safety specifications. For each class of observer, it is also possible to define a series of test cases to be executed in order to validate the corresponding specification. The execution of the test cases and posterior use of the observers to check against the PLC behavior allow a validation of the implemented program without the need to deal with the PLC source-code. The methodology has been implemented as an automatic test tool to demonstrate its utility at pointing the presence of safety errors in the code of a programmed PLC as well as its feasibility and ease of use. Furthermore, *C&E* Matrix is a standard document widely used in automation projects, making it possible to extend the proposed methodology not only to other oil and gas automation projects but also to other application domains.

REFERENCES

Bel Mokadem, H., Berard, B., Gourcuff, V., De Smet, O., and Roussel, J.M. (2010). Verification of a timed multitask system with uppaal. *Automation Science and Engineering, IEEE Transactions on*, 7(4), 921–932.

Biallas, S., Brauer, J., and Kowalewski, S. (2012). Arcade. plc: A verification platform for programmable logic controllers. In *Automated Software Engineering (ASE)*, 338–341. IEEE.

Farines, J.M., de Queiroz, M.H., da Rocha, V.G., Carpes, A.M.M., Vernadat, F., and Crégut, X. (2011). A model-driven engineering approach to formal verification of plc programs. In *Emerging Technologies & Factory Automation (ETFA)*, 1–8. IEEE.

Murata, T. (1989). Petri nets: Properties, analysis and applications. *Proceedings of the IEEE*, 77(4), 541–580.

N-1883 (2002). Petrobras Internal Standard 1883, Project Instrumentation Presentation.

N-2595 (2012). Petrobras Internal Standard 2595, Specification for Project and Maintenance of Safety Instrumented Systems in Industrial Unities.

Oliveira, K.V., Silva, L.D., A, P., and Gorgonio, K.C. (2012). Uma abordagem para geração e execução de casos de teste em programas de sistemas instrumentados de segurança. In *Anais do XIX Congresso Brasileiro de Automática, Campina Grande, Brazil*.

Rossi, O. and Schnoebelen, P. (2000). Formal modeling of timed function blocks for the automatic verification of ladder diagram programs. In *Proc. 4th Int. Conf. Automation of Mixed Processes: Hybrid Dynamic Systems (ADPM'2000), Dortmund, Germany*, 177–182.

Silva, M.K. (2009). *Pré-Detalhamento da Instrumentação e Automação de um Forno Industrial de um Complexo Petroquímico*. Master's thesis, UFSC.

Skogdalen, J.E. and Smogeli, Ø. (2011). Looking forward-reliability of safety critical control systems on offshore drilling vessels. Technical report, Deepwater Horizon Study Group.

Soliman, D. and Frey, G. (2011). Verification and validation of safety applications based on plcopen safety function blocks. *Control Eng. Practice*, 19(9), 929–946.

Squillante, R. (2011). *Diagnostico e tratamento de falhas críticas em sistemas instrumentados de segurança*. Master's thesis, USP.

Squillante, R., Santos Filho, D., Junqueira, F., and Miyagi, P. (2010). Safety instrumented system designed based on bayesian network and petri net. In *8th ICNPAA, Sao Jose dos Campos, Brazil*.

Zoubek, B., Roussel, J.M., and Kwiatkowska, M. (2003). Towards automatic verification of ladder logic programs. In *IMACS-IEEE" CESA'03":" Computational Engineering in Systems Applications"*.