HAL
open science

Transforming your computer center to an Emulated Industrial Laboratory

Mohamad Haffar, Jean-Marc Thiriet, Khaled Mechref, H. Ziade

To cite this version:

Mohamad Haffar, Jean-Marc Thiriet, Khaled Mechref, H. Ziade. Transforming your computer center to an Emulated Industrial Laboratory. CIFMA 2010 - 4ème congrès international francophone de mécanique avancée, Apr 2010, Alep, Syria. 8 p. hal-00529329

HAL Id: hal-00529329

https://hal.science/hal-00529329v1

Submitted on 25 Oct 2010

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Transforming your computer center to an Emulated Industrial Laboratory

Mohamad HAFFAR[1], Jean-Marc THIRIET[2], Khaled MECHREF[3], Haissam ZIADE[3]

1 Euro System – Grenoble – France, mohamad.haffar@euro_system.fr
2 GIPSA Lab – Grenoble – France, jean-marc.thiriet@ujf-grenoble.fr
3 Lebanese University – Tripoli – Lebanon, kmechref@ul.edu.lb; hziade@ul.edu.lb

Abstract: In this paper we will show the method we adopt to transform normal laboratories to Emulated Industrial Laboratories 'EIL' for industrial research studies. We will also explain the tools and communication protocols that we have developed to accomplish this migration. Finally we will give an idea on how we evaluate Industrial Automation System (IAS) network performance and respond a lot of industrial interrogations such as network industrial response time, system reliability etc.

Keywords: PLC, Simulator, Modbus Protocol, Industrial network.

1. Introduction

The automation of industrial installations is nowadays ensured using the programmable logic controllers 'PLC'. Supervision control and data acquisition system 'SCADA' is used in these kind of installations to monitor, control and command all the PLCs equipments inside the installation. SCADA system and PLCs are interconnected via Ethernet network in order to form the whole industrial automation system 'IAS' architecture.

Substation Automation System 'SAS' is one of these industrial automation systems. SCADA system, PLCs and Intelligent Electronic Devices are incorporated in SAS architecture. In this kind of architectures, critical and safety networks are implemented in order to solve critical situation, ensure the security and avoid the blackout of the whole system. This is considering one of the most important strategic research problems in industries.

The reliability of the system relies on sending a large number of real time messages via the communication network which increase the usage of the network bandwidth and degrade the time performance of the IAS architecture. In some cases, a large number of queries are dropped due to the network charge which causes a real actual problem in word of industry.

The IAS network could be separated into two levels: process level (PLC's level) and station level (supervision level). Our paper will introduce the way we simulate these two levels.

Our approach consists on transforming any computer centre to an Emulated Industrial Laboratory (EIL) in order to realize any IAS project and give a performance study of the IAS network architecture according to the scenario of exchanging data defined by the user. Using this EIL, we can study and install any PLC program, SCADA application, build up the whole network architecture and finally setup new research applications that evaluate the performance of the IAS network. In such a way, any computer in the EIL can be transformed to a PLC or to a supervisor panel. This permits the user to develop and build any PLC industrial project at the process level and develop any SCADA applications at station level with large number of scenarios for exchanging data between the PLCs and SCADA system.

Different kind of SCADA such as servers, redundant servers, light clients and heavy clients will be installed to ensure the reactivity of the EIL laboratory. PLC computers will be interconnected to the IAS network in order to serve the queries coming from SCADA client or SCADA servers. Once the PLC program is done and the SCADA application is well configured, different networks topologies will be proposed in order to setup communication between IAS equipments. This is done using real networks equipments such as switches, routers and hubs.

Network analyzers and dedicated software can be installed in all computers in order to evaluate and discuss the performance of the network. If needed, the topology/ scenario of the IAS architecture can be modified.

In our paper, we will show the method we adopt to transform normal laboratories to EIL industrial research laboratories. We will also explain the tools that we have developed to evaluate IAS network performance and respond a lot of industrial interrogations such as network industrial response time, system reliability etc.

2. Architecture Overview

Each industrial automation system IAS is composed of two essential bus, station bus and process bus. In the process bus we can easily identify the existence of PLCs interconnected via a local area network. The station bus permits the transmission of data between PLCs and Interface Human Machine 'IHM' in order to ensure the supervision, control and command of the process.

The figure 1 shows a typical IAS architecture.

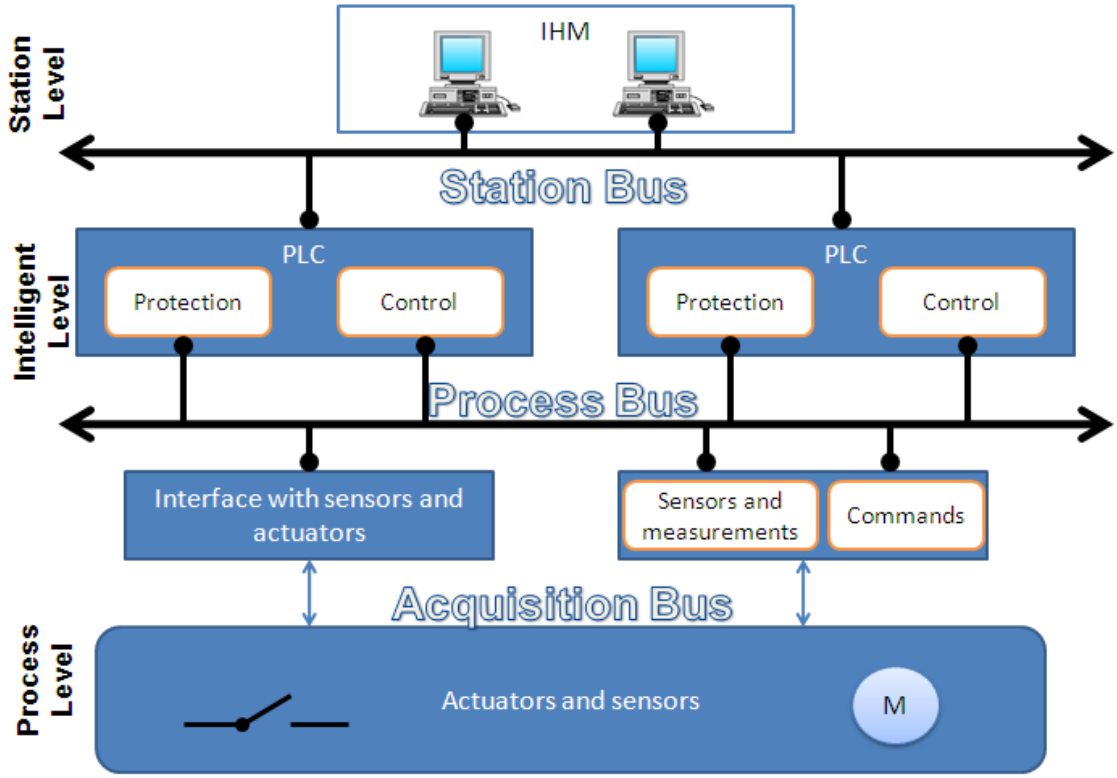

Figure 1: IAS Architecture

2. PLC Composition

2.1. Rack of cards

Each PLC is composed of several card interconnected through a metallic rack. Each card has a specific job to ensure the complete work of the automation process.

As shown in the figure 2, the most essential cards that we can find are the power supply, processor module, input card, output card, digital input card, digital output card and communication card.

Communication card are usually used inside the processor module.

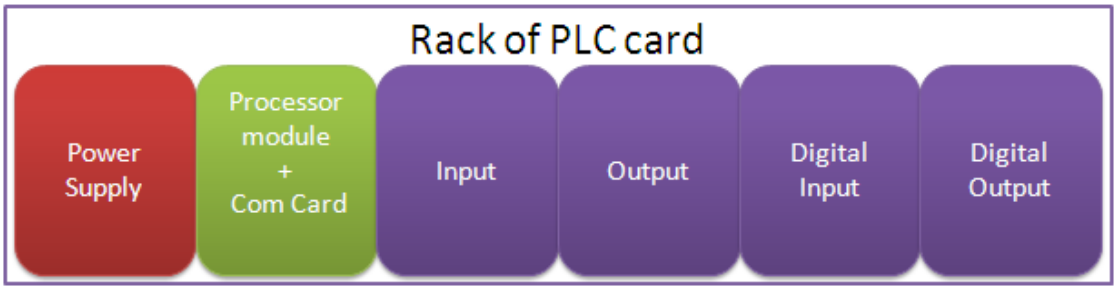

Figure 2: PLC components

The connection between the processor module and input/output cards is ensured using several buses that exists inside the rack. We can identify three different buses:

- Data Bus.
- Address Bus.
- Control Bus.

2.2. Program Execution

The execution mode of a PLC program is divided into three phases:

1- Input acquisition.
2- Program processing.
3- Output activation.

The scheduling of these phases is very important. The execution of each program cycle must begin with the phase 1 and finish with the phase 3.

At the input acquisition phase, the real inputs are transmitted to a specific memory area of the processor module through the rack busses. Once finish, the program processing phase uses the input memory area to realize the program. At the end of the cycle, the statuses of all outputs are transmitted from the outputs area memory of the processor module to the outputs cards. This transmission uses also the Rack busses.

The figure 3 illustrates the execution mode of a PLC program.

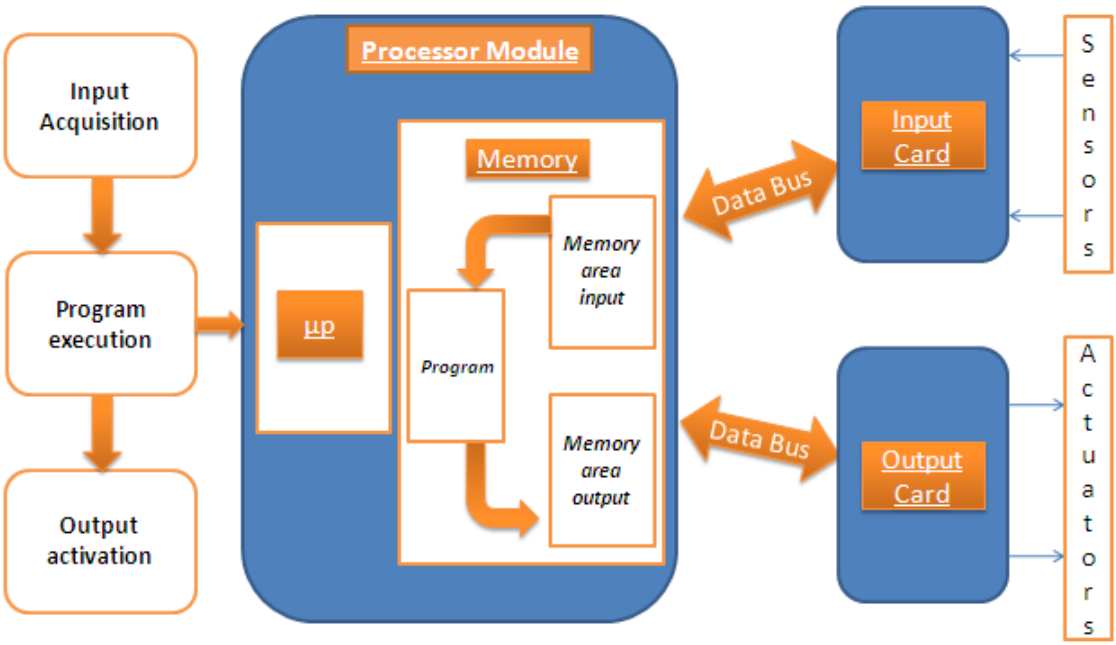

Figure 3: PLC execution mode

3. PLC Simulation

3.1. Software simulation

Many PLC constructors such as Schneider, Siemens, ABB, and General Electric exist in the market. Each constructor distributes programming software with their PLC in order to ensure two essential points:

- Programming the PLC.
- Simulation of the program before its transfer to the PLC.

The PLC constructor we choose in our study is the Schneider constructor and the programming software that we adopt is the UNITY Pro software.

In our study we will give a big importance to the PLC programming software more particularly its simulation part. This paper shows how to transform the PLC simulator to a real PLC so that we can use a PC instead of a PLC to realize the complete PLC application.
The major difference between a PLC simulator and a real PLC is that the simulation cannot be connected to the real world via real inputs and outputs. The inputs and outputs are modeled as internal bits inside the simulation software. In the execution mode of the simulated PLC, the input acquisition and output activation will disappear as shown in the figure 4.

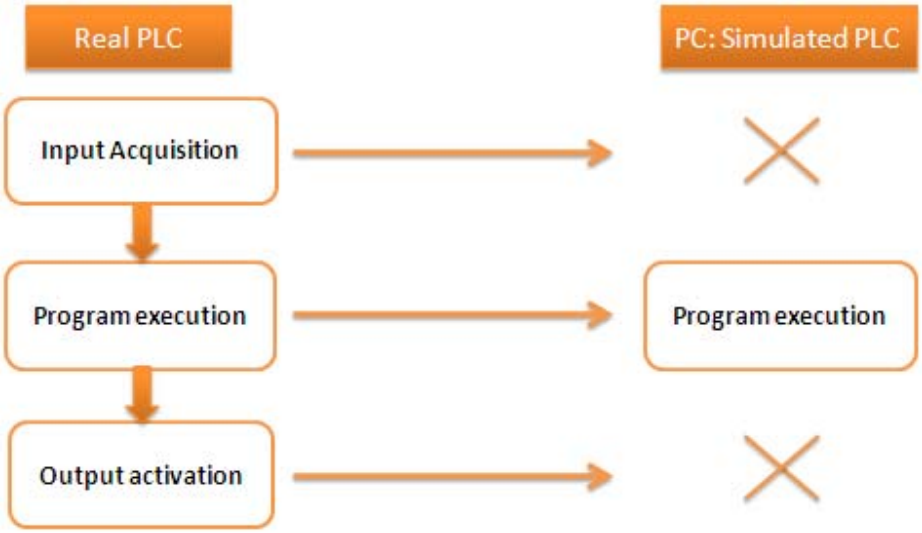

Figure 4: Execution mode in real and simulated PLC

3.2. Migration from Real to Simulated PLCs
In industrial world, we can find equipments named deported inputs and deported outputs. These equipments aim to transmit the status of inputs and outputs to the PLC through a local area network.
The usage of deported inputs and outputs equipment take place habitually when the sensors and actuators are distant from the processor module of the PLC.
The migration from real to simulated PLC is based on these deported modules. The simulation part of Unity Pro software permits the exchanging of the internal memory of the software through the network. In fact any IHM operator can modify internal bits and words inside the simulated program. The communication part of the PLC software and the deported inputs and outputs leads to the creation of the simulated PLC as shown in the figure 5.

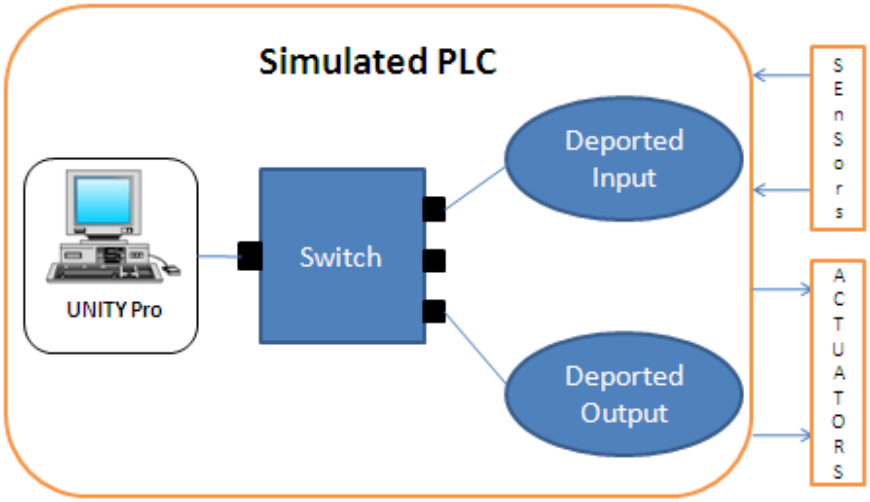

Figure 5: Execution mode in real and simulated PLC

3.3. Communication intelligent core

The transmission of the deported inputs at the beginning of each simulated program cycle and the activation of the deported outputs at the end of each simulated program cycle is based on a Communication Intelligent Core 'CIC' that we have developed in our study.

As shown in the figure 6 this core permits to accomplish the mission below:

1- Acquisition of inputs from the deported inputs module.
2- Copy the status of inputs it in the simulated program.
3- Acquisition of output from the simulated program.
4- Activation of outputs in the deported outputs module.

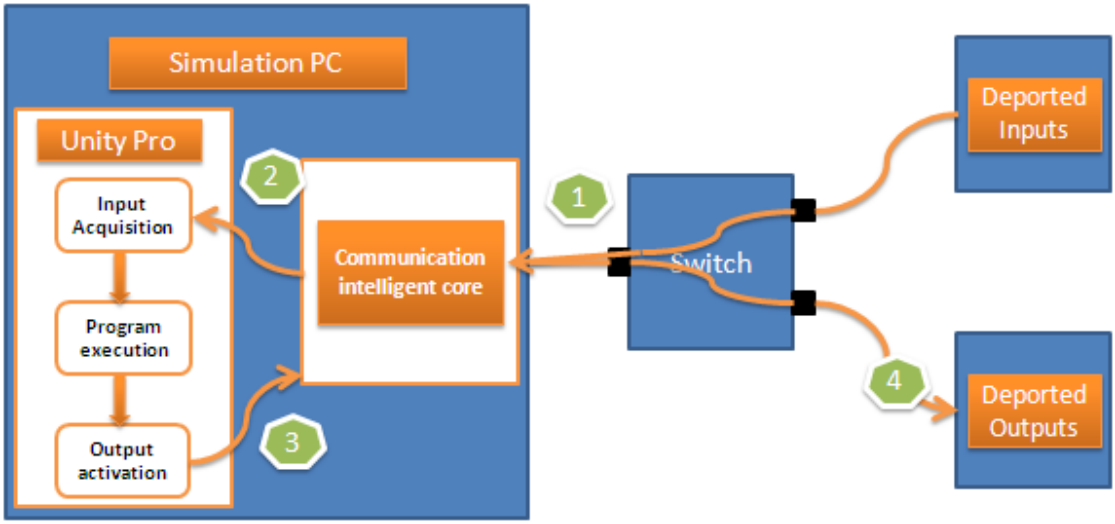

Figure 6: Goal of the CIC driver

3.4. Protocol and architecture of communication of the CIC

The CIC software is based on Modbus architecture. To accomplish its mission, our CIC software makes the job of a Modbus Client and a Modbus Server.

In fact, the deported modules are normally a Modbus server, in this case a Modbus communication client

mode must be installed inside the CIC in order to make the acquisition of deported inputs and activate the deported outputs. To respect the same execution mode of a PLC, the first section of the simulated program must be a Modbus Client in order to read status of inputs inside the CIC. The final section must be also a Modbus Client in order to write the status of the outputs inside the CIC software.
The figure 7 illustrates the communication mode of the CIC software.

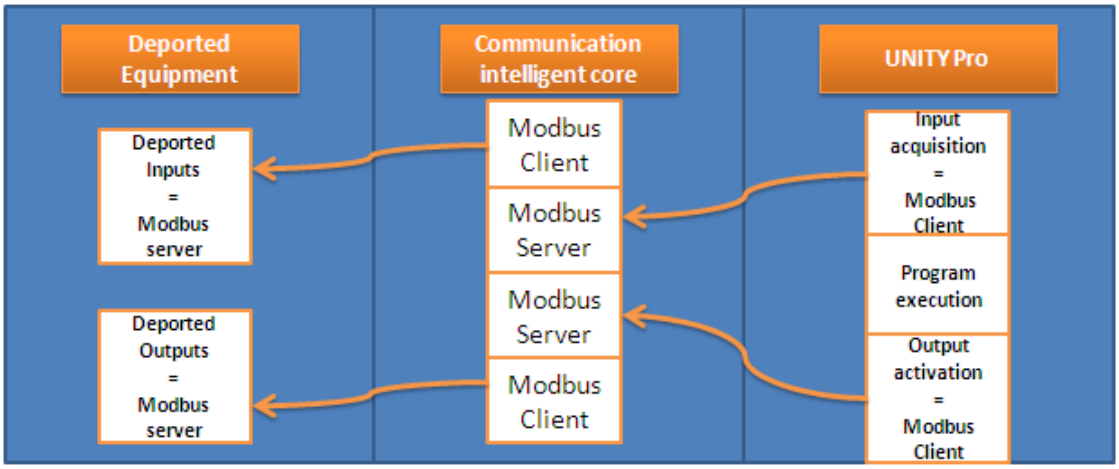

Figure 7: CIC internal architecture

4. EIL network performance
After transforming a single PC to an emulated PLC, the next step is to connect the emulated PLC to the IHM PC. The evaluation of network performance is based on the calculation of the End To End time parameter between the transmission of a command coming from the IHM and the reception of its signalization coming from the emulated PLC. This is done by installing network analyzer software in the IHM computers. A network packet analyzer aims to capture network packets and tries to display them as detailed as possible. The collected data are then exported to Excel editor. Finally an executable application is developed in our study in order to generate performance curves and determine response time.

The figure 8 shows the principal parts of EIL network performance.

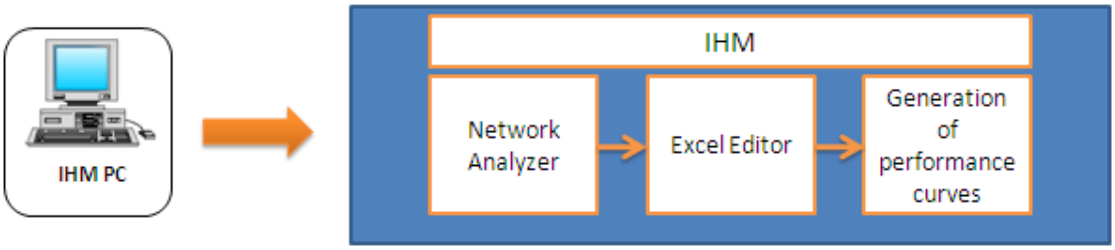

Figure 8: Evaluation of EIL performance

5. Conclusion
This paper permits to show the procedure to transform any computer center to an emulated industrial laboratory. Real PLCs are transformed to emulated PLC using personal computers. The whole IAS architecture could be constructed using the simulated PLCs and the IHM software.
In this paper we also give the procedure to evaluate the performance of the IAS architecture.
The figure 9 shows the importance we bring to the industrial domain

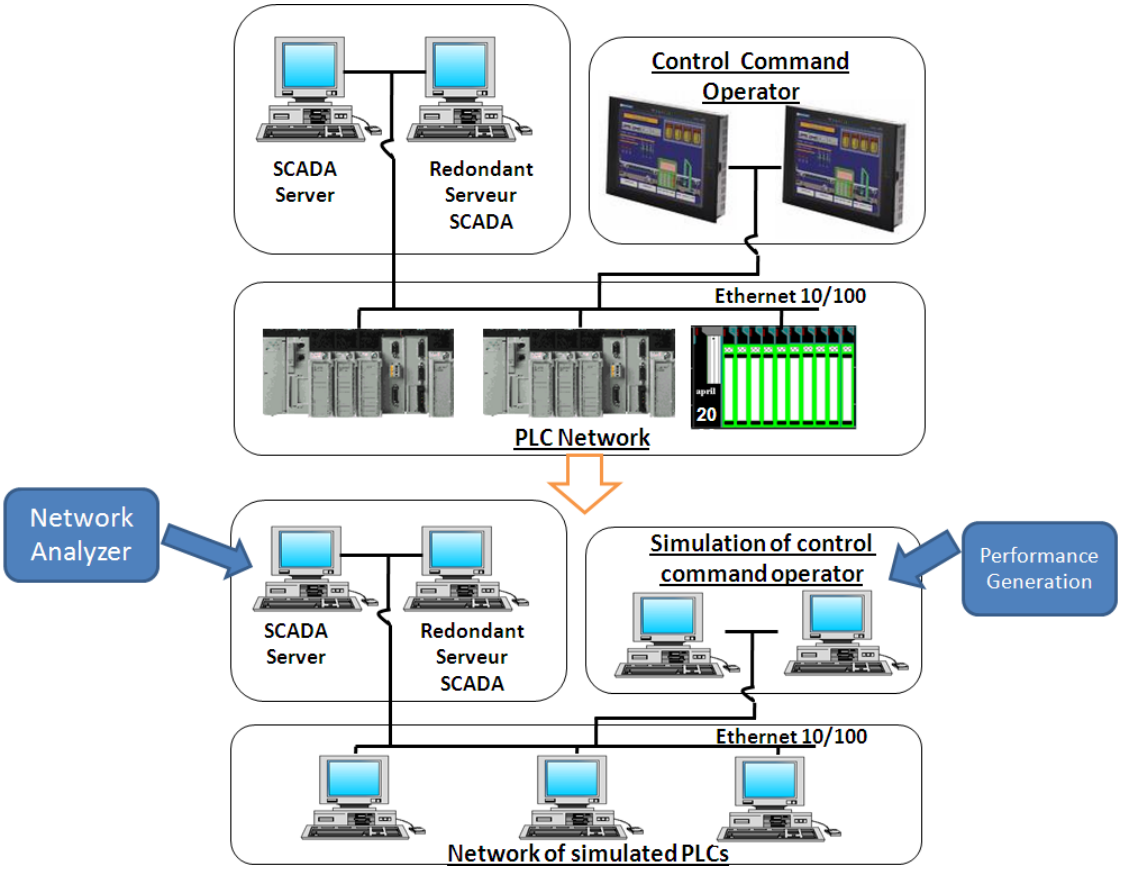

Figure 9: From normal to emulated architecture

In this figure we can see that the final EIL architecture is formed by a group of personal computers 'PCs' interconnected between them via a network which means that any computer center can be transformed to an Emulated Industrial Laboratory.
Each of these PCs replaces specific equipment in IAS architecture, more particularly PLCs, IHM operators and SCADA System.

6. Acknowledgments

We would like to thank the company EURO SYSTEM for their work collaboration.
The authors would like to thank OPNET Technologies, Inc. for their licenses under OPNET university program (OUP).

7. References

Haffar M., Thiriet J.M, Savary E., Modeling of substation architecture implementing IEC 61850 protocol and solving interlocking problems. *FeT '2007 7th IFAC International Conference on Fieldbuses and Networks in Industrial and Embedded Systems FET (2007), Toulouse France.*

Haffar M., Khan Z., Thiriet J-M., Savary E., An extension to IEC 61850 for solving selectivity problem in electrical substations. *23rd IAR Workshop on Advanced Control and Diagnosis 2008, Coventry, 27-28 November 2008.*

Tarlochan S. Sidhu, Yujie Y., Modeling and Simulation for Performance Evaluation of IEC61850-Based Substation Communication Systems, *IEEE TRANSACTIONS ON POWER DELIVERY, VOL. 22, NO. 3, JULY 2007.*

Adamiak M., Redfern M., Communication Systems for Protective Relaying, *IEEE Computer Applications in Power, Vol.3, and No: 3, pp. 14-22, July 1998.*

Marsal G., denis B., Faure J.M, Frey G., Evaluation of Response Time In Ethernet-based automation systems, *6th IEEE International workshop on factory communication Systems, WFCS'2006, Turin (Italy), pp. 95-98, June 27-30 2006.*