POLITECNICO DI TORINO

Master of Science in Mechatronic Engineering

Master Thesis

Design and implementation of two comprehensive automated systems with Siemens PLCs

A case study in the automation laboratory at the university of Belo Horizonte (Brazil).

Supervisors:
Prof. Marco Aurélio de Souza Birchal
Prof. Alessandro Rizzo

Student:
Matteo Mecca
s233392

April 2018

Contents

List of Figures

List of Tables

Acknowledgments

This work was not only an engaging and interesting project. First, it is the result of an experience which makes me draw important conclusions on my person and that led me to meet people and situations that will always be meaningful.

Os mais sinceros agradecimentos vão para o professor Marco Aurélio de Souza Birchal, o professor Márcio José da Silva e o professor Cláudio Campos por me darem esta grande oportunidade de trabalhar com aparelhos industriais modernos, utilizados na maioria das empresas do mundo. Durante toda a duração do intercâmbio, eles sempre estive disponível para me dar seu ponto de vista, para guiar-mi e ajudar-mi tanto no projeto quanto fora dele.

Infine, ringrazio il professor Alessandro Rizzo per la professionalità avuta nel seguirmi a distanza e per aver dato a questo progetto la validità necessaria a essere presentato come lavoro di tesi magistrale in questa università.

Introduction

This work has been developed during my Extra-UE exchange program at the Pontifícia Universidade Católica de Minas Gerais (Belo Horizonte, Brazil).

The project regards the complete design of an automated system and the subsequent construction of it in the industrial automation laboratory of the university.

The realization has been carried out both from hardware and software perspectives. The design of the network and the configuration of the devices have been executed via TIA Portal; afterward, the system has been implemented on the specific worktables of the lab.

This lab is an application of the industrial pyramid concept from the point of view of data exchange between different levels. The list of the apparatus used includes PLCs, HMIs, SCADAs and remote CPUs that have been recently acquired by the university and they all belong to Siemens (Simatic family) for an overall cost of more than 400.000 €.

The devices have been connected to each other using several network protocols (PROFIBUS DP, PROFInet, and AS-i) and adopting different transmission media (copper, optical fiber, and wireless) in order to implement a hybrid network.

The entire system has then been tested simulating a primary crushing process.

Later, a wireless communication between this laboratory and another one has been performed with the aim of collecting important data which regarded the behaviour of a water pump-tank system located in this second lab. These information have been used to design a Proportional Integrative controller which has then been implemented in order to remotely regulate the water level inside the mentioned tank.

This document is divided into several chapters. The first Chapter will be introductory to many concepts, which are all related to the industrial automation field. Starting from general definitions regarding the concept of 'automated production system', the analysis will go on with a description of the industrial automation pyramid. A special focus will be given to its levels, technologies, devices and network types, which have been all implemented at the laboratory. Differently, the second Chapter will be more specific, aimed at giving detailed information about Fieldbus protocols.

After that, the third Chapter will deal with the job description, with an initial explanation of laboratory n. 201. The writing approach used will be a 'top-down' one, in order to provide a general overview of the project and to show it in its overall functioning. In this Chapter an introduction to the main Siemens software used for configuring and supervising the system will be present. Moreover, the network topology and the redundant configuration of some parts of the network will be also analyzed. In Chapter four, the designed ladder program which runs in the system will be described. This program consists of a simulation of a primary crushing process, which has been developed with the purpose of verifying the correct configuration and communication between the devices, as well as providing a challenging exercise for the students.

After this, I decided to better test the wireless communication. Thus, I performed it in order to collect data and to remotely control a plant located in laboratory n. 119, which is about thirty meters away and is separated by a couple of walls from laboratory n. 201. This part of the work will be described in the fifth Chapter together with the use that has been done of the mentioned connection, which consists of the design of a PI controller to regulate the water level in a tank.

Finally, Chapter six will show all the results achieved for both systems, as well as my considerations on the two plants.

After the conclusions, an Appendix will be included in order to find an exhaustive list regarding all the Siemens devices used.

Chapter 1

Industrial automation pyramid: concept and technologies

Automation can be defined as:

> *"any computer-based system that replaces human work in favour of human safety, product quality, speed of production or cost reduction, thus improving the complex objectives of industries and services" [3].*

The chapter is an introduction to many concepts all related to the industrial automation field. Starting from the initial definitions of automated production system, the automation pyramid and its levels, as well as the technologies, devices and communication networks used will be described.

1.1 Automated production system

A production system is a collection of people, equipment and procedures organized to perform manufacturing operations. Nowadays this type of systems is often automated. A definition of 'automatic machine' is given in DIN19223: it is indeed stated that it can be seen as a manufactured setup which depends on the association of devices together with their conditions. What's more, the responses generate particularly specific wished reactions.

With these definitions, it is possible to consider an automated production system as a system in which processes are performed by machines without direct participation of human workers. A list of instructions, together with a control system which is able to execute them, are the main components that usually composed an automated system. There are many advantages of having an automated production line [5]:

- fewer staff are needed;
- 24-hour no-stop production, except for few maintenance interval periods;

- the commodity is normally of excellent quality;
- as the procedure last less, a greater amount of products can be transferred quickly;
- monotonous, abundant or uncertain works are minimized;
- procedures that cannot normally be done physically are achievable.

The automated elements of a production system can be separated into two categories:

1. automation of the manufacturing facilities systems;
2. automation of the manufacturing support system.

The automated manufacturing systems operate in the factory on the physical product. They perform operations such as processing, assembly, inspection, material handling and more, with a reduced level of human participation compared to the corresponding manual process.

Differently, the automation of the manufacturing support system is aimed at reducing the amount of manual effort in product design, manufacturing planning and business function.

1.1.1 Process or discrete industries

Another important distinction is the one related to how the system performs its production. Based on this distinction there are two different types of industries since all the subsystems of the process will vary accordingly.

Process industries perform their production on an amount of materials because the materials are usually liquids, gases, powders. The typical unit operations are chemical reaction, distillation, mixing, blending and many more. Due to this, the variables are mainly continuous and analog (i.e. temperature, flow rate, pressure, current etc.) [7].

On the contrary, discrete manufacturing industries perform their production on quantities of materials, because the materials are usually discrete parts or products. Typical unit operations are forging, extrusion, assembly, stamping. Due to this, the variables are mainly discrete and digital (i.e. limit switch open or closed, motor on or off) [7].

Since these types of industry deal with two different types of variables, also the control that they must implement is different. In particular, in a process industry, there will be a continuous control, while in a manufacturing industry a discrete control will have to be used. Table 1.1 shows a valid juxtaposition.

Sometimes, most operations in process/discrete industries include both continuous and discrete variables. Consequently, many industrial controllers are able to receive, operate on and transmit both types of signals and data. Moreover, since computers began replacing analog controllers, also continuous variables are sampled periodically (sampled-data systems).

For how the laboratories are equipped, PLCs will be the controllers used.

Table 1.1: Comparison between process and discrete industry

Comparison factor	Process industries	Manufacturing industries
Control system	Continuous control	Discrete control
Measures of output	Weight, volumes etc.	Number of products
Variables	Temperature, flow rate etc.	Position, force etc.
Sensors Actuators	Pressure sensors etc. Heaters, pumps etc.	Limit switches etc. Motors, pistons etc.
Time constants	Seconds, minutes, hours	Less than a second

1.1.2 Closed-loop automation system

The controller causes the process to accomplish its function. In the most general view, control systems can be divided in:

- closed loop control (feedback control);
- open loop control (feedforward control).

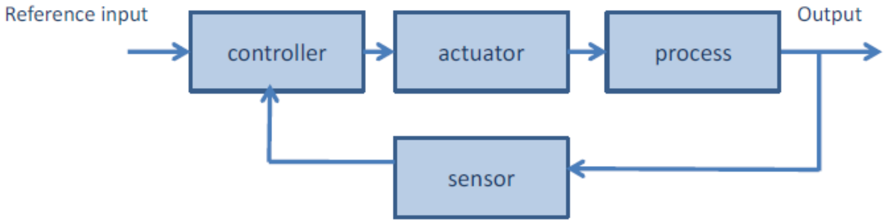


Figure 1.1: General closed loop system

In a feedback control system, the variable in output is continuously compared with the desired value (reference input) and it is driven by the mathematical subtraction (so-called error) between the output and the reference. Moreover, the feedback has many interesting properties since it allows the system to be insensitive both to external disturbances and to variations in its individual elements.

Unfortunately, feedback has also potential disadvantages. It can create dynamic instabilities, causing oscillations, sensor noise in the system or even runaway behaviour [1].

On the contrary, a feedforward control operates without the feedback loop and, thus, there is no comparison between the output variable and the reference input. However, it is generally simpler and less expensive, and it is appropriate when the action performed by the controller is very simple and the actuating function is reliable.

Most industrial processes require more control loops, one for each process variable that must be controlled.

Due to the fact that both control systems which have been implemented in the laboratories are of the closed loop typology, in the following the focus will be on the characteristics of the control with feedback. A closed-loop automation system is broadly divided into three subsystems, as it can be noticed in Figure 1.2.

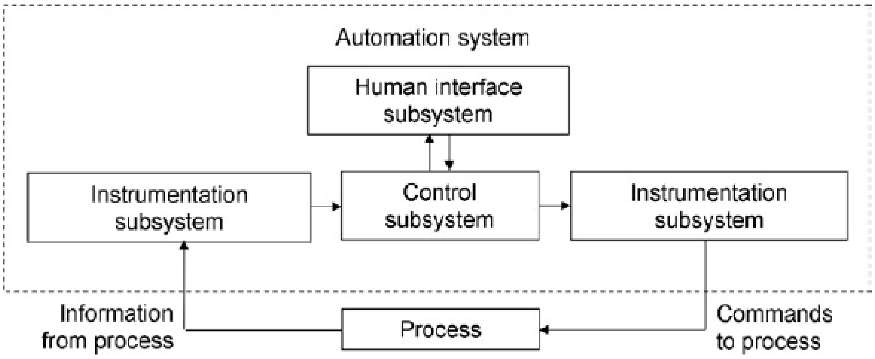


Figure 1.2: Closed-loop automated system

The control subsystem is the heart of the automation system and it performs the following functions.

- With the instrumentation subsystem:
  - receives the information which are necessary to understand the behaviour of the process;
  - compares the received information with the desired behaviour of the process;
  - decides with actions on whether or not to issue commands for correcting the behaviour of the process.
- With the human interfaces subsystem:
  - receives the information which are necessary to control or supervise the process;
  - routes the received information to the process for manual control via instrumentation;
  - collects the information from the process and routes it to the human interface subsystem for display.
- Safety monitoring: involves the use of sensors to track the system operation to identify conditions and events that are potentially unsafe.
- Maintenance and repair diagnostics: it refers to the capability of the system to assist in identifying the source of potential failures by monitoring the system status.
- Detection of errors: use the available sensors to determine when a deviation is occurred and bring back the system to the normal state.

Another important subsystem is the human interface, which allows the operator to manually interact with the process. In fact, the operator may observe and monitor what is happening in the process, or it may issue manual commands, if required, to force a change in the process behaviour.

For what concerns the instrumentation subsystem, it can be said that it has the aim of acquiring information on the behaviour of the process, through measurements, and it sends this to the control subsystem in an acceptable form, through a signal conditioner. Moreover, the instrumentation devices have names which are different with respect to the type of output that they provide. They are called transducers if their output is suitable for transmission (in voltage or current form) over a relatively short distance. Differently, an instrumentation device is called transmitter if the output is suitable for transmission (in current form) over a relatively long distance.

1.2 Automation pyramid

The automation pyramid can be described as a hierarchical structure which organizes the stream of information which is useful to the factory and the process automation. The aim of this model is that of producing a network made of several levels which are easy to supervise. Normally, the automation pyramid included maximum five levels, or, in some cases, more [24]. It can be represented schematically according to Figures 1.3 and 1.5.

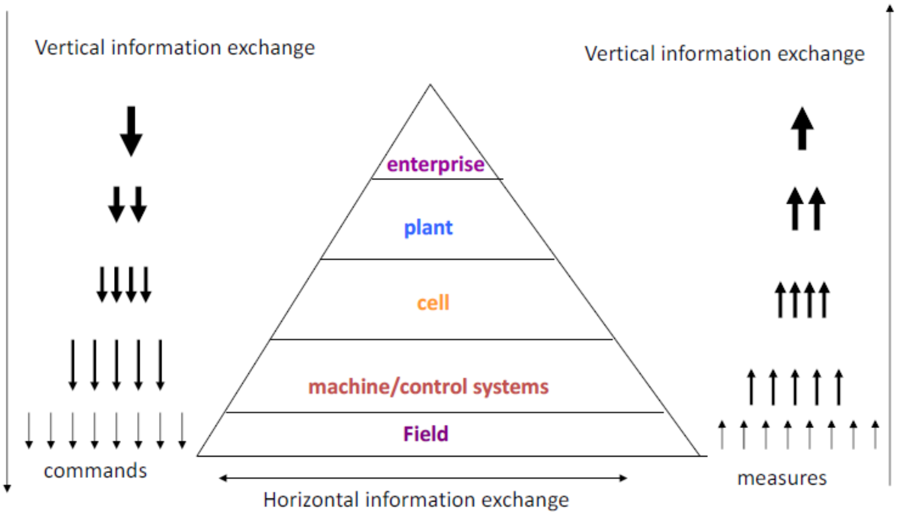

Vertical information exchange
Vertical information exchange
enterprise
plant
cell
machine/control systems
Field
commands
measures
Horizontal information exchange

Figure 1.3: Automation pyramid and its information exchange

In Figure 1.3 the amount and the kind of information exchanged are shown. First of all, it can be noticed that information goes both in vertical (exchange of information between levels) and horizontal direction (exchange of information between different branches of the same level). Moreover, going up, the exchange becomes more structured and essential. Hence, more complex control strategies must be used and larger actuation and elaboration times are needed.

Each level can be automated and controlled. They are five but the general structure can be different from company to company.

Figure 1.3 shows the vertical information flow, highlighting the fact that the amount of data decreases in parallel with the rising of the pyramid. Furthermore, procedures and resolutions become more complicated going up as well as timing requirements are slowed down. On the contrary, the levels closest to the plant are more exacting in response time: the amount of information is big while processing is ordinary. Nowadays, this latter part of the pyramid is controlled by computers, excluding some particular situations (i.e. emergency, maintenance or commissioning).

The characteristic response times for each level are shown in Figure 1.4.

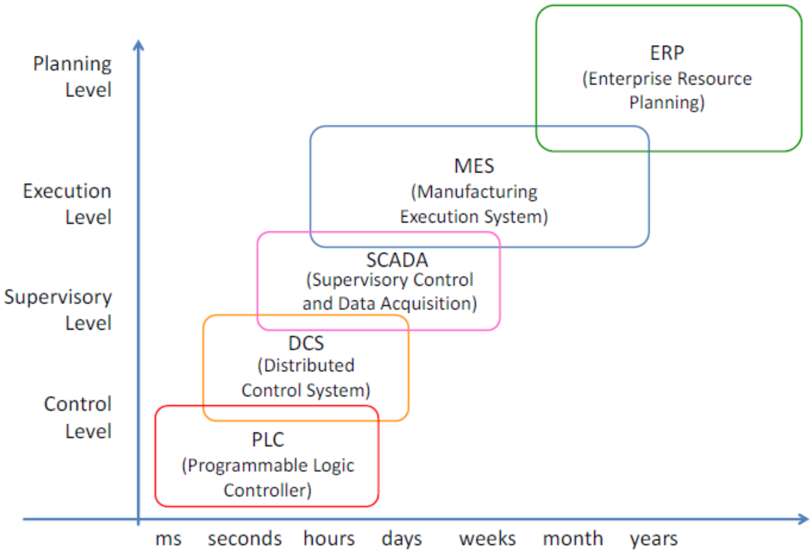

Planning Level
Execution Level
Supervisory Level
Control Level
ERP (Enterprise Resource Planning)
MES (Manufacturing Execution System)
SCADA (Supervisory Control and Data Acquisition)
DCS (Distributed Control System)
PLC (Programmable Logic Controller)
ms
seconds
hours
days
weeks
month
years

Figure 1.4: Response times in the different levels of the automation pyramid

In the right part of the pyramid illustrated in Figure 1.5, the network protocols which usually perform the communication between pyramid levels are written. Structured and correlative industrial communication systems enable to have optimum conditions for creating a transparent network in every area of the process.

Currently, due to its great technological improvement, industrial networks are widely used, presenting advantages with respect to conventional cabling systems [3]:

- decreasing of wiring;
- easy maintenance;
- increasing network flexibility;
- possibility to diagnose the devices;
- integration of devices produced by different manufacturers.

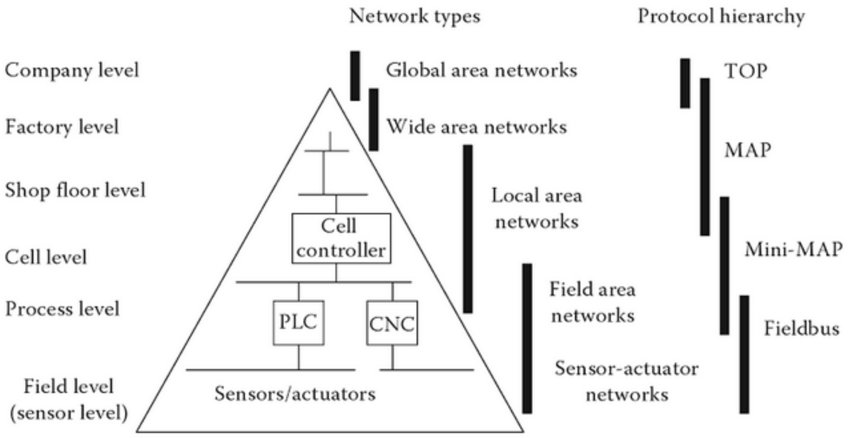


Figure 1.5: Automation pyramid and its network protocols [3]

A detailed description regarding the industrial network protocols which have been used during the development of the project can be found in the second Chapter.

In the following a brief definition of each level of the pyramid.

Field level - It is the lowest level in the hierarchy. It includes actuators, sensors and any other hardware device that perform the physical transformation required by the production. Individual machines arrange the hardware part of this level: industrial robot, powered conveyors, automated guided vehicles etc. All these apparatus represent the machine level.

The communication occurs both horizontally and vertically at the same time. This level transmits to the upper one the measures coming from field sensors and receives commands for the actuators generated from the control systems. Thus, control loops included devices belonging to different pyramid levels. These control algorithms are usually implemented on embedded systems.

Many devices can be included in this level. In laboratory n. 201, proximity sensors, pushbuttons, lights and an induction motor have been used as field apparatus.

Control systems level - It is the level associated with the controllers of the production system and with some types of supervisory systems. The control function at this level includes the monitoring of chain of steps in the instructions program and ensures that each step is carried out correctly. The control algorithms are usually implemented on embedded systems or on PLCs.

It has been already stated that the control type depends on the industry type, process or manufacturing.

Cell level - An industrial cell includes devices supported by computer and associated to material handling systems. Their functions comprise machine loading, coordination among apparatus and material handling systems, collections and evaluating inspection data. It is the level which allows the control of the production system in the plant.

Instructions for operations come from the plant level and the control systems are usually implemented on PLC or other digital devices (DCS).

Sometimes, this group of machines has its own human-machine interface for controlling locally the functioning and for mainteinance.

Plant level - Plant level is the factory or production system level. Instructions come from the enterprise level and are translated into operational schemes for production.

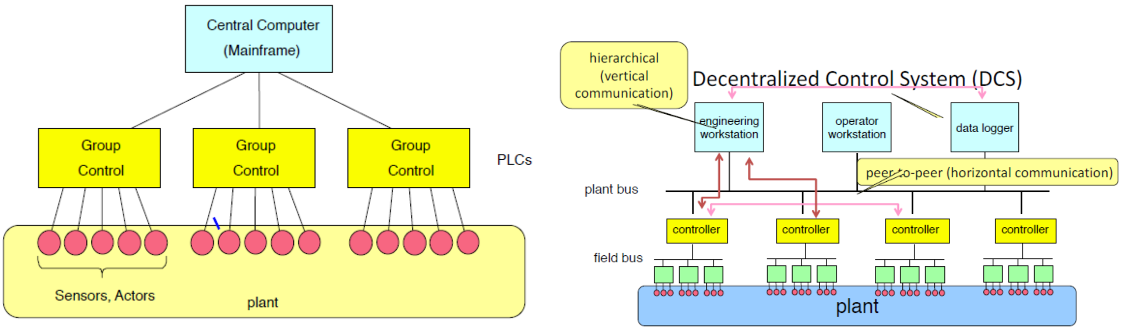
Functions include:

- order processing,
- process planning,
- inventory control,
- purchasing,
- material requirement planning,
- quality control.

The control system can be a Supervisory Control And Data Acquisition (S.C.A.D.A.) system and it is implemented on a workstation.

Enterprise level - It consists of the corporate information system. The enterprise level aims at managing the company from scheduling and researching to the processes of marketing and sales.

1.2.1 Centralized and decentralized system



(a) *Centralized control system.*

(b) *Decentralized control system.*

Figure 1.6: Scheme of centralized and decentralized system

The introduction of microprocessors in the industry allowed to realize a centralized digital control, in which the monitoring task is executed by a central computer which transmits commands to the PLCs. Main features of a centralized control system are [3]:

- parallel cabling using pair locked wires and star topology;
- exchange of information between sensors/actuators and control unit can be both in the form of digital or analog signal.

However, the presence of many I/O modules and long distances to be travelled cause a very high cost of installation and maintenance. Moreover, a centralized system is not flexible if it is needed some extension or modification of the network.

For passing these difficulties, decentralized control system has been developed. In this type of systems is commonly performed a peer-to-peer communication between all the controllers so that the transmission doesn't go through a central master. Information exchanged is limited by the rate of transmission and modular considerations. For big industry plant this is the best solution and permits the following characteristics [3]:

- many communication modes;
- completely flexible for any network topology.

1.3 Programmable Logic Controller

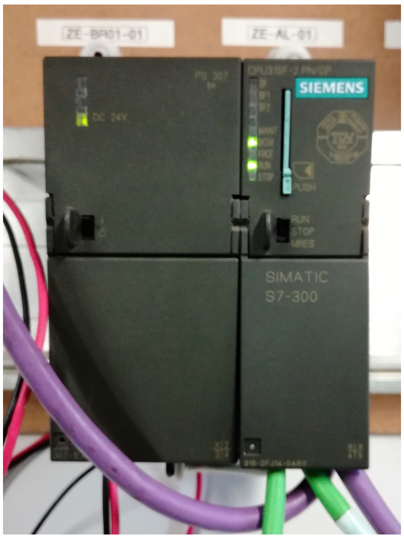


Figure 1.7: Siemens SIMATIC S7-300 PLC, available in laboratory n. 201

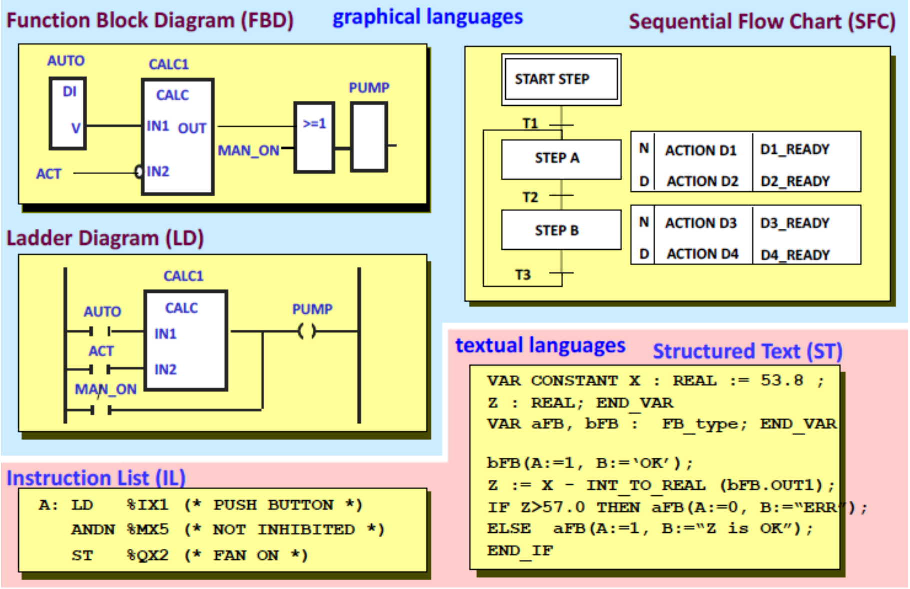
According to William Bolton,

> "a Programmable Logic Controller (PLC) is a special form of microprocessor-based controller that uses programmable memory to store instructions and to implement functions such as logic, sequencing, timing, counting, and arithmetic in order to control machines and processes." [2]

The main advantages of using this device as a controller are the following [3].

- control of complex system becomes more convenient;
- it is flexible because it can be easily expanded or configured again in order to control other processes;
- support of advanced control methods, due to its computational abilities;
- easy to program;
- simplification of the system panel, because all the control wiring is composed of a set of input/output;
- it is constituted of reliable components;
- it can perform data collection and information exchange through the network.

Today, one of the prevalent techniques which is used to program a PLC is the Ladder diagram. Nevertheless, many other methods are commonly adopted and Figure 1.8 illustrates the languages standardized by the IEC 61131-3. This standard includes the most important automation languages in industry. More than 80% of PLCs support it, and all new developments are based on it.



```
A: LD   %IX1 (* PUSH BUTTON *)
   ANDN %MX5 (* NOT INHIBITED *)
   ST   %QX2 (* FAN ON *)
```

```
VAR CONSTANT X : REAL := 53.8 ;
Z : REAL; END_VAR
VAR aFB, bFB :  FB_type; END_VAR

bFB(A:=1, B:='OK');
Z := X - INT_TO_REAL (bFB.OUT1);
IF Z>57.0 THEN aFB(A:=0, B:="ERR");
ELSE  aFB(A:=1, B:="Z is OK");
END_IF
```

Figure 1.8: The five IEC 61131-3 programming languages

1.3.1 Control Loop

During the control of a process, the PLC receives inputs from sensors and sends output signals to the actuators. Hence, the inputs are used to choice while the outputs are updated time to time to drive the actuators.

The control loop of a PLC consists of exactly the following sequence of actions.

1. PLC reads the inputs;
2. CPU solves the ladder logic;
3. PLC updates the outputs, according to the logic previously computed.

However, there is another important check, the so-called self-test. It belongs to the control loop of a PLC and it consists in an initial quick sanity check to guarantee that the hardware is functioning in the correct way. If this check provides no errors, then the CPU moves to the scan of the inputs. Of course, the self-test is carried out before any read of the inputs.

The typical times for each step of the control loop is some milliseconds. This time is not fixed but can vary according to the process behaviour and the complexity of the ladder program.

1.3.2 Hardware components

The main hardware components of a PLC are the following.

- Power supply - It can be an external unit or internal to the PLC.
- Rack - It guarantees both mechanical and electrical connection of the different modules and protection from external environment.
- CPU - The Central Processing Unit can be single or multiprocessor.
- I/O modules - They can be analog or digital.
- Memories - They can be fixed or volatile.
- LED - Indicator lights are located on the front surface of the PLC and they inform about the CPU status (i.e. power on, run mode on or faults detection).
- Special modules - i.e. signal conditioning, noise filtering, DAC and ADC, mux and demux.

Typically, three configurations of a PLC are possible, all of them regarding the mode in which the components are arranged. It is achievable to have: Micro (up to 64 I/O), or Mini (up to 512 I/O) or also Rack (up to thousands I/O) configurations. Another possibility is the use of a software-based PLC which utilizes a PC with an interface card.

Central Processing Unit

The most important component of a PLC is, without doubts, its CPU. As it can be imagined, it is a microprocessor which coordinates all the control activities. The CPU is able to [9]:

- read all the instructions in the user memory in the correct sequence;
- solve logic operations in bits or words;
- solve arithmetic operations;
- generate clock pulses;
- perform counting and timing functions.

The CPU performs its tasks in a sequential order of operations called scanning or scan cycle, as it has been stated in subsection 1.3.1.

Input Modules

The physical phenomena which happen in the process are translated into electrical signals by means of sensors. These electrical signals can be both continuous or logic and they are read as input variables by the PLC. In particular, an input signal can come from a sensor, a button, a switch, or many other devices.

The input ports in a PLC can be:

- integrated cards in the device (as in SIMATIC S7-1200 PLC);
- external modules or cards, which are specific devices with 8 or 16 ports that can be added to the hardware configuration.

Output modules

The output ports of a PLC are connected to actuators of different types, depending on the process. Typically, it is possible to have solenoid valves, lights, motor starters, etc.

Relays are the common output switches which are responsible for opening/closing the power to the actuators. Instead of relays, solid state electronic devices such as transistors (if the supply is DC) or Triacs (if the supply is AC) can also be found. Of course, if the output is a continuous signal the output card will need a digital to analog converter.

However, these types of switches don't support enough energy for any situation and, thus, an external source which is responsible for supplying additional power is almost always connected to the output card.

As for the input, also the output modules have 8 or 16 points.

Memory

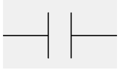
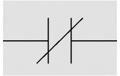
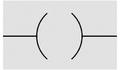
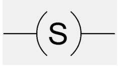
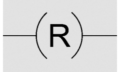
Usually, in a PLC there are four types of memory [3].

1. P.R.O.M. (Programmable Read Only Memory) - It contains the program which runs the device, built by the manufacturer. This type of memory is not accessible from the user.
2. Program memory - It stores the user program. The CPU runs this program and updates the internal data memory and the I/O memory. This memory cannot be deleted if the device is running.
3. Internal data memory - It contains data relating to the processing of the user program.
4. I/O memory - This memory reproduces the state of the input and output.

1.3.3 IEC 61131-3 languages: ladder diagram

As depicted in Figure 1.8, there are five types of programming languages which belong to the IEC 61131-3, and they are subdivided into two main groups: graphical and textual languages. In this document, only the Ladder diagram logic will be analyzed since it is the one adopted for the development of the programs.

Table 1.2: Basic Ladder diagram elements

Representation	**Meaning**
	Normally open contact - NO - Logical continuity when the state variable is 1
	Normally closed contact - NC - Logical continuity when the state variable is 0
	Coil - it activates if the line has state 1
	Set Coil - when activated, sets the state of the memory
	Reset Coil - when activated, resets the state of the memory

Ladder diagram takes its name from the ladder-like form of the diagrams it uses, it is also called relays diagram or contacts diagram. It allows programming from easy binary functions to complex mathematical functions.

Inputs are represented by contacts and the outputs by coils. The basic elements are shown in table 1.2 [7], while an example is shown in Figure 1.9.

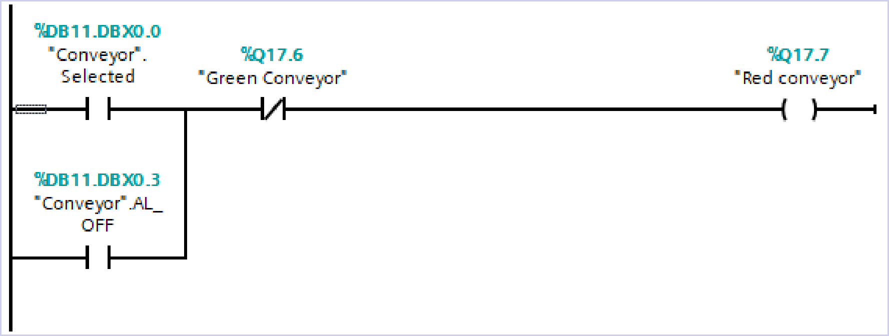
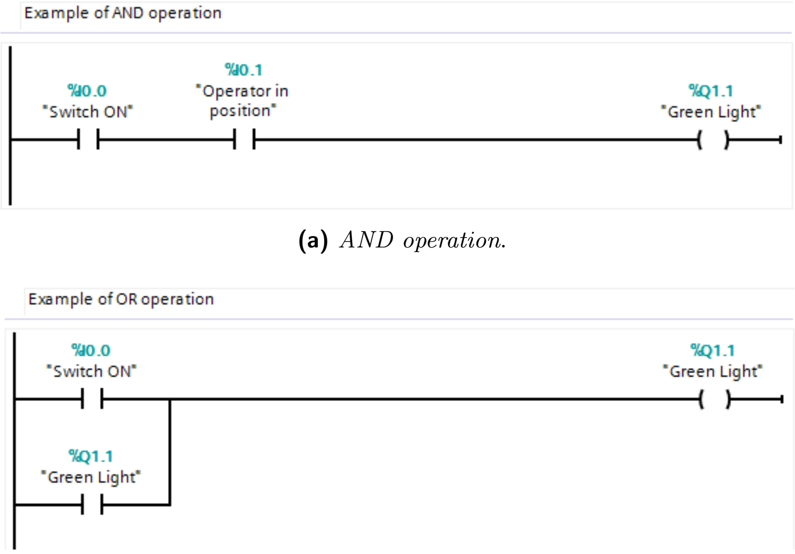


Figure 1.9: Example of Ladder diagram

The right side of the diagram is neutral, while the vertical line on the left is the powered rail. A Ladder program can be structured in different rungs in which several combinations of inputs and outputs are located. When the input contacts are activated/deactivated in the exact combination, the power can move from the energized rail, through the inputs, to power the output coils and close the circuit reaching the neutral line.

Thus, as it can be noticed in Figure 1.10, a combinatorial logic can be implemented adopting the Ladder language. For instance:

- two or more contacts disposed in series on a rung realize an AND logic operation;
- two or more contacts perform an OR logic operation once they are placed in parallel.



(a) *AND operation.*

(b) *OR operation.*

Figure 1.10: Examples of combinatorial logic operations

Nevertheless, combinatorial logic is not enough for controlling complex systems [7]. Hence, the conditions of such systems can be evaluated using event-based Ladder instructions. A memory with the possibility to latch/unlatch itself is an event-based Ladder logic which can be adopted to secure something on (SET) or turn it off (RESET).

All this stated, it has to be to said that there are other important instructions to structurize the Ladder diagram on event-based logic. For example, timers and counters have been widely used during the development of the program which runs in the system of the laboratory n. 201. For this reason, they will be shortly described in the following. In addition, Ladder instructions for arithmetic operations and data manipulation will be introduced, even if they are not event-based instructions.

Timer

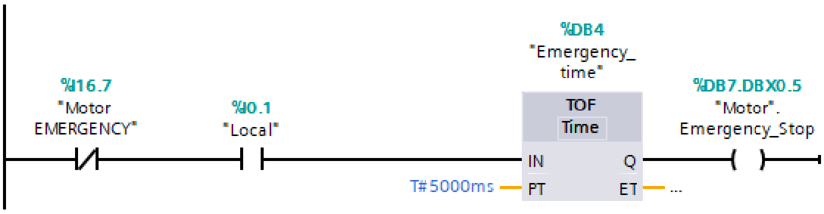


Figure 1.11: Example of Timer instruction

Essentially, two types of timers are achievable [9].

Delay on - when the timer instruction is energized, it enables the output at the end of the set time. The reset happens when the power goes off or when a specific variable is activated. These timers may be incremental (count-up) or decremental (count-down) type.

Delay off - when the instruction is powered on, it turns on immediately the output for then resetting it at the end of the set time.

As shown in Figure 1.11, the timer instruction consists of a start input, an output coil and a preset value which can be programmed between a minimum and a maximum duration. The timers most commonly used in PLCs are the delay-on type.

Counter

Counters are used when an action must depend on a certain event which takes place a specified number of times. For this purpose, PLCs use counting instructions which make it possible to simulate two types of counter [9]:

1. unidirectional, which can be up-counters or down-counters;

2. reversible.

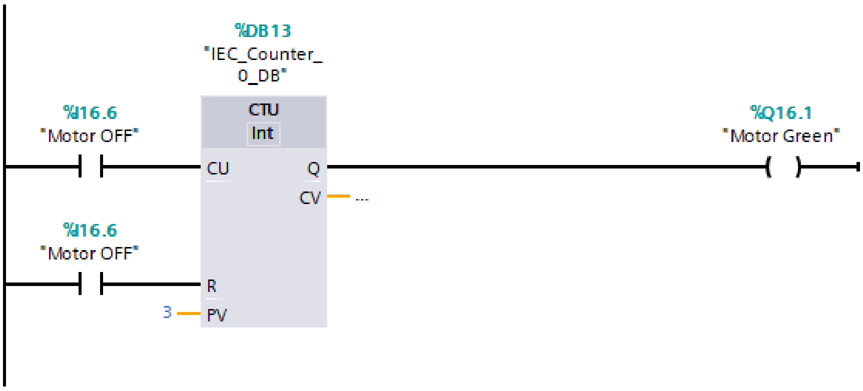


Figure 1.12: Example of Counter instruction

As shown in Figure 1.12, unidirectional counters consist of a counting input (CD) and a resetting input (R), an output coil (Q), a preset count value (PV) and an accumulator (CV which stores the current value).

Unlike timers, counters require two logic lines: the input condition (counting input) and the zeroing condition (reset input). The input condition establishes when the accumulator value must be increased for up-counters (or decreased for down-counters). Each time the condition switches from off to on the accumulator increases (or decreases) by one unit. The reset condition controls that the current CV value is put to zero for up-counters (or to the preset value for down-counters) [9].

Arithmetic operations

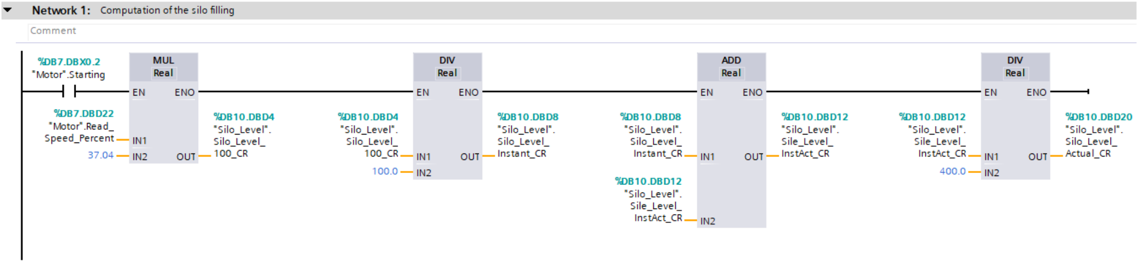


Figure 1.13: Representation in ladder language of arithmetic instructions

Modern PLCs have functions for arithmetic calculations. Addition (ADD), subtraction (SUB), multiplication (MUL), division (DIV), and square root (SQR) are the main operations which are supported.

At each scan cycle the PLC operates the data contained in IN 1 with those of IN 2 and places the result in the OUT. Of course, this type of instructions is not based on events.

Data manipulation

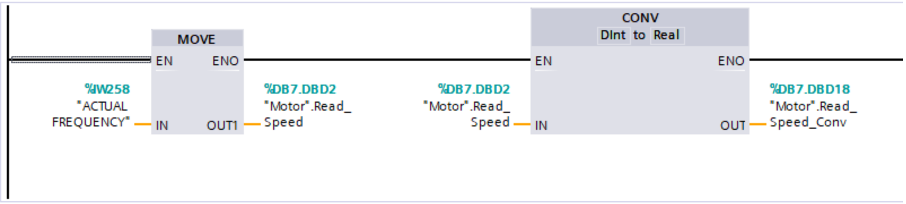


Figure 1.14: Representation in Ladder language of MOVE and ROUND instructions

PLCs have also Ladder instructions for data manipulation. The principal functions are: MOVE, CONV, ROUND, AND, OR, XOR, NOT, FFL (first in first out) [3].

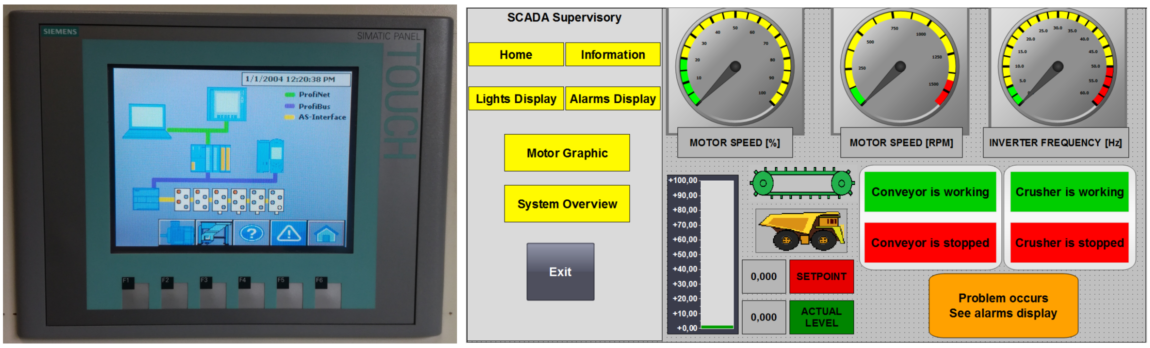
In figure 1.14 the MOVE and ROUND functions are shown. These instructions copies the value of an address from IN to another destination. As long as the line is true, the instruction moves the data at each scan.

1.4 Supervisory systems: H.M.I. and S.C.A.D.A.

Supervisory systems are digital systems for monitoring and controlling an industrial plant. They manage process variables which are continuously updated and can be stored in local or remote databases for historical registration purposes [3].

Nowadays, an industrial process can have two types of variable: digital or analog, as it has been stated in subsection 1.1.1. However, supervisory systems can be classified according to their complexity, robustness and number of input/output managed.

The two principal stations are H.M.I. (Human Machine Interface) and S.C.A.D.A. (Supervisory Control And Data Acquisition). Both of them have been used in the laboratory n. 201 adopting two software for designing the process screens and the supervisory program.



(a) *Siemens KTP600, available in the laboratory n. 201).*

(b) *WinCC V7.3 process screen.*

Figure 1.15: Examples of supervisory systems

Supervisory systems have features which have allowed them to be widely used in existing industrial plants [7].

Easy interpretation - The representation of the plant by areas and process equipment facilitates its rapid interpretation. In addition, the actuated parts of the process can be displayed in different colours or in movement to improve the operator's ease of learning.

Flexibility - Changes in the process, adjustments or implementations can be easily realized using the software of the supervisory system.

Structure - The entire industrial plant is subdivided into areas; it is recommended that they are displayed following a natural subdivision. This systemic visualization of the plant allows objective navigation in the process, decreasing the time that the operator needs to access to the desired variables.

Production performance parameters - The software developed for these systems allow the creation, modification or even the import, in real time, of production performance parameters.

1.4.1 Human Machine Interface

As it can be noticed in Figure 1.15a, an HMI is an industrial hardware composed of a liquid crystal display and a set of keys for navigation. It uses a proprietary software for its programming. This supervisory system is normally located in those industrial plants which are characterized by an hazardeous environment. An HMI has an extremely robust construction, resistant to direct water jet, humidity, temperature and dust [3].

For this reason, an HMI is typically installed close to the line production, normally in a working area and it aims to translate the signals coming from the PLC into graphic signals easier to understand.

The development of the human-machine interface, with alphanumeric displays, function keyboards and serial communication, brought the following benefits [3]:

- saving wiring and accessories, because the communication with the PLC is based on a serial transmission with one or two pairs of wire locked;
- reduction of manpower for installation, because instead of several devices only the HMI is mounted;
- synoptic panels are not used anymore;
- increasing in command and control capability because an HMI can help a PLC in some duties (i.e. data storage);
- flexibility;
- easy programming and maintenance.

The supervisory system only responds to signals from the PLC or sends signals to the PLC. Thecontroller sends signals followed by a TAG. These TAGs take with them information about the address of the PLC and the TAG type. The most common TAG type are [7]:

- DEVICE, which means that data are originated from the PLCs for the supervisory system;
- D.D.E. (Dynamic Data Exchange), which means that data are originated from another network computers;
- MEMORY, which means that data are already present in the supervisory system.

1.4.2 Supervisory Control And Data Acquisition

A SCADA system is a configurable, supervisory and control system, created in order to control and supervise a large number of data, coming from all over the industrial plant. It has a lower cost than DCS (Distributed Control System) and, for this reason, it is very common in the industry. Nowadays, SCADA and DCS functions are analogous. The main difference between the two is that DCS is often used in continuous process systems where reliability and security are fundamental, together with the fact that the control room must not be geographically distant [3].

In SCADA systems, the communication between the worker and the process is guaranteed through graphic interfaces which allow a friendly and very easy interaction. The hardware can be an ordinary PC, which facilitates and optimizes hardware costs.

This supervisory system aims at the physical integrity of people, equipment and production, often consisting of redundant hardware systems and allowing rapid identification of failures. Some SCADA systems also allow to change and repair the damaged hardware without switching off the entire production.

Moreover, they make it possible to configure alarms and event files, as well as reports and interfaces, to control the performances and the advanced functions.

Generally, a SCADA system:

- shows the status of the process (visualization);
- displays messages which can regard alarms and events (alarm log, logbook);
- shows the trends of the variables (historians) and is able to analyze them;
- displays documentation which concerns the devices involved in the process (documentation);
- allows the exchange of information and the data synchronization with other centers.

There are two communication methods that are used by SCADAs [3].

Polling communication - This communication method is based on master/slave interaction. The central station (master) has absolute control of the communications, sequentially reading the data of each remote station (slave), which only responds to the central station. Each remote station is identified by a unique address. In the case in which a slave does not respond during a predetermined period of time, a new polling will be realized before declaring time-out.

Report by exception - In this communication method the remote station monitors its input signals and when the signal overcome a default threshold, it starts the communication and the data sending with the central station. Hence, errors are automatically determined by the system.

Table 1.3: Polling and report by exception: advantages and drawbacks [3]

Type	Advantages	Drawbacks
Polling	• Simple communication • Impossible to have network traffic collision • Ensures response time • Detects connection errors • Can work with non-intelligent slaves	• Cannot detect level of information (urgent, ordinary) • The more are the slaves, the more time is needed • All information pass through the master
Report by exception	• Capable of identifying the level of information • Allows communication between slaves	• Can only detect connection faults after a certain period of time

1.5 Communication networks

A communication network is the backbone of a network-based control. Reliability, security, ease of use and availability are the main features while choosing the communication type. In addition, it should have deterministic end-to-end message response as the principal property. In fact, this is the only way for ensuring the real-time response which is required by the control algorithm [24].

As already said before, automation networks are widely used due to its great technological improvement which introduced advantages with respect to conventional cabling systems [3]:

- decreasing of wiring;
- easy maintenance;
- increasing network flexibility;
- possibility to real-time diagnose the devices;
- possibility to integrate devices produced by different manufacturers.

Essentially, the following variables are necessary for specifying an industrial network [3].

Transmission rate - it is the medium amount of data which is transmitted in a certain period of time. Usually is called throughput and it is measured in kilobits per seconds (kbps).

Network topology - this variable is related to the constructive arrangement in which the devices are connected.

Physical medium of transmission - the physical medium of transmission is related to the cabling used for the interconnection of the devices. They can be many and each of those with particular characteristics, thus, they are selected with respect to the application in which they will be used. The choice depends on the devices and protocols used, the desired throughput, etc.

Communication relationship between nodes - is the management method between the communication points (nodes) of the network with respect to the exchange of data.

Bus access algorithm - is the algorithm used by the nodes to access or send information in the network.

In the following will be described all these variables. For what concerns the analysis and the description of the network protocols used, it is possible to see the second Chapter.

1.5.1 Network topology

There can be different network topologies, all related to the constructive arrangement in which the devices are connected.

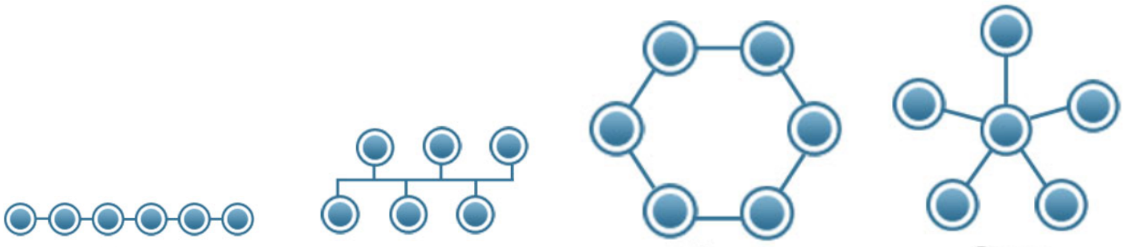
The eight basic topologies are point-to-point, bus, star, ring or circular, mesh, tree, hybrid and daisy chain. In the following are described the most common, represented in Figure 1.16.

Point-to-point topology - It is the simplest type of network topology that links two endpoints. As the Figure 1.16a suggests, each CPU receives information, uses what it needs and then sends the remainder to the others. In point-to-point networks, the communication is established between two or more CPUs which are not necessarily directly connected with each other. In addition, the use of the other nodes as routers is possible. This topology is not commonly used since a failure of one device causes the failure of the entire communication.

Bus topology - In this topology, the physical medium of communication is shared among all the CPUs. Both centralized and distributed control are achievable adopting this configuration. Bus topology is widely used since the network can be extended with ease and it is not entirely affected by the failure of a single device.

Ring topology - It is a point-to-point topology in which the last CPU is connected to the first one for closing the ring. Difficulties in adding new devices can happen since the communication must be interrupted to do this. Moreover, another issue depends on the transmission delay: the number of stations in the ring affects it in a proportional way. The principal advantage of this configuration is that a faulting node can be detected and, if there is communication in both directions, the network continues to operate, degraded only by the failed CPU.

Star topology - This topology uses a central node in order to manage the communication between machines. The external nodes don't affect other. Differently, the central station is the principal one and it can cause the collapse of the entire network. For this reason, most of the time are used two CPUs as central nodes, in order to give internal redundancy to the system.



(a) *Point-to-point.* **(b)** *Bus.* **(c)** *Ring.* **(d)** *Star.*

Figure 1.16: Common network topologies

1.5.2 Physical medium of transmission: copper cable

Normally, in the industrial environment, the communication is implemented adopting two different types of copper cable. They are [8]:

1. coaxial cable also referred to as coax;
2. twisted-pair cable, which can be shielded (STP/FTP/ScTP) or unshielded (UTP).

The following list introduces the components which always compose a copper cable [8].

Conductor - it constitutes the physical medium of transmission for the signal. Essentially, the conductor can be unique (a single wire) or diversified (stranded wire).

Insulation - protection and conservation of the signal from outside interferences is the principal purpose of the insulating layer. It is commonly built of a dielectric material (i.e. polyethylene).

Cable sheath - it is an outer sheath which is used to contain the elements that constitute the cable. The sheath differs for indoor and outdoor exposure. Usually, outdoor cable sheaths are black, resistant to water and UV light. Indoor cable sheaths can be divided into two classes: plenum and non-plenum. The plenum sheath is fire resistant and it doesn't produce toxic fumes while burning because it is composed of non-flammable fluoropolymers (i.e. Teflon, Kynar). On the contrary, due to the fact that they are made of polyethylene (PE) or polyvinyl chloride (PVC) which are both flammable and can produce toxic fume, non-plenum sheaths can be used only in restricted areas. Obviously, the cost is highly different, with the plenum sheath which is much more expensive.

From theory, it is well-known that the transmission of a signal through any medium is affected by the distance which must be covered. In fact, the amplitude decreases as the physical medium opposes resistance to the flow of energy. Moreover, a signal can be affected by distortion due to the increase of the attenuation phenomenon which happens at the higher frequencies.

Copper cables are a good technology for transferring information, but attenuation, crosstalk and/or impedance mismatches can affect negatively the signal quality [8].

Attenuation - It is the measurement in decibels [dB] per unit length of the decline of the strength of the signal. Higher is the frequency and the resistance of the cable, faster will be the attenuation phenomenon.

Impedance mismatches - The impedance of a transmission cable is defined as "the resistance offered to the flow of electrical current at a particular frequency" [8]. The characteristic impedance is the impedance of an infinitely long cable, where the signal never reaches the end and thus cannot bounce back. The situation can be replicated placing a resistor at the end of the transmission (so-called termination resistor). In this way, from an electrical point of view, the cable seems to have an infinite length and the signal is not reflected from the remote end. Reflection is one of the principal sources of interference and must be avoided in any case. RS-485 connectors have the possibility to implement the electrical termination at the ends of a bus topology.

Crosstalk - Crosstalk is another form of electrical interference which concerns the pick up of signals from an adjacent cable or circuits.

Coaxial cables

Coaxial cables are often used for data transmission because they are particularly stable in terms of their electrical properties at frequencies below 4 GHz [8].

The structure of the cable is coaxial, as the name suggests. The center is occupied by the conductor wire which can be solid or stranded. The insulating layer is usually composed of Teflon or polyethylene. The double shield is the main feature of this type of cable, it consists of two different layers [8]:

- Foil shield. Normally consisting of a thin foil of aluminium tied to both sides.
- Braid shield. It is usually composed of copper or aluminium in braid (or mesh) shape. This shield covers the insulation and the foil shield and it ensures protection from electromagnetic and radio frequency interferences. While the foil shield is not always necessary, the braided shield is required and utilized in any coaxial cable.

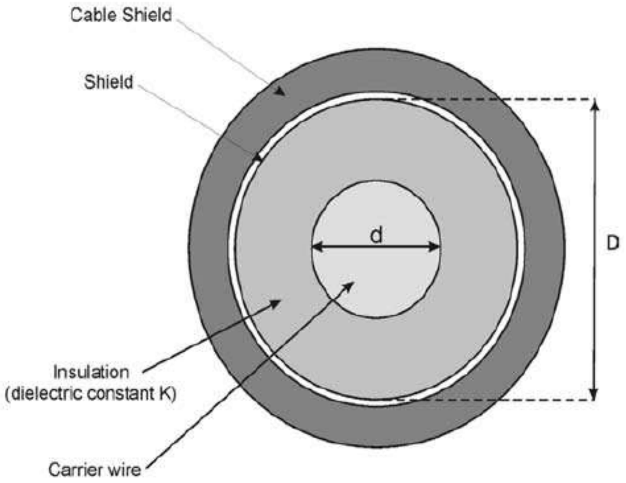


Figure 1.17: Cross section of coaxial cable [8]

In addition to the previously described issues which can happen in any copper cables, the performance of a coaxial cable is affected by its composition, diameter, and impedance.

Obviously, the composition of the central wire determines in large part the quality of the cable. The electrical demand that the cable is able to tolerate can be determined by its diameter. In general, the larger the diameter of a coaxial cable is, the more it will support the electrical activity.

To compute the impedance Z of a coaxial cable, the following formula can be used [8].

$$Z = \frac{138}{\sqrt{k}} \log \frac{D}{d}, \tag{1.1}$$

where k is the dielectric constant of the insulation.

Table 1.4: Coaxial cable: advantages and drawbacks [3]

Advantages	Drawbacks
• Easy to install • Cost effective with respect to other cable types • Highly resistant to signal interference	• It is easily damaged • More difficult to work with than twisted-pair cable • Connectors can be expensive

Twisted-pair cable

This type of cables is very common on the market thanks to the ease of installation and the price which characterize them. In addition, they provide a good rate of data transmission (up to 1000 Mbps) [8]. As it has been already stated, twisted-pair cables can be shielded (STP, FTP, and ScTP) or unshielded (UTP).

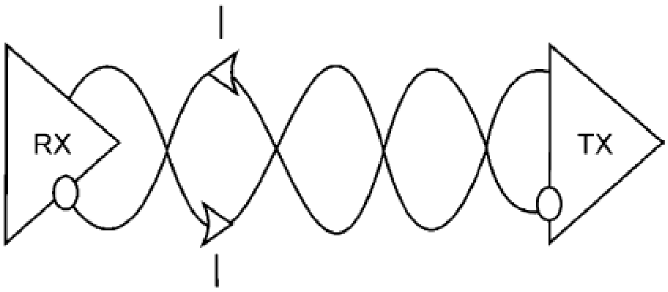


Figure 1.18: Current flow in a twisted pair [8]

Inside these cables, two identical conductor wires are braided with each other and, individually, they can be solid or stranded. These wires are twisted a specific number of times per meter, generally forty. The capacitance of a twisted pair cable is low (from 40 to 160 pF/m) and it allows a moderate bandwidth and a feasible slew rate. As it is shown in Figure 1.18, inside each conductor the current flows in opposite directions [8].

The twisting of associated pairs and the method of transmission reduce the interference from the other pairs of wire throughout the cable. The currents inside the two conductors are equal and opposite, producing the elimination of the magnetic fields which are induced by the current. Therefore, this type of cables is self-shielding.
The sheath is made of PVC or Teflon or Kynar. Unshielded twisted pair cables are normally composed of a sheath which includes four pairs of wires. Here, the colour of the wires is standardized and there is one wire each of brown, blue, green, and orange, and four white wires which are intertwined with each of the previous ones (see figure 1.19) [8].

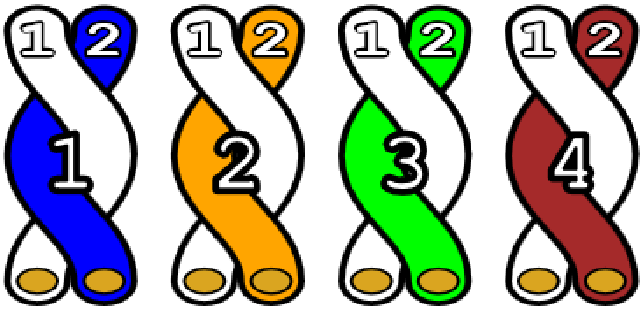


Figure 1.19: Color coding in a four pair UTP cable

For what concerns the shield, many different methods are used, but it is not the purpose of this document go into details of this technology.

The United States EIA/TIA (Electronic Industries Association/Telecommunications Industries Association) has composed various categories which include all the different typologies of UTP cables. There is no intention of entering into details of these categories, but it is important to show the application and the throughput of each one (see Table 1.5).

Table 1.5: EIA/TIA categories [3]

Category	Throughput [Mbps]
Category 1	Telephone cable
Category 2	4
Category 3	10 (Ethernet)
Category 4	20
Category 5	100 (Fast ethernet)

Table 1.6: Twisted-pair cable: advantages and drawbacks [8]

Advantages	Drawbacks
• Easy for connecting devices • STP has good blocking ability of interference • UTP is inexpensive • UTP very easy to install	• STP difficult to work with • UTP is more susceptible to noise and interference than coaxial or fiber-optic cable

1.5.3 Physical medium of transmission: fiber optic

The use of light signals driven through a fiber core is the fundamental concept on which the optical fiber communication is based. Hence, this type of cables serves as wave-guides for the light thanks to the presence of a cladding with a lower refractive index that covers the central core of the cable. Hence, no energy from inside or outside is able to exit/enter the core and, thus, electromagnetic interferences can't disturb the transmission [8].

Providing that the light ray collides with the cladding at an angle greater than the critical angle, the core and the cladding are capable of confining the signal in the center. In this way, the light ray moves inside the cable thanks to a series of total internal reflections.

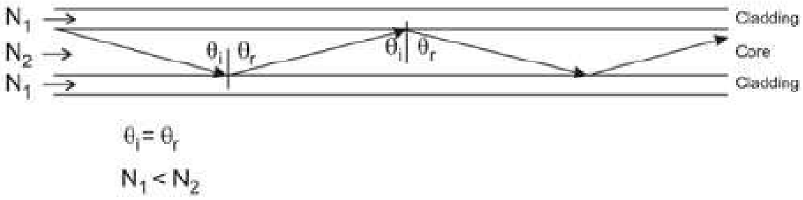


Figure 1.20: Light tray traveling through an optical fiber

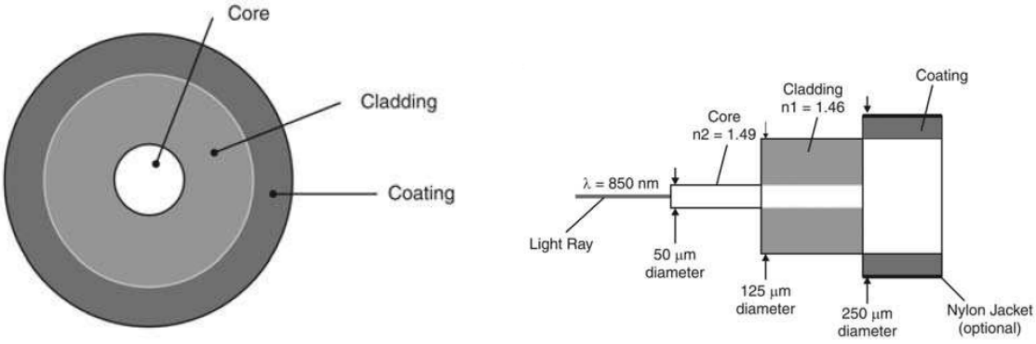
Of course, the signal must be amplified or repeated if the distance between the two end-points is considerable because the glass core absorbs a little part of the light signal at each collision.

Optical fiber technology offers great advantages [8]:

- electromagnetic interference or electrical crosstalk are heavily reduced;
- interference with other signals is completely avoided and, thus, areas in which there is a high presence of electromagnetic fields can be covered with optical fiber connections.
- frequency bandwidth is wider and more flat, such that equalizers are not required;
- attenuation of the signal is much lower than in other applications, signals can be transmitted further before having the necessity to amplify or repeat them;
- the cables don't conduct electricity and, thus, electrical shocks, lightning harms as well as ground loops are avoided;
- the optical fiber cables are usually thinner and lighter than the copper cables;
- data are safer with respect to the security ensured by copper cables.

Figure 1.21 shows the principal components which compose a fiber-optic cable: the core, the cladding, the buffer, the strength members, and the sheath.

The glass fiber is the main object which constitutes the core of a fiber-optic cable because, through it, the light signal travels. Usually, the core and the cladding are produced as a single unit.



(a) *Face view.*

(b) *Profile.*

Figure 1.21: Main components of a fiber-optic cable

The buffer is composed of several plastic layers which enclose the cladding. Essentially, it decreases the probability of microcracks which could damage the fiber and it guarantees a major mechanical resistance of the cable. The buffer aims also to give water resistance to the core and the cladding, together with the protection from other materials (i.e. powder).

Additional important components are the strength members which are filaments of very robust material (i.e. steel, or Kevlar) that contribute giving a tensile robustness to the cable. In the end, the sheath is an external jacket which ensures primary mechanical protection [8].

Fiber-optic cable parameters

The main parameters which characterize a fiber-optic cable are described [8].

Attenuation - Wavelength and fiber construction are the main characteristics which affect the attenuation phenomenon.

Diameter - Two optical fiber types are achievable.

- Multimode fibers range from 50 to 62.5 micron of core diameter. Inside, the light ray has enough space to move with multiple ways through the core.
- Single-mode fibers are usually made of 8.5 microns of core diameter. A unique path is available for the light ray to move inside the core.

Wavelength - 850 nm, 1300 nm, and 1550 nm are the most common three wavelength bands which are used by the fiber-optic systems. The shorter the wavelength is, the greater will be the attenuation of the signal.

Bandwidth - By definition, the bandwidth of a fiber is "the range of frequencies across which the output power is maintained within 3 dB of the nominal output"[8]. It is computed as the frequencies of the bandwidth multiplied by the distance (i.e. 100 MHz km).

Dispersion - Nanoseconds of pulse spread per kilometre (ns/km) is the unit of measure of the modal dispersion. This value defines an upper constraint for the bandwidth: the signal must have a larger continuation than the time of propagation of the pulse.

1.5.4 Industrial Wireless transmission: IWLAN

Nowadays, wireless systems are utilized in a large number of application areas. The wireless technology provides two important benefits that are on the base of its success: reduction of cabling and the fact that the technology can be mobile both for computers and users point of views. Obviously, these advantages save the costs while facilitating new applications.

Bluetooth, GPRS, and UMTS for phones are just some of the technologies that are utilized for establishing a wireless network. For the purposes of the project, this subsection will regard the Industrial Wireless Local Area Network in its strict sense: a radio network which follows the IEEE 802.11 standard.

The wireless technology is adopted in various ways inside the industrial plants [24].

- IWLAN can offer communication support in distributed control applications which regard mobile subsystems (i.e. robots, turntables, etc.).
- Dangerous areas of the plant can be covered with wireless communication without the use of cables. This improves the safety of the plant itself.
- Plant reorganization is less complicated since fewer cables are used.

Despite all the advantages, there is always a certain complexity originating from the fact that a wireless network is nothing but a radio field. Radio waves propagate through space and they can be diffracted, reflected and/or attenuated when passing through objects. In fact, unlike signals in a line, radio signals propagate three-dimensionally in space as electromagnetic waves. The objects which are located within the range of the radio waves influence the propagation and effects like reflection, diffusion, absorption and interference may occur. All these properties generate a complex radio field that can even change when obstacles move. Then, connection reliability, eavesdropping security and interference immunity of the network can be badly affected by these characteristics [15].

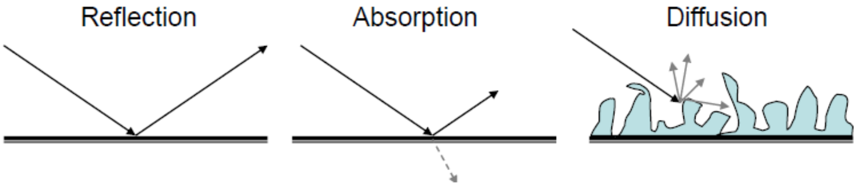


Figure 1.22: Reflection, absorption and diffusion of radio waves

Two properties have to be specifically pointed out.

- On the one hand, radio waves can expand or extinguish one another (so-called fading or interference).

- On the other hand, propagation features depend on the wavelength of the radio waves. In particular, radio waves with long wavelength (which means low frequency) can be diffracted around objects.

Thus, the wavelength affects the previously described properties: the shorter is the oscillation of the wavelength (high frequency of the radiation), the more the radio waves resemble the characteristics of the light [15]. In fact, if the frequency is low (wide wavelength), the signal can pass deeper through non-conducting obstacles or can completely go through them, which is exactly the contrary of what is able to do the light.

In addition, each object that produces signals on the same frequency of the wireless network and it is placed within it can disturb the system. Unlike lines, radio waves are very susceptible to interferences and the network must be mapped in detail in order to avoid it.

Among other things, the frequency is also important for the possible transmission range and the achievable data rate. In fact, short wavelength radio waves can reach shorter distance with respect to the range obtainable with a transmitter of long wavelength. In any case, the communication range can be extended by using directional antennas. The same reasoning can be applied to the data rate: larger is the bandwidth, greater will be the attainable data rate [15].

For having an idea of the possible range, the Fresnel Zone was defined. This zone analyzes specific areas between receiver and transmitter for characterizing the signal propagation. Normally, the Fresnel zone has ovoid shape but it doesn't take into consideration the frequency of the transmission (see Figure 1.23).

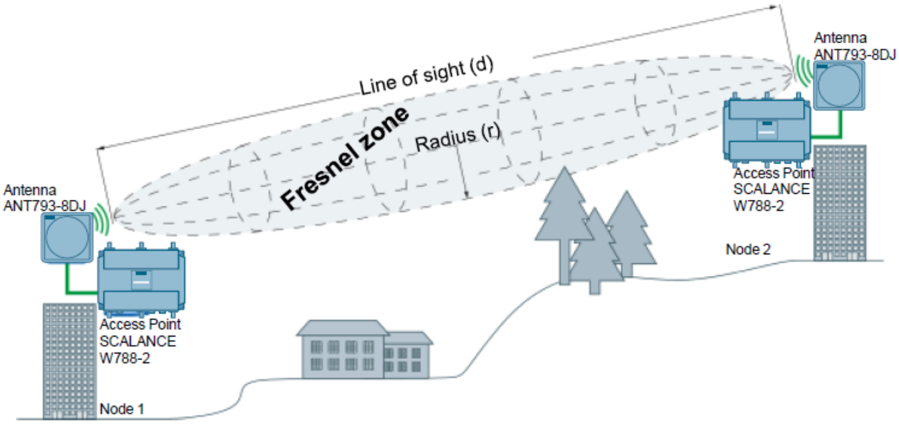


Figure 1.23: Example of Fresnel zone

For the free space loss calculation, the following variables are required.

1. Direct line-of-sight distance of the transmission path between transmitter and receiver.

2. An area around this distance must also be free of obstacles.

The Fresnel zone is subdivided into various order. The first order is the most important one since it describes the area where the main part of the signal energy is transferred. The diameter of the ovoid becomes smaller with the increase of the bandwidth frequency, while it becomes wider with the augmenting line-of-sight distance.

Antenna

An antenna has the purpose of transforming electrical currents into electromagnetic waves and vice versa. An electrical field vector $\mathrm{E_x}$ and a magnetic field vector $\mathrm{H_y}$ constitute electromagnetic waves. These two field vectors are always at a 90 °angle to each other (see Figure 1.24).

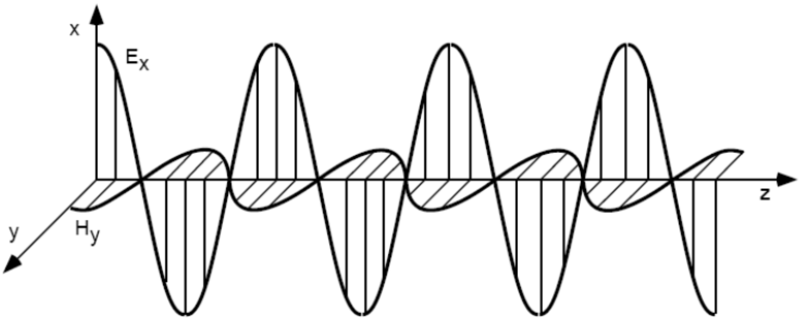


Figure 1.24: Propagation of the electrical (E_x) and magnetic (H_y) field vectors.

Essentially three parameters are important in a wireless network antenna.

Impedance - It refers to a frequency dependent resistor which is typically 50 Ohm [15].

Polarization - The electrical field vector direction is specified by this parameter. The direction can be:

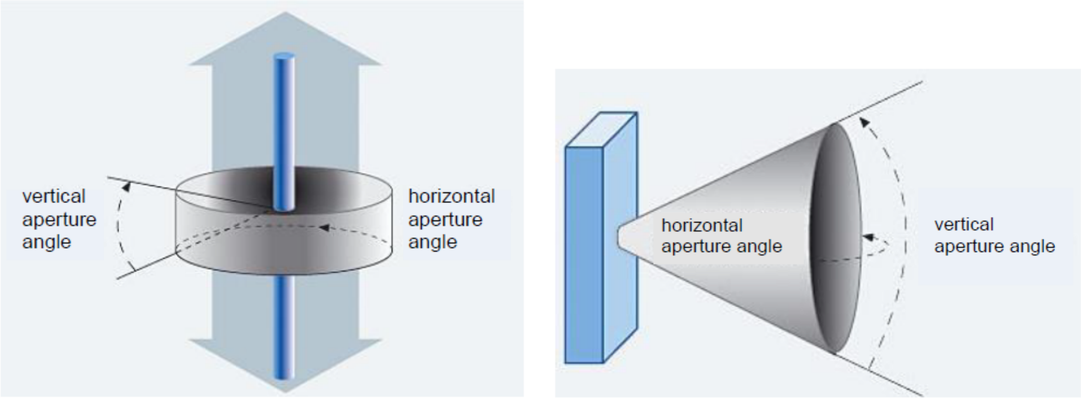
- linear, which causes the electric field lines to run in a plane (vertical or horizontal with respect to the ground);
- circular, which causes the lines of the electrical field to run continuously in a circle shape (clockwise or counterclockwise).

For excellent signal acquisition, it is important that the polarization of both antennas is identical.

Gain - It defines how strong an antenna sends and receives with respect to a reference emitter [15]. The unit of the gain is usually [dBi], where the "i" stands for "isotropic" radiator. A gain of 3 dBi provides an almost doubled send/receive line.

Typical distinction between antennas is the one which refers to the direction of radiation. Radiation can be omnidirectional or directional depending on the shape of the radio field.

Normally, more distance can be covered using directional antennas. As shown in Figures 1.25, the omnidirectional antenna has the form of a rod or a straight wire while the directional one is a small flat box. The latter one generates a radio field which is cone shape and the field intensity decreases quickly outside of the cone.



(a) *Omnidirectional antenna.* **(b)** *Directional antenna.*

Figure 1.25: Angles of radiation in omnidirectional and directional antennas [15]

IEEE 802.11

The IEEE (Institute of Electrical and Electronics Engineers), with the project number 802, has grouped the standards which regard the installation and functioning of the networks. In particular, the task group 802.11 is entirely dedicated to the wireless LANs.

The institute always improves the regulations in order to adapt them to new necessities and technical restriction. Table 1.7 furnishes a review of the topics of some IEEE 802 standards concerning IWLANs.

Table 1.7: Main topics and characteristics of 802.11 network standard [15]

Standard	**Definition area**	**Frequency band**	**Max. gross data rate**
802.11a	Communication	5 GHz	54 Mbit/s
802.11ac	Communication	5 GHz	7 Gbit/s
802.11ad	Communication	60 GHz	7 Gbit/s
802.11b	Communication	2.4 GHz	11 Mbit/s
802.11e	Quality of service	-	-
802.11g	Communication	2.4 GHz	54 Mbit/s
802.11h	Interference reduction	5 GHz	54 Mbit/s
802.11i	Data security	-	-
802.11n	Communication	2.4 and 5 GHz	600 Mbit/s
802.11Q	Virtual LANs	-	-
802.11X	Data security	-	-

For what concerns the wireless network which has been implemented in the laboratories, the 802.11 standard is of interest since it defines the radio communications in frequency bands at 5 GHz and 2.4 GHz [15].

Apart from the frequency, another important distinction between these standards is the maximum gross data rate reachable (see Table 1.7). Obviously, if the connection condition is bad for maintaining the maximum data rate, this value is automatically reduced until a stable communication can be performed.

The wireless transmitter in laboratory n. 201 is able to generate maximum two of these connections simultaneously. At the same time, each receiver must be configured for searching the proper standard.

1.5.5 Types of communication relationship between nodes

Before introducing the bus access schemes which are typically used in the industrial environment, the end-to-end communication relationship between nodes must be defined. The most common relationships are the master-slave, producer-consumer and client-server [24].

Master-Slave - The network has master nodes and slave nodes. Slave nodes react only react to master nodes commands. Usually, master nodes share the channel access by using token passing scheme. Both single-master and multi-master approaches are possible. Normally, single-master is adopted in networks which have a simple structure; differently, networks which have a complex system and all the nodes equal are controlled with the multi-master approach.

Producer-Consumer The network has nodes that are producers, consumers or both. A producer node when it has a message to send looks for the first opportunity to send in a broadcast way. Consumer nodes pick up this message contents as soon as they need it.

Client-Server - In this case, the network has client nodes and server nodes. The client nodes send requests to the server nodes for services. Based on the best effort, the server provides this service and notifies the completion. This scheme is not necessarily deterministic as the server nodes take as much time as they need.

1.5.6 Bus access algorithm

The nodes which belong to the system have a specific procedure (algorithm) to access the information of the network. In literature, the algorithms that will now be treated are focused on the subject of the communication technology seen previously in section 1.5.5.

The main algorithms used nowadays are CSMA/CD, token passing, cyclic polling, CoS and CTDMA.

CSMA/CD - [3] Carrier Senser Multiple Access/Collision Detection. Using this algorithm, the data transfer begins at the same moment in which the device recognizes that the channel is available. If two devices try to transmit simultaneously, there will be a collision. When a device detects that the transmission collided with another, it aborts its transmission and it tries to transmit again after a random time. There are different types of CSMA/CD, one of these is NDA (Non-Destructive Bitwise Arbitration) which deals with the deterministic resolution of collisions through priorities.

Token Passing - [24] The token is a particular piece of information which symbolizes the license to control the network. It is transmitted from node to node and only the device which is holding it may start the communication. Of course, there is a set of rules which guarantees that possible errors (i.e. lost token, duplicate token) are recognized and resolved.

Two methods can be used to implement the token passing algorithm: adopting a dedicated short message (explicit form) or utilizing distributed, synchronized access counters in all nodes (implicit form). The master-slave mechanism is usually merged with this algorithm with the aim of controlling a subset of nodes.

PROFIBUS, both DP and PA versions (see Figure 1.26), adopts the token passing algorithm in its explicit form. Since various PROFIBUS networks may exist together on the same bus, the right configuration of the "target token rotation time T_{TR}", which is nothing but a timing parameter, is necessary. T_{TR} defines the period of time in which a master can occupy the bus. When the token is received by a master, the latter starts a timer to measure the rotation time. The next time that it receives the token, the information exchange with other masters or slaves is authorized until the time required for the transmission doesn't reach the T_{TR} value. When the time expires, the token is moved to the next master which is involved in the communication. In the case in which a master receives the token when the time is already completed, it can transmit one high-priority message before passing the token.

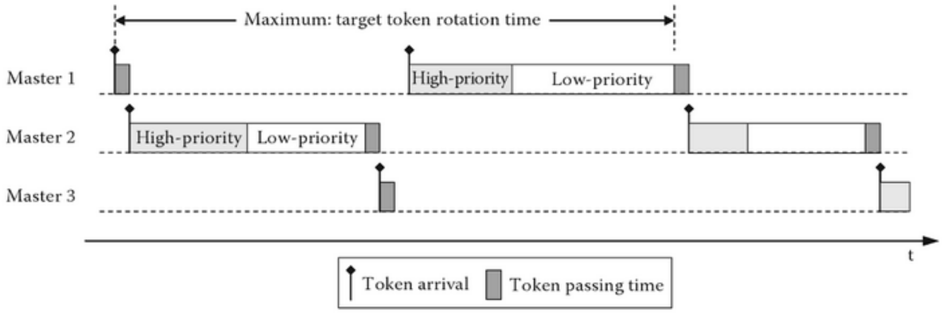


Figure 1.26: Token passing in PROFIBUS

Cyclic polling - [24] Polling is a master-slave algorithm which allows a central master to explicitly command to a slave node the beginning of data transfer. Hence, in the network, there is always an exchange of poll messages between master and slaves.

Most of the times the polling mechanism is cyclic: the master polls the slaves one by one for then restarting. The AS-i network protocol, which has implemented in laboratory n. 201, is a bus system which adopts this type of algorithm.

This data exchange method is efficient for applications in which the transmitted signals vary slowly over time. For example, analog input/output signal. Discrete signals, in fact, can have a rapid change of their state and this type of algorithm may have the information lost.

Change of State - [3] Devices only produce data when it changes its state. In the background, a signal is transmitted cyclically to confirm that the device is operating normally. The advantage of CoS for data exchange is that this method significantly reduces network traffic. Indicated for communication of data of digital input and output.

CDTMA - [3] In this method, the network access is controlled by a time-slice algorithm which regulates the data transmission in the network nodes in each time interval. It is possible to set the time adjusting the NUT (network update time).

Chapter 2

Industrial network protocols

This chapter deals with all the network protocols that have been used during the development of the system. A quite detailed description of the Fieldbus communication protocols which have been implemented in the laboratory n. 201 can be found.

The first section of this chapter introduces to an overall description which regards the Fieldbus protocols, comprehensive of the OSI Model and normative. After this, AS-interface, PROFIBUS and PROFInet will be described in details.

2.1 Fieldbus protocols

2.1.1 Open Systems Interconnection Reference model

The so-called "Reference Model for Communication between Open Systems" has been defined in 1978 by the ISO (International Organization for Standardization). This Reference Model has become acknowledged as the "Open Systems Interconnection Reference Model", or, more briefly, as the "OSI model".

The OSI Model (ISO/IEC 7498) roughly consists of a data communications management body which subdivided the data transmission into a reasonable chain of commands composed by seven different layers. Each stratum of this chain has a precise objective and communicates both with the upper and the underlying layers.

Initially, it could be argued that the OSI Reference Model doesn't include a set of regulations, but differently, it consists of a global scheme through which protocols can be described. In addition, the OSI Model framework precisely shows the tasks or the utilities that the seven layers must have [8].

As a minimum of two sites is required to interact, a sort of virtual peer-to-peer communication is performed between the same layers which belong to the different communication channels. This concept is illustrated in Figure 2.1. The tasks of each layer are given by abstract devices entities, for instance, programs, functions, and protocols which realize the work for a precise layer. More than a single entity is achievable by a single layer. In contiguous layers, they communicate through the upper limits and the lower ones by providing physical information over SAPs (Service Access Points) [8].

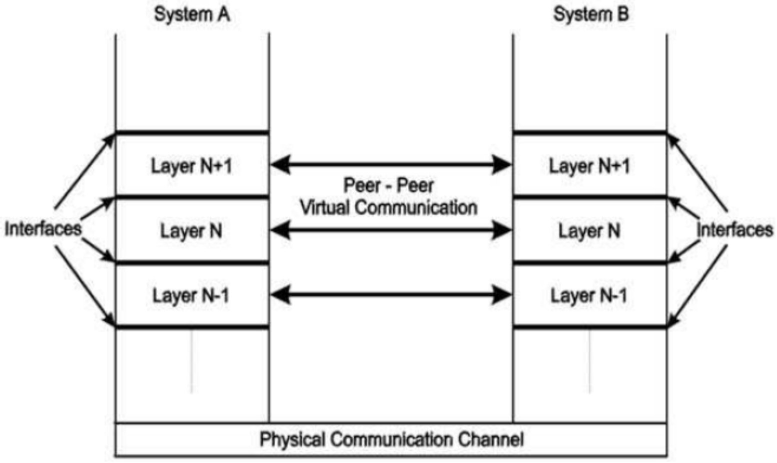


Figure 2.1: OSI layering concept

Furthermore, the abstract entity which is located in the next overhead layer is indicated as $N + 1$, while the entity in the next lower layer as $N - 1$. Being a chain, the utilities of the upper layers are subject to the changing behaviours of the lower services.

In the OSI Model, it is not specified how these services should or could be enforced. Indeed, this model tends to specify the 'interconnection' aspect of this layering concept and, in addition, to define the information flow which occurs through this network [8].

Once received the data from the user at the top of the chain, the system physically delivers them down through the layers, attaching headers (and eventually trailers), and calling upon to functions according to the protocol guidelines. The combination of data and header packets is called PDU (Protocol Data Unit). Of course, the opposite situation verifies at the collecting point: the data are deprived of the headers as they moved up to the top of the chain. These headers and control messages appeal to services and to peer-to-peer logical communications of entities over the sites.

It is important to point out that there is no relation or straight data transmission between the same layers of the two architectures since this communication is only virtual between them. Instead, the whole process of interaction only occurs at the physical layer. In Figure 2.2 the full architecture is shown.

Shortly, the utilities given at each layer of the chain are [8] [24]:

Application layer - It is the dominant layer in the model since it provides the network services to the application program of the user. In addition, because of the whole range of usable applications and task possibilities that can be found in this layer, it offers a higher number and variety of services than those offered by lower layers.

Presentation layer - It outlines the information representing them into formats which are readable by external applications or users. Its tasks can include data encryption and compression.

Session layer - It aims to synchronize and put in sequence the information during a 'session'. Other two objectives of this layer are, on the one hand, to guarantee that the interaction remains stable until the communication is concluded; on the other hand, it secures proper security measures.

Transport layer - The main task of the transport layer is to provide a transmission of data at an agreed level of quality. It is a central layer since it is located between the layers which are highly dependent on the applications (upper) and the layers which are network based (lower).

Network layer - Several functions are provided by this layer.

- Regulation of addresses or translation from hardware to network addresses. These addresses can be located on a LAN (local area network), as well as hinting at remote networks (internetwork).
- Looking for a free path between the sender and the receiver nodes, or among intermediate devices.
- Creation and conservation of a logical connection between the source and the destination nodes, together with the actualization either of a connectionless or a connection-oriented communication.
- Division of a large group of data into small frames, so that they can be carried by the underlying data-link layer.

Data-Link layer - The tasks of the Data-Link layer are to form, transfer, and get packets of data. This layer also creates packets that are suitable for the network architecture used. Besides, demands and data from the network layer also form part of some of the data of these packets.

Physical layer - This layer is the model lowest one. Data packets are taken from the Data-Link layer above and the physical layer converts it into electrical signals which symbolize binary values. Then, it aims to transmit the signals to the receiving end through a medium of transmission (e.g. copper, optical fiber, air, etc.). The opposite work is carried out by the physical layer at the reception point: it transforms them into a list of bit values. The electrical and mechanical characteristics of the physical transmission medium are described at this level of the OSI model.

The Manufacturing Automation Protocol (MAP) has been the first application of the OSI model in the industrial automation domain. According to Figure 1.5, the MAP is a particular protocol which is applied for data exchange between factory, shop floor and cell level. The MAP was created for being a structure which could control all the pyramid levels and, thus, the entire automated process [24]. However, due to its complexity, the implementations were extremely costly for a general-purpose use. For this reason, a reduced version called MiniMAP which used a model that was based on the OSI layers 1, 2 and 7 was proposed. Despite the fact that this model aimed to deal with the problems which affected the lower pyramid layers, also the MiniMAP had no success [24].

The fact that the MAP standard was not applicable to time-critical systems and the missing acceptance of MiniMAP have been the reasons for the IEC to develop a Fieldbus protocol which was based on the MiniMAP model, but adjusted to the needs of the field level.

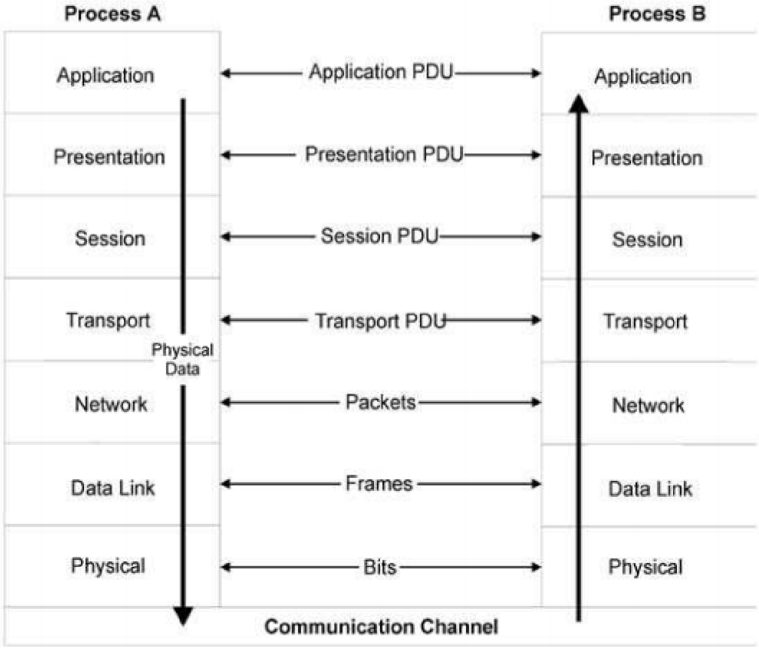


Figure 2.2: Layers architecture of the OSI model

2.1.2 IEC 61158 and IEC 61784

Starting from 1980, automation made a great leap forward with the utilization of PLCs and more intelligent sensors/actuators. At the same time, there was an increasing request for cables reducing such that the development of detailed communication protocols began. During these years, the market had to convince the users of such new concepts and followed an intense selection process.

As the final step, international standardization has been carried out in order to authorize Fieldbus in the industry. In fact, a standard organizes a specification rigidly and formally, avoiding the possibility of modifications in short times. In this way, the specification is more reliable, stable, and, in consequence, ensures the trust of the costumers and the market position [24]. Furthermore, the fact that the standard is vendor-independent certifies openness.

Hence, IEC 61158 was developed. According to it:

> "a Fieldbus is a digital, serial, multidrop, data bus for communication with industrial control and instrumentation devices such as - but not limited to - transducers, actuators and controllers." [4]

The IEC 61158 defines various types of Fieldbus protocols. Each of these types delineates multiple measurements and allows to connect different stations. Only the devices which have the identical protocol type can communicate directly with each other [4]. This standard divides the Fieldbus protocol into several layers basing on ISO/IEC 7498, the OSI reference model. Respect to the OSI model, it uses only three levels: Application, Data-Link and Physical layer. In this case, the IEC 61158 Data-Link layer or the IEC 61158 Application layer can include the functions of the OSI model layers from three to six which otherwise were not represented. If this is not possible, another separated layer can be added to the stack.

The IEC 61158 basic Fieldbus reference model is represented in Figure 2.3. The OSI layers, their functionalities and equivalent layers in the Fieldbus standard are shown in Figure 2.4.

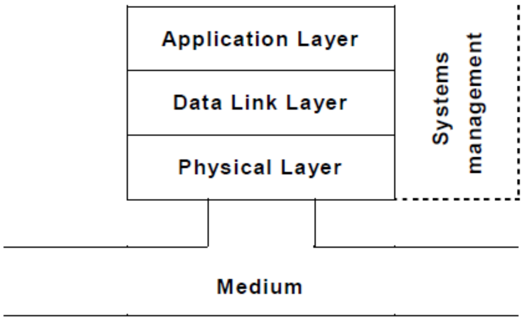
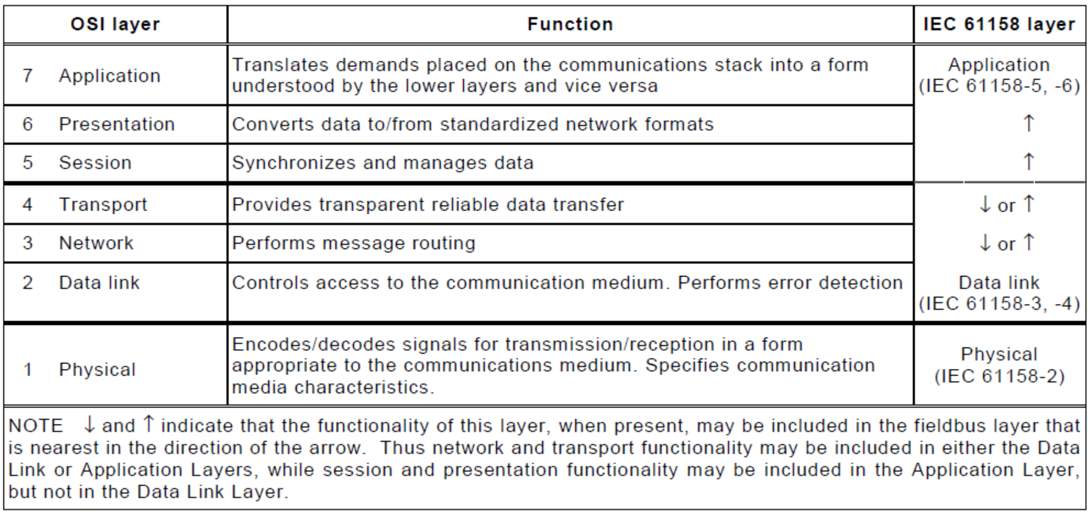


Figure 2.3: The layers involved in the Fieldbus model



OSI layer		Function	IEC 61158 layer
7	Application	Translates demands placed on the communications stack into a form understood by the lower layers and vice versa	Application (IEC 61158-5, -6)
6	Presentation	Converts data to/from standardized network formats	↑
5	Session	Synchronizes and manages data	↑
4	Transport	Provides transparent reliable data transfer	↓ or ↑
3	Network	Performs message routing	↓ or ↑
2	Data link	Controls access to the communication medium. Performs error detection	Data link (IEC 61158-3, -4)
1	Physical	Encodes/decodes signals for transmission/reception in a form appropriate to the communications medium. Specifies communication media characteristics.	Physical (IEC 61158-2)

NOTE ↓ and ↑ indicate that the functionality of this layer, when present, may be included in the fieldbus layer that is nearest in the direction of the arrow. Thus network and transport functionality may be included in either the Data Link or Application Layers, while session and presentation functionality may be included in the Application Layer, but not in the Data Link Layer.

Figure 2.4: Comparison between the OSI and the Fieldbus models [24]

IEC 61158 Physical Layer - In this layer, the data packets are received from the Data-Link layer and then encapsulated with communication frames. The new packets which are comprehensive of bits and communication framing information are thus encoded into signals. After this, the purpose of the physical layer is exactly the same as in the OSI model: it has to transfer the signals to the destination node through a physical medium [4]. At the receiving end, is always the physical layer which ensures the verification and the removal of the framing information. In the end, it sends the data packets to its Data-Link layer [4].

IEC 61158 Data Link Layer - Time-critical assistance for data exchange among devices is the main functionality of the Data-Link layer. The term "time-critical" is used to define applications that have a certain time-window in which they are required to perform actions [4]. The failure to terminate the indicated actions within the requested time can cause the malfunction of the other applications which are waiting the on-time completion of the tasks as well as equipment or plant failure risk, and, possibly, dangerous situations for human life.

IEC 61158 Application layer - In an automation environment, the principal task of the Application layer is to furnish an assistance to the transference of time-critical applications calls and answers among devices.

The IEC 61158 is a huge opera which contains more than four thousand pages, divided into parts. Each part describes different contents in details (see Table 2.1).

Table 2.1: Structure of IEC 61158 [4]

Standards part	Contents	Meaning
IEC 61158-1	Introduction	Only technical report
IEC 61158-2	PhL: Physical Layer	8 types of data transmission
IEC 61158-3	DLL: Data Link Layer	8 types
IEC 61158-4	DLL: Data Link Layer Protocols	8 types
IEC 61158-5	AL: Application Layer Services	10 types
IEC 61158-6	AL: Application Layer Protocols	10 types

Clearly, the collection of Fieldbus specifications in the IEC 61158 standard is useless for any implementation. A manual is needed for the practical use, showing which sections can be compiled into a functioning system and how this can be accomplished. This guideline was compiled later on as a definition of the so-called Communication Profile Families (CPFs) and it has been included in the international standard IEC 61784.

The Table 2.2 shows that the Fieldbus today consists of seven different main profiles that can be further subdivided. All the important Fieldbus systems from industrial and building automation are listed here, and the world's biggest automation companies are represented with their developments.

These CPFs were listing during the first compilation of the IEC 61784, in the 2003/04. Approximately every 3 years the standardization is uploaded, adding or removing some profiles and making changes.

Table 2.2: Profiles and protocols according to IEC 61784 and IEC 61158 [6]

IEC 61784 Profile	IEC 61158 Protocols			Brand names
	PhL	DLL	AL	
CPF-1/1	Type 1	Type 1	Type 9	Foundation Fieldbus (H1)
CPF-1/2	Ethernet	TCP/IP	Type 5	Foundation Fieldbus (HSE)
CPF-1/3	Type 1	Type 1	Type 9	Foundation Fieldbus (H2)
CPF-2/1	Type 2	Type 2	Type 2	Control Net
CPF-2/2	Ethernet	TCP/IP	Type 2	EtherNet/IP
CPF-3/1	Type 3	Type 3	Type 3	PROFIBUS-DP
CPF-3/2	Type 1	Type 3	Type 3	PROFIBUS-PA
CPF-3/3	Ethernet	TCP/IP	Type 10	PROFInet
CPF-4/1	Type 4	Type 4	Type 4	P-Net RS-485
CPF-4/1	Type 4	Type 4	Type 4	P-Net RS-232
CPF-5/1	Type 1	Type 7	Type 7	WorldFIP (MPS,MCS)
CPF-5/2	Type 1	Type 7	Type 7	WorldFIP (SubMMS)
CPF-5/3	Type 1	Type 7	Type 7	WorldFIP (MPS)
CPF-6/1	Type 8	Type 8	Type 8	INTERBUS
CPF-6/2	Type 8	Type 8	Type 8	INTERBUS TCP/IP
CPF-6/3	Type 8	Type 8	Type 8	INTERBUS Subset
CPF-7/1	Type 6	Type 6	-	Swiftnet transport
CPF-7/2	Type 6	Type 6	Type 6	Swiftnet full stack

In the automation pyramid, Fieldbuses are actually located into two levels: the field and the cell/process level.Therefore, they are sometimes separated into two classes [24].

1. Field level buses are known as device buses or sensor-actuator buses. They have very limited capabilities and they are used to connect simple devices with controllers (e.g. PLCs).

2. At the cell level, closer to computer networks, Fieldbuses connect control and supervisory devices among them.

However, only few Fieldbus systems can be immediately allocated to one of the previous groups, most of them are being used in both.

Hence, this type of systems can be applied in many areas, with different purposes. This results in several applications for developing different solutions.

Laboratory n. 201 is equipped with PROFIBUS and PROFInet cables that have been used for low to high communication and an AS-i cable for communication in the sensor-actuator level at the base of the pyramid. Not only copper cables have been adopted: wireless LAN devices and fiber-optic were available and thus a hybrid network has been implemented. Therefore, a detailed description of these protocols is present below for understanding their operation and their characteristics before moving to the third chapter in which the laboratory n. 201 is introduced.

2.2 Actuator Sensor interface: AS-i

At the basis of the field level, the communication between sensors and actuators occurs in binary and a sensor-actuator bus is used to transmit signals. This is not a complex solution and it permits to transfer both the power and the information using a mutual medium. The bus system implemented by AS-interface is very suitable for this purpose.

The Actuator Sensor interface (AS-i) is a networking system designed for the lowest levels of automation in the field, particularly for binary devices since it is a bit-oriented communication link. Moreover, it is an open system which has been developed by eleven manufacturers, including: Allen-Bradley, Siemens, and Festo [8].

It has been already stated that at the field level, the data volume is very high. A large portion of the devices requires or provides binary signals. Hence, in this level of the automation pyramid, an extremely high transmission speed of the data is needed. The AS-i communication is based on bit messages which increase the efficiency of the binary sensors/actuators since they don't need a high amount of bytes to transmit the required information. Obviously, due to its functioning mode, it is not possible to connect intelligent controllers using AS-i.

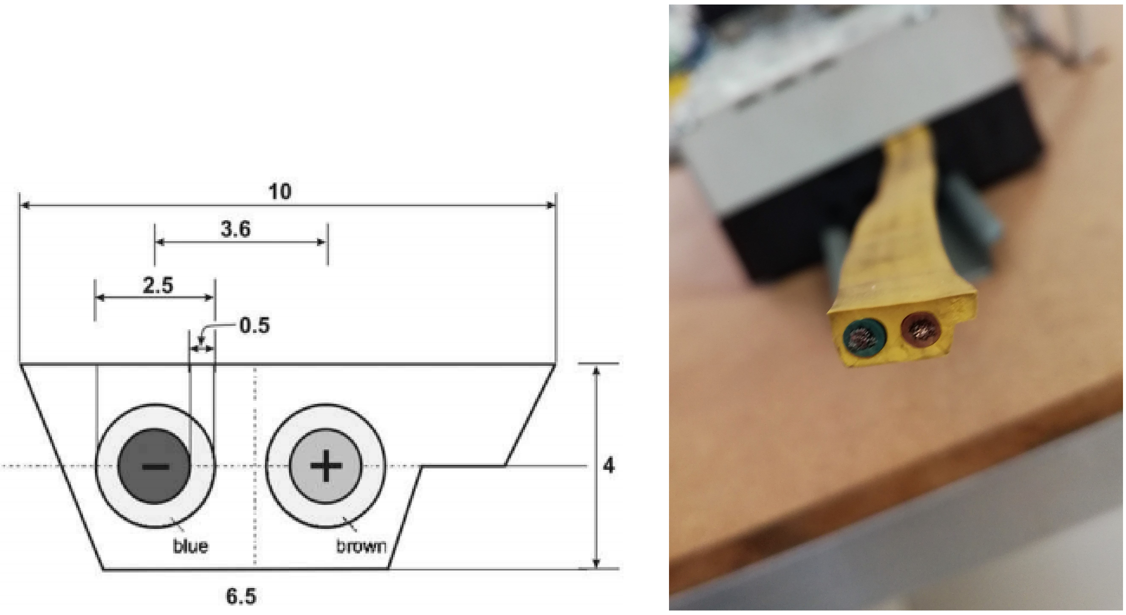
The main advantages of the AS-i are the following [14]:

- elimination of cables between sensors/actuators and the associated controls;
- saves on I/O modules;
- it is electrically and mechanically defined, therefore it is not supplier specific;
- simple quick installation;
- automatic connection prevents polarity reversal;
- high ingress protection (International Protection IP67), locally installed;
- high degree of control security via automatic monitoring;
- compact AS-i chip. Direct installation of sensors/actuators provides new functions such as self-control and parametrization.

2.2.1 Physical layer

Two-wire untwisted and unshielded cable is used by AS-i protocol. This cable aims to provide power for the slaves as well as it serves as the communication link. The slaves have a maximum limit number which depends on the type of AS-i [14].

- Standard interface (AS-i V2): max. 31 slaves with max. 4 input and 4 output each. Response time approximately 5 ms.
- Extended interface (AS-i V2.1): max 62 slaves with max. 8 input and 8 output each. Response time approximately 40 ms.



(a) *Cross-section of the AS-i cable (mm).*

(b) *AS-i cable in the lab.*

Figure 2.5: AS-i cable

A single master device can be used to control the communication. Several topologies can be implemented: line, tree and star are the main ones.

30 VDC power supply allows each slave to provide a maximum of 65 mA [14]. If there are devices which require more than this current value, separate supplies must be linked to the specific slave.

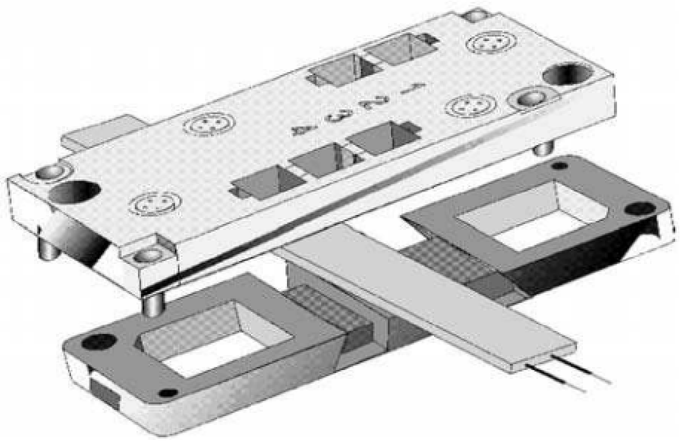


Figure 2.6: Connection of the I/O module with the cable [14]

Since the allowed length of the network is maximum 100 m, 2 Ampere has been determined as the upper limit for preventing excessive voltage drop over this length [8]. In Figure 2.6 is shown the particular design of the slaves: the bus is directly linked inside the field module for increasing safety and maintaining network integrity.

A transfer rate of 167 kbps is achievable by an AS-i network [8]. The access procedure used is cyclic polling which ensures significantly rapid update times. The monitoring cycle contains a slave request, a parameter request and a diagnostic request (see Figure 2.7). A complete cycle requires a total time of maximum 5 ms for V2 AS-i [14].

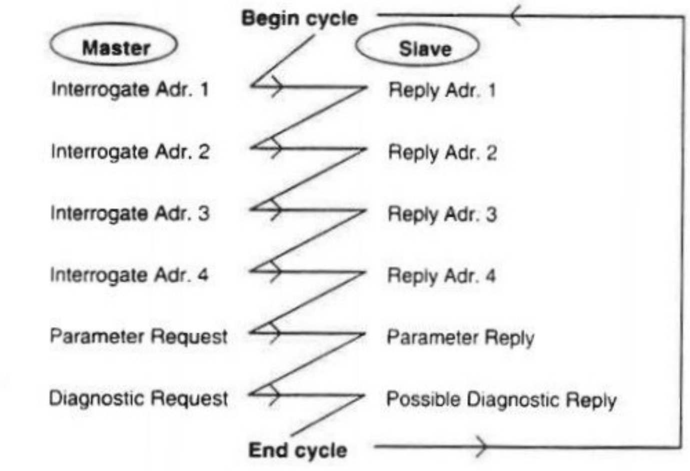


Figure 2.7: Example of communication flow with addresses 1-4 available

2.2.2 Data-link layer

The data-link layer consists in a call-up of the master (14 bits in length) and a slave response (7 bits) [8]. Synchronization is carried out pausing each transmission.

The modulation technique used by AS-i is known as the Alternating Pulse Modulation (APM). Referring to the following figure, the coding of the information is similar to Manchester II coding but utilizing a "sine-squared" waveform for each pulse (see Figure 2.8). This waveform has several unique electrical properties which can reduce the bandwidth required of the transmission medium (faster transfer rates) and reduce the end of line reflections common in networks using square wave pulse techniques [8]. Also, notice that each bit has an associated pulse during the second half of the bit period. All the AS-i modules use this property to detect errors.

In addition, AS-i developers also established a set of rules for the APM coded signal that is used to further enhance data integrity.

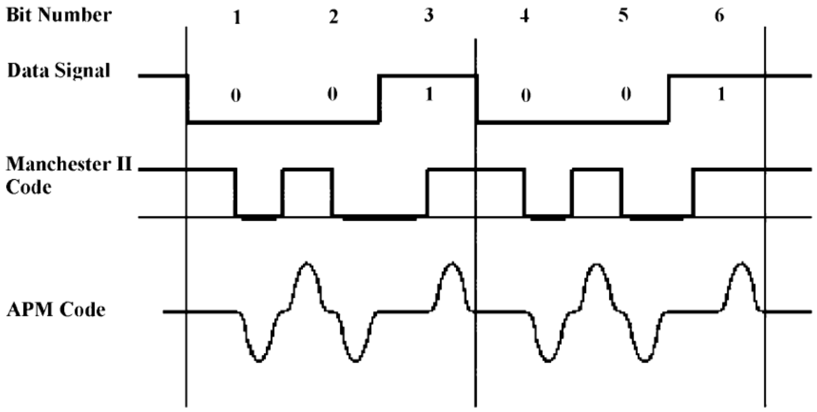
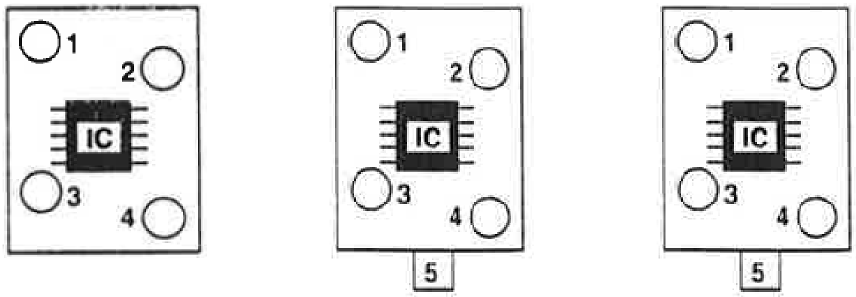


Figure 2.8: Sine-squared wave form of the APM code

2.2.3 AS-i modules

The field module has been already shown in Figure 2.6; it is constituted of two sections which are fastened together once the cable has been collocated inside. When the device is closed, appropriate contact points penetrate the self-sealing cable thus providing access to the I/O interfaces and network propagation.

The modules link existing actuators or sensors with the AS-i system, via AS-i cable, and they are protected to IP67.



(a) 3RG9001-0AA00

(b) 3RG9001-0AB00

(c) 3RG9001-0AC00

Figure 2.9: Sketches of AS-i modules

Figure 2.9 shows a schematic representation of the three AS-i modules that are available in the laboratory n. 201.

4-way input module (3RG9001-0AA00) - Up to four standard sensors can be connected using the 4-way input module. These can be pushbuttons, proximity sensors, position switches or many others. The connection is made via M12 plugs.

4-way output module (3RG9001-0AB00) - Up to four standard actuators can be connected using the 4-way output module. The module contains relay contacts (24V 1A). The power for the auxiliary supplies must be carried out by means of the external M12 socket (socket 5 in the figure, maximum 2A). Only the internal electronics (chip, LEDs) are supplied via the AS-i cable, the actuator is not supplied. The connection is made via M12 plugs.

2I/2O module (3RG9001-0AC00) - Up to two sensors and two actuators can be connected using the 2I/2O device. The connection for this module is the same as for the 4-way input module and the 4-way output module. The sensors are supplied via the AS-i cable, the supply for the actuators comes from an external source. The connection is made via M12 plugs.

The slave electronics are incorporated within the module, with the four available data bits being outputted via standard M12 connectors. Depending on the configuration, up to four binary devices can be connected to each module.

The supply of the modules and the linked sensors takes place via the AS-i cable (maximum 100 mA per module). The AS-i output modules have inside relay contacts that open/close the energy flow for the actuators (24 VDC 1A - maximum 2A per module). The supply of the power to the actuators is made externally by means of M12 plugs [14].

The AS-i network unit has six connections (screw terminals). The connection cover should always be replaced by the distribution unit to ensure the symmetry of the AS-i cable.

Table 2.3: Technical data of the user modules [14]

	3RG9001-0AA00	**3RG9001-0AB00**	**3RG9001-0AC00**
Entry 1	Input	Output (relay)	Input
Entry 2	Input	Output (relay)	Input
Entry 3	Input	Output (relay)	Output (relay)
Entry 4	Input	Output (relay)	Output (relay)
Plug 5	n.a.	Auxiliary supply	Auxiliary supply
Module rated voltage	26.5V ... 31.6V	26.5V ... 31.6V	26.5V ... 31.6V
Total current consumption	$\leq$ 120mA	$\leq$ 60mA	$\leq$ 120mA
Bus voltage led	green	green	green
Inputs led	yellow	n.a.	yellow
Outputs led	n.a.	yellow	yellow
Input switching level-high	$\geq$ 10V	n.a.	$\geq$ 10V
Input current low/high	$\leq$ 1.5mA / $\geq$ 5mA	n.a.	$\leq$ 1.5mA / $\geq$ 5mA
Sensor rated voltage	20V ... 30V	n.a.	20V ... 30V
Total current of all sensors	100mA (short-circuit proof)	n.a.	100mA (short-circuit proof)
Relays rated current DC12	n.a.	1A (max. 2A/module)	1A (max. 2A/module)
Elec. life	n.a.	2 million	2 million
Auxiliary supply 24V DC	n.a.	via Plug 5	via Plug 5

The auxiliary power for the electronics and sensors together with the data is transmitted by means of the AS-i cable. This special form of transfer requires a specific network to couple up the power. The laboratory is equipped with a network unit which supplies 30 Volts and 2.4 Ampere of power to the slaves via the AS-i cable. It is shown in Figure 2.10.

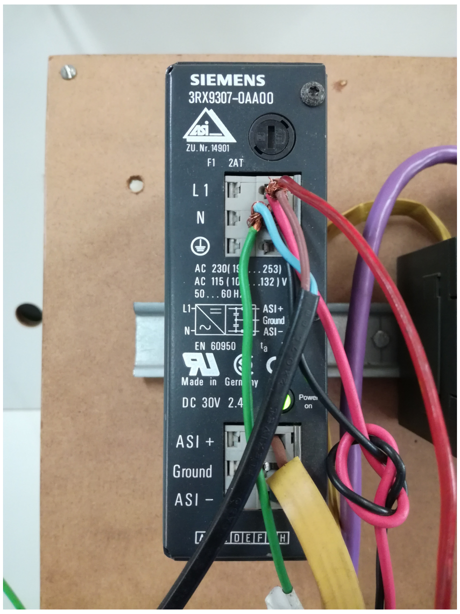


Figure 2.10: Supply unit 3RX9307-0AA00 which is available in the laboratory n. 201

2.3 PROcess FIeld BUS: PROFIBUS

Moving to the upper hierarchical level, a real-time communication is required between the sensor-actuator field and the control system level of the automation pyramid. This type of data transmission is cyclic but there are tasks such as stations diagnosis, devices configuration, and additional interrupts that need to be acyclically executed. A universal solution is represented by the PROFIBUS protocol which is suitable both for discrete and continuous automation.

PROcess FIeld BUS is an open and vendor-independent network standard which is based on the OSI model. It is normally used for controlling processes and it supports single-cable wiring, ensuring the communication between devices of different brands [8].

The first PROFIBUS standard has been developed in 1999. Updates of IEC 61158 continued until 2002. Due to these updates, both PROFIBUS and PROFInet have been included in these regulations. The profiles for PROFIBUS implementation are summarized under the designation “Family 3” (see Table 2.4) [11].

Table 2.4: The third Communication Profile Family

Profile set	Data link	Implementation
Profile 3/1	IEC 61158 subsets; asynchronous transmission	PROFIBUS
Profile 3/2	IEC 61158 subsets; synchronous transmission	PROFIBUS
Profile 3/3	ISO/IEC 8802-3; TCP/UDP/IP/Ethernet	PROFInet

PROFIBUS uses nine-pin D-type connectors (with the possibility to have or not impedance terminated) or 12 mm quick disconnectable connectors [11]. 125 is the maximum number of nodes allowed, while it can support a distance up to 90 km (using repeaters and/or fiber-optic transmission), with speeds varying from 9.6 kbps to 12 Mbps.

For what concerns the message size, maximum 244 bytes of data per node per message can be transmitted. Polling and token passing are the medium access control mechanisms [11].

The first PROFIBUS communication protocol was Fieldbus Message Specification (FMS), then substituted by DP (master/slave) and PROFIBUS PA (intrinsically safe) which are the main forms in which PROFIBUS is available nowadays.

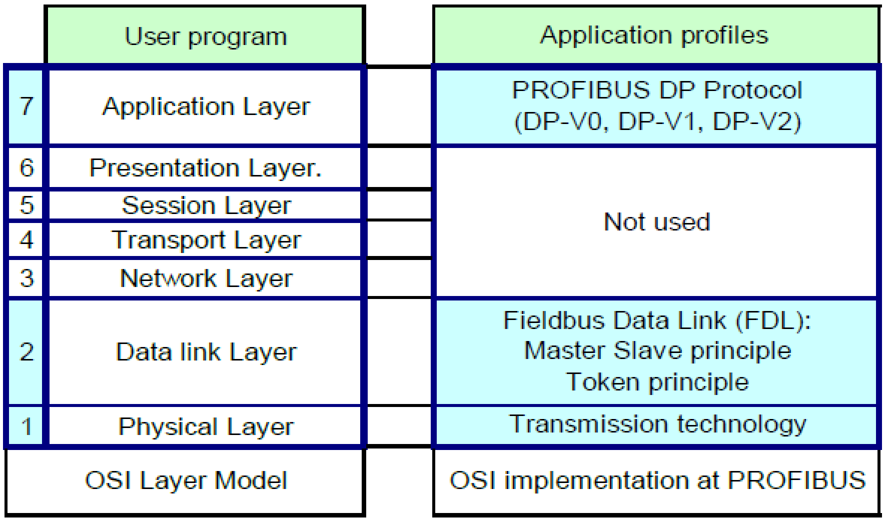
PROFIBUS DP - Distributed Peripheral PROFIBUS permits the use of several master devices within a unique network. In this case, each slave will be assigned to one master. This means that various masters can access the device in reading but only one master is allowed to write to that device. The main task of the PROFIBUS DP is to fast exchange data at the field level. Using this protocol, the bus master is able to communicate with its slaves in a deterministic, simple and fast way. The original version (DP-V0) included only cyclic data transmission; the acyclic information exchange has been implemented with the DP-V1 version. In addition, slave-to-slave communication using an isochronous bus cycle has been provided by a later version, called DP-V2 [11].

PROFIBUS PA - Voltage and current values are reduced in order to satisfy the safety conditions of the process industry. Except for this aspect, the Process Automation PROFIBUS is identical to the PROFIBUS DP-V1 [8].

2.3.1 PROFIBUS protocol layers

The layers of both PROFIBUS variations are summarized in Figure 2.11.

All PROFIBUS variations use the same Data-Link layer. Differently, as the Physical layer, the DP version uses an implementation called RS-485, while PA uses a variation called MBP, in order to satisfy safety requirements [8].



	User program	Application profiles
7	Application Layer	PROFIBUS DP Protocol (DP-V0, DP-V1, DP-V2)
6	Presentation Layer.	Not used
5	Session Layer	
4	Transport Layer	
3	Network Layer	
2	Data link Layer	Fieldbus Data Link (FDL): Master Slave principle Token principle
1	Physical Layer	Transmission technology
	OSI Layer Model	OSI implementation at PROFIBUS

Figure 2.11: PROFIBUS layers [11]

It can be noticed in Figure 2.11 that another layer has been added respect to the normal subdivision and it is named "User program". This level doesn't belong to the OSI Model but it is very important. In fact, here are defined all the application profiles available using PROFIBUS (see Figure 2.12). As written in the Siemens white paper which regards the PROFIBUS, the application profiles are the "specifications defined by manufacturers and users regarding specific properties, performance features and behaviour of devices and systems" [11]. Hence, the profile specifications define characteristics and behaviours of devices and systems which belong to that specific profile family.

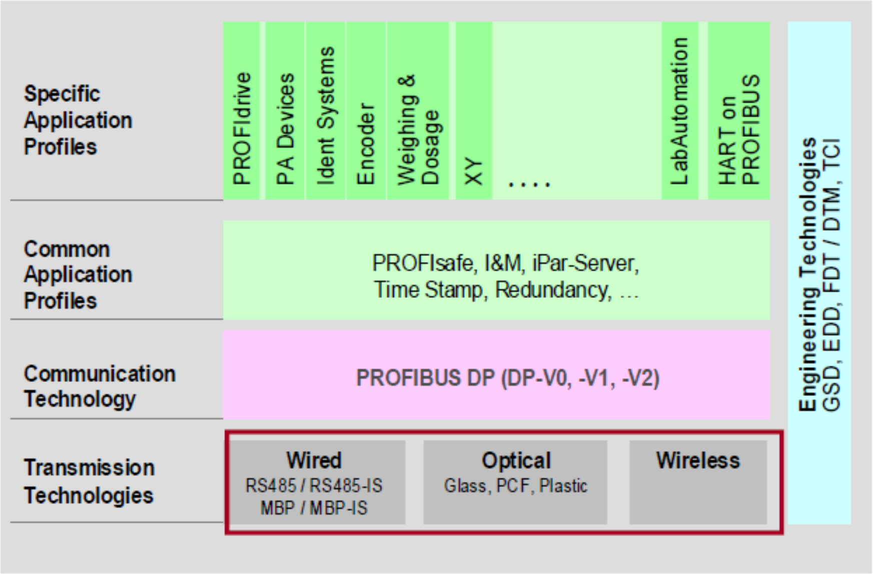


Figure 2.12: Technical system structure PROFIBUS

The profile definition can range from just some details for a particular instrumentation class until an extensive designation regarding specific applications. As Figure 2.12 shows, the general application profiles and the specific application profiles are different. The first ones are developed for several general applications (e.g. PROFIsafe) while the seconds are more specific, as the name suggests (e.g. PROFIdrive). In particular, system and master profiles are ones of the most definite since they describe the performance of a specific system which is built with some particular field devices [11]. A wide range of application profiles is available using PROFIBUS, thus to allow an application-oriented implementation of devices.

In the following, the PROFIBUS three layers will be shortly described.

Physical layer

To connect nodes to the bus line, bus connectors are used. The bus connector RS-485 (degree of protection IP20) for electrical power systems is available in various designs with the cable outlet at various angles.

The transmission methods used during the work is based on RS-485 standard with copper cables and fiber optic. For a detailed discussion about these technologies, one can refer to the Subsection 2.3.2, which deals with the most important transmission methods available in PROFIBUS.

Data link layer - FDL

Medium Access Control and Logical Link Control are the functions that the Data-Link layer implements in the PROFIBUS protocol. The Bus Access, or Data-Link layer, determines when a station may transmit on the bus. PROFIBUS supports two mechanisms: token passing and polling (as explained in Subsection 1.5.6). PROFIBUS can be configured using the two mechanisms separated or as a hybrid system which includes both [8].

PROFIBUS layer 2 transmits frames without prior checking if the receiving device is able or willing to get them. In most cases, the destination of the frames is a specific device (“unicast” frames), but broadcast and multicast communications are also possible [8].

Broadcast communication - An unconfirmed message is sent from an active device to all the other stations (masters and slaves).

Multicast communication - An unconfirmed message is sent from an active device to a group of stations (masters or slaves).

Data-link layer provides data transmission services to layer 7. All services are accessed by layer 7 in software through so-called service access points or SAPs.

Application layer

The interface to the application software is represented by the Application layer. Through this layer, the user can set various applications for performing cyclic and/or acyclic data exchange. These services make an efficient and open (as well as vendor independent) data transfer possible between the application programs and data-link layer.

2.3.2 Transmission technologies

It has been already said that this layer defines the method which regards the physical data transmission both from an electrical and/or mechanical point of view. This includes also the standard used for the transmission.

However, PROFIBUS physical layer is not uniquely defined and it can present several transmission technologies. Both IEC 61158 and IEC 61784 assign these technologies to PROFIBUS, regulating their use [8].

During the development of the project, it has been possible to use RS-485 standards with copper cables and fiber optic for performing the PROFIBUS DP connections. This hybrid network part was built thanks to the use of two Optical Link Modules (OLMs) that are able to change transmission medium from copper to optical fiber and vice versa. Unfortunately, no material was available in the laboratories for implementing Wireless PROFIBUS. Due to this, only RS-485 standard and fiber optic have been used.

RS-485 - It is a simple and cost-effective solution which is principally used in applications that require high transmission rates [8]. A twisted-pair cable is used as a transmission medium; cable shielding can be omitted depending on the application, as shown in Figure 2.13. A line bus topology is often used for connecting the devices because it permits to add or remove stations without affecting the others which are included in the network. Obviously, network extension is constrained: up to 32 devices can be linked in a bus segment [11]. The terminals of each line have an electrical termination which can be selected in order to avoid the reflection of the signal. In cases where more than 32 stations are installed, the use of repeaters is mandatory.

Table 2.5: Specifications for cable types A and B of RS-485 standard [11]

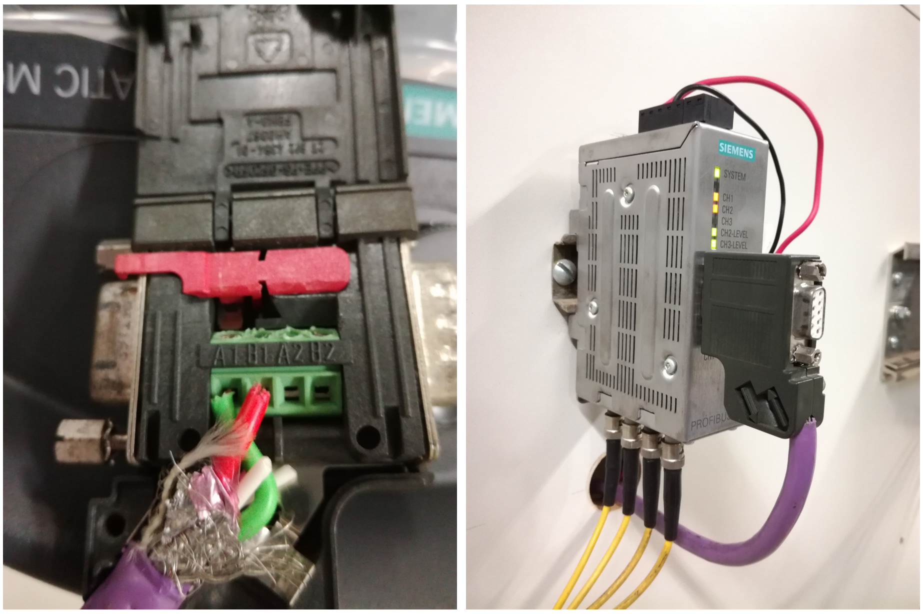
Parameter	**Type A cable**	**Type B cable**
Impedance	135 up to 165 Ω (frequency 3÷20 MHz)	135 up to 165 Ω (frequency >100 kHZ)
Cable capacity	< 30 pF per meter	< 60 pF per meter
Core cross-section	> 0.34 mm^2	> 0.22 mm^2
Loop resistance	< 110 Ω per km	< 110 Ω per km
Signal attenuation	max. 9 dB over total length	max. 9 dB over total length
Shielding	Cu shielding braid	Cu shielding braid

Table 2.6: Type A cable characteristics [11]

Transmission rate [kbit/s]	Range per segment [m]
9.6 - 19.2 - 45 - 93.75	1200 m
187.5	600 m
500	200 m
1500	200 m
3000 - 6000 - 12000	100 m

There are different cable types (designation from A to D) for various applications. When using RS-485 standard, Profibus International recommends the use of type A or B cable (see Table 2.5) mainly because they are shielded and thus immune to high electromagnetic interferences.

Various transmission rates are achievable: from 9.6 kbit/s to 12 Mbit/s. Depending on these values, the line length will have a maximum limit.



(a) *Building of the RS-485 connectors.* **(b)** *Optical Link Module with both RS-485 connector and fiber optic.*

Figure 2.13: RS-485 standard and fiber optic used in the lab

RS-485-IS - [11] It consists of a four-wire medium with a high degree of protection which allows it to be used in very dangerous areas (i.e. explosive). In addition, the current and the voltage levels correspond to the safety-relevant peak evaluations that must be violated neither in a single station nor during interconnection in the system. It is an RS-485 standard which is able to operate in intrinsically safe conditions.

Fiber Optic - In cases where large distances have to be covered and the plant have high electromagnetic interference conditions, it is possible to use fiber optic transmissions for performing the communication. The supported types for PROFIBUS are shown in the Table 2.7.

Table 2.7: Supported optical fiber types [11]

Fiber type	**Core diameter [μm]**	**Range [m]**
Multimode glass fiber	62.5 - 125	2000 - 3000
Singlemode glass fiber	9 - 125	$>$ 15000
Plastic fiber	980 - 1000	up to 100
HCS fiber	200 - 230	approx. 500

In the laboratory n. 201, the optical fiber connection of the PROFIBUS DP has been implemented using electrical/optical transformers (i.e. the Optical Link Module which is shown in Figure 2.13b) that are linked to the devices over an RS-485 interface.

Shortly, the characteristics of these technologies are summed up in the Table 2.8.

Table 2.8: Transmission technologies available for PROFIBUS [11]

	RS-485	**RS-485-IS**	**Fiber Optic**
Data transmission	Voltage differential signals	Voltage differential signals	Optical
Transmission rate	9.6 to 12000 kbit/s	9.6 to 1500 kbit/s	9.6 to 12000 kbit/s
Cable	Shielded, twisted pair copper type A	Shielded, twisted 4-wire type A	Glass fiber, PCF, plastic
Protection type	None	Instrinsic safety	None
Topology	Line with termination	Line with termination	Star, ring, line
Number of stations	Up to 32 per segment, up to 126 with repeaters	Up to 32 per segment, up to 126 with repeaters	Up to 126 per network
Number of repeaters	Max. 9 repeaters	Max. 9 repeaters	Unlimited

2.3.3 Communication protocol DP

Decentralized Periphery PROFIBUS is suitable for connecting controllers, HMIs, distributed field devices, valves, drives, and PCs [16].

It is clear that this communication protocol has been designed to perform high-speed data transmission at the control system level and at the field level, where all the previous technologies can be normally found.

Usually, among these distributed devices the communication is chiefly cyclic.

The DP basic functions specify the communication functions required for cyclic data exchange and they form the first DP version, named DP-V0. These basic functions have been expanded during years in order to better fit with more areas of application. Thus, now, DP is available in three version: DP-V0, DP-V1, DP-V2. In Figure 2.14 are shown the key features of the three versions.

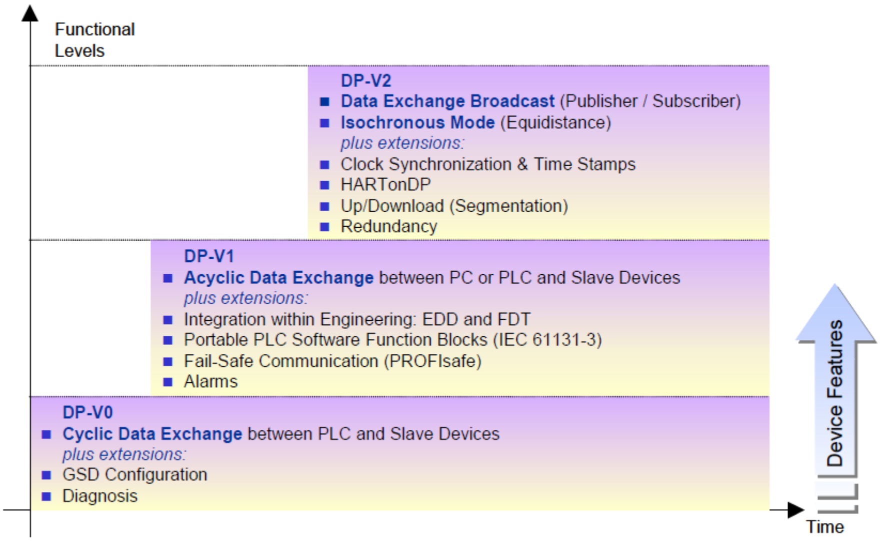

Functional Levels
DP-V2
■ Data Exchange Broadcast (Publisher / Subscriber)
■ Isochronous Mode (Equidistance)
plus extensions:
■ Clock Synchronization & Time Stamps
■ HARTonDP
■ Up/Download (Segmentation)
■ Redundancy
DP-V1
■ Acyclic Data Exchange between PC or PLC and Slave Devices
plus extensions:
■ Integration within Engineering: EDD and FDT
■ Portable PLC Software Function Blocks (IEC 61131-3)
■ Fail-Safe Communication (PROFIsafe)
■ Alarms
DP-V0
■ Cyclic Data Exchange between PLC and Slave Devices
plus extensions:
■ GSD Configuration
■ Diagnosis
Device Features
Time

Figure 2.14: PROFIBUS DP versions with their key functions [11]

Basic functions DP-V0

The first version of PROFIBUS DP provides the basic functionalities which include cyclic communication and devices diagnostic. The principal controller (master) cyclically reads and writes the information which is coming from the slaves.

The cycle time of the program must be longer than the bus cycle time otherwise the network could lose the information since the status of the devices could vary within a cycle. However, the use of a transmission technology which is interference-proof, a proper diagnosis capability, and the ease to handle are all important characteristics of a bus system which must be taken into account for a good implementation [11]. The DP protocol gives an excellent combination of these features.

For what concerns the transmission speed, DP only takes approximately 1 ms at 12 Mbit/s to transfer 512 bits of inputs and 512 bits of output data distributed over 32 stations [11]. In Figure 2.15 are shown the typical transmission times of PROFIBUS DP depending on the slave station numbers located in the network and the transmission rate.

A unique message cycle is necessary for DP protocol to manage both input and output information. The data are transmitted using the “Send and Receive Data Service” (SRD) of the Data-Link layer.

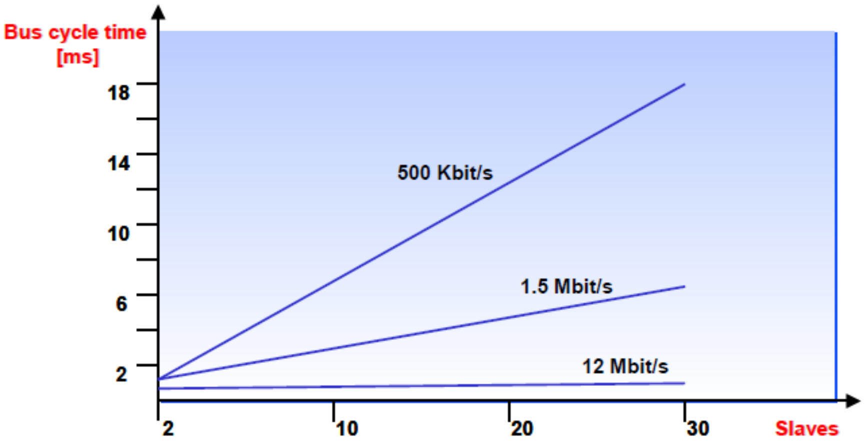


Figure 2.15: Bus cycle time of a DP mono-master system

As already said in Subsection 1.5, one of the great advantages of using a new automation network is the real-time diagnostic function. PROFIBUS DP diagnosis functions make possible to fast discover faults. The diagnostic messages are sent through the bus line and received by the master. Three levels of messages are present [11].

1. Device-specific diagnosis. They are messages on the general behaviour of stations, such as "Overheating", "Undervoltage" etc.

2. Module-related diagnosis. They are messages which indicate a pending diagnosis in a specific I/O subdomain.

3. Channel-related diagnosis. They are messages which regard faults that are related to a single channel (I/O bit), such as "Short-circuit at output".

In general, a system which is based on a PROFIBUS DP network is assembled with three distinct device types [11].

DP Master Class 1 - This class represents the principal controller which aims to cyclically transmit data to its slaves. Transmission happens at an exact message cycle. Normally, DPM1 devices are PLCs or PCs and they always have an active bus access.

DP Master Class 2 - These devices are operating stations. The configuration set up, commissioning, maintenance and diagnosis are the main operations that they carry out. Usually, a DPM2 station doesn't need to be always linked to the bus system.

Slaves - They are peripheral and passive devices that receive information coming from the process and/or uses output data coming from the DPM1 device to act in the process. It can be an I/O device, a drive, an HMI, a valve as well as a transducer.

Another basic feature that makes PROFIBUS DP more used is the fact that it supports both mono-master and multi-master implementations. In this way, the DP protocol provides a high degree of flexibility to the system configuration.

- Mono-master system. As the name suggests, a single master is functioning on the network. Generally, the cycle time of a bus in this configuration has the shortest value achievable.
- Multi-master system. In this case, various masters are linked to one bus. Using this configuration, all the DP masters can read information coming from the slaves but only the DPM1 assigned to those specific slaves can write/access the outputs.

As already mentioned above, data communication between DPM1 and its slaves occurs in a well defined and recurring sequence. Essentially, parametrization, configuration and data transfer are the three phases in which the sequence is divided. [11].

DPM1 autonomously managed the device-related user information exchange; in addition to this, all the slaves can receive the commands that are coming from the master (which sent them as multicast commands). These signals are very useful since they permit to change the slaves status for an event-controlled synchronization of devices.

Moreover, to detect communication failures, controls are used and the time interval for monitoring is defined during the configuration of the devices. DPM1 uses a time monitor to detect communication errors. Differently, the slaves have a watchdog control for detecting errors in communication [11].

In the end, it is important to highlight the system behaviour. This PROFIBUS DP version has been standardized and it is mainly defined by the functioning status of DPM1. The principal advantage which comes from the standardization is that it guarantees a good flexibility among stations of the same type, allowing devices interchangeability. The operating conditions of a DPM1 device are three: “stop”, “clear” and “run”.

In “stop” condition there is no data communication between master and slaves. During the “clear” status the DPM1 receives and reads the information which comes from the slaves and it maintains the output of its slaves in a fail-safe state (“0” state). In “run” situation the DPM1 is in data transfer phase. The system reaction to a fault which occurs during the operating modes is defined by the auto-clear configuration parameter [11].

Version DP-V1

Extended function for the acyclic data communication is the principal feature which characterizes the version DP-V1. Essentially, cyclic and acyclic data transmission are carried out at the same time but the latter has a lower priority.

A system with a master, an operating station and N slaves can be taken as an example. Initially, the token belongs to the DPM1 device which performs the cyclic data transmission until the list of slaves doesn’t finish. Then, the token passes to the DPM2 which can use the residual available time (called “gap”) of the configured cycle to establish an acyclic transference of information to any slave. Once the current cycle time expired, the token is sent back to the DPM1.

Thus, DP-V1 permits a station-specific diagnosis that was not performable with the precedent version. Alarms and status messages are the two categories in which this acyclic diagnosis is divided (see Figure 2.16).

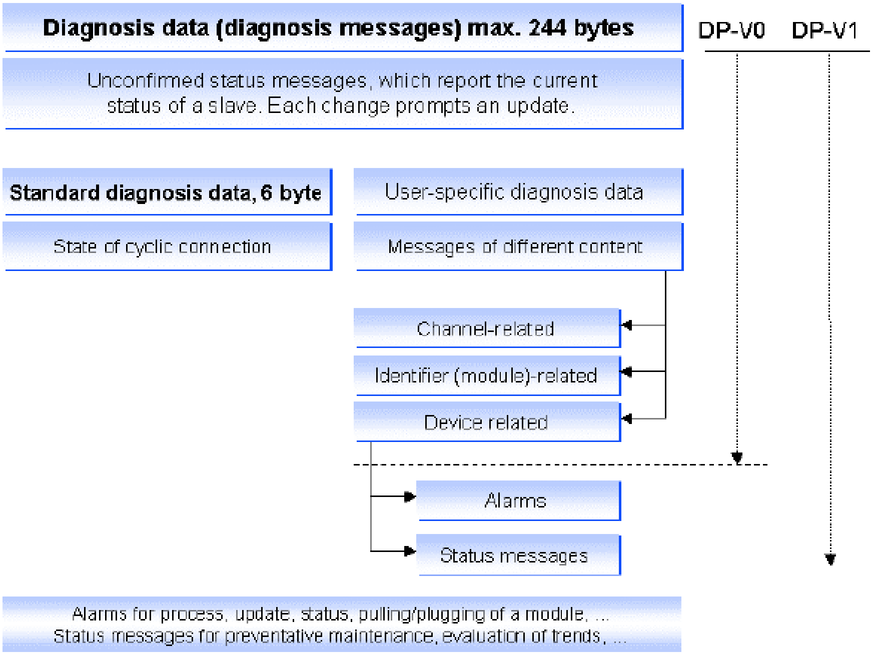

Diagnosis data (diagnosis messages) max. 244 bytes
DP-V0
DP-V1
Unconfirmed status messages, which report the current status of a slave. Each change prompts an update.
Standard diagnosis data, 6 byte
User-specific diagnosis data
State of cyclic connection
Messages of different content
Channel-related
Identifier (module)-related
Device related
Alarms
Status messages
Alarms for process, update, status, pulling/plugging of a module, ...
Status messages for preventative maintenance, evaluation of trends, ...

Figure 2.16: Acyclic diagnosis data in DP-V0 and DP-V1 [11]

Many other functions are implemented by the PROFIBUS DP-V1. They are listed in Figure 2.14.

Version DP-V2

DP-V2 version introduces to various innovative functions, shortly described below.

Slave-to-Slave communication (DXB) - [11] Using broadcast communication without deviations through master devices, this function allows direct and time-saving data transmission between slaves. This is a huge advantage which opens up to totally new applications and, moreover, decreases the response times in the network up to 90%.

Isochronous mode - [11] The isochronous function sets up a control which is based on a synchronous clock for masters and slaves. This clock is regardless of the amount of data which are circulating on the bus. In this way, all the devices linked to the bus have a synchronized time cycle with respect to the bus master time cycle. This synchronization is possible thanks to a “global control” broadcast message.

Clock control - [11] This function synchronizes to a common system time all the devices which are involved on the bus. Less than a millisecond is the difference guaranteed by this function. This permits an accurate monitoring of events, diagnosis of faults and chronological scheming of occurrences.

Upload and download - [11] With version DP-V2, few commands are necessary to load any amount of data in a field station.

2.3.4 Device integration: GSD

As it has been already stated, one of the main advantages brought by the network protocols is the openness. This is valid also for PROFIBUS which is a protocol compatible with a large number of devices produced by different manufacturers. Integration between stations is achievable since their functionalities are described in specific file formats which can be read by the operator software. Figure 2.17 shows a shortened portrayal of the device integration.

During the development of the project, not all the devices were initially present in the TIA Portal database. In order to add some stations to the system, GSD files have been used. Hence, only this technology will be briefly analyzed in the following.

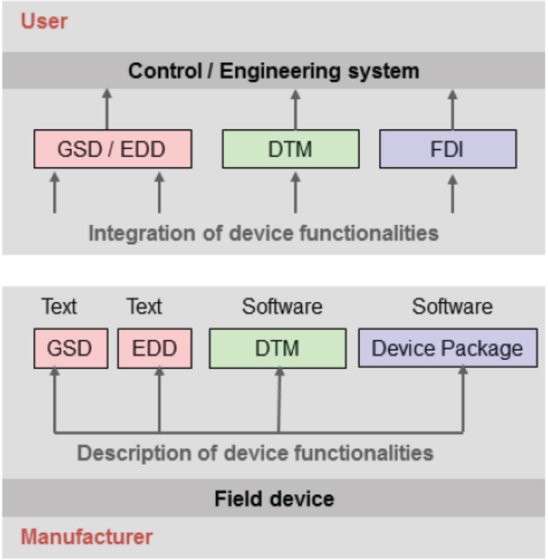

User
Control / Engineering system
GSD / EDD
DTM
FDI
Integration of device functionalities
Text
Text
Software
Software
GSD
EDD
DTM
Device Package
Description of device functionalities
Field device
Manufacturer

Figure 2.17: Technologies for device integration [11]

The General Station Description (GSD) file is an electronic data sheet which completely describes all the properties and functionalities of a certain PROFIBUS station. All the information that are necessary for cyclic data exchange, for the configuration of the PROFIBUS network, and for many other functions, are included in these files as a text-based description. Thus, the GSD file is a complete data sheet that comprehends all the device key data: information about its connection capabilities, diagnostic values, etc.

This technology is very well integrated with the TIA Portal software. Once added the GSD file in the TIA Project, it is possible to immediately start the configuration of the new station. On the other hand, application-specific functions, as well as some parameters of complex devices, are not properly described in this type of file alone. Electronic

Description Language (EDDL), for example, is a more powerful language which allows the configuration, diagnosis and support of complex stations.

2.4 Industrial Ethernet: PROFInet

Programmable Logic Controllers and PCs that are used in the control system level of the automation pyramid have to exchange large data packets with each other as well as with the devices located in the upper levels. To do this, Ethernet, TCP/IP, and Intranet standards are commonly adopted, since this type of communication needs a series of specific functions as well as the possibility to exchange a considerable amount of data.

Ethernet is born in the 1970s. It was based on a bus structure and it was used as a communication medium for transmitting information with the same authorization between various stations in a local area. The term "Ethernet" refers to both the hardware transmission medium (i.e. connectors, cables, etc.) and the data transmission (i.e. protocols, transference forms, etc.). Ethernet is a defined application of first and second layers of the OSI Model and it is implemented with different protocols on higher levels.

In order to make Ethernet suitable for the industry, industrial Ethernet has been designed. Principally, the following features characterize it [19].

- Networking of different application areas, from production field to offices.
- Robust design and electromagnetic interference immunity.
- High transmission performance even with a great number of nodes.
- Different transmission media (from copper cables to fiber optic as well as wireless).
- Scalable performance with switching technology.
- Possibility to implement redundant network topologies.
- Presence of several protocols which satisfy the necessities of the industry (e.g. real-time capability).

Based on the Industrial Ethernet transmission characteristics (both hardware and software), PROFInet is the open standard which has been designed and developed by the PROFIBUS&PROFInet International (PI). IEC 61158 and IEC 61784 provided the standardization as CPF 3/3 (see Table 2.4).

Found on an integrated and Ethernet-based communication, PROFInet conforms to a large range of requirements. In fact, it provides really fast I/O data transmission thus to allow automation in real-time. Moreover, it gives a transparent interface to the Information Technology level. In the following, the principal benefits are listed [13].

Flexible network topology - According to IEEE 802.3, PROFInet is perfectly Ethernet compatible and it can be configured for implementing different network topologies. In addition, it supports several physical media: copper cables, fiber-optic and wireless solutions.

Scalable real time - A single cable is used for the communication, both in simple or highly demanding applications. Moreover, for high-precision feedback control operations in processes which required time-critical data, an isochronous and deterministic transmission with a jitter less than one microsecond is achievable.

High availability - The network and the stations which are involved in the communication can be diagnosed automatically by the acyclic diagnostic function. Important information which regard, for example, the real-time functioning of the devices and the analysis of the topology of the network, are collected by PROFInet thanks to a combination of automatically reacting redundancy concepts and intelligent diagnostic solutions.

Safety integrated - PROFIsafe is a specific profile of PROFInet that guarantees functional safety of the applications.

2.4.1 Communication relations

For what concerns the type of communication relationship between nodes (see subsection 1.5.5), PROFInet IO, which is the communication service adopted in the laboratory (see subsection 2.4.2), implements the provider/consumer model. With respect to PROFIBUS, different device classes are adopted here.

- IO-Controller. This class is very similar to the 'DP master class 1' of PROFIBUS. Typically, it includes the Programmable Logic Controller (PLC) or, in a general sense, all those devices that provide output data for the involved IO-devices and receive input data from them.

- IO-Device. All the distributed I/O field devices belong to this class. Thus, an IO-Device is usually connected to IO-Controllers via PROFInet IO. This class is similar to the 'slave' class of PROFIBUS.

- IO-Supervisor. A supervisory device can be a PC or an HMI with the main purpose of diagnosing and commissioning devices. It is comparable to the 'DPM2' class.

Hence, generally speaking, all the field devices are modelized and standardized according to their technical and functional characteristics. The role of the access point which aims to establish the exchange of information between the PROFInet IO interface and the software program is played by the Device Access Point (DAP). It describes the structure of the IO-Device model, which is typically standardized as follows.

- The location in which an I/O card is placed in an I/O field device is defined by the 'slot' number.

- Within a slot, the interfaces which are active in the communication with the process are represented by the 'sub-slots'. The status information are always included in the data transmission of a sub-slot.

- The data index defines the type of information inside a sub-slot. The index is not used for cyclic I/O data because only a combination of slot/sub-slot is required in this case. Differently, for acyclic communication, read and write services use also the index information for addressing data in the right way.

Again as in PROFIBUS, the GSD files can be used for having a complete device description.

During the system startup, the transmission circuit is set up by the IO-Controller in order to establish the communication with its IO-Devices. The information which regards the transaction is included in an Application Relation (AR). Inside the AR, several Communication Relations (CR) precisely defines the information in order to transmit the configuration, the user data, and the alarm messages (see Figure 2.18). An IO-Controller is able to set up one AR each with different IO-Devices.

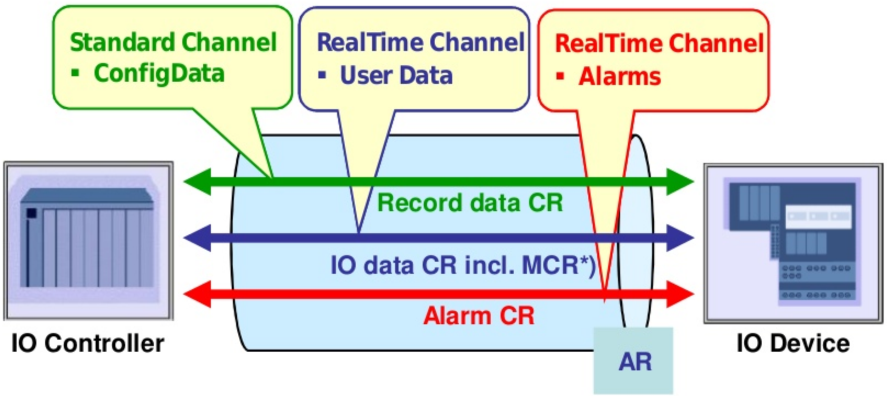


Figure 2.18: Application relations and communication relations

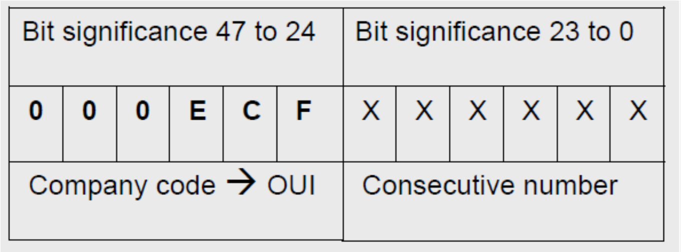
A last consideration is that in PROFInet IO each device (field device, controller and supervisor) has a particular name that uniquely classifies it inside the system. The IP and MAC addresses are associated with this name which must be unique and different respect to all the PROFInet IO names of the devices that are involved. For this purpose, DCP (Dynamic Configuration Protocol) is integrated into every device.

The IP address is designated with DCP basing on the device name. This address is fundamental for accessing the device and for changing the configuration or the functioning status. An automatic assignation of the name using neighbourhood detection is also achievable.

For direct data transmission, a PROFInet IO-Device is addressed by its MAC address which is unique worldwide. As shown in Figure 2.19, MAC address is composed of a company code and a consecutive number.

- Company code. Also called Organizationally Unique Identifier (OIU), it is included between the 47th and the 24th bits and it is given directly from the IEEE Standards Department. Profibus & Profinet organization has a fixed OUI: 00-0E-CF.

- Consecutive number. From the 23rd bit to the least significant bit, it is the manufacturer-specific portion of the MAC address.



Bit significance 47 to 24						Bit significance 23 to 0					
0	**0**	**0**	**E**	**C**	**F**	X	X	X	X	X	X
Company code → OUI						Consecutive number					

Figure 2.19: MAC address structure

2.4.2 Perspective and Conformance Classes

PROFInet supports two communication services which are called PROFInet IO and PROFInet CBA, as well as many profiles similar to the PROFIBUS profiles (e.g. PROFIsafe and PROFIdrive). PROFInet IO and CBA services guarantee the required functions for automation systems.

- PROFInet IO (Input/Output) is a transmission service which is used for direct connecting distributed field devices (IO-Devices). It adopts Industrial Ethernet hardware and software and it can be used in real-time (RT) applications for real-time communication as well as isochronous real-time (IRT) data transmission for cyclic process data.
- PROFInet CBA (Component Based Automation) is useful for implementing a machine-machine data exchange via TCP/IP technology, as well as for transferring data in real time. It is used in those network parts where time is not critical, for example in the conversion from PROFInet into PROFIBUS DP.

Most of the times, PROFInet CBA is integrated into the PROFInet IO networks for implementing a machine-machine communication. Both services can work together or separately in the same system.

In both laboratories, only PROFInet IO has been used. Thus, in the following, PROFInet IO will be take in particular consideration.

PROFInet IO consists of several functions whose field of application is divided into Conformance Classes (‘CC’). The different properties are practically summarized by three classes (CC-A, CC-B, CC-C) which are adapted to standard applications.

Basic functions - Conformance Class A

The Conformance Class A provides the fundamental functions for the PROFInet IO with real-time communication. Essentially, the main functionalities are three and they are described below as well as in Table 2.9.

Cyclic data exchange - The cyclic I/O data transmission between provider and consumer takes place over a configurable time base; the information is sent as real-time data. In addition, the cycle time in which the transmission occurs can be defined individually for each connection of the single stations. Hence, the system can accommodate the conditions of the application and, at the same time, it is very flexible thanks to several configuration possibilities of the cycle time which ranges from 250 μs and 512 ms [12]. Data are sent with much other information which provide reports about the data's validity, redundancy and diagnostic status. The supervision of the connection occurs in pre-defined cycle times (monitoring times) which are typically multiple of the basic cycle time. The consumer sends a message of error to the provider if the information doesn't arrive within the monitoring time.

Acyclic parameter data - Selection of parameters, configuration of I/O devices, read out of the status information, performance of the Identification and Maintenance function, and many more actions are performed with the acyclic data exchange.

Device/Network diagnostics - Devices and components are able to identify and divulge their status adopting certain mechanisms. This concept includes both system-defined events (e.g. adding or removing devices) and signals of faults that are detected by the controller technology (e.g. wire break).

The diagnostic alarms are automatically identified by the I/O device or its connected components. In addition, it is possible to configure alarms which inform about hazardous process conditions (e.g. silo limit exceeded).

Table 2.9: Technical functions of Conformance Class A [12]

Requirement	Technical function
Cyclic data exchange	PROFInet with real time communication
Acyclic parameter data	Read-Write record / Identification&Maintenance
Device/Network diagnostics	Diagnostics and maintenance

Conformance Class B

This class includes further functions which regard the network diagnostic and the analysis of the topology.

Network management protocol - The protocol used by PROFInet is the Simple Network Management Protocol. Through the SNMP, PROFInet is able to detect the network components and read out the information that regard the network integrity and the neighbourhood detection [12].

Neighbourhood detection - Lower Link Discovery Protocol (LLDP) is the protocol used by PROFInet to detect the exact connection ports of each device. In this way, field devices exchange their IP address information with the linked nearby resident devices. Thus, all the devices are clearly identified and their physical position is determined [12].

Representation of the topology - All data found during neighbourhood detection are stored using SNMP protocol. Then, via TIA Portal, it is possible to display the resultant topology (see Figure 2.20).

Device replacement - If a new device is inserted for replacing a previously faulting station, the network detects it automatically. In addition, if the replaced device is of the same model as the previous one, PROFInet autonomously provides the name and the parameters as those of the precedent station [12].

Integration of diagnostics – A switch device can be configured as PROFInet IO device which is able to show the faults and certain operating status to its controller by sending acyclic alarms using the "alarm CR". In this way, the IO system diagnostic has the network diagnostics which come from the switches integrated into its functions.

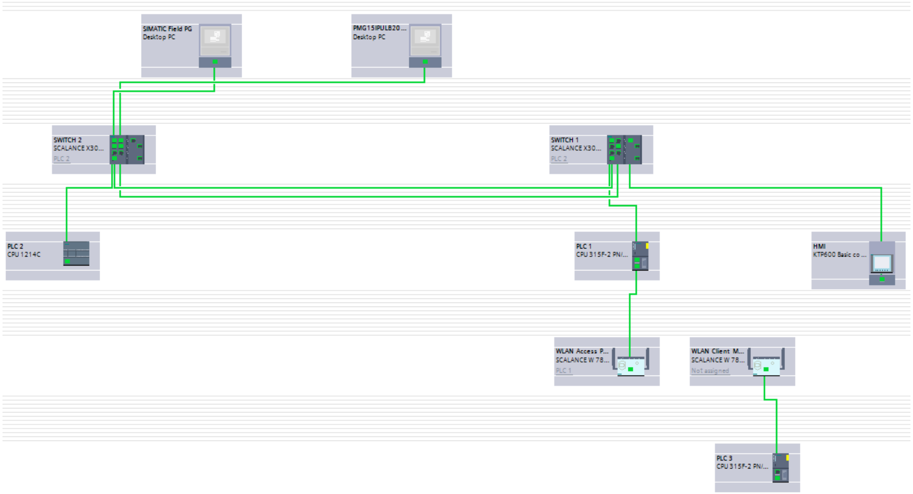


Figure 2.20: Topology view from the TIA Portal V13 SP1

Isochronous real time - Conformance Class C

The main characteristic of this class is the fact that it provides performances with a jitter less than one microsecond [12]. Due to this, the networks that are based on CC-C are suitable for applications that require the most rigorous conditions for deterministic behaviour. Part of the transmission bandwidth is occupied by the synchronized cyclic data packets while all the other packets share the rest of the bandwidth.

Due to the fact that the bus cycle and the cycle time of each device must run synchronously having a deviation of one microsecond maximum, a clock in common is required. Hence, a master clock is used to send synchronization frames. These signals command the clock of each device for generating the pulse at the same time [12]. Within this common clock system, it is mandatory that the devices are directly connected among them without combinations with non-synchronized stations.

This type of communication is called Isochronous Real Time (IRT). The bus cycle is thus divided into several intervals and the data transmission is synchronized. The different intervals are shown in Figure 2.21; data transmission occurs during the real-time phase (red interval in Figure) in which deterministic transfer and protection from delays are ensured. All other data, such as diagnostics information or TCP/IP, are transmitted in the blue interval (TCP/IP phase) according to IEEE 802.

Anyway, a combination of asynchronous and synchronous transmissions is possible within the same system. Of course, certain requirements must be met before.

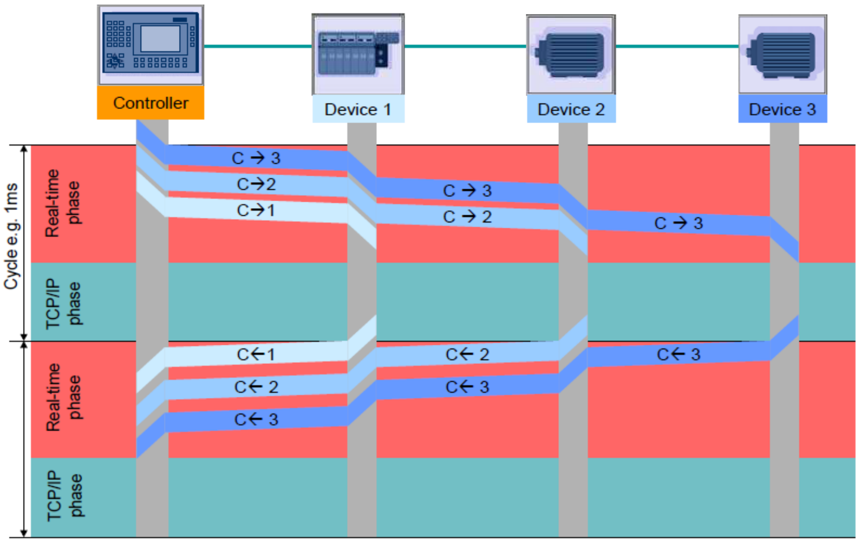


Figure 2.21: Bus cycle division. Reserved interval in red while open interval in blue

Table 2.10: PROFInet IO optional functions [12]

Requirement	Technical function
Multiple access to inputs Functions are distributed to several controllers	Shared input Shared device
Extended device identification Parameter set for automatically assigning the parameter Variations of the configuration during functioning	Identification and Maintenance IM1-4 Individual parameter server Configuration in Run (CiR)
Time stamping of I/O data Fast restart after voltage recovery	Time sync Fast start-up (FSU)
Higher availability through ring redundancy Call of a device-specific engineering tool	MRP/MRPD Tool Calling Interface (TCI)

Optional functions

The Conformance Classes don't provide all the functions that are available. PROFInet furnishes several optional functionalities which are briefly introduced in Table 2.10.

2.4.3 Physical installation

It has been already mentioned that PROFInet is based on 100 Mbps, full-duplex Ethernet network [12]. The communication between devices takes place on copper cables or fiber optic cables as well as using wireless transmission systems. Obviously, a device is not able to perform all those types of communication but at maximum two of them, depending on its technology.

The technology of each apparatus and its capability to support various transmission media is in accordance with the Conformance Class of the network. Due to this and according to the information which are shown in Table 2.11, a PROFInet network only made of wireless connections is not able to provide the particular functions of CC-B and CC-C.

Table 2.11: Available conformance classes for different network applications [12]

Network cabling and components	**Technological solution**	**Conformance Class**
Passive network components (connector, cable)	RJ45/M12 connectors	A, B, C
Copper and fiber optic transmission systems	TX, FX, LX	A, B, C
Wireless connections	WLAN, Bluethoot	A
IT switch	With VLAN tag according to IEEE	A
Switch with device function	PROFInet with RT	B
Switch with device function and bandwidth reservation	PROFInet with IRT	C

All the devices used in the laboratories belong to the SIMATIC family (see Appendix A). The PROFInet network developed is hybrid because copper cables, optical fiber and wireless technology have been adopted. In the following, a short description which regards the implementation of wired and wireless network based on the PROFInet IO protocol can be found.

Wired network

Essentially, as it has been already stated, the choice of using copper cables or fiber-optic cables depends on the required data transmission and the environment. A wired PROFInet network doesn't avoid these considerations.

For what concerns the electrical PROFInet interface of a device, it is commonly used an RJ45 connector as the connection method between the interface and the cable. The latter is, in general, a 2x2 twisted, symmetrical and shielded copper cable which can achieve a transmission rate of 100 Mbps in full duplex mode [12]. However, several types of cable are adopted in the industry and they are normally classified as follow.

- PROFInet type A. Standard forever-routed cable which doesn't permit movement during functioning.
- PROFInet type B. Flexible cable, not habitual movement after installation.
- PROFInet type C. For special applications in which constant movement is required.

For electrical data transmission the maximum segment length allowed with copper cable is 100 m. The main advantages of this technology are that it is cheap and very simple to install.

On the other hand, several solutions are achievable with the optical fiber technology. The main advantage of adopting an optical medium is the fact that it is intrinsically safer than the copper cables. It can be safely used when the network nodes are under a considerable voltage drop or also in cases of extreme electromagnetic compatibility requirements. Moreover, low line attenuation and the possibility to perform considerably longer segments are features that make optical fiber very used in industry.

All the solutions that can be adopted with this technology depend on the cable types. Table 2.12 shows four optical fiber cable types together with their characteristics.

Table 2.12: Technical specifications of PROFInet fiber-optic interface [19]

Connection methods	**Cable type**	**Transmission rate**	**Max. length**
SCRJ 45 ISO 61754-24	Polymer Optical Fiber (POF) 980/1000 μm (core/external diameter) ISO 60793-2	100 Mbps full duplex	50 m
	Polymer Cladded Fiber (PCF) 200/230 μm (core/external diameter) ISO 60793-2	100 Mbps full duplex	100 m
BFOC and SC connectors ISO 60874	Monomode glass fiber optical cable 10/125 μm (core/external diameter) ISO 60793-2	100 Mbps full duplex	26 km
	Monomode glass fiber optical cable 50/125 and 62.5/125 μm (core/external diameter) ISO 9314-4	100 Mbps full duplex	3000 m

For what concerns PROFInet IO active components, the laboratory is equipped with two industrial switches (Scalance X 308-2) which have been used in order to have more PROFInet interfaces available and, in particular, to implement a redundant communication in a key point of the system. A detailed explanation of this network part can be found in the third Chapter.

Essentially, an industrial switch is implemented to link a single network node with many other nodes. In fact, such station is designed with several PROFInet ports and it is able to regenerate and share the incoming signals. A point-to-point communication is the type of connection which is always performed between a node and the switch.

In the laboratory n. 201, two Scalance X 308-2 (Version 3.0.0) switches which are equipped with eight electrical and two optical ports have been used. Using the software TIA, it has been possible to configure these devices and perform a ring redundant communication using optical fiber cables.

Wireless network

Normally, in an industrial Wireless LAN, data transmission ranges from 11 Mbps to 54 Mbps without full-duplex mode [19]. This data rate is intended as gross value in the sense that if the connection condition is not good for maintaining the maximum transmission rate, this value is automatically reduced until a stable communication can be performed. This parameter changes according to the standard version that is adopted ‘a’, ‘b’, ‘g’, ‘h’ or ‘n’ (see Table 1.7).

The laboratory is equipped with wireless devices and antennas that belong to the SIMATIC Scalance W family. In addition to what has been already said about wireless networks, these devices provide several very useful enhancements (so-called ‘ifeatures’) [19].

- Forced roaming activated automatically when connection to industrial Ethernet is interrupted.
- Cheap connection to stations in remote environments.
- Deterministic data traffic with determined response times.
- Usable in the hazardous area of zone 2.
- Wireless link cyclical supervision.
- Configuration and supervision via TIA Portal.

Chapter 3

Overview of laboratory n. 201 from the perspective of the TIA Portal

At this point of the document, it is necessary to introduce the software used for configuring and supervising the system. Hence, TIA Portal V13 SP1, WinCC 2008 Flexible and WinCC V7.3 will be shortly described.

Then, laboratory n. 201 will be explained, especially focusing on the network configuration from the TIA Portal perspective. In addition, a description of the logic connections and the ring topolgies established is present.

3.1 TIA Portal V13 SP1

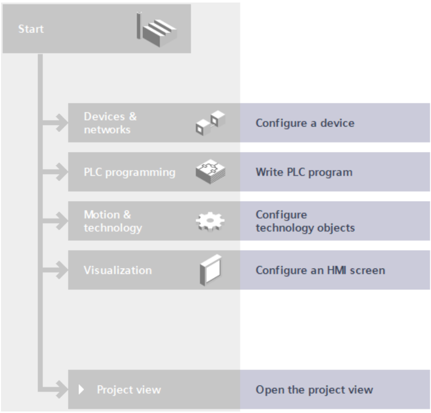


Figure 3.1: Starting window of the TIA Portal

The Totally Integrated Automation Portal is a unique development environment that have been widely used during programming. Most of the devices present in the lab are Siemens brand (from SIMATIC family), not only the PLCs but also HMIs, the motor inverter, wireless PROFInet devices, industrial Ethernet switches etc. For this reason, the software used for programming the entire system is the one briefly introduced here.

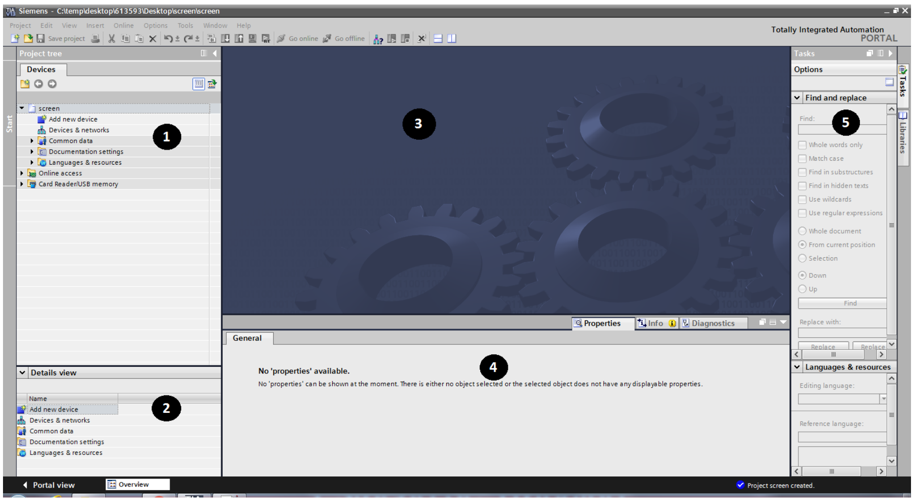
All the computers in the automation laboratory have already installed it with the proper library for working.

With the TIA Portal, it is possible to have a centralized design environment and, hence, a common user interface for all automation tasks, with common services (such as configuration, communication, diagnostic, etc.) and a single database in which the various software packages access.

It allows programming both new systems as well as older ones. In addition, the interface allows the operator to easily switch from one device to another as needed, without applying changes in the programming philosophy.

A good look at what this software is capable to do is given by its first window (see Figure 3.1). It is evident that it is possible to design the entire network step by step: starting from the devices and the network configurations, one can write the PLC program, assign I/O addresses and tags, and design also the HMI screens.

Moreover, once that the program has been compiled and uploaded, through the TIA Portal it is possible to diagnose the network and the devices while they are working. This is the main advantage that network protocols brought with respect to the previous technologies, very useful in order to find faults. In the following is briefly described the project window, the main window in the TIA Portal.



No 'properties' available.

No 'properties' can be shown at the moment. There is either no object selected or the selected object does not have any displayable properties.

Project screen created.

Figure 3.2: Project window of TIA Portal

1. ‘Project navigation’ window - it is possible to access all open project components and navigate quickly within the project.

2. ‘Details view’ window - the contents of the selected object in the ’Project navigation’ window are displayed here.

3. ‘Work Window’ - is the one where the user makes changes to the project. It is possible to see various editors for software writing, hardware definition or panel page definition.

4. ‘Inspection Window’ - here one can view the properties and details of the objects selected in the ‘Job Window’.

5. ‘Task Card’ - is a window that varies according to the editor that is presented in the ‘Work Window’. In addition, here we have the possibility to view and use the ‘Libraries’ tool of the TIA Portal.

3.1.1 Devices and network configuration

‘Devices & networks’ section is present in the ‘Project navigation’ window. This section is composed of three working areas:

- ‘Device view’ where it is possible to find all the information concerning the selected device and parametrize it.
- ‘Network view’ in which it is possible to see the entire network from a protocol point of view. Here, logical connections between devices can be set up and, in addition, new stations can be added to the project through the use of the hardware catalogue (located in the right part of the window).
- ‘Topology view’. In this section it is possible to physically design the network, drawing the cables which connect the various device interfaces.

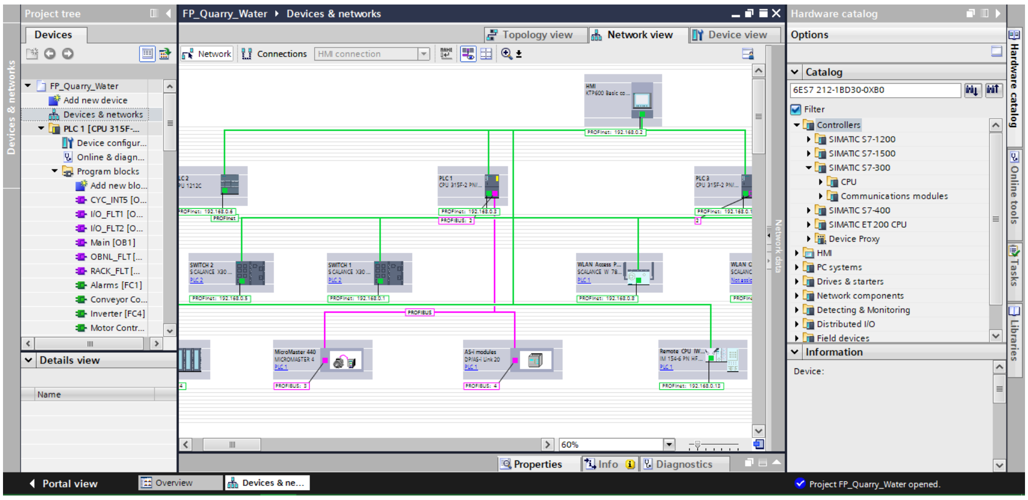


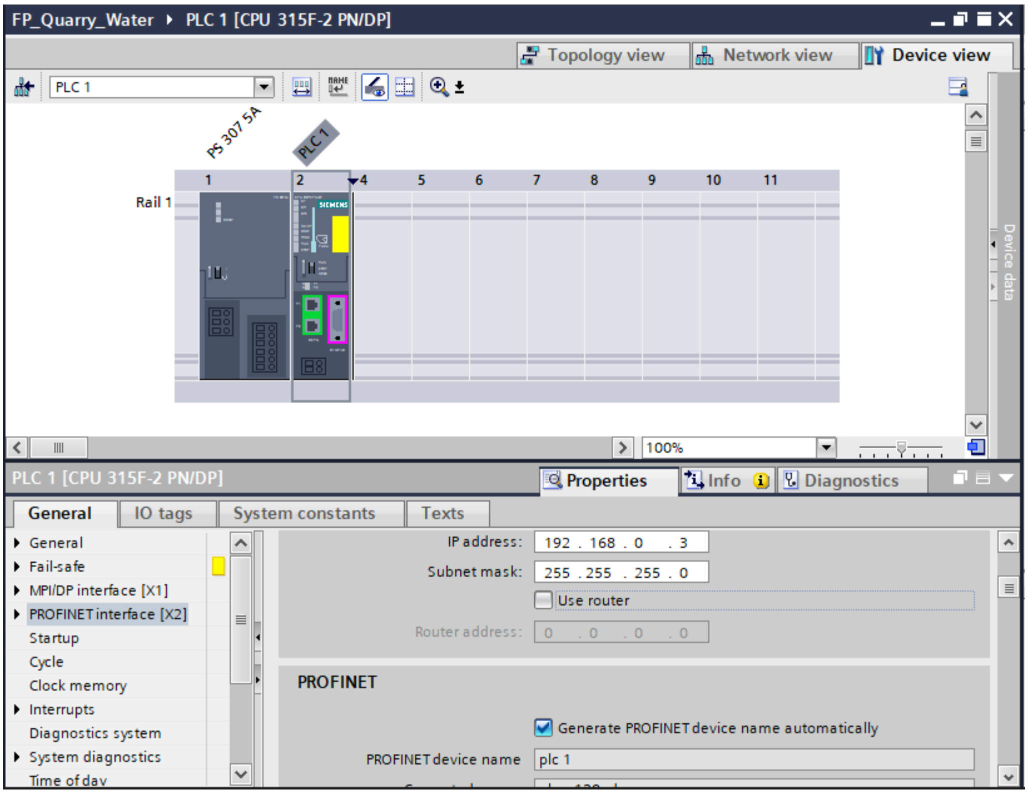
Figure 3.3: Network view section

The catalogue which is shown in Figure 3.3, located in the ‘Task card’ when ‘Network view’ is open, contains all the devices available for the project and all the GSD files installed in the software. From here it is possible to choose a device and add it to the project. It is very important that the Siemens code and the software version of the chosen device are exactly the same as the physical apparatus which is used. If the configuration is different with respect to the real implementation, the controller which is responsible to monitor/access to these devices will send back an error message.

As explained in Section 2.4, for performing the communication is mandatory the assignment to each PROFInet IO device of a specific name and address. This can be easily done using TIA and it is shown in Figure 3.4. The same method can be used for assigning the PROFIBUS DP address if the PROFIBUS DP interface has to be used.

The address assignment can also be done using the ‘Online & diagnostic’ tool under the section ‘Functions’. This is an online method, in the sense that the software has to be linked with the system and the device must be switched on in ‘Stop’ mode. On the contrary, Figure 3.4 shows an offline method that becomes effective only when the program has been downloaded to the controller.

Most of the time, the online method is used at the first configuration of the device. Thanks to the MAC address provided by the manufacturer, it is possible to access the stations through ‘Accessible device’ window in the TIA Portal and then change its name and address.



IP address: 192 . 168 . 0 . 3

Subnet mask: 255 . 255 . 255 . 0

□ Use router

Router address: 0 . 0 . 0 . 0

PROFINET

☑ Generate PROFINET device name automatically

PROFINET device name: plc 1

Figure 3.4: Device view section and PROFInet assignment

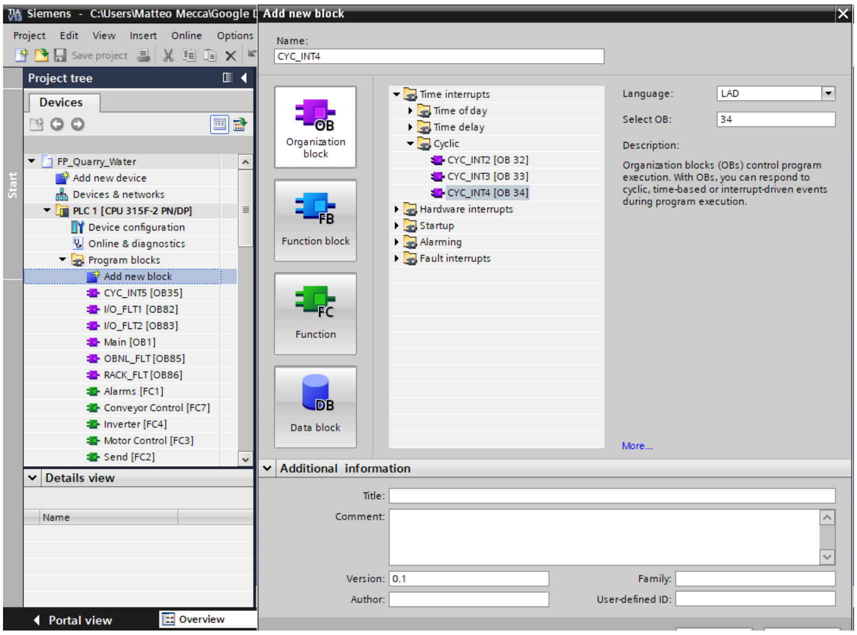
Several types of communication can be designed using the TIA Portal. In fact, the software supports the creation of various logic connections between devices: S7, HMI, FDL, ISO, ISOonTCP, TCP, point-to-point, etc. Only S7 and HMI connections have been implemented in laboratory n. 201.

S7-communication - It is suitable for logic communication between two PLCs. It allows the use of PUT and GET Ladder instructions for data exchange between controllers.

HMI-communication - This connection can be set up only between an HMI and a PLC. It allows the transmission of information to control/supervise the system through the HMI device.

3.1.2 PLC programming with TIA

Once added a controller in the TIA Project, it is possible to design a certain Ladder program to work with. The Siemens environment is predefined for a symbolic programming. Several 'program blocks' are available in order to structure the code and make it clearer.



Name: CYC_INT4

Language: LAD

Select OB: 34

Description:

Organization blocks (OBs) control program execution. With OBs, you can respond to cyclic, time-based or interrupt-driven events during program execution.

Version: 0.1

Figure 3.5: Program blocks in TIA Portal V13

As shown in Figure 3.5, four types of program blocks are available [22].

Organization blocks (OB) - They constitute the interface between the operating system and the user program. These types of blocks are called by the system and they control various CPU operations, such as the behaviour of the system during start up or the error treating. Obviously, they are different with respect to the CPU in use.

Functions (FC) – Essentially, they are code blocks without memory. Due to the fact that they don't have memory, when the function is called by the program all the formal parameters must be substituted by the actual parameters. Normally, a function contains a program written by the user that runs when the block is called by another code block. For permanently saving data, functions can use Global Data Blocks.

Function blocks (FB) - Code blocks that store input, output or transient parameters in a permanent way. They can work both with Global Data blocks and temporary variables. The latter, obviously, is not saved but remain in memory just for one cycle. This block type contains programs which are run when the FB is called by another block.

Global Data blocks (DB) - These blocks are used for storing program data. A DB contains variable data which are used in the user program. These data can be also used by all the other blocks.

Laboratory n. 201 is equipped with a new generation PLC (S7-1200 model). New generation controllers support the same blocks previously described but in an optimized form. Optimized program blocks are able to work only in symbolic without requiring specific addresses for the data. However, standard blocks are still available for these PLCs, since they are useful in many cases (for example in communication with other controllers). Principal features of optimized blocks are the following [22].

- Variables have no offset. The CPU organizes data internally and automatically. Due to this, both memory space and access time to variables are optimized and reduced.
- Each variable has its retention. It is possible to decide the retention of each variable. In standard blocks, this is not possible.
- Download without reset. It is possible to add or reduce variables and, during download to the device, only the changed data are reinitialized.
- No external devices can access the blocks (except HMIs with symbolic access).

Several functions are already available in TIA, as PID, mathematical and conversion functions. All these can be found as FC blocks which is possible to add to the program.

Table 3.1: STEP 7 elementary data types

Type	**Size in Bits**	**Format options**
BOOL (Bit)	1	Boolean text
BYTE (Byte)	8	Hexadecimal number
WORD (Word)	16	Binary number Hexadecimal number BCD Decimal number unsigned
DWORD (Double word)	32	Binary number Hexadecimal number Decimal number unsigned
INT (Integer)	16	Decimal number unsigned
REAL (Floating point)	32	IEEE floating point number
S5TIME (SIMATIC time)	16	S7 time in steps of 10 ms
TIME (IEC time)	32	IEC time in steps of 1 ms
DATE (IEC date)	16	IEC date in steps of 1 day
TIME OF THE DAY (Time)	32	Time in steps of 1 ms
CHAR (Character)	8	ASCII characters

Before or during the design of the program, several tags which describe the process variables must be defined. When a variable is defined, it is mandatory to specify its data type, address and symbolic name. For the controller, the data type indicates the number of bits which that data will occupy in the memory.

TIA Portal V13 support many data types and the most important ones are described in Table 3.1 [22].

Integrated in the software there is also the possibility to add HMI devices and design their screens. The configuration of the supervisory device can entirely pass through the TIA Portal: from the HMI logic connection set up to the definition of the variables until the design of the process pictures which constitute the interface between the operator and the system.

3.2 Plant supervision: WinCC

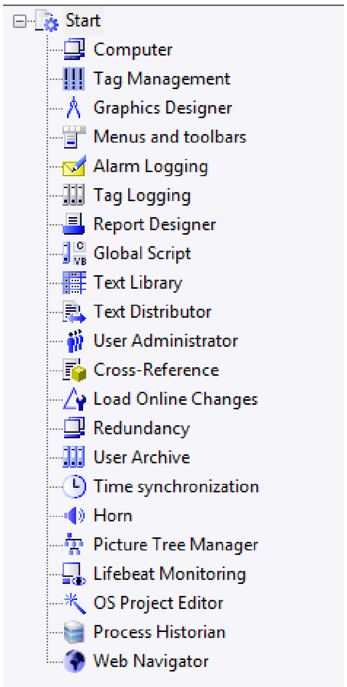


Figure 3.6: Main menu of WinCC V7.3

WinCC is a SCADA system developed by Siemens for supervising but also controlling industrial processes. It is a matter of fact that not all the SCADA systems produced by Siemens are integrated into the TIA Portal. It is the case of WinCC V7.3 and WinCC 2008 Flexible. Laboratory n. 201 is equipped with only one PC which has WinCC in its version 7.3. Moreover, to work with WinCC 2008 an old SIMATIC Field PG has been used.

3.2.1 WinCC V7.3

This version of WinCC is suitable for performing plant supervision and control through any personal computers.

First of all, it is necessary to define the connection with which the software will access the specified PLC variables. Through 'Tag Management' window it is possible to do this and create the system table. If the data must be stored, using 'Tag Logging' one can define the archive. Archived variables are those data whose value remains in memory for a certain period of time. If the archiving is not specified, the data values are taken in real time during RunTime mode and they will not be stored.

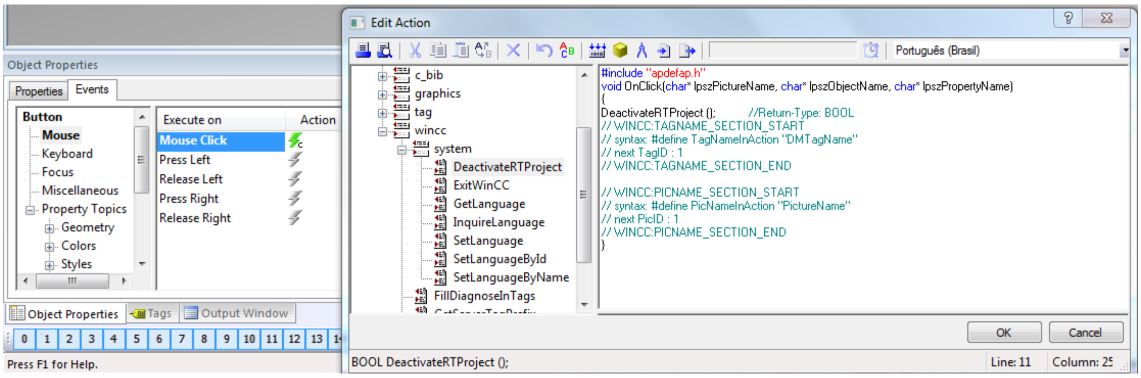
To manage alarms or messages to the operator, the assignment of the trigger bits can be made in the 'Alarm Logging' window.

Once defined the variables that the SCADA must manage, it is possible to create the screens in 'Graphics Designer' section. All the SCADA systems implemented in the laboratory n. 201 have been designed using only these four sections, without entering into the details of all the others shown in Figure 3.6.

WinCC furnishes various ways for dynamizing the objects in a process picture. Essentially, it permits three different methods.

1. Direct contact. The direct contact method is used to react to events. It improves the functionality and the speed of the RunTime but it is not very flexible since it is possible to assign only one variable for each object [23].

2. C language. C actions are used to dynamize an object property or to react to events. Through this method, it is possible to assign a certain action which can be triggered by different tags. Using C language many functions/actions are supported and already present in the software. These functions allow the user to not only interact with the process but also with the RunTime itself.



```
#include "apdefap.h"
void OnClick(char* lpszPictureName, char* lpszObjectName, char* lpszPropertyName)
{
DeactivateRTProject ();         //Return-Type: BOOL
// WINCC:TAGNAME_SECTION_START
// syntax: #define TagNameInAction "DMTagName"
// next TagID : 1
// WINCC:TAGNAME_SECTION_END

// WINCC:PICNAME_SECTION_START
// syntax: #define PicNameInAction "PictureName"
// next PicID : 1
// WINCC:PICNAME_SECTION_END
}
```

```
BOOL DeactivateRTProject ();
```

Figure 3.7: Example of C action implementation for deactivating RunTime mode

3. VBS language. It allows the user to perform the same actions provided by C language but, in addition, Virtual Basic Scripts can be used to customize the Windows environment [23]:

    - transferring data to another application (Excel, etc.);
    - starting external applications;
    - creating files and folders.

With the dynamization of objects in the process picture, it is possible to give to the operator an easier and immediate understanding concerning the plant operations. In addition to the basic graphic symbols, WinCC V7.3 provides several control objects. In particular, ActiveX controls can be used to monitor and display the variables and the system parameters.

A list of ActiveX control elements is the following [23].

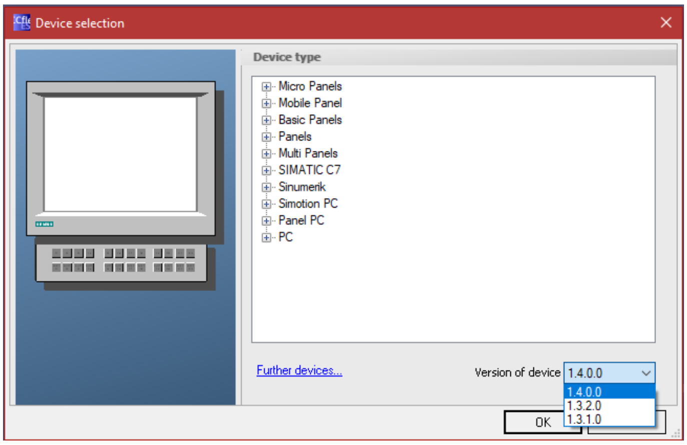
WinCC AlarmControl
WinCC Digital/Analog ClockControl
WinCC FunctionTrendControl
WinCC GaugeControl
WinCC MediaControl
WinCC OnlineTableControl
WinCC OnlineTrendControl
WinCC RulerControl
WinCC PushbuttonControl
WinCC SliderControl
WinCC UserArchiveControl
WinCC WebBrowserControl

Both in laboratory n. 201 and n. 119, the following control objects have been implemented.

Gauge Control - It is used to display the monitored values of a certain variable in the form of an analog clock.

Alarm Control - It is a message window used to display information which regards events. Each message is associated with a specific trigger bit defined in ‘Alarm Logging’ section. When the trigger bit is 1, the associated message is shown in this window during RunTime.

Online Trend Control - It is a window which shows data as a trend. The information can be fixed in time or displayed in real time. Moreover, it is possible to print the graph and save the values in .csv files. An important feature of Trend Control is the possibility to show real time as well as archived values. The stored values are safer from a point of view of possible data loss due to unexpected events.



Version of device 1.4.0.0

Figure 3.8: Supported devices in WinCC 2008 Flexible SP3

3.2.2 WinCC 2008 Flexible

This WinCC version was installed in the Industrial Field PG notebook. Its main feature is the flexibility: it provides the possibility to create SCADA/HMI programs for almost all the supervisory devices of the SIMATIC family (see Figure 3.8). For this reason, it has been used not only to create an additional SCADA system but also to perform the design of the HMI program of the SIMATIC Mobile Panel.

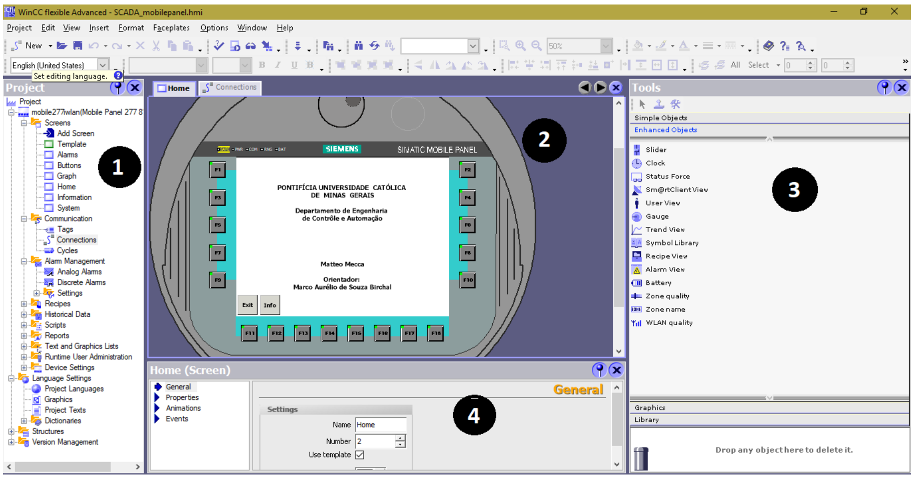
Once selected the device, the main page opens. The environment is briefly described in the following.

1. ‘Project Navigation’ window - Here is possible to navigate within the project, designing the process pictures and setting up the variables and the connection between the controller and supervisory device.

2. ‘Job Window’ - This window shows the contents of the section selected in the project window.

3. ‘Tools Window’ - In the tools window are located all the graphic and control objects that can be added to the process screens. It can be noticed from Figure 3.9 that the control elements are similar to the ones described for WinCC V7.3.

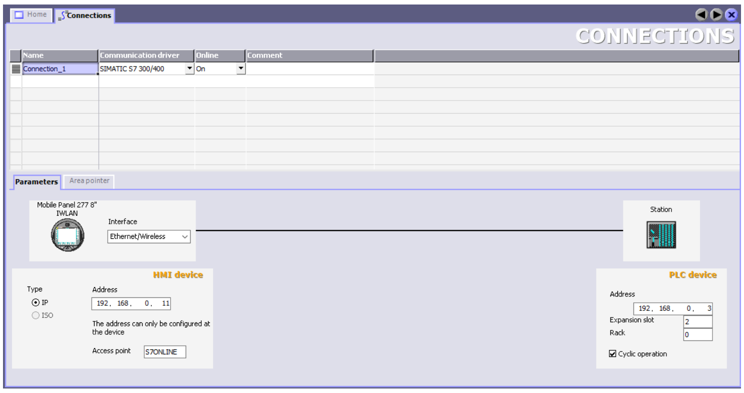
4. ‘Inspection Window’ - Here one can view the properties and details of the objects selected in the ‘Job Window’.



Name Home
Number 2
Use template ☑

Figure 3.9: Principal page in WinCC 2008 Flexible

Essentially the functioning criteria and the control elements of WinCC 2008 are the same as in WinCC V7.3. However, as it is an older software, it does not support new-generation devices (i.e. PLCs S7-1200 and S7-1500). Nevertheless, the connection between the supervisory device and the new-generation PLC can be configured with a communication driver called ‘SIMATIC S7-300/400’. This driver allows the exchange of information between devices which belong to the SIMATIC family, without controlling the CPU model.



Name	Communication driver	Online	Comment
Connection_1	SIMATIC S7 300/400	On	

Mobile Panel 277 8" IWLAN

Interface: Ethernet/Wireless

Station

HMI device

Type: ● IP ○ ISO

Address: 192. 168. 0. 11

The address can only be configured at the device

Access point: S7ONLINE

PLC device

Address: 192. 168. 0. 3

Expansion slot: 2

Rack: 0

☑ Cyclic operation

Figure 3.10: Connection set up in WinCC 2008 Flexible

3.3 Laboratory n. 201

Located on the first floor of building n. 15, 'laboratório de automação industrial' (room n. 201) is a recently built lab for teaching activities in the PUC Minas campus of Belo Horizonte. The space is equipped with 15 PCs and, initially, the automated system used during lectures consisted of a small panel with an S7-300 PLC, an AS-i network which implemented digital I/O modules, an inverter which ran an asynchronous motor and several buttons, lights and proximity sensors (see Figure 3.11). PROFInet and PROFIBUS DP were also used in order to establish connections between almost all the stations involved.

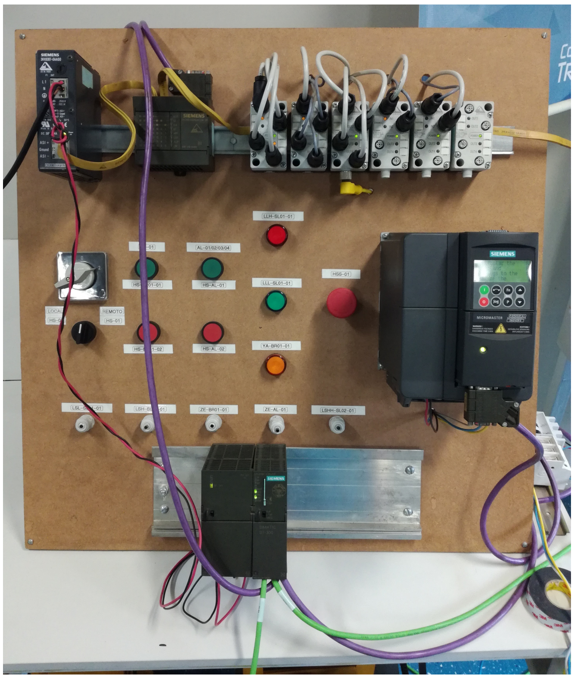


Figure 3.11: Initial plant of Laboratory n. 201

The main purpose of the project was to increase as much as possible this panel, with the design and implementation of a hybrid industrial network. To support this aim, the university acquired many devices, connectors and communication cables for an overall cost of more than 400.000 €.

Starting from the initial system, I structured the job in five steps. Each step constitutes a different process which has a different program that runs in it. In this way, taken individually, each system is in its own right and it can be reproduced entirely as an exercise for students. Nevertheless, all these systems are related to each other, thus it is sufficient to describe the last one in order to have a good overview of the work done. As a matter of clarity, the five steps followed are:

1. Project 1 - Rebuilding of the initial panel and its components: PLC S7-300, AS-i interface, DP/AS-i converter (the inverter has been added to the system later). Implementation of an industrial switch Scalance X308-2 and an HMI KTP600 for system supervision. First design of SCADA WinCC V7.3.

2. Project 2 - Addition of a second Scalance X308-2 and configuration in ring topology of the two switches. Implementation of a new-generation PLC (S7-1200 model) and set up of a wired S7-connection to exchange data between S7-300 and S7-1200 PLCs. Realization of the second version of SCADA WinCC V7.3 and first version of WinCC 2008 Flexible using the SIMATIC Field PG.

3. Project 3 - Implementation of the PROFInet wireless communication using Scalance W 788-2 PRO and Scalance W 744-1 PRO. Addition of a third PLC, S7-300 model, and set up of wireless S7-connection for data exchange between PLCs.

4. Project 4 - Inverter (MicroMaster 440) and asynchronous motor are added to the system, unused until now. Realization of both SCADA and HMI new programs (third version for WinCC V7.3 and second version for WinCC Flexible). Implementation of redundant communication between PLC S7-300 (the initial one) and MicroMaster 440 using two OLMs (Optical Link Modules) which have been configured in ring topology. Change of Scalance X308-2 ring topology using fiber optic cables.

5. Project 5 - Addition of two remote CPUs: ET 200PRO with wireless technology and ET 200M with electrical interface. Implementation of a SIMATIC Mobile Panel 277 IWLAN for wireless monitoring with HMI program designed using WinCC 2008 Flexible. Last program changes for SCADAs and wired HMI (fourth version for WinCC V7.3 and third version for WinCC Flexible).

For clarity, a detailed list of the devices used can be found in the Appendix.

In order to test the communication between devices, a program has been thought and increased in each step. The final version is widely described in Chapter four, but for now, it can be said that it deals with a primary crushing process. The idea comes from the fact that the asynchronous motor was linked to a crusher model, and the Minas Gerais state is famous for its mining activity.

In the first construction, the wireless PROFInet was used only inside the laboratory n. 201 with, obviously, an almost perfect data exchange. Then, I decided to better test this part of the network moving the third PLC (S7-300) and the client module Scalance W 744-1 PRO in another lab (laboratory n. 119). This work section is explained in Chapter 5.

3.3.1 Plant topology

As explained in Subsection 3.1.1, the software TIA Portal has been used for designing the system and configuring almost all the devices involved. The plant can be seen entirely represented in this program through two sections: 'Topology view' and 'Network view' (see Figures 3.12 and 3.13). Both figures are structured as an industrial pyramid, with field devices at the pyramid base and supervisory stations at the top.

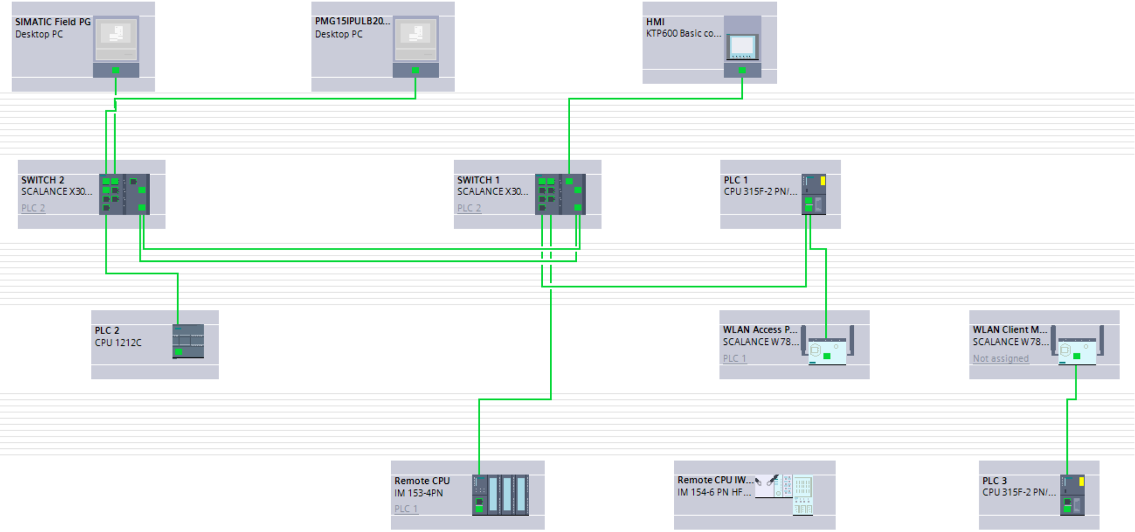


Figure 3.12: Laboratory n. 201 - PROFInet topology view

From Figure 3.12 emerges the complexity of the PROFInet network. It can be noticed that the TIA Portal does not support all the devices involved and so general stations have been used instead of them. For example, the two SCADA systems are represented as normal PC stations while the wireless HMI (Mobile Panel) is completely missing. Anyway, this fact does not affect the behaviour of the system because these apparatus are not involved in the PROFInet diagnostic which is performed by the IO-Controllers and, thus, no problems occur during functioning. However, the connection configuration of these supervisory devices is very important in order to use them: all the communication parameters (PROFInet addresses, names, MAC addresses) have to be the right ones.

For what concerns the wireless part, Scalance W 788-2 PRO has been used as Access Point in order to generate two different wireless networks, at 2.4 GHz (802.11g standard) and 5 GHz (802.11a). In this way, the connections don't overlap or collide with each other and it was possible to connect both stations ET 200PRO (with 802.11a) and Scalance W 744-1 PRO (with 802.11g). Since, for now, the communication is performed only inside the laboratory, standard antennas of 3 dBi have been used.

Final consideration regards the industrial switches. In Figure 3.12 all the interfaces are indicated and the green ones are the ports used. It can be noticed the ring redundancy configuration between ports 9 and 10, the optical fiber ones, of both devices.

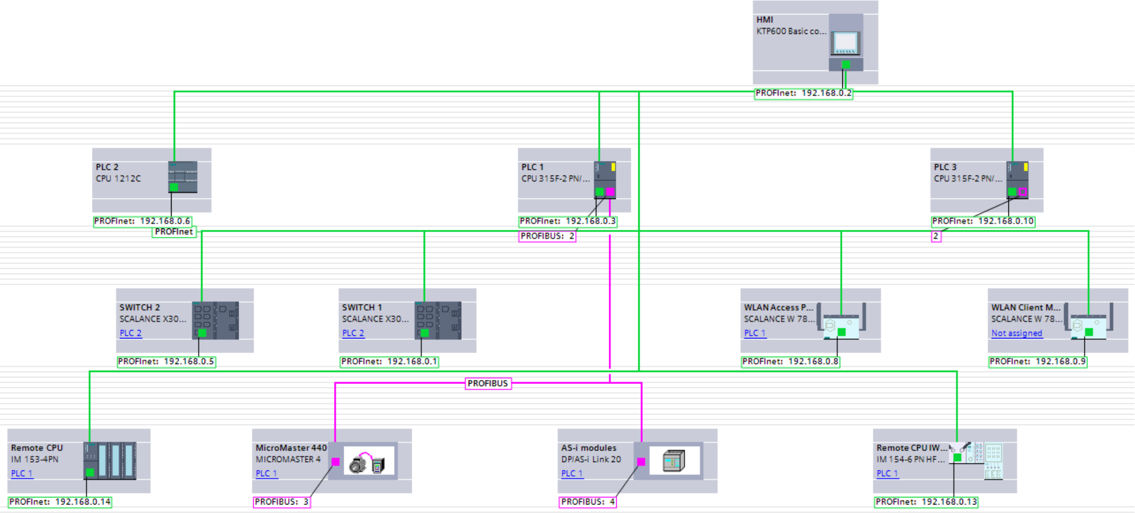


Figure 3.13: Laboratory n. 201 - network protocols view

In Figure 3.13 the system is represented from the point of view of the adopted protocols. Several considerations can be made here.

- No AS-i protocol is shown. This is due to the fact that the AS-i network part is embedded in the station called 'AS-i modules'. In fact, to perform a conversion from PROFIBUS DP and AS-i, a converter DP/AS-i has been used. The laboratory was equipped with a very old gateway DP/AS-i Link 20 (Siemens code 6GK1415-2AA00 - see Appendix) which is not supported by the TIA Portal. However, from the Siemens website, it has been possible to download the .gsd file and integrate it into the program. Thus, this station is identified with a certain PROFIBUS address and it includes both the gateway DP/AS-i and the AS-i digital modules. These modules can be configured in order to be recognized by the DP/AS-i converter with proper addresses.

- Hybrid and unique PROFInet. This network part has not been divided consequently to the various transmission media adopted but it has been configured with a sole name. Thus, it can be considered as hybrid because made of different transmission media but, at the same time, unique. This brings huge advantages, especially for what concerns device diagnostic and individually station configuration, because every device is reachable, configurable and monitorable from any point/interface of the network.

- No OLMs are shown. It can be noticed that the Optical Link Modules used for redundant connection between PLC 1 and MicroMaster 440 are not represented.

This is due to the fact that these stations are not supported and, more important, it is not necessary having them in the hardware configuration, since they can be configured via physical switches located on top of the device. Further comments will be made in Subsection 3.1.3.

- Master selection. In ‘Network view’, IO-Controllers for each IO-Device are also defined; this establishes which controller is the ‘master’ of a certain IO-device. During functioning, the master controller has the task to continuously diagnose the network and the specified devices for which it has been configured as the master. In most cases, when errors are detected, the master IO-Controller shows a visible blinking red LED on its interface; then, through ‘Online & Diagnostics’ section in the TIA Portal, the user can identify and correct the fault. As it is evident in the figure, PLC 1 has master tasks for all the field devices and the remote CPUs while PLC 2 supervises the industrial switches functioning.
- No master has been selected for Scalance W 744-1 PRO. This is due to the fact that this Scalance model does not support PROFInet diagnostic and, thus, for this device, the assignment of a master controller unequivocally leads the latter to always identify an error of non-presence of the wireless switch. From this consideration, it emerges that it is not necessary to integrate the device in the hardware configuration but it would be enough to configure it on its own and then, in TIA, connect the PLC 3 directly to the PLC 1 in order to perform the required s7-connection. However, exclusively for a question of clarity, it has been included.

In the following are reported the PROFInet names and addresses of all devices, together with the DP address, where it is the case.

Table 3.2: PROFInet parameters for all devices

Model	PN IO name	IP address	DP address
CPU 315F-2 PN/DP	plc 1	192.168.0.3	2
	plc 3	192.168.0.10	-
CPU 1212C AC/DC/Rly	plc 2	192.168.0.6	-
IM 154-6 PN HF IWLAN	remote cpu iwlan	192.168.0.13	-
IM 153-4 PN	remote cpu	192.168.0.14	-
SCALANCE X 308-2	switch 1	192.168.0.1	-
	switch 2	192.168.0.5	-
SCALANCE W 788-2 PRO	wlan access point	192.168.0.8	-
SCALANCE W 744-2 PRO	wlan client module	192.168.0.9	-
KTP600 Basic color PN	hmi	192.168.0.2	-
SIMATIC Industrial Field PG	notebook	192.168.0.7	-
SCADA WinCC	desktop pc	192.168.0.4	-
Mobile Panel 277 8” IWLAN	mobile 277iwlan	192.168.0.11	-
DP/AS-i Link 20	-	-	4
MICROMASTER 440	-	-	3

3.3.2 Logic connections

Within the network, two important logic connections have been performed.

HMI connection - Communication is implemented between PLC 1 and the wired HMI (KTP600). Via TIA Portal, process screens have been created with the purpose to inform the operator about the entire process and the possibility to intervene into it.

S7 connection - Two S7 communications have been established, between PLCs n. 1-2 and PLCs n. 2-3. These connections are used to exchange data adopting two Ladder function blocks, both supported by S7-300 and S7-1200, which are called PUT and GET. As shown in Table 3.3, this type of connection needs identification numbers (in hexadecimal format) for the local station and the partner one. Furthermore, it is necessary to specify if the local station is 'active' or not: an active device, in this case, is a controller that carries the communication and sends the data first. On the other hand, the partner device will be passive and will wait to receive data before sending it in turn. Obviously, the devices can't be set as active or passive at the same time, otherwise the data exchange will never happen due to collision (both active, not in reception mode) or inactivity (both passive, waiting for the other device starts communication).

Table 3.3: Logic connections established within the network

Connection name	Local end point	Partner	Local ID (hex)	Partner ID (hex)
HMI connection	HMI	PLC 1	-	-
S7 connection 1	PLC 1	PLC 2	1	100
S7 connection 2	PLC 1	PLC 3	2	1

PLC 1 has been set up as the active device in both S7 connections. From Figures 3.12 and 3.13 emerges that these communications take place through different transmission media. In particular:

- HMI connection is performed through electrical cables,
- S7 connection 1 uses both electrical and optical cables,
- S7 connection 2 adopts almost always the air via wireless technology.

It is also evident from Table 3.3 that the HMI connection does not require any identification number. The communication only needs Internet Protocol addresses (PROFInet addresses) of both devices which are involved. These parameters can be found in Table 3.2.

3.3.3 Ring configurations

It has been already mentioned that there are two parts of the network which have been configured in ring topology. Despite these rings have the same purpose, they adopt different devices and technologies as well as they need dissimilar configurations. Due to this, in the following are described separately.

Media redundancy using Scalance X 308-2

Industrial ethernet switch Scalance X 308-2 supports two media redundancy methods [17].

- MRP (Media Redundancy Protocol);
- HRP (High speed Redundancy Protocol).

Both of them can be assumed to be 'media redundancy' methods since the functionalities are very similar, but they can't be used at the same time in a ring topology. External switches and/or switches which are integrated in modules are the nodes in these types of ring topology.

Essentially, a ring topology with media redundancy consists of linking together the two free ends of a linear bus topology in one device. A device in the ring is responsible to have both the initial and the final ends of the linear bus and this station is called 'redundancy manager' while all the other devices in the ring are 'redundancy clients'.

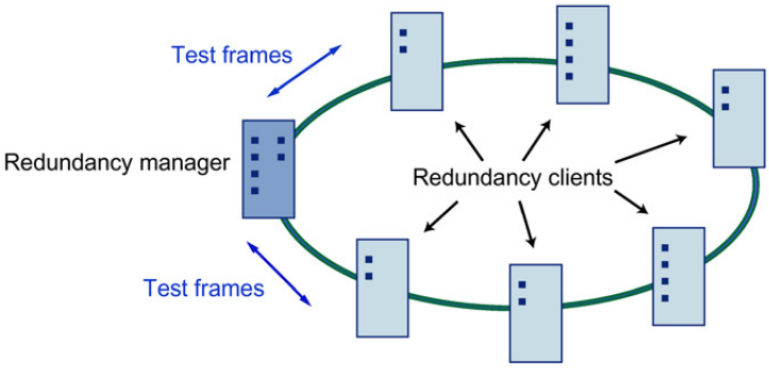


Figure 3.14: Media redundancy ring topology [17]

If the network is uninterrupted, the redundancy manager has the two ring ports which are disconnected from each other in order to prevent circulating data frames. Thus, in this case, the ring topology is nothing more than a linear bus topology with a device which has the task to continuously monitor the network.

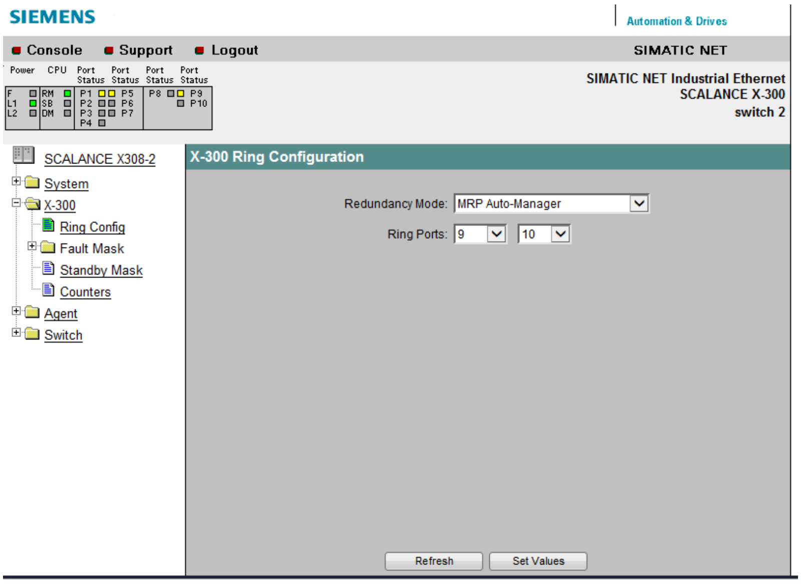
Redundancy manager station tests the channel by sending test frames from both ring ports; these frames run around the ring in both directions until they arrive at the other ring port of the redundancy manager [17].

An interruption of the ring can be caused by the failure of a station in the channel or by the loss of connection between devices. Faults are detected immediately by the manager because its test frames no longer arrive at the destination; in this case, the redundancy manager connects its two ring ports. This new path restores a functioning connection between all remaining devices in the form of a linear bus topology [17]. Moreover, as soon as the interruption is eliminated, the original transmission paths are established again.

The time between the ring interruption and restoration of a functional linear topology is known as the reconfiguration time. If it is the manager that fails, the ring becomes a functional linear bus.

The greatest difference between the two methods is the reconfiguration time: MRP has 0.2 seconds, while HRP has 0.3 seconds of reconfiguration time [17].

In TIA Portal, using the 'Web Based Management' window, it has been possible to configure both IE switches in MRP mode, selecting ports 9 and 10 as ring ports and setting Auto-Manager as redundancy mode in both devices. Auto-Manager is a functionality which implies that the devices configure themselves automatically as manager or client. This is not enough because the Scalance X 308-2 needs also to be enabled as the manager using the SET/SELECT button on its front surface [17].



X-300 Ring Configuration

Redundancy Mode: MRP Auto-Manager

Ring Ports: 9 10

Figure 3.15: Media Redundancy Protocol configuration via 'Web Based Management'

Since 9 and 10 are optical fiber ports, fiber optic cables have been used for implementing the topology.

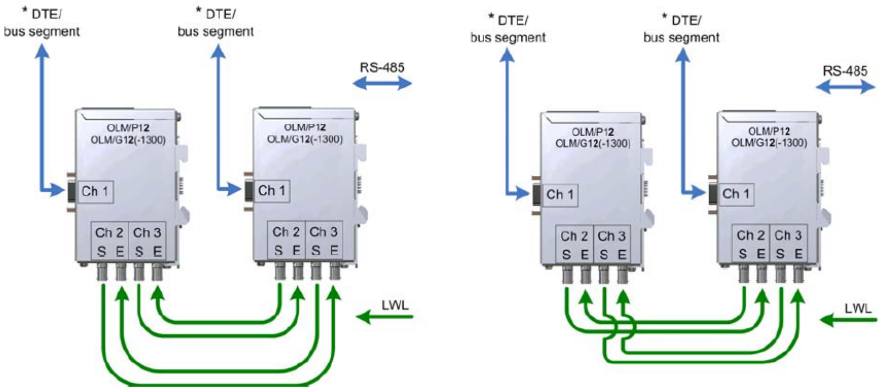
The main advantage of having this topology in the plant is that the S7-connection between PLCs 1 and 2 is redundant (see Figure 3.12). As it will be explained later, PLC 2 has the only task to collect the data which are needed by all the SCADAs. Hence, PLC 2 remains linked to the system and the SCADAs can still operate even in case of connection faults.

Optical Link Modules ring topology

The connection between PLC 1 and MicroMaster 440 has been implemented in redundancy mode adopting a ring topology. It is better to have this communication redundant because if a fault of a cable happens the operator is still able to control the motor.

In this case, the ring topology has been performed using two Optical Link Modules G12. These devices can support three different transmission channels, one electrical (CH1) and two optical (CH2 and CH3). Hence, they are able to convert the transmission medium from electrical to fiber optic and vice versa and they support RS-485 standard for PROFIBUS DP (see Figure 2.13b).

Two different hardware configurations are possible in order to establish the redundant connection, as shown in Figure 3.16. In laboratory n. 201 the first configuration has been adopted (refers to Figure 3.16a).



(a) *Configuration 1.* **(b)** *Configuration 2.*

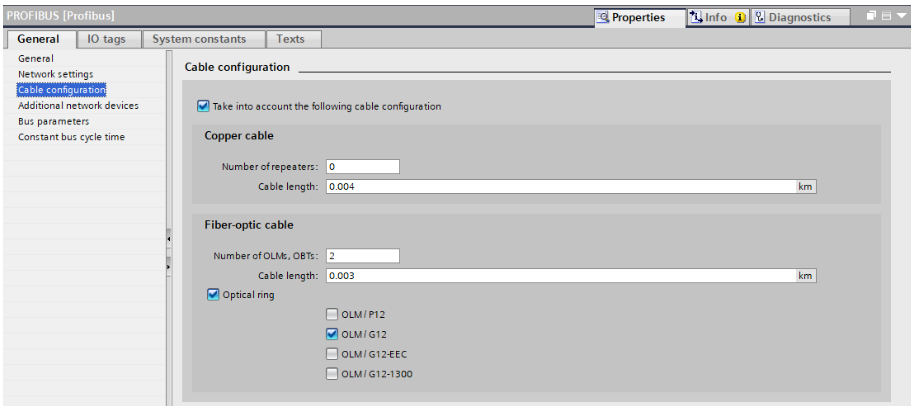
Figure 3.16: Hardware configurations of ring topology using two OLMs [21]

The devices can be configured using the DIL switches located on top of the modules [21]. Once set up, a frame received by any channel is moved on to all other channels. If the frame is received at an optical channel, it will also be sent back to the sender on the same channel as an echo and therefore as a monitoring frame to test the fiber optic links between the OLMs. The OLM recognizes whether a received frame is an echo or a frame. In the case of an echo signal, the channel LED (located on the front surface of the module) stays off whereas in the case of a forwarded frame it will light up yellow.

For how the connection has been implemented in laboratory n. 201, the communication happens through fiber optic cables of the same length. Under this circumstance, the receiving OLM gets a frame on both of the optical channels at the same time. To manage this case, the OLM prioritizes the two optical channels. By definition, the frame on one optical channel will then be taken as an echo (channel LED = off) and the frame on the other optical channel will then be taken as a forwarded frame (channel LED = yellow).

As already mentioned in Subsection 3.1.1, TIA Portal does not support the Optical Link Modules, principally because they can be configured entirely via DIL switches. However, this network part has to be set in TIA, as well as PLC 1 has to be informed about this configuration because it is the IO-Controller of the MicroMaster and so responsible of monitoring the communication.

The network configuration can be done in TIA Portal, adding the exact parameter values as shown in Figure 3.17. After this, the hardware configuration can be downloaded in all the IO-Controllers of the network.



Cable configuration

☑ Take into account the following cable configuration

Copper cable

Number of repeaters: 0
Cable length: 0.004 km

Fiber-optic cable

Number of OLMs, OBTs: 2
Cable length: 0.003 km

☑ Optical ring

☐ OLM / P12
☑ OLM / G12
☐ OLM / G12-EEC
☐ OLM / G12-1300

Figure 3.17: PROFIBUS DP cable configuration

Chapter 4

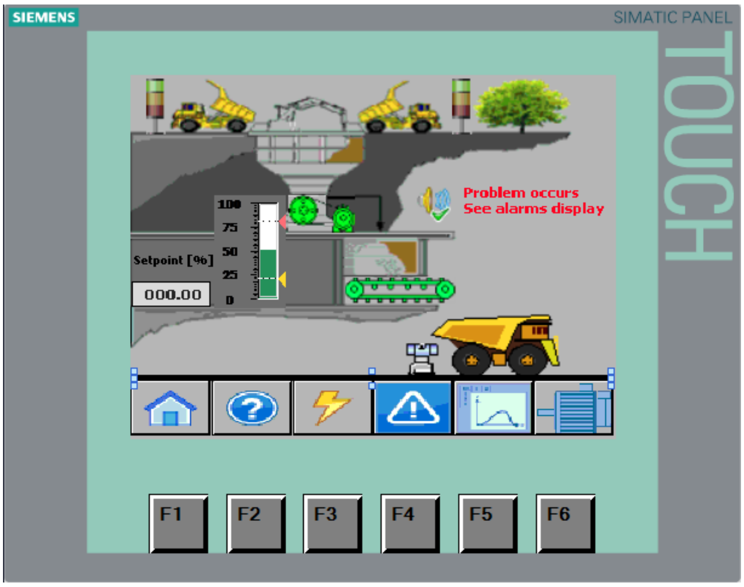
Primary crushing process

In order to test the communication within the hybrid network of laboratory n. 201, a process has been invented and then simulated. As the title suggests, a primary crushing process has been performed. The idea came from the fact that the asynchronous motor was linked to a crusher model and the Minas Gerais state is famous for its mining activity.

Hence, the chapter deals with a wide explanation of this process, discussing the task of each device involved in the system as well as the implementation of ladder logic of PLCs and process pictures of SCADAs and HMIs.

4.1 Process to be controlled

The industrial system simulated in laboratory n. 201 regards a primary crushing process.



Problem occurs
See alarms display

Setpoint [%] 000.00

Figure 4.1: Plant overview, seen from the main HMI process control screen

An overview of the plant is shown in Figure 4.1, which is one of the process pictures designed for the wired HMI. The treated material is calcium carbonate ($CaCO_3$).

As illustrated, the system simulates a very common crushing process which has been divided in three phases.

1. The material is crushed in the crusher which is driven by the asynchronous motor (see Figure 4.2).
2. The processed material is stored in a silo, waiting to be transported.
3. Started by operators, a conveyor belt transports the crushed material into a quarry truck in order to be processed elsewhere.

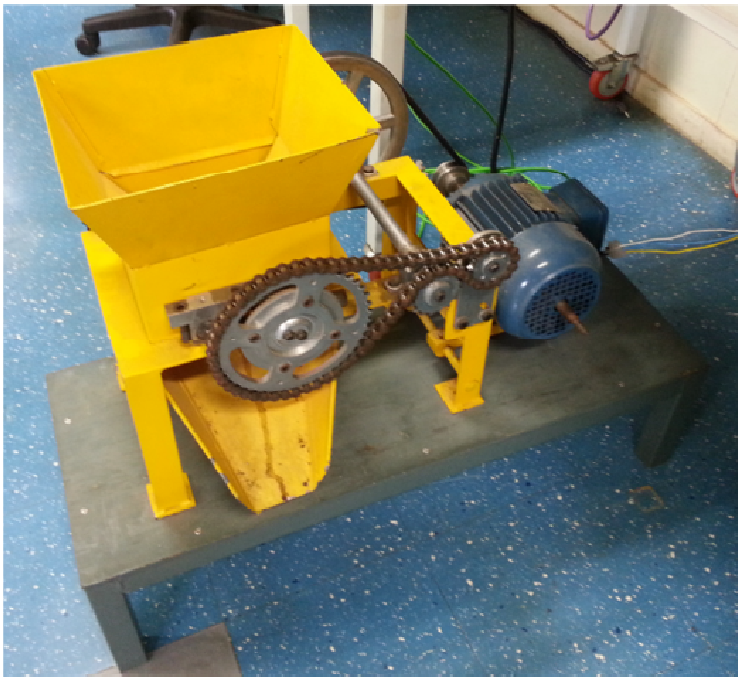
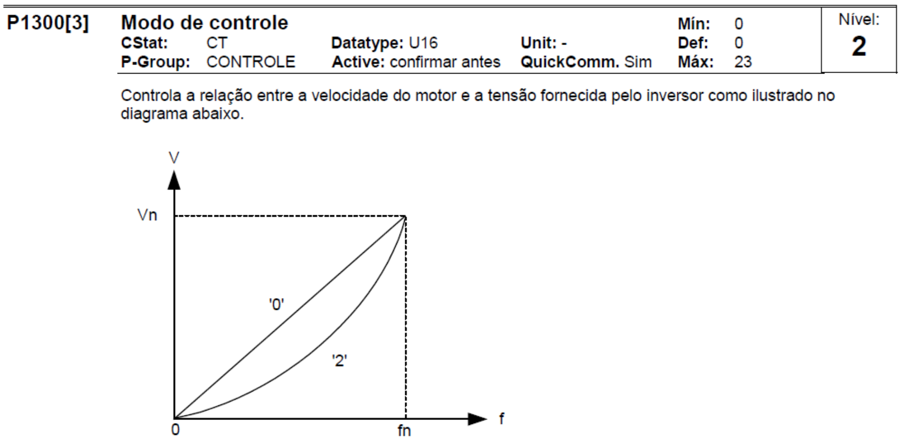


Figure 4.2: Crusher model

The automated process has the principal purpose to regulate the silo level with respect to a previously inserted setpoint via HMI. Therefore, the system should be able to always keep this level close to the selected setpoint. To do this, a speed control of the motor is necessary because the crusher fills the silo while the conveyor belt empties it in a constant way. The laboratory was not equipped with a conveyor machine and, thus, it has been simulated using ladder logic: when active, the conveyor empties the silo transporting a constant quantity of material equal to 40 t/h. It is automatically stopped by the system when no quarry truck is detected in the parking slot.

MicroMaster 440 has been parametrized in order to have a linear variation of the ratio motor speed over inverter frequency (see Figure 4.3). This means that when the inverter provides 50 Hz (set as the maximum frequency), the motor rotates at 100% speed. In this condition, it has been assumed that the crusher produced 100 t/h of material.



P1300[3]	Modo de controle			Mín: 0	Nível:
	CStat: CT	Datatype: U16	Unit: -	Def: 0	2
	P-Group: CONTROLE	Active: confirmar antes	QuickComm. Sim	Máx: 23	

Controla a relação entre a velocidade do motor e a tensão fornecida pelo inversor como ilustrado no diagrama abaixo.

Figure 4.3: V/f characteristic set up in MicroMaster440 [18]

Therefore, due to this characteristic, the flow variation of the material entering the silo is linear with respect to the speed variation.

The processed material is calcium carbonate which has a density that is variable from 2.62 [g/cm^3] to 2.71 [g/cm^3]. The value 2.70 [g/cm^3] has been used for computations; applying the density formula it is possible to obtain the occupied material volume for a certain time period.

$$d = \frac{m}{V} \to V = \frac{m}{d}, \tag{4.1}$$

where d is the material density, V is the occupied volume, and m is the mass.

When the crusher rotates at maximum speed, the produced volume of material is shown in Eq. 4.2. This value is linearly dependent on the speed variation and, thus, to the inverter frequency.

$$V = \frac{100000\,[\mathrm{kg}]}{2700\,[\mathrm{kg/m^3}]} \to V = 37.04\,[\mathrm{m^3}] \tag{4.2}$$

On the other hand, the conveyor belt is able to transport a constant volume of material which is the value of Eq. 4.3

$$V = \frac{40000\,[\mathrm{kg}]}{2700\,[\mathrm{kg/m^3}]} \to V = 14.816\,[\mathrm{m^3}] \tag{4.3}$$

Considering these volumes, it is possible to say that the maximum silo filling rate is 37.04 m^3/h while the constant exit rate is 14.816 m^3/h.

For increasing the dynamic and accelerating the simulation of the process, a time conversion has been made such that one hour time became one minute. Due to this, the final two rates are:

1. linearly variable filling rate with max. 37.04 m^3/min;

2. constant exit rate of 14.816 m^3/min.

In addition to these considerations, other important assumptions have been made to further detail the process.

- The system can be controlled both in local (wood workstations located close to the machines) and in remote (wired and wireless HMIs) mode.

- Instead of using automatic control, workers can intervene in the process switching in 'manual mode control' for controlling the motor speed manually using an analog dimmer.

- The entire process is monitored by two SCADAs. One, far away from the plant, can only supervise the system, while the second one can also control it.

- The motor can be started pressing the green button. It is required to press three times in a row the red button in order to stop it. The semaphore in the system follows the two engine states, lighting up red when the engine has no speed and green in the opposite case. When problems occur, the orange light switches on with a delay-off time of 5 seconds. This logic is always implemented, both in local or remote mode.

- The conveyor belt can be activated both in local or remote. Even in this case, a semaphore which indicates the status of the machine is located close to it. The conveyor is automatically turned off by the system if the truck is not detected.

- Three proximity sensors are located in different plant parts, all communicating via AS-i. These devices are used in order to detect the presence of the quarry truck in the parking slot, to recognize a rupture of the belt of the conveyor and to notice if the silo level is too high.

Laboratory n. 201 has been divided into three work tables and all the devices listed in the Appendix have been mounted on them. The supply of each work table has been linked to the SIMATIC Power Supply devices (PS 307) which are responsible to provide energy for all the stations involved. The cables used for supply have been welded at the ends in order to provide safety and avoid short circuits.

In addition, as it can be noticed in Figure 4.4, the work tables have been pierced and most of the network cables have been passed behind the stations.

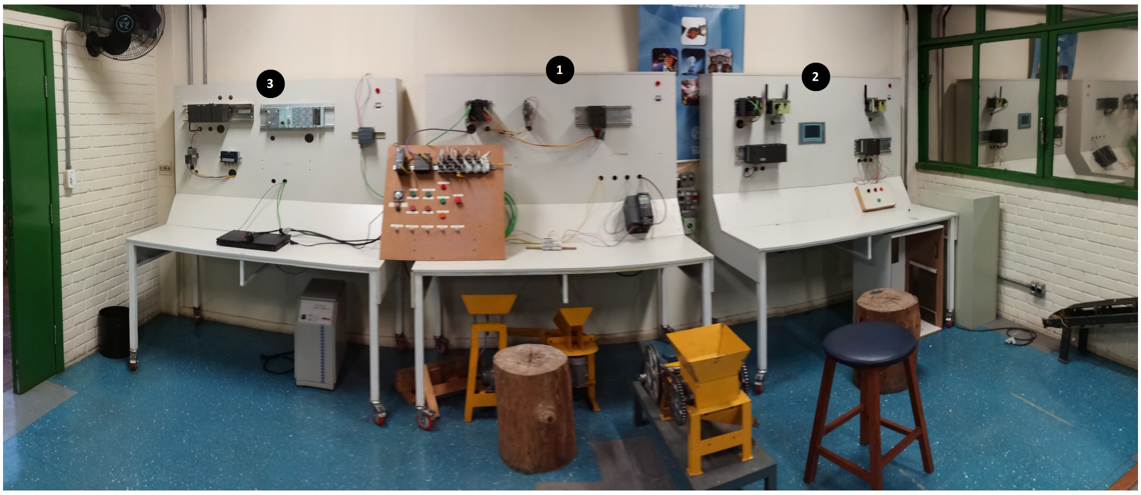


Figure 4.4: Numeration of the three work tables

4.2 Process variables

Each device has a specific purpose and the central piece is constituted by PLC 1 which is, as it has been already said, the master IO-controller for both remote CPUs and PROFIBUS DP master for both inverter and DP/AS-i converter. In the following are shown the process variables involved in the system and, in addition, it is possible to notice the different roles that each station has within the plant.

According to Table 4.1:

- AS-i station has been used only for implementation of some proximity sensors and switches which have been used to change the operating mode;
- the wireless remote CPU (ET 200PRO station) has been linked to a handmade wood panel to locally control the motor;
- the wired remote CPU (ET 200M station) has been connected to a handmade wood panel which has been used to locally control the conveyor.

As already stated and indicated in the table, all these addresses refer, and were therefore managed, by PLC 1. It controls almost all the plant and, at the same time, it is monitored by the wired HMI mounted on the second worktable. Moreover, the wireless mobile panel (SIMATIC Mobile Panel 277 IWLAN) can access directly to this controller in order to supervise and control the process.

Differently, the SCADA systems have not been performed in this way: they access to PLC 2 only. Both WinCC V7.3 and WinCC 2008 Flexible have been programmed in order to exchange data with PLC 2 only. This choice comes from the fact that has been assumed that PLC 2 is the controller responsible to collect all the significant data from all over the plant. This is possible using S7-connections between all the controllers involved.

Table 4.1: System table of PLC 1

Station	Logic address	Tag name	Description
AS-i M1	I0.0	Remote	Switch for remote mode
	I0.1	Local	Switch for local mode
	I0.2	Manual	Switch for manual mode
	I0.3	Automatic	Switch for automatic mode
AS-i M2	I1.5	Conveyor belt rupture	Sensor for detecting the conveyor belt
AS-i M2	I1.7	Truck present	Sensor for detecting the truck presence
AS-i M5	I2.0	Too high	Sensor for detecting the silo level when it is greater than 95%
ET 200PRO	I16.5	Motor ON	Button for motor starting
	I16.6	Motor OFF	Button for motor stopping
	I16.7	Motor EMERGENCY	Emergency stop button
	Q16.1	Motor Green	Motor green light
	Q16.2	Motor Red	Motor red light
	Q16.3	Motor Orange	Motor emergency light
ET 200M	I17.5	Conveyor ON	Button for starting the conveyor belt
	I17.6	Conveyor OFF	Button for stopping the conveyor belt
	Q17.6	Green Conveyor	Conveyor green light
	Q17.7	Red Conveyor	Conveyor red light
MM440	IW256	STATUS WORD	Inverter status word
	IW258	ACTUAL FREQUENCY	Inverter frequency read
	IW260	ACTUAL CURRENT	Inverter current read
	QW256	CONTROL WORD	Inverter control word
	QW258	FREQUENCY SETPOINT	Inverter setpoint control

PLC 2 gets and stores the important information that the SCADA operators required for supervising the process and, when necessary, using WinCC 08 Flexible, it is also able to send commands to the master PLC 1.

Hence, the second controller manages all the most important process variables in order to provide, through SCADA programs, a complete overview of the process. Most of these data are stored as Global Data Blocks and the adopted mechanism of PUT/GET blocks, which have been used to exchange information between controllers via S7-connections, will be explained more in details in Subsection 4.3.3.

PLC 2 is also used for two more tasks.

1. Monitoring of the Scalance X 308-2 ring configuration.
2. Analog dimmer has been linked to the analog input port of this device. In this way, when 'manual mode control' is active, the controller receives the value of the voltage coming from the sensor, transforms it into a percentage value and sends this information to the PLC 1 which reads it as the motor speed percentage.

In the end, PLC 3 has been added to the system in order to perform a simple task: energy saving. Adding a S7-connection between PLC 1 and this device, PLC 3 is continuously informed about the behaviour of the process and intervenes only in a specific situation. When the controller detects for more than 10 seconds that the setpoint value has been overpassed by the silo level, together with the fact that the motor has a speed lower than 20%, it puts in standby all the plant. In addition, the digital I/O module has been linked to a small panel which includes three lights, for showing the standby status, and a restart button.

Table 4.2: System table of PLC 3

Name	Data type	Logic address	Description
Green	Bool	Q0.0	Standby green light
Red	Bool	Q0.2	Standby red light
Orange	Bool	Q1.5	Standby orange light
GET_setpoint	Real	MD0	Get the setpoint value
GET_motor_speed	Real	MD8	Get the motor speed value in %
GET_actual_level	Real	MD4	Get the silo actual level
Stand-by	Bool	M9.1	Merker for stand-by status
Restart	Bool	I1.5	Restart button

4.2.1 Warning messages

Both in HMI and SCADA programs, a list of messages has been created in order to show to the operators some information when the functioning of the system requires a particular attention.

These messages are displayed in the proper process picture of SCADAs and HMIs when particular boolean tags in the system are activated. For simplicity, these tags have been grouped in a single word-type data, called 'Alarm word' with address MW0 in PLC 1.

Table 4.3: Warning messages from PLC 1 and PLC 3

ID	Alarm text	Trigger bit	Trigger address
1	EMERGENCY OFF button pressed. When released it, the system returns available after 5 seconds.	8	M0.0
2	System in energy saving stand-by. When ready press RESTART.	9	M0.1
3	Manual mode is active!	10	M0.2
4	Truck is not present. The conveyor is stopped.	11	M0.3
5	Conveyor belt is broken. Check the sensor.	12	M0.4
6	Silo level is greater than 95%. Check the sensor.	13	M0.5

Nevertheless, this is not the only method used for displaying warning messages but other two mechanisms have been adopted. The first one regards PLC 1 and it consists in the activation of the 'System Diagnostic' function. Thanks to this feature, automatically the controller sends to the connected HMIs important information which concerns the overall status of each device that can be supervised via PROFInet and PROFIBUS diagnostic functions. The operator can see these messages using 'System diagnostic view' (see Figure 4.10a).

While the texts which are shown in Table 4.3 are the same both for SCADAs and HMIs, the messages automatically generated by the 'System diagnostic' function have been established to be shown only in the HMIs (wired and wireless). This choice is according to the fact that data are reduced and more structured when ascending the control hierarchy of an automation pyramid (a concept already expressed in Chapter 1).

The second mechanism which regards the production of system status messages is the one programmed between PLC 2 and SCADAs. This controller is responsible to monitor the ring topology constructed with the two industrial switches (Scalance X 308-2) and, so, it is able to show malfunctions by switching on its LED. Of course, the led status of the PLC 2 and its internal messages can be read using 'Online&Diagnostic' function of the TIA Portal. However, it is necessary to immediately inform the SCADA operators about this diagnosis. With this purpose, a ladder logic which read the LED status of the controller, together with proper tags which trigger the messages, have been implemented in the PLC 2 ladder program.

Table 4.4: Warning messages from PLC 2

ID	Alarm text	Trigger bit	Trigger address
1	Master PLC detects an error. Check the plant and diagnostic via TIA Portal	10	M20.2
2	Master PLC detects an error. Check the plant and diagnostic via TIA Portal	11	M20.3
3	Master PLC detects an error. Check the plant and diagnostic via TIA Portal	12	M20.4

In this case 'led_ERROR' variable has been created using logic address MW20 in PLC 2. Inside this word, the trigger bits are listed in Table 4.4. The functioning is very simple: when the ladder program detects that the red LED of the controller is lit or is blinking, a trigger bit is activated.

Since the messages are based only on a detection of the activation of the red LED, the information texts displayed for the operators are general. Nevertheless they consist of a very important warning for the workers, who otherwise would be unaware of any problems.

4.3 Important Ladder solutions

In this section, three important ladder solutions will be discussed. These logics are fundamental since they regard the implementation of the system controller, the simulation of the conveyor belt, the computation of the silo level as well as the set up of PUT/GET instructions for performing data exchange between IO-Controllers.

As can easily guess, the whole functioning is based on the correct design and operation of all these parts.

4.3.1 Computation of the silo level

While the laboratory was equipped with an electric motor and the model of a crusher, no possibilities for implementing a conveyor belt have been found. Most important, an analog measuring sensor was missing in order to close the feedback loop of the system. Due to all these problems, it has not been possible to truly build the system, but ladder solutions have been adopted in order to have the silo and the conveyor functioning, even if in an imaginary way.

Essentially, this ladder part pretends to compute the material stored in the silo by subtraction.

$$\mathrm{V}_{silo} = \mathrm{V}_{cr} - \mathrm{V}_{conv}, \tag{4.4}$$

where V_{cr} is the volume produced by the crusher and V_{conv} is the volume of the processed material which is transported by the conveyor.

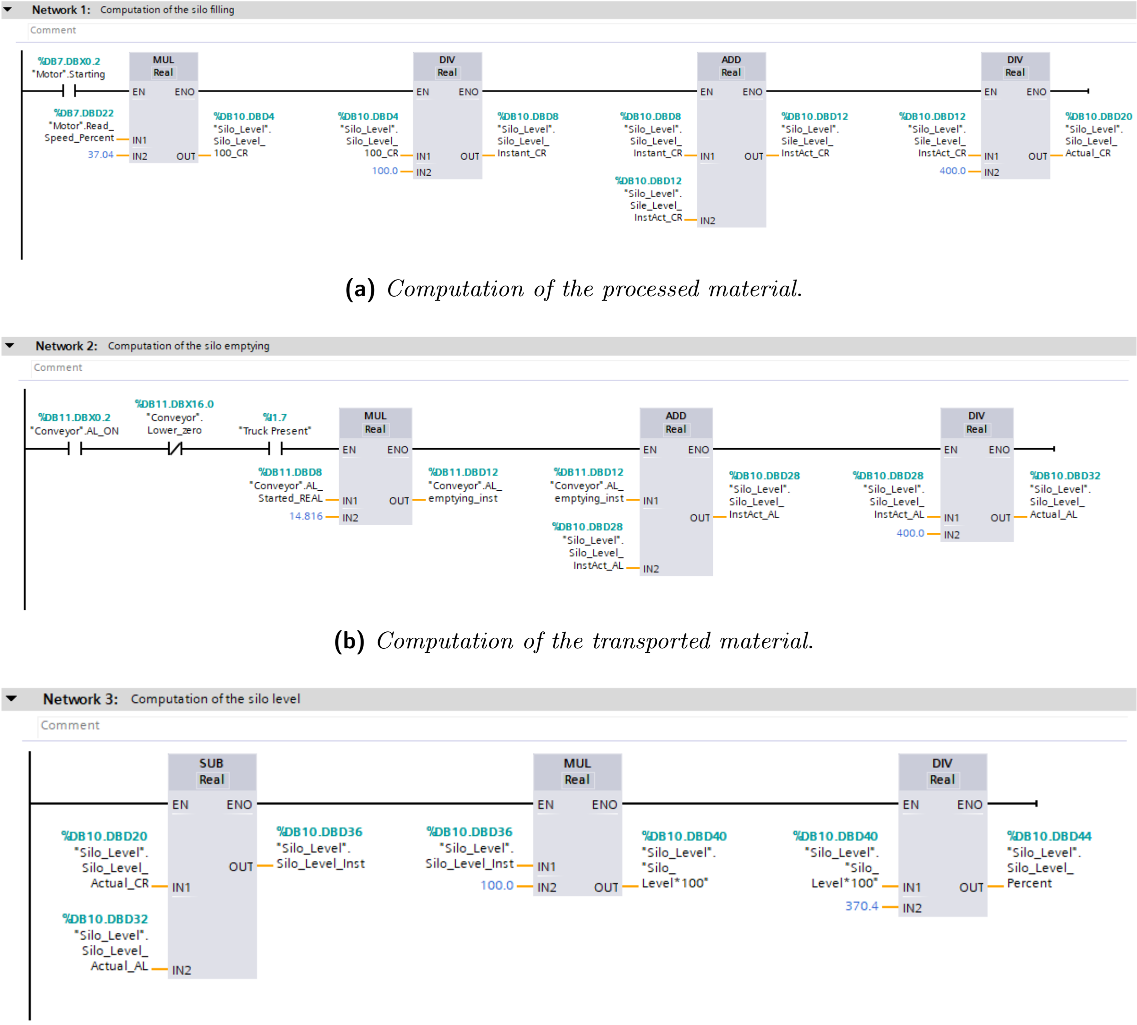
However, PLC is a digital controller and it computes operations every scan cycle. This means that the values must be converted taking into account the sample time adopted by the CPU. This scan cycle is variable due to the characteristics of the ladder program and the operations of the system, but a maximum time can be set to avoid malfunctions during functioning. This high limit has been set up to 150 ms. Hence, it follows that minimum 400 samples are executed in a single minute.

With this information, it is easy to understand the computations shown in Figures 4.5 and the following considerations can be stated.

- The crusher computations are active only when the motor is on. On the other hand, the conveyor belt calculations are active only when the machine is activated, the truck is in position and, at the same time, the silo level is not lower than zero.
- The maximum volume that can be stored is 370.4 [m^3].
- All the variables adopted for conversions and calculations are Global Data Blocks. In this way all these computations are optimized since they are performed and stored more efficiently.
- A problem of using this method is the fact that the variables are never reset and they maintain always a certain value which depends on the time in which the CPU and the two machines (the crusher and the conveyor belt) are active.

- Another possible problem is constituted by the fact that the scan cycle could be faster than expected, producing a very fast dynamic of the sytem which becomes harder controllable.

All the issues and the possible solutions regarding not only this part but the overall system are explained in the sixth Chapter.



(a) *Computation of the processed material.*

(b) *Computation of the transported material.*

(c) *Computation of the stored material.*

Figure 4.5: Ladder function blocks regarding the calculation of the silo level

4.3.2 PID controller

As it has been already stated, the main purpose of the system is to regulate automatically the silo level according to a certain setpoint selected by the operators.

SIMATIC S7-300 controllers have the opportunity to easily implement a PID controller via ladder logic and this has been the adopted solution. To control the motor speed, and thus regulate the silo level, a PID controller has been performed in PLC 1.

To implement this type of control, the 'CONT_C' instruction has been located inside a 'cyclic interrupt OB35' organizational block. This program block can be set to have faster scan cycle than the CPU normal one and, in addition, this scan is called at regular intervals during operation.

The CONT_C instruction is used on SIMATIC S7-300 to control technical processes with continuous input and output variables. The instruction implements a complete PID controller and the option of manually influencing the value of the output variable. The calculation of the values in the control blocks is only correct if the block is called at regular intervals. Hence, it is better to call it in a cyclic interrupt OB (OB 30 to OB 38).

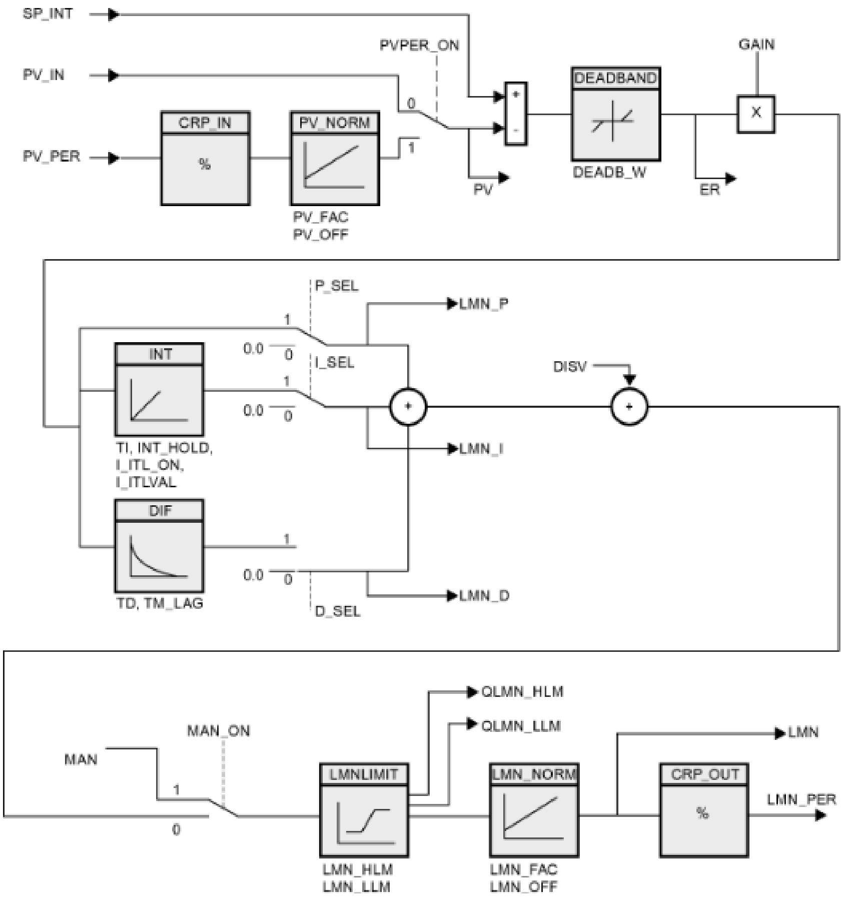


Figure 4.6: CONT_C blocks diagram

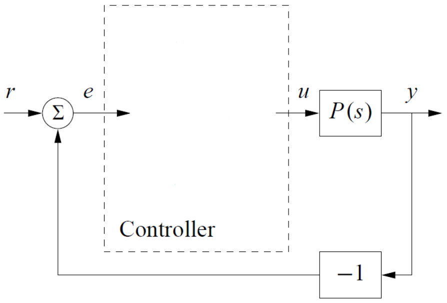


Figure 4.7: System blocks diagram [1]

From a control theory point of view, the system can be easily represented as in Figure 4.7, where *P(s)* is the plant previously described (see Subsection 4.3.1). Inside the 'Controller' area, the 'CONT_C' controller has been inserted. According to the literature of SIMATIC S7, the CONT_C instruction performs an ideal PID controller and the algorithm operates as a position algorithm. The proportional, integral, and differential actions are connected in parallel and can be activated or deactivated individually (see Figure 4.6). This allows P, PI, PD, and PID controllers to be configured.

The input/output relation for an ideal PID controller is [1]

$$u = k_p e + k_i \int_0^t e(\tau)\,d\tau + k_d \frac{\mathrm{de}}{\mathrm{dt}} = k_p \Big(e + \frac{1}{T_i} \int_0^t e(\tau)\,d\tau + T_d \frac{\mathrm{de}}{\mathrm{dt}} \Big). \tag{4.5}$$

The control action is the sum of three terms: proportional feedback, the integral terms and the derivative action. The controller parameters are thus the proportional gain k_p (indicated as 'GAIN' in Figure 4.6), the integral time constant T_i ('TI' for SIMATIC S7) and the derivative time constant T_d ('TD').

The parameters has been set according to the blocks diagram of the CONT_C instruction and the configuration is shown in Table 4.6. Several Global Data Blocks have been adopted as controller parameters and they are listed in Table 4.5.

Table 4.5: Global Data Blocks used in CONT_C instruction

Logic address	Name	Parameter	Description
DB8.DBD28	TD	TD	Derivative time constant.
DB8.DBD24	TI	TI	Integral time constant.
DB8.DBD20	GAIN	GAIN	Proportional gain.
DB10.DBD0	SETPOINT	SP_INT	Setpoint assigned via HMI.
DB10.DBD44	Silo_Level_Percent	PV_IN	Silo level in %, computed as shown in Figure 4.5.
DB7.DB30	Write_Speed_Percent	LMN	Motor speed in %.
DB9.DBD6	Actual_Level_PI	PV	Silo level internal computation.
DB9.DBD2	ER	ER	System deviation.

Table 4.6: Parameters set up for CONT_C instruction

Parameter	Data Type	Set Up	Description
MAN_ON	Bool	False	If it is set the control loop is interrupted. A manual value is set as the manipulated value.
PVPER_ON	Bool	False	If it is set, the control loop takes as input the PV_PER variable which comes directly from I/Os and it computes the percentage and normalization.
P_SEL	Bool	True	Activation of the proportional action.
I_SEL	Bool	True	Activation of the integral action.
D_SEL	Bool	True	Activation of the derivative action.
CYCLE	Time	T#100ms	Sampling time input which specifies the time between block calls.
TI	Time	DB8.DBD24	Integral time constant.
TD	Time	DB8.DBD28	Derivative time constant.
SP_INT	Real	DB10.DBD0	Used to specify a setpoint. Permissible are values from -100 to 100 %.
PV_IN	Real	DB10.DBD44	Input process value. Permissible are values from -100 to 100 %.
GAIN	Real	DB8.DBD20	Proportional gain.
LMN_HLM	Real	100.0	High saturation limit for the manipulated variable.
LMN_LLM	Real	2.0	Low saturation limit for the manipulated variable.
LMN	Real	DB7.DBD30	Effective manipulated output variable.
PV	Real	DB9.DBD6	Effective process output variable.
ER	Real	DB9.DBD2	Effective system deviation.

The Global Data Blocks stored the information necessary for the operation of the CONT_C instruction, optimizing the functioning of the controller. On the other hand, also the parameters used for the control actions (k_p , T_i and T_d) have been assigned to Global Data Blocks. In this way it is possible to use the 'Online tuning' method of the TIA Portal. Essentially, it is an online operation which allows to tune the PID parameters during functioning and, at the same time, to collect data for a simplified design of the controller.

Hence, no design of a specific controller has been carried out. In fact, no values have been inserted as k_p , T_i and T_d but they have been assigned to general Global Data Blocks in order to let the student to try different solutions.

4.3.3 S7-connections

Another important Ladder solution is the one concerning the use of S7-connections between controllers. As it has been already explained, PLC 2 has the role of collecting all the relevant data that the SCADA systems require in order to supervise and control the plant. Due to this, two S7-connections have been performed to exchange information.

At this point, it is interesting to present the adopted Ladder solution which permitted to use in a proper way this type of logic connection. Essentially, all the PLCs involved in the communication use PUT/GET Ladder instructions within their programs to send/receive data (see Figure 4.8).

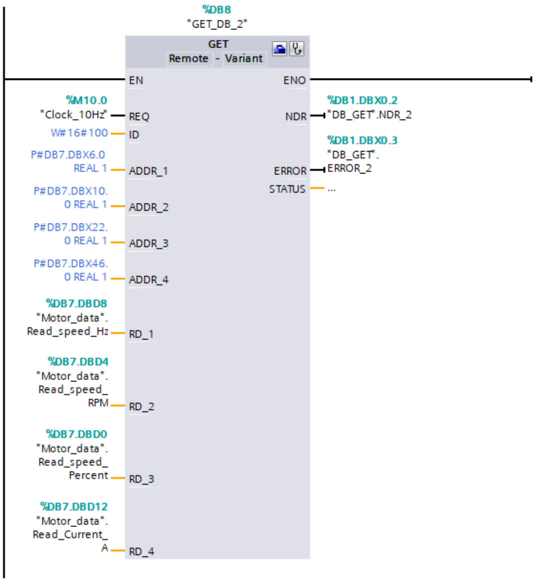


Figure 4.8: Example of GET instruction for reading motor data from PLC 1

With the instruction 'GET' it is possible to read data from a remote CPU. Differently, with 'PUT' it is possible to write data into a remote CPU. It is clear that the two instructions don't work together but only one of the two is necessary for performing data exchange. In fact, one can use a GET instruction in the CPU that has to receive the information as well as use a PUT instruction in the PLC that is storing the data and aims to write this information into the other controller.

On the other hand, the two solutions work more or less the same way, reading or writing on the basis of the setting of two parameters.

- REQ. Boolean variable that activates the instruction on a positive edge.
- ID. Word data-type that identifies the S7-connection to refer to.

As shown in Figure 4.8, the 'REQ' parameters have been assigned to a clock merker. A clock merker is an internal clock memory bit which produces a high logic level with a certain frequency (in this case 10 Hz). This choice is due to the fact that the instructions PUT/GET require a positive edge of the 'REQ' parameter in order to be activated. In addition, these data flow must be continuous as much as possible, thus it has been assigned the 10 Hz clock which is the fastest available.

For what concerns the ID parameter, the choice is unique depending on which S7-connection it is being used (see Subsection 3.3.2, in particular Table 3.3).

A central role is held by PLC 2, responsible to collect all the relevant information from the system and, also, to send the SCADA commands to the controllers. In Tables 4.8 and 4.7 are shown all the variables that this CPU read from the other PLCs (input) or write into the other controllers (output).

Table 4.7: PLC 2 output data

Instruction	Tag name	Logic address	Description
PUT (PLC 2)	AL SEL	DB3.DBX4.2	Conveyor selection.
	AL DESEL	DB3.DBX4.3	Conveyor deselection.
	CONVEYOR ON	DB3.DBX4.0	Conveyor activation.
	CONVEYOR OFF	DB3.DBX4.1	Conveyor deactivation.
	MOTOR ON	DB3.DBX0.3	Motor activation.
	MOTOR OFF	DB3.DBX0.4	Motor deactivation.
	EMERGENCY	DB3.DBX0.5	Emergency stop.
	Manual_send	MD72	Manual control value.

Table 4.8: PLC 2 input data

Instruction	Tag name	Logic address	Description
PUT (PLC 1)	Alarm word	MW0	16 bits for alarms.
	ALARM_DETECTED	DB2.DBX0.3	HMI alarms detection.
	SETPOINT	DB10.DBD0	HMI setpoint.
	Silo_Level_Percent	DB10.DBD44	Actual silo level in %.
GET (PLC 2)	MOTOR RED	DB3.DBX0.1	Motor status red.
	MOTOR GREEN	DB3.DBX0.0	Motor status green.
	MOTOR ORANGE	DB3.DBX0.2	Emergency status.
	CONVEYOR GREEN	DB3.DBX4.4	Conveyor status green.
	CONVEYOR RED	DB3.DBX4.5	Conveyor status red.
	Read_speed_Percent	DB7.DBD0	Motor speed in %.
	Read_speed_RPM	DB7.DBD4	Motor speed in RPM.
	Read_speed_Hz	DB7.DBD8	Inverter frequency in Hz.
	Read_Current_A	DB7.DBD12	Motor current in A.

For what concerns the outputs, they are the commands that the operator can use via SCADA WinCC 2008 Flexible to intervene in the process. These commands have the highest priority within the system: they are always executed, no matter in which operating mode the system is working (local, remote, manual or automatic).

On the other hand, the inputs are all the necessary information that the SCADAs require to provide a detailed overview of the system.

4.4 Supervisory systems

As it has already been explained in the previous Chapter, two HMIs and two SCADA systems have been adopted in order to supervise and control the process. Table 4.9 shows which software has been used for programming each station. The screens layout followed the concepts of simplicity and ease of operation, giving the operator only the possible functioning options according to the available sequencing. Thus, the developed process control logic has been made safer and more effective.

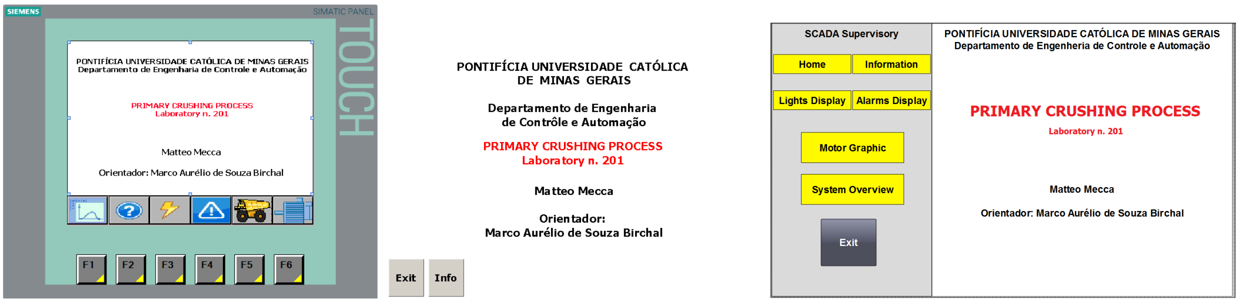
Moreover, relevant didactic information have been considered for the understanding of the project and interaction of people with it.

Table 4.9: Software used for programming supervisory systems

Device name	Purpose	Software used
KTP600 Basic Color PN	Supervisory & Control	TIA Portal
Mobile Panel 277 8" IWLAN	Supervisory & Control	WinCC 2008 Flexible
SIMATIC Industrial Field PG	Supervisory & Control	WinCC 2008 Flexible
PC of lab n. 201	Supervisory	WinCC V7.3

The following are the process screens that are in common to each supervisory system.

- Home screen. Project and developer names, as well as the university and department of belonging, are shown here.



PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS
Departamento de Engenharia de Controle e Automação

PRIMARY CRUSHING PROCESS
Laboratory n. 201

Matteo Mecca

Orientador: Marco Aurélio de Souza Birchal

(a) *TIA Portal.*

PONTIFÍCIA UNIVERSIDADE CATÓLICA
DE MINAS GERAIS

Departamento de Engenharia
de Contrôle e Automação

PRIMARY CRUSHING PROCESS
Laboratory n. 201

Matteo Mecca

Orientador:
Marco Aurélio de Souza Birchal

(b) *WinCC Flexible.*

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS
Departamento de Engenheria de Controle e Automação

PRIMARY CRUSHING PROCESS
Laboratory n. 201

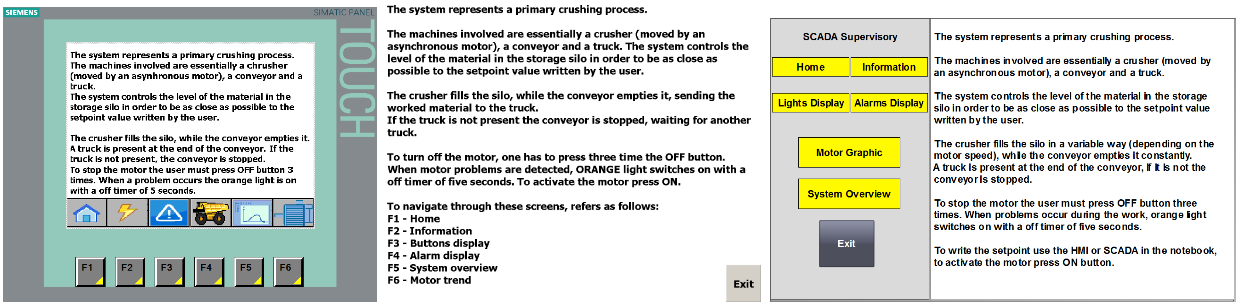
Matteo Mecca

Orientador: Marco Aurélio de Souza Birchal

(c) *WinCC V7.3.*

Figure 4.9: Home screen

- Information screen. It informs how the system works.



The system represents a primary crushing process.
The machines involved are essentially a chrusher (moved by an asynhronous motor), a conveyor and a truck.
The system controls the level of the material in the storage silo in order to be as close as possible to the setpoint value written by the user.

The crusher fills the silo, while the conveyor empties it.
A truck is present at the end of the conveyor. If the truck is not present, the conveyor is stopped.
To stop the motor the user must press OFF button 3 times. When a problem occurs the orange light is on with a off timer of 5 seconds.

(a) *TIA Portal.*

The system represents a primary crushing process.

The machines involved are essentially a crusher (moved by an asynchronous motor), a conveyor and a truck. The system controls the level of the material in the storage silo in order to be as close as possible to the setpoint value written by the user.

The crusher fills the silo, while the conveyor empties it, sending the worked material to the truck.
If the truck is not present the conveyor is stopped, waiting for another truck.

To turn off the motor, one has to press three time the OFF button.
When motor problems are detected, ORANGE light switches on with a off timer of five seconds. To activate the motor press ON.

To navigate through these screens, refers as follows:
F1 - Home
F2 - Information
F3 - Buttons display
F4 - Alarm display
F5 - System overview
F6 - Motor trend

(b) *WinCC Flexible.*

The system represents a primary crushing process.

The machines involved are essentially a crusher (moved by an asynchronous motor), a conveyor and a truck.

The system controls the level of the material in the storage silo in order to be as close as possible to the setpoint value written by the user.

The crusher fills the silo in a variable way (depending on the motor speed), while the conveyor empties it constantly.
A truck is present at the end of the conveyor, if it is not the conveyor is stopped.

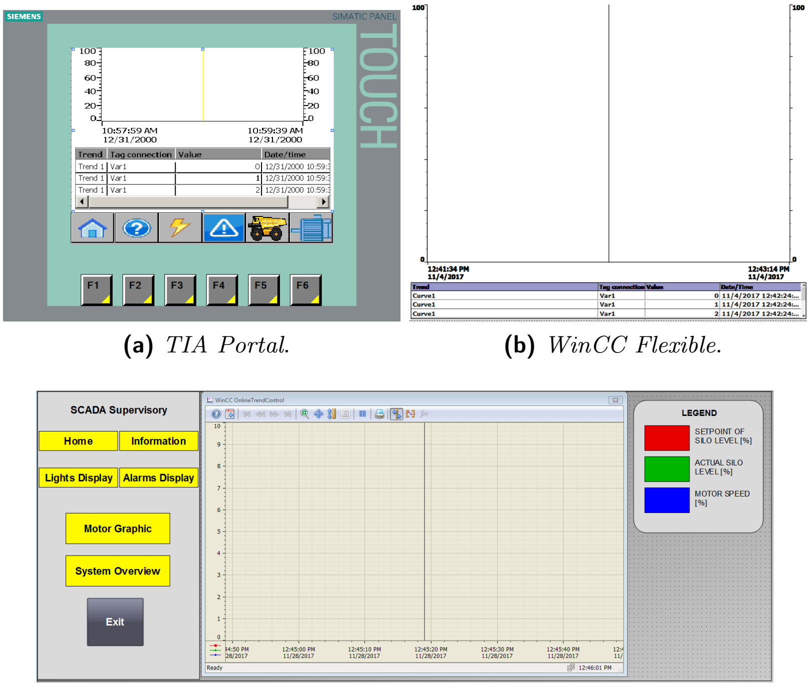
To stop the motor the user must press OFF button three times. When problems occur during the work, orange light switches on with a off timer of five seconds.

To write the setpoint use the HMI or SCADA in the notebook, to activate the motor press ON button.

(c) *WinCC V7.3.*

Figure 4.10: Information screen

- Trend screen. Silo level, motor speed and setpoint are shown in real time using WinCC OnlineTrendControl.



Trend	Tag connection	Value	Date/time
Trend 1	Var1	0	12/31/2000 10:59:3
Trend 1	Var1	1	12/31/2000 10:59:3
Trend 1	Var1	2	12/31/2000 10:59:3

Trend	Tag connection	Value	Date/Time
Curve1	Var1	0	11/4/2017 12:42:24:...
Curve1	Var1	1	11/4/2017 12:42:24:...
Curve1	Var1	2	11/4/2017 12:42:24:...

LEGEND	
🟥	SETPOINT OF SILO LEVEL [%]
🟩	ACTUAL SILO LEVEL [%]
🟦	MOTOR SPEED [%]

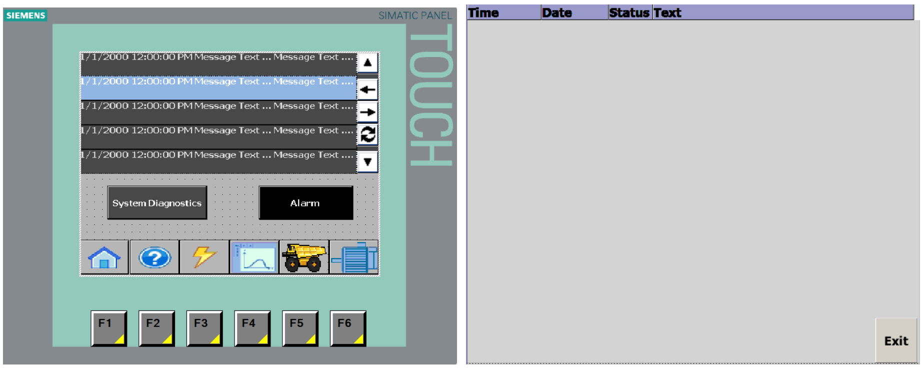
(a) *TIA Portal.*

(b) *WinCC Flexible.*

(c) *WinCC V7.3.*

Figure 4.11: Process trend screen

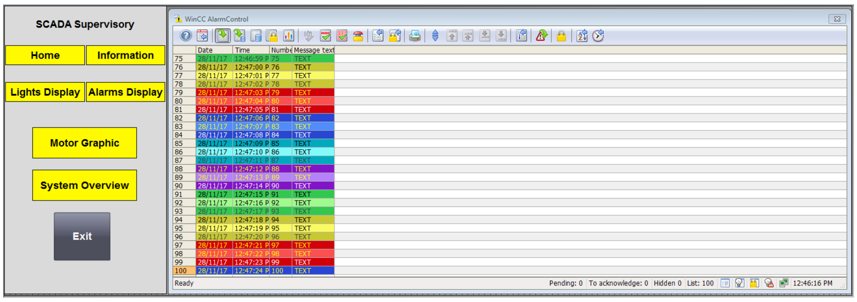
- Alarms screen. Using WinCC AlarmControl, this screen shows alarms or warning messages when the system detects problems. It can be noticed that the wired HMI presents both ‘Alarms view’ and ‘System diagnostics’, as explained previously in Subsection 4.2.1.



1/1/2000 12:00:00 PM Message Text ... Message Text ...
1/1/2000 12:00:00 PM Message Text ... Message Text ...
1/1/2000 12:00:00 PM Message Text ... Message Text ...
1/1/2000 12:00:00 PM Message Text ... Message Text ...
1/1/2000 12:00:00 PM Message Text ... Message Text ...

(a) *TIA Portal.*

(b) *WinCC Flexible.*



	Date	Time	Numbe	Message text
75	28/11/17	12:46:59 P	75	TEXT
76	28/11/17	12:47:00 P	76	TEXT
77	28/11/17	12:47:01 P	77	TEXT
78	28/11/17	12:47:02 P	78	TEXT
79	28/11/17	12:47:03 P	79	TEXT
80	28/11/17	12:47:04 P	80	TEXT
81	28/11/17	12:47:05 P	81	TEXT
82	28/11/17	12:47:06 P	82	TEXT
83	28/11/17	12:47:07 P	83	TEXT
84	28/11/17	12:47:08 P	84	TEXT
85	28/11/17	12:47:09 P	85	TEXT
86	28/11/17	12:47:10 P	86	TEXT
87	28/11/17	12:47:11 P	87	TEXT
88	28/11/17	12:47:12 P	88	TEXT
89	28/11/17	12:47:13 P	89	TEXT
90	28/11/17	12:47:14 P	90	TEXT
91	28/11/17	12:47:15 P	91	TEXT
92	28/11/17	12:47:16 P	92	TEXT
93	28/11/17	12:47:17 P	93	TEXT
94	28/11/17	12:47:18 P	94	TEXT
95	28/11/17	12:47:19 P	95	TEXT
96	28/11/17	12:47:20 P	96	TEXT
97	28/11/17	12:47:21 P	97	TEXT
98	28/11/17	12:47:22 P	98	TEXT
99	28/11/17	12:47:23 P	99	TEXT
100	28/11/17	12:47:24 P	100	TEXT

Ready Pending: 0 To acknowledge: 0 Hidden 0 List: 100 12:46:16 PM

(c) *WinCC V7.3.*

Figure 4.11: Process trend screen

4.4.1 KTP600 Basic Color PN

Being connected to PLC 1, this device can both supervise and control the process. It is located near the plant, but in a zone which is safer respect to the one where are located the machines button panels.

- Process overview screen. It displays an overview of the process where the operator can check the status (on, off, selected) of the equipment. It offers a simple and immediate understanding of the process functioning, with the possibility to select the setpoint value and check the current silo level.

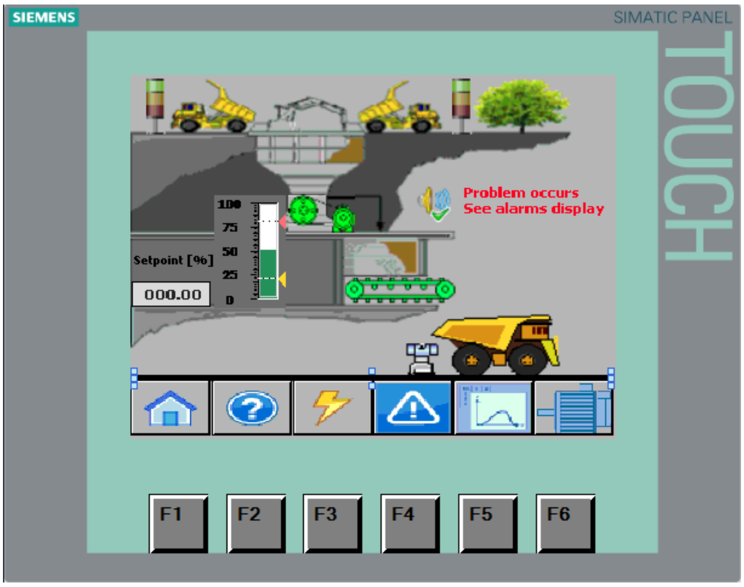


Figure 4.12: Process overview screen in TIA Portal

- Buttons screen. It shows the individual status of the motor and the conveyor belt together with the possibility to start/stop them or stop in emergency the system.

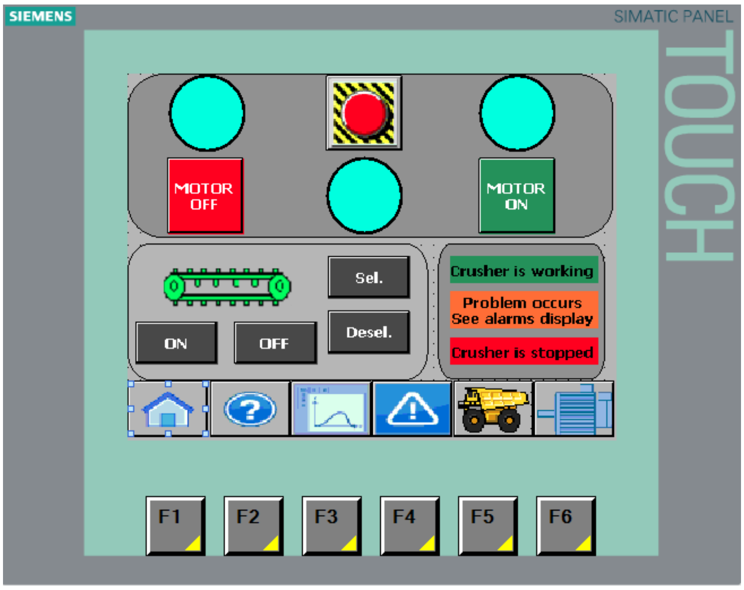


Figure 4.13: Buttons screen in TIA Portal

- Motor data screen. Motor speed (both in % and RPM value), frequency and current are displayed on this screen. In this way, the operator can get an idea of the safe operation of the machine.

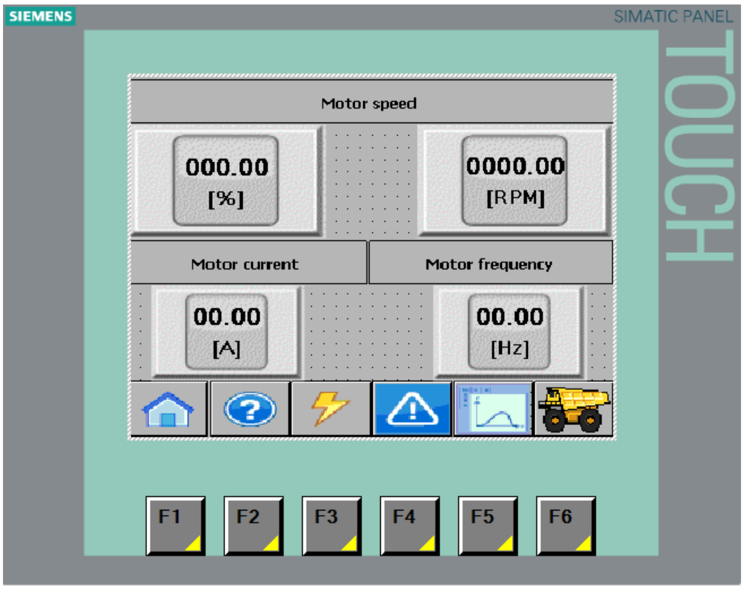


Figure 4.14: Motor data screen in TIA Portal

4.4.2 WinCC V7.3

Since it has been thought to be far away from the plant, this system is able to only supervise the process. Due to this fact, the operator is expected to know the system very well and, thus, the following screen has been created for giving a schematic and detailed overview of the process.

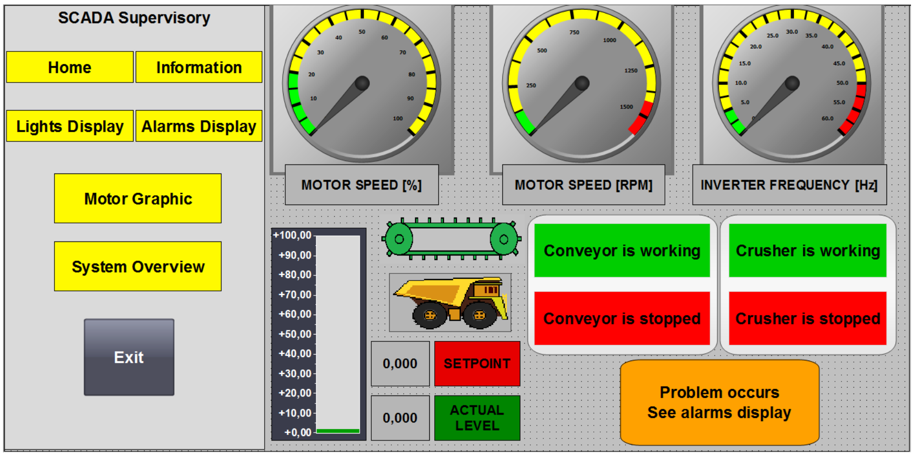


Figure 4.15: Process overview screen in WinCC V7.3

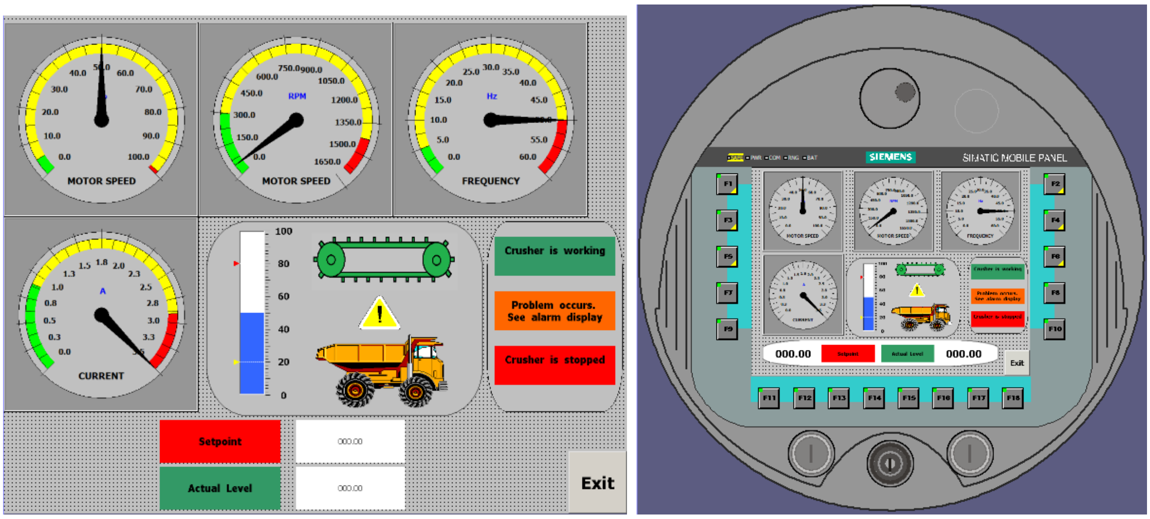
The operator can remain in this display for having a perfect knowledge of the system working and, in addition, can easily go through other screens if more information are necessary. It can be noticed that the motor data have been designed to be displayed with WinCC GaugeControl which offers an immediate and simple information regarding the safe operating zone of the motor.

4.4.3 Industrial Field PG & SIMATIC Mobile Panel

As shown in Table 4.9, these two devices have been programmed using WinCC 2008 Flexible and, due to this, their screens are very similar. Essentially these systems are intended for monitoring but also controlling the process. In particular, it has been thought that the industrial notebook was an emergency device that the operators can use for controlling the plant in some problematic situations.

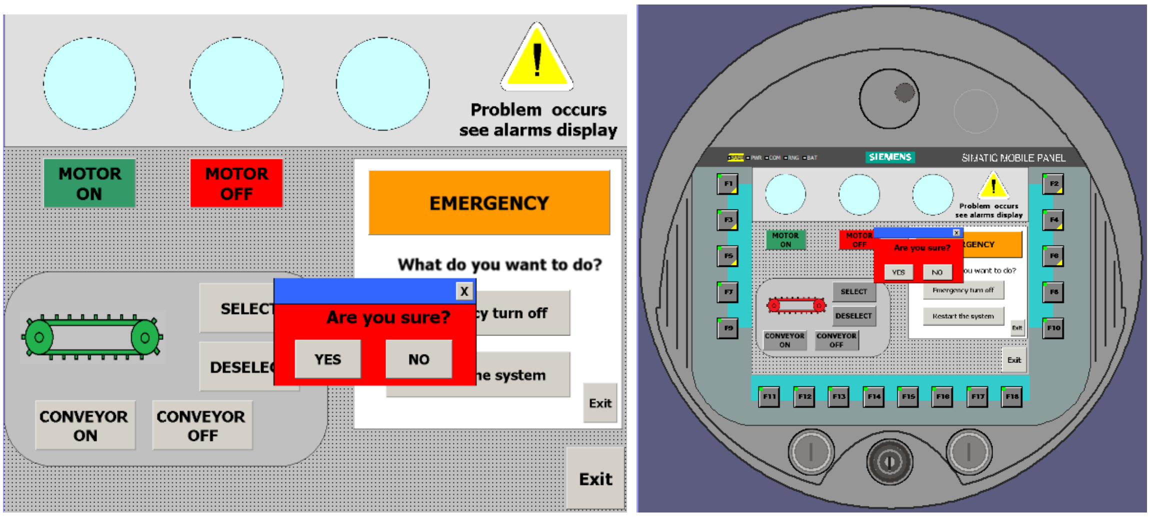
- Process overview screen (Figure 4.16). Here, exactly as in WinCC V7.3, the operator is informed about the status of all the equipment involved. In addition, there is the possibility to select the setpoint and check the actual silo level.

- Buttons screen. Since both devices can be used for controlling the process, a buttons screen was necessary. It displays the buttons to start/stop the machines as well as put in emergency stop the system. In particular, this latter instruction has been implemented with a double check window, as shown in Figure 4.17.



(a) *Industrial Field PG.* **(b)** *SIMATIC Mobile Panel.*

Figure 4.16: Process overview screen in WinCC 2008 Flexible



Problem occurs
see alarms display

What do you want to do?

Are you sure?

(a) *Industrial Field PG.* **(b)** *SIMATIC Mobile Panel.*

Figure 4.17: Buttons screen in WinCC 2008 Flexible

Chapter 5

Regulation of the water level at the laboratory n. 119

The wireless communication between PLC 1 and PLC 3 has been executed inside the laboratory n. 201 and, therefore, it was absolutely perfect without collisions or interferences. Hence, it has been decided to better test it performing a connection between two different laboratories.

This chapter deals not only with the establishment of this new connection but also discusses the use that has been done of it: design and test of a new PID controller, in order to regulate the water level in a tank located in laboratory n. 119.

5.1 Process to be controlled

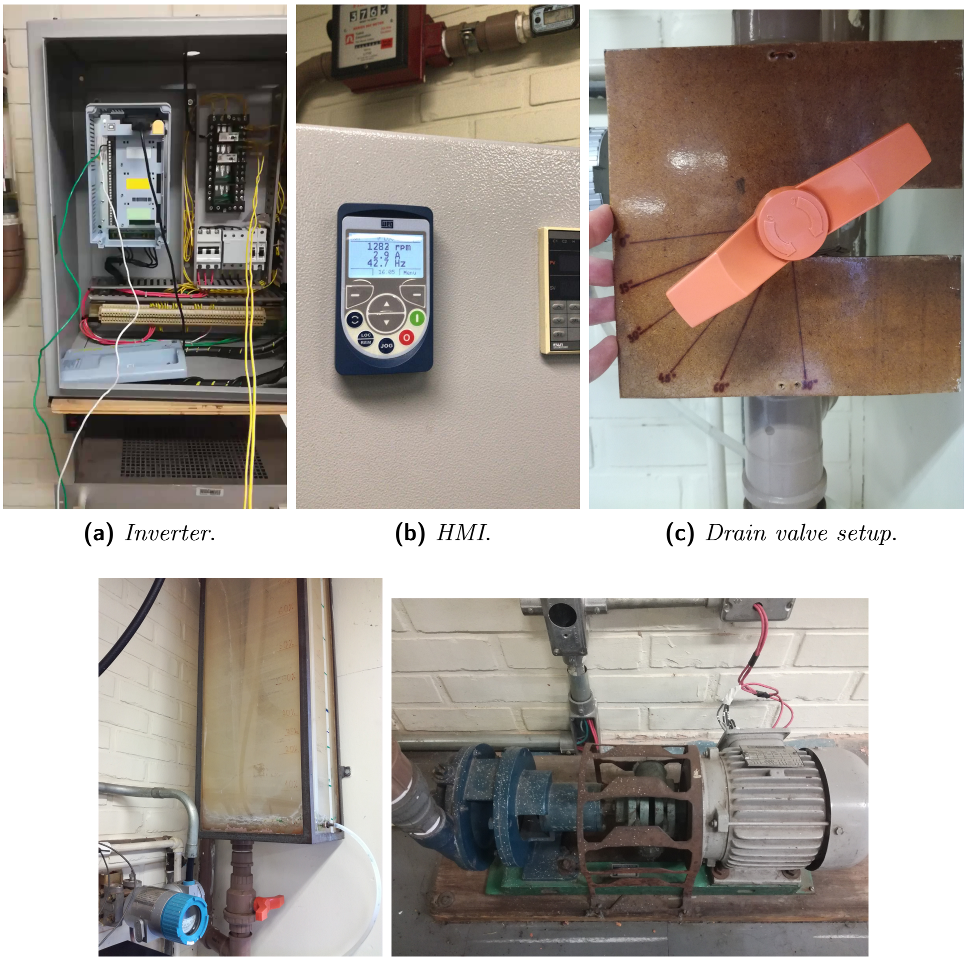
Located on the ground floor of building n. 15, 'Laboratorio de Instrumentaçao Industrial' (room n. 119) is a lab for teaching activities in the PUC Minas campus of Belo Horizonte. Respect to laboratory n. 201, this lab is located in a different building floor and the distance between the two has been calculated as more or less 30 meters of open space with two walls of separation in between.

The space is equipped with 10 PCs that have neither TIA nor WinCC installed. The most interesting part of the laboratory is a plant composed by an inverter, an asynchronous motor connected to a pump, a tank, and a pressure sensor at its basis (see Figure 5.1). The water flows in pipes (10 cm of diameter) which connect the system in a circular way with the aim of filling the tank.

Here we are not dealing anymore with SIMATIC devices, but the system was already mounted and functioning. The water level could be regulated thanks to a manual control of the motor speed using an HMI located in front of the inverter (Figure 5.1b).

The sensor pressure gives as output an analog signal of value from 4 (water level equal zero) to 20 mA (maximum level). In addition, it is present another sensor: a flow meter which displays the input flow rate in litres over minutes.

The induction motor is more powerful than the one previously used since it can rotate at 1800 rpm with a maximum driving frequency of 60 Hz.



(a) *Inverter.* **(b)** *HMI.* **(c)** *Drain valve setup.*

(d) *Tank and pressure sensor.* **(e)** *Motor and pump.*

Figure 5.1: Water tank plant in laboratory n. 119

The tank has dimensions 210x320x850 mm. Below it, an output valve which opens/closes the water recirculation is located. From a control theory point of view, this is nothing but a disturbance on the process variable (water level) and, thus, it has been decided to set it constant at 30°, as shown in Figure 5.1c, because it has been discovered to be a value which permits a good dynamization of the process. Despite the constant position of the drain valve, the water output flow is not constant because it depends on the height of the water column in the tank. In fact, from Bernoulli's principle [10]:

$$P_0 + \frac{1}{2}\rho v_0^2 + \rho g h_0 = P_1 + \frac{1}{2}\rho v_1^2 + \rho g h_1 \,. \tag{5.1}$$

Assuming that the water at the top is stationary and the height equal to h, together with the fact that the height of the output hole is zero and the two pressures P_1 and P_0 are equal, it is possible to find the water output speed:

$$v_0 = \sqrt{2gh}\,, \tag{5.2}$$

which is the well-known Torricelli's law [10].

The output flow rate can be computed knowing the section area of the hole A and the contraction coefficient K_c:

$$Q_{out} = AK_c v_0 = AK_c\sqrt{2gh}\,. \tag{5.3}$$

As demonstrated, it depends on the h parameter, which is the height of the water column in the tank [10]. This implies that for any opening of the valve there will always be a height h such that the output flow equals the input flow thus causing the water level to remain constant.

Obviously, all these equations are valid if [10]:

- The fluid is considered incompressible.
- Fluid flow is laminar (or stationary) and irrotational.
- Viscosity is neglected.

Nevertheless, the purpose now is not to check the turbulent or laminar regime of the flow. What is important is the qualitative result of the Torricelli's law: in Section 5.3 such result will be used to verify if the output flow rate changes its regime when the pump is active.

5.2 Data collection

5.2.1 Wireless communication set up

The purpose is to design a controller in order to automatically regulate the water level in the tank in accordance with a previously selected setpoint. For this reason, it has been decided to use PLC 3 of laboratory n. 201, as it was the least used, keeping all the work previously done intact. Obviously, TIA Portal was needed as well as WinCC for collecting the data which were necessary to design and test the system.

Since this laboratory was not equipped with both software, it has been mandatory the use of a PC of laboratory n. 201. Therefore, to communicate between these two labs, a wireless communication has been performed.

PLC 3 and its digital and analog modules, together with the wireless client module (Scalance W 744-1 PRO), to which it was connected, have been mounted on a single rack (see Figure 5.2).

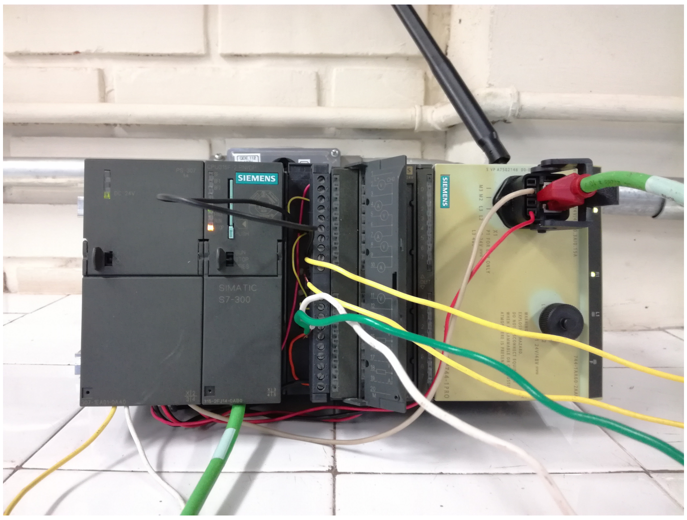


Figure 5.2: PLC 3 rack for laboratory n. 119

Respect to the previous configuration between the wireless client module and the access point (Scalance W 788-2 PRO), in which the normal antennas of 3 dBi were enough, now, due to the fact that the distance has been greatly increased and there is the presence of two walls, more powerful antennas are needed to keep the connection stable. Thus, they have been used:

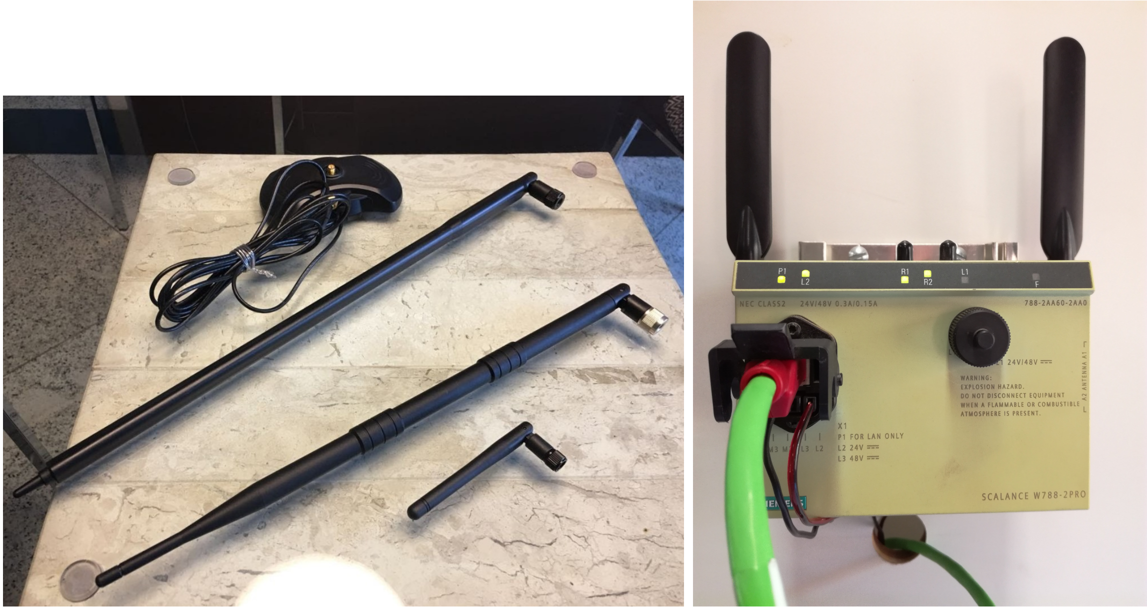
- 9 dBi omnidirectional antenna for the client module;
- 3 dBi directional antennas for the access point.

For what concerns the configuration of this communication, nothing has been modified in the TIA Portal. The network is exactly the same as the one described in the third Chapter (see Figures 3.12 and 3.13) with the only difference that now the PLC 3 and the Scalance W client module are located in another room.

On the contrary, the configuration of the wireless devices has been modified: the access point has been set up for providing a wireless communication using standard 802.11h at 5 GHz. Obviously, the other connection which used the 802.11a standard, utilized for the communication with the remote CPU ET 200 PRO, has been maintained.

This new configuration has been necessary to ensure a stable communication between the two stations that are now far more distant. It allows to have a signal strength of 25-30% in reception but with a very stable data throughput of 20-22 MBit/s. All other solutions had not such performances, especially the standards with a frequency band of 2.4 GHz, mainly due to interference from the university's local network.

The main advantage of having the same PROFInet configuration in both laboratories consists in the possibility to connect the PC (in which the TIA Portal and WinCC run) in any free PROFInet ports for detecting all the devices involved, including the rack which is now located in laboratory n. 119.



(a) *From top to bottom: 9-7-5 dBi omnidirectional antennas.* **(b)** *Scalance W 788-2 PRO with directional 3 dBi antennas (in lab n. 201).*

Figure 5.3: Antennas adopted for communication

5.2.2 Remote control for data collection

In order to collect data for acquiring information regarding the dynamic of the system, the analog output port of the PLC 3 has been linked to the inverter and the input one with the pressure sensor. Then, a SCADA program to control the plant has been created.

Obviously, for now, there is the only interest of performing a remote manual control in order to manage the functioning of the system and, at the same time, store the necessary data. 'CONT_C' instruction has been used in PLC 3. The instruction has been configured in a different way respect to what done in laboratory n. 201; the blocks diagram is the same as the one shown in the fourth Chapter (see Figure 4.6), while the new parameters configuration is reported in Table 5.1.

MAN_ON has been selected and the MAN value has been associated with a Global Data Block variable modifiable with the SCADA screen. The other relevant input is the signal which comes from the pressure sensor and identifies the water level value (PV_PER). Practically, this is the feedback of the system.

Interesting outputs to be read are LMN and PV. LMN is the motor speed selected through the MAN variable. LMN and MAN variables are equal in value but they have different meanings. The first one is the control signal that the PLC sends to the inverter for changing the motor speed, while the latter is an input that comes from the SCADA.

Table 5.1: CONT_C parameters set up for a remote and manual configuration

Parameter	Data type	Set up	Description
MAN_ON	Bool	True	If it is set the control loop is interrupted. A manual value (MAN) is set using the SCADA process screen.
MAN	Real	DB9.DBD6	Input manual value. It is the motor speed value in % that is selected manually from the SCADA process screen. Permissible are values from 0 to 100 %.
PVPER_ON	Bool	True	If it is set, the control loop takes as input the PV_PER variable which comes directly from the pressure sensor.
PV_PER	Word	DB4.DBW4	Peripheral input process variable. It is the water level value which comes directly from the pressure sensor measuring.
PV	Real	DB9.DBD14	Process variable. It is the water level normalized and in percentage.
LMN	Real	DB9.DBD18	Control signal. It is the motor speed information in % which goes to the inverter.
LMN_HLM	Real	100	High limit restriction for the control signal.
LMN_LLM	Real	0	Low limit restriction for the control signal.
PV_FAC	Real	1.261	Process variable factor. It is multiplied by the process value. The input is used to scale the process value range.
PV_OFF	Real	-36.277	Process variable offset. It is added to the process value. The input is used to scale the process value range.

For what concerns PV, a normalization has been carried out utilizing PV_FAC and PV_OFF in accordance with the blocks diagram explanation. This normalization has been necessary because the analog module of PLC 3 and the pressure sensor treated the signal in different ways. In fact, the module 'AI4/AO2 x 8BIT' (see Table 6.3) reads the input analog signal within a range of 0-20 mA. Differently, the pressure sensor provides the analog output signal in another range (4-20 mA). This difference implies unacceptable errors: it has been noticed that when the water level was 100%, the reading detected 108%. Similarly, the reading was 28.75% when the level was zero. Therefore, a simple system of equations has been solved (see Eq. 5.4) to find the values of factorization and offset necessary for normalizing the PV signal and thus having a perfect reading of it.

$$\begin{cases} 100 = 108 \cdot \mathrm{PV\_FAC} + \mathrm{PV\_OFF} \\ 0 = 28.75 \cdot \mathrm{PV\_FAC} + \mathrm{PV\_OFF} \end{cases} \Rightarrow \begin{cases} \mathrm{PV\_FAC} = 1.2611 \\ \mathrm{PV\_OFF} = -36.277 \end{cases} \tag{5.4}$$

Therefore, a specific SCADA screen has been created using WinCC V7.3. PV and MAN variables are the main values managed and, in addition, WinCC OnlineTrendControl has been used for having a graph over time of the behaviour of the system, together with the possibility of storing data both in graphic form and .csv file.

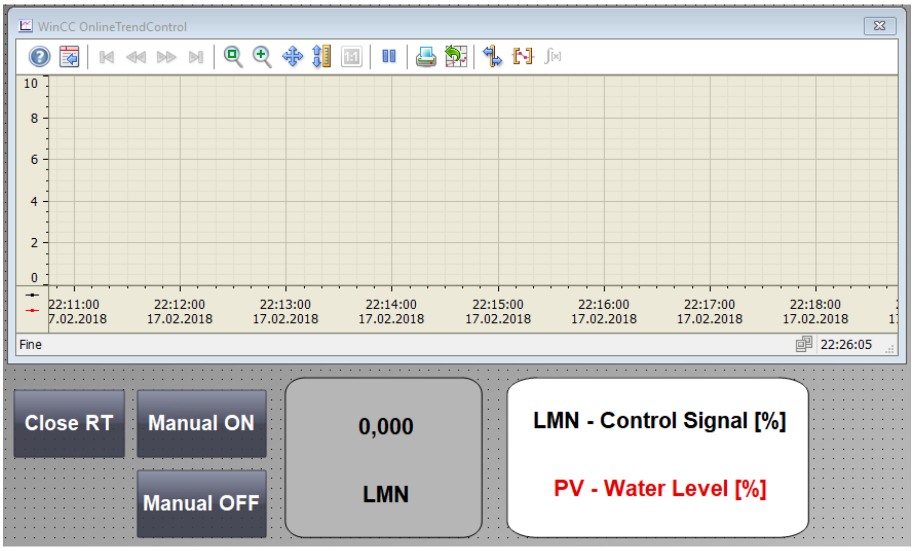


Figure 5.4: SCADA screen for remote manual control and data collection

5.3 Tests

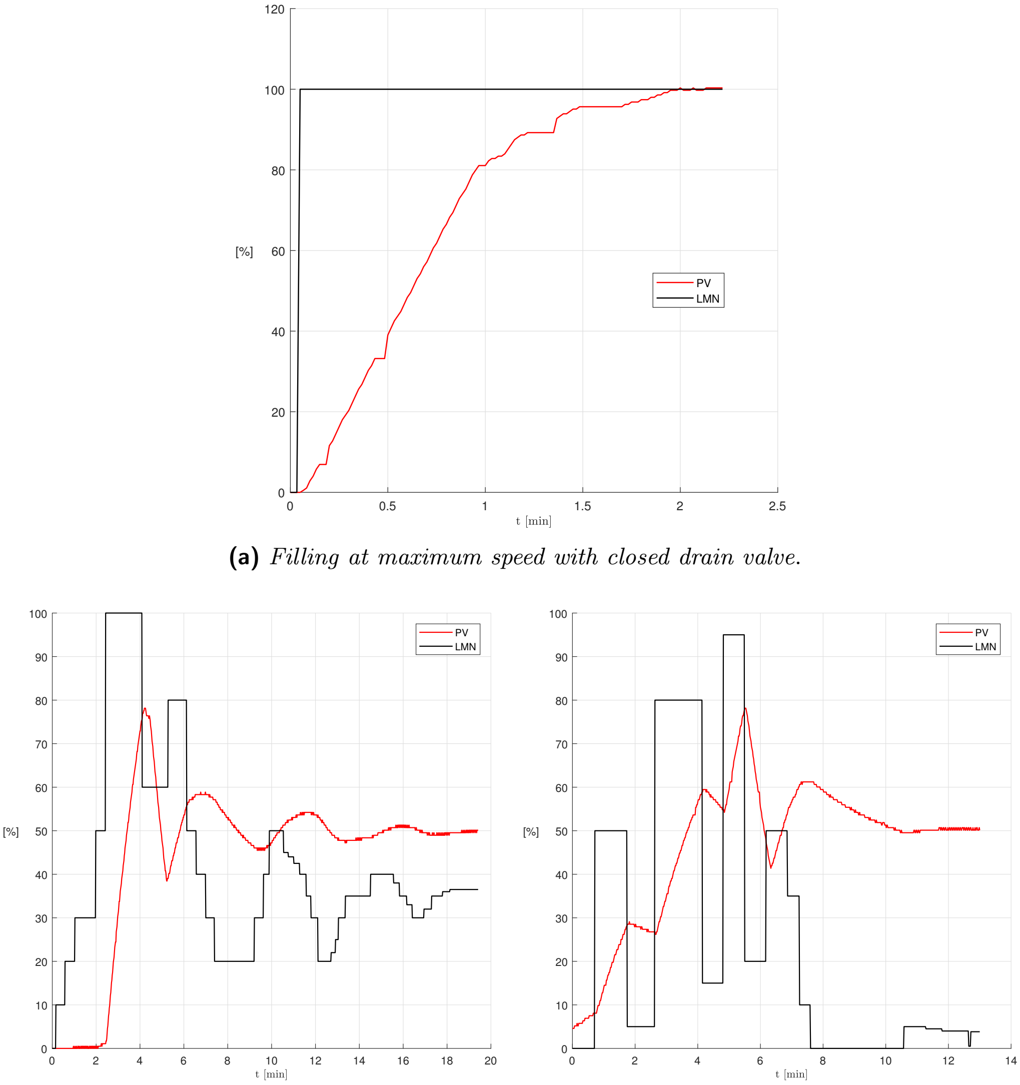
Utilizing the previously described wireless connection and the SCADA display for remotely and manually controlling the plant, several tests have been performed. These experiments had the purpose to collect data for checking the dynamic of the system and detect possible malfunctions.

5.3.1 Tests 1: air presence inside pipes

Figure 5.5 shows the first tests performed. Data has been collected using WinCC Online-Trend Control and then processed with MATLAB (version R2017b).

Figure 5.5 shows the tank filling executed at the maximum motor speed and with the drain valve closed. Here the presence of delays during the filling is interesting. While in some periods of time the filling is carried out with the same constancy, in others suddenly undergoes a considerable slowdown and, in some cases, seems that the input flow rate is no more able to fill the tank, for then restarting normally seconds later.

This issue is even more serious taking into account the successive experiments. 'Dynamic test' is just a simple test in which the control signal was varied for reaching the 50% of the water level. It has been repeated several times, but the two most important results are the ones shown in Figures 5.5b and 5.5c.



(a) *Filling at maximum speed with closed drain valve.*

(b) *Dynamic test 1.*

(c) *Dynamic test 2.*

Figure 5.5: Dynamic of the system

Essentially, in the 'Dynamic test 2', the system appears to be more reactive and without great slowdowns respect to the 'dynamic test 1'. It can be noticed that some values are completely different, so much that they seem to be two completely different systems. In particular:

- In 'dynamic test 1' is needed a motor speed equal to 50% for starting to increase the water level. On the contrary, in 'dynamic test 2' the pump is able to fill the tank even at the minimum speed value set (control signal at 0% - motor speed is 1280 rpm).

- In ‘dynamic test 1’ the 50% value of water level is reached with a 37% value of control signal. Differently, in ‘dynamic test 2’ is needed a motor speed equal to ≈ 5%.

These tests have been significant for the discovery of a problem which appears to be intrinsic to the way the system has been constructed. The highlighted slowdowns and the different behaviours in filling the tank are due to an input flow rate which varied from time to time. This variation is caused by air presence inside pipes (see the sixth Chapter for a further explanation and the possible solutions).

5.3.2 Tests 2: Torricelli’s law

Obviously, to continue with tests, it has been necessary to monitor the presence of the air inside the pipes and each time verify that the input flow rate was at its maximum value. To do this, the flow meter (to check the flow rate value) has been used, together with the use, in case of malfunctions, of a secondary drain valve located close to the pump output.

Three tests (grouped as the seconds) have been carried out increasing the control signal in a step way. Each step lasts the time which was necessary for the values to stabilize themselves. When the stabilization was completed, data are collected and the step increased. Obviously, many tries have been done in order to discover the maximum flow rate in each situation. Table 5.2 shows the results.

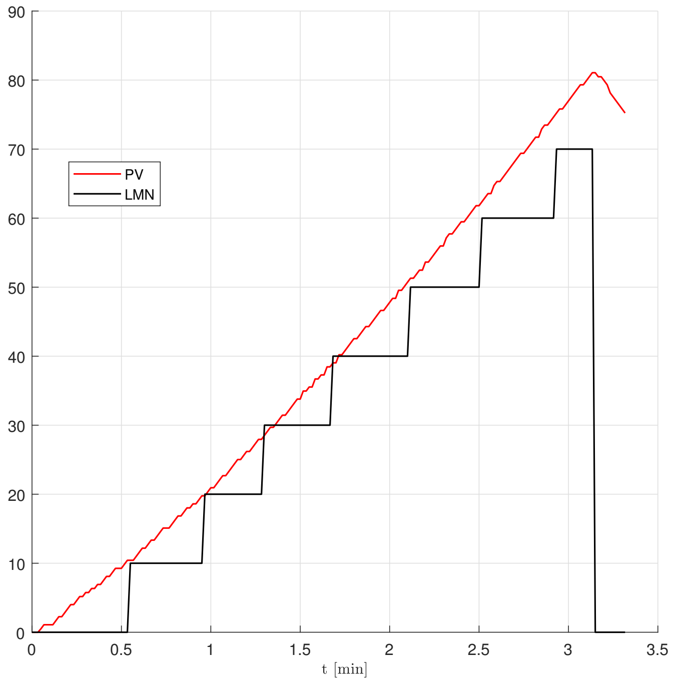


Figure 5.6: Step variation in tests n. 2

With these data, the arithmetic average of the flow rates has been computed. In Figure 5.7 are shown some interesting combinations. For instance, given the motor speed, the graph shows which is the input flow rate provided by the pump in that situation.

Table 5.2: Data collected via tests n. 2

LMN	**Motor**		**Flow rate [L/min]**		
	Speed [rpm]	Frequency [Hz]	Test 1	Test 2	Test 3
0	1280	42.7	21.5	21.5	21.5
10	1335	44.4	24.0	23.5	23.0
20	1386	46.1	26.5	26.0	26.5
30	1437	47.9	29.0	29.5	29.0
40	1488	49.6	31.5	31.5	31.0
50	1540	51.3	32.5	33.0	32.5
60	1591	53.0	35.0	35.0	35.0

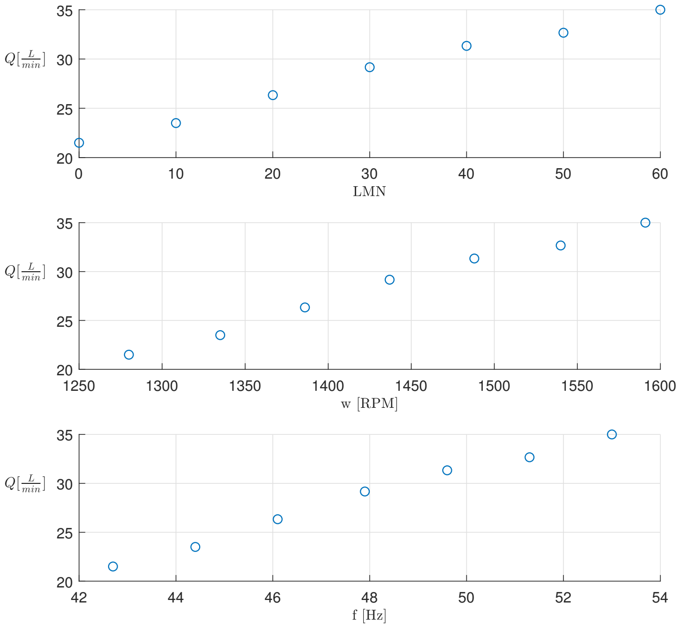


Figure 5.7: Input flow rate in different situations

Thus, knowing the input, the output flow rate has been analyzed checking qualitatively the Torricelli's law. A test has been carried out to analyze the emptying of the tank when the pump is not active and the valve open at 30°(see Figure 5.8). Following the graph, two important observations can be stated.

- From now on, the water level will be expressed in liters. The conversion is very easy and takes into account geometric dimensions of the tank as well as liquid conversion from mm^3 to liters.
- A quadratic fitting of the curve has been computed with Matlab. The function shows the relation between water level and time:

$$\text{PV} = 3.63t^2 - 33.1t + 57.1\,. \tag{5.5}$$

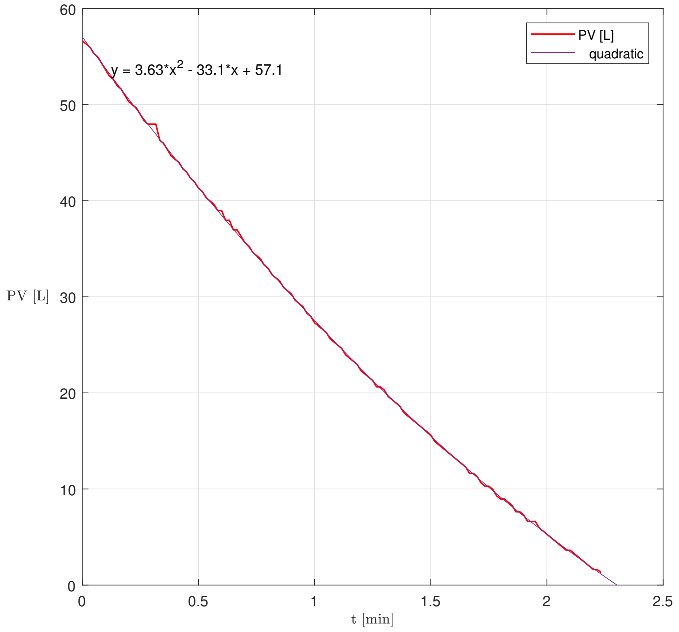


Figure 5.8: Tank emptying

With this relation, it is possible to calculate the derivative with respect to time:

$$\frac{d\text{PV}}{dt} = 7.26t - 33.1\,. \tag{5.6}$$

Eq. 5.6 expresses, according to the definition of derivative, the measure of the rate at which the water level changes with respect to the change of the time. This is a fundamental source of information because it is now possible to associate the output flow rate (which is $d\text{PV}/dt$ when the tank is not being filled) with the water level (PV) since the two relations found have the same time period of developing, expressed in minutes. Therefore, the output flow rate can be evaluated knowing the water level in the tank.

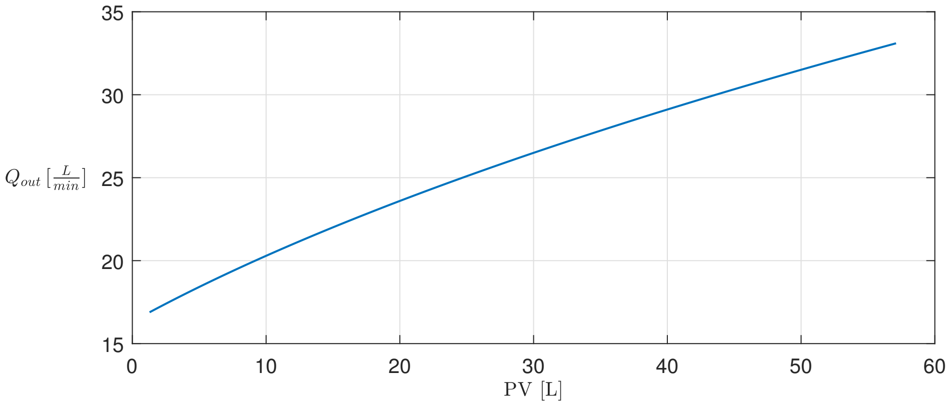


Figure 5.9: Torricelli's law

As Figure 5.9 suggests, this is nothing but the behaviour that is expected by the Torricelli's law (Eq. 5.3), obtained in an experimental way for the case in question.

Having all these information, it has been possible to check if the output flow rate followed the previous graph even during filling situations and, therefore, that the system didn't modify its flow regime from one circumstance to the other. Essentially, the verification has been carried out checking the output flow rate knowing the input and the level of the water. For instance:

1. From Figure 5.7, it is known that a control signal equal to 20% implies an input flow rate of $\approx 26.33\,\mathrm{L/min}$.
2. According to Figure 5.9, an output flow rate which equals the input one is given by $\approx 29.38\,[\mathrm{L}]$ ($\approx 51\%$) of water in the tank.
3. Thus, the level has been set to 51% and the system has been started with 20% of control signal and the drain valve open at 30°. To follow Figure 5.9, the level of the water must remain more or less at the same value.

Several tests of this type have been carried out, but all of them reported negative results. It is evident that the filling situation affects the output flow rate producing a different flow regime through the drain valve respect to the condition in which the pump was not active.

5.4 Controller design

All the tests carried out until now showed some malfunctions or situations in which is very difficult to operate due to intrinsic nonlinear behaviours of the flow. However, the second purpose of this work section is to design a simple but effective controller using PLC 3 and CONT_C instruction of SIMATIC.

Therefore, if the previous experiments were aimed at providing a better overview of the system and its operation, these last tests have been done in order to collect data for using the system identification toolbox of Matlab and then getting a Laplace transform of the plant.

Essentially, several tests have been carried out changing time by time the control signal and collecting the level values. Obviously, the input flow rate has always been under supervision to detect malfunctions due to the air presence inside pipes. These experiments were very similar to the 'dynamic tests' of Figures 5.5b and 5.5c and an example is shown in Figure 5.10.

Starting from this one and using the System Identification Toolbox of Matlab, the plant has been modeled as the following transfer function which gave the best fit (95%) respect to the process behaviour:

$$P(s) = \frac{K_p}{(1 + T_p s)}, \tag{5.7}$$

with $K_p = 0.67994$ and $T_p = 97.9118$.

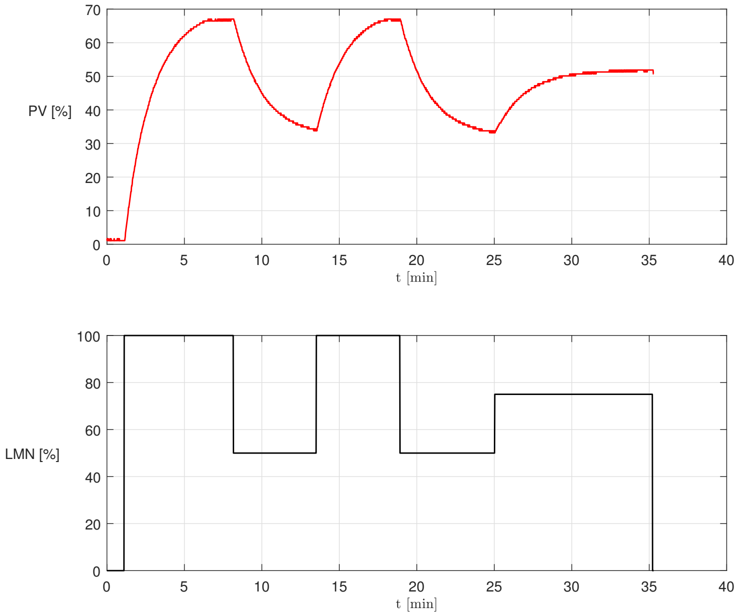


Figure 5.10: Final test for modeling the system

Obviously, the motor and the inverter have not been included in the model because the inverter has the appropriate control loop inside itself to control the engine and it is able to govern this loop by itself, according to how it was configured. Thus, P(s) is the most simple and linear identification in Laplace transform of the tank and the valve behaviours. In addition, it can be noticed that P(s) is stable, which is obvious due to the Torricelli's law, since the unique pole is located in $p = -1/T_p = -0.0102$ and has a negative real part.

For what concerns the feedback, it has been assumed that the pressure sensor is ideal (H(s)=1).

5.4.1 PI controller

Having both the plant P(s) and the feedback H(s) Laplace transforms, it has been possible to design the controller C(s). Essentially, the control action must satisfy the following requirements:

1. Keep the system stable, in particular without oscillations.
2. Have a very small overshoot ($\xi < 2\%$, which is approximately 1 liter).
3. Time requirements have not been established in details since the slowness of the plant derives from its construction. However, the control signal must drive the motor speed on time without being too slow.

To satisfy the first condition, implementation of a PI controller is enough. The proportional action produces an output value which is proportional to the current error value. A high gain implies a large change in the output but, if the proportional gain is too high, the system can become unstable [1]. On the contrary, a small gain has the consequence of producing a small output response when the error is large. In this situation, a less responsive controller is performed because the control action may be too scanty. In addition, due to the fact that a non-zero error is required to drive the action, a proportional controller generally operates with a steady-state error.

This error may be corrected dynamically by adding an integral term [1]. The integral action contributes proportionally to both magnitude and duration of the error: essentially, it is the sum of the instantaneous error over time. This term produces an acceleration of the process towards the setpoint and corrects the steady-state error described before. However, it can cause the process variable to overshoot the setpoint.

It has been decided to not implement the derivative action in order to avoid possible system instability during operation.

Therefore, Matlab SISOtool toolbox has been used to tune the controller and for meeting the specifications. A good simulation result has been obtained from the following values.

$$C(s) = K_c(1 + \frac{1}{T_i s}), \tag{5.8}$$

with $K_c = 4.37$ and $T_i = 78.3$.

The step response of the system is shown in Figure 5.11, while in Table 5.3 are listed the characteristic values of the time domain nominal performance of the closed loop system.

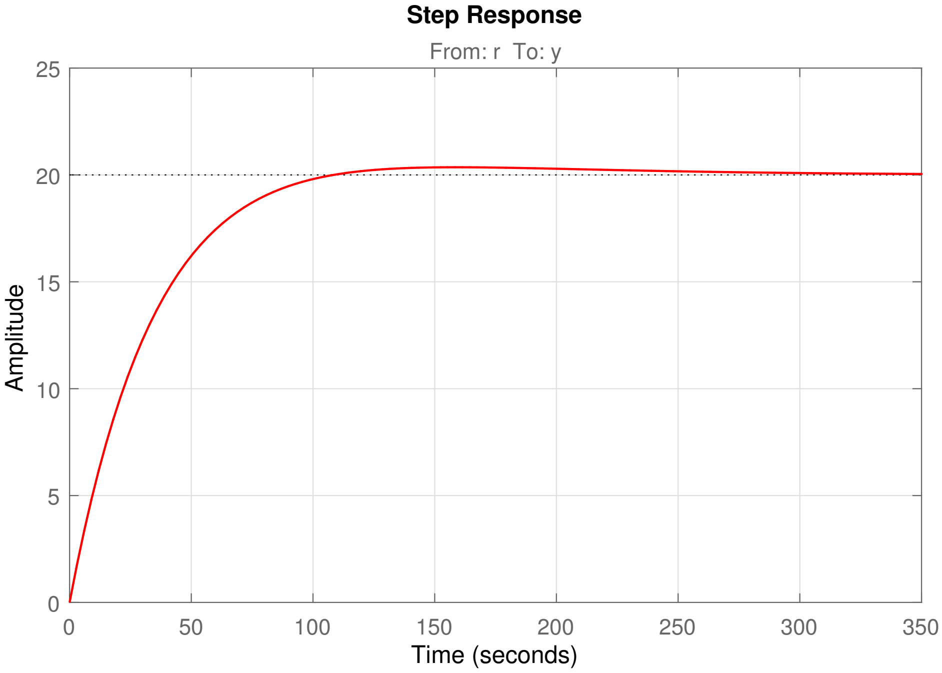


Figure 5.11: Step response of the simulated closed loop system

Table 5.3: Time domain nominal performance of the closed loop system

Characteristic	**Value**
Rise time	108 [s]
Settling time	93.336 [s]
Overshoot	1.791 [%]
Peak	20.358

For clarity, the rise time has been computed as the time that the response takes to rise from 0% to 100% of the steady-state response. Furthermore, the settling time has been considered as the time that the error (computed between response and steady-state value) takes to fall within 2% of the steady-state response.

The controller has been configured in the TIA Portal and loaded into the PLC 3. The results of the implementation are discussed in the following chapter.

Chapter 6

Results and final considerations

This final Chapter shows the results obtained in both laboratories. Furthermore, some considerations have been added together with the possible future developments of the work.

6.1 Laboratory n. 201

To briefly resume, the automated production system constructed in laboratory n. 201 has the following characteristics.

- An hybrid network, which uses copper cables, optical fiber, and wireless transmission adopting PROFIBUS, PROFInet, and AS-i protocols.
- Two network parts configured in a ring topology in order to provide redundant communication in key points of the plant.
- Three PLCs, which adopt S7 logic connections to establish communication among each other.
- Two SCADAs and two HMIs that supervise the process. They can supervise and/or control the process as well as inform the operator about several possible malfunctions.
- The system simulates a primary crushing process. The plant is in part constructed in the laboratory (the inverter, the asynchronous motor, and the crusher model are used) and in part simulated using ladder logic (simulation of the conveyor belt and the material production/storage).
- The process can be controlled by operators locally, using workstations, or remotely, with HMI or SCADA. In addition, a manual control of the motor speed has been implemented.
- PID controller is implemented in PLC 1 through 'CONT_C' instruction in order to control the process and regulate the silo level. The controller has not been tuned here, but the program is set for tuning it online, adopting the online diagnostic function of the TIA Portal.

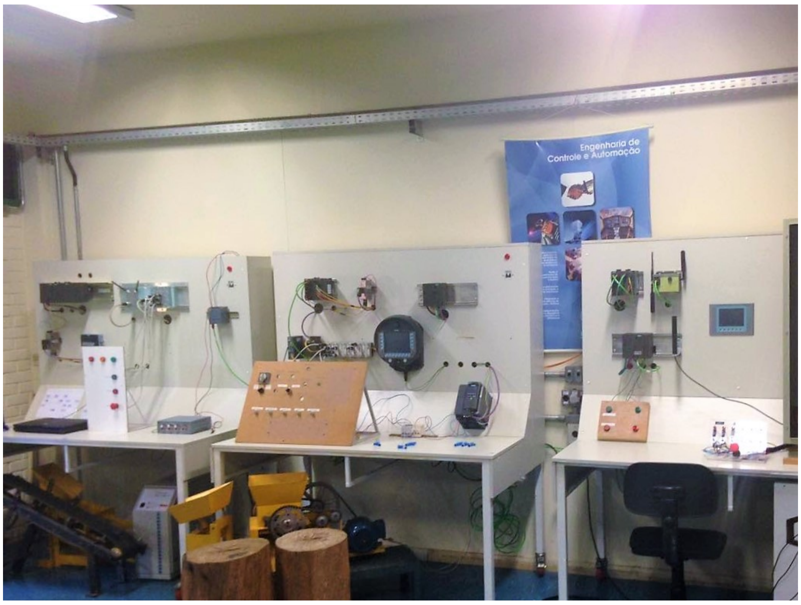


Figure 6.1: Laboratory n. 201

The construction has been carried out both from hardware and software points of view. Comparing Figure 6.1 with the initial plant shown in Figure 3.11, it is possible to notice the size of the work done.

Regarding the hardware, all stations have been mounted on racks and then on the work benches. Each wood workstation has been built by hand inserting lights, buttons and switches to manually control the process. In addition, supply cables have been welded at the ends to improve safety and avoid short circuits.

Software part has been developed using the TIA Portal and the WinCC software. Almost all the devices involved have been configured with the TIA Portal and the ladder program has been written with it. Differently, WinCC has been used to design the SCADA programs.

The system behaved almost perfectly both in terms of the process operations and, above all, of the data exchange between devices. In fact, the communication didn't undergo evident delays or problems although being forced to pass through various transmission media and network protocols. The only issue concerned the wireless communication: 2.4 GHz of band frequency went in collisions with the university internet network. Setting up the frequency to 5 GHz solved the problem. Essentially, data transmission is clear because:

- All the rules of each protocol have been carefully followed.
- No significant electromagnetic disturbances are present in the lab.
- Cables length is not too long.

Both redundant ring topologies have been tested to check the right functioning. Manager devices of the two rings worked very well: when communication faults are detected, the ring manager immediately set the new connection. In addition, they are able to automatically establish the principal configuration after the fixing of the fault.

The Ladder program is able to simulate the process without problems in any operational modes (manual/automatic and local/remote). However, it can be improved because the simulation of the process makes computations in each scan cycle and it is well-known that the PLC cycle is not fixed but can vary according to the process operations and the complexity of the Ladder program. Due to this, the system may be faster than expected and the storage silo can be filled easily in few minutes. In addition, a very fast dynamic of the process implies a harder controller design. Despite this issue, no malfunctions or bug have been detected.

Thanks to the SCADA and HMI screens, the operator is well informed on how the plant operates. A list of warnings, error messages and lights has been designed to guide the operator in case of problems.

Two other checks have been carried out with the instrumentations.

1. The SIMATIC Mobile Panel has an operational range of about 10 meters. Obviously, this value is due to the configuration of the wireless network and the antenna chosen for the access point. The range is supposed to be more meters using a band frequency of 2.4 GHz. Anyway, 10 meters is a good result which permits to remotely control the system even from other rooms.

2. The Scalance W 744-1 PRO doesn't support the PROFInet diagnostic function. This was clear after the first installation and has been confirmed by the manual [20]. Due to this fact, the wireless switch must be connected to a device that is not a controller of other stations or a remote device that needs to be supervised. Therefore, PLC 3 has been programmed to not control any remote device but only to exchange data with the other PLCs through logic connections which didn't require PROFInet diagnostic.

Last considerations about the network: this part of the work gave the opportunity to implement a hybrid industrial network and understand its functioning and connectivity characteristics. The three industrial network protocols worked in different pyramid levels allowing a vertical flow of information from the field level to the plant one. The diagnostic function has been used during the development of the project because it permitted to diagnose all the devices involved without using any additional system. Thus, this feature optimized the work during the configuration and the troubleshooting of all the stations.

An additional comment can be made on the PROFInet protocol. The figure 3.13 shows that the PROFInet network has been implemented to connect any device type from the field level (Remote CPU) to the plant level (SCADA) passing through the control and the cell levels as well. Hence, a unique network for the entire automation pyramid has been created implementing connections which used simple IP addresses and names. This is one of the principal objectives that PROFInet is trying to get from Industry 4.0 perspective: demolition of the pyramidal model, obtaining a structure where all the levels are in simultaneously communication between each other. This leads to time savings, communication, and autonomy in the production process, together with an increase of flexibility, optimization, and customization of the plant.

With this and many other revolutionary characteristics, it is not a coincidence that the industrial world is moving towards the 'Industrial Internet of Things'.

In the end, for what concerns future developments of the laboratory, the PUC Minas university has the following plans:

- Create a PROFInet network which connected all the Siemens devices located in each lab of the building. In this way, one can configure and communicate with any stations from laboratory n. 201, which will then be used as a 'configuration&diagnostic laboratory'.
- Start a collaboration with 'Associação Profibus Brasil' to use this system for their teaching activities and not only for university students.

6.2 Laboratory n. 119

As it has been explained in the fifth Chapter, the system has been modeled from a data collection (Figure 5.10), completely ignoring the turbulent regime of the flow and the complexity of the dynamic. Essentially, P(s) is a forced approximation of first-order linear system dynamics.

The PI controller C(s), found using SISOtool, has been implemented in PLC 3 via CONT_C instruction. The set up of the block in the Ladder program is shown in Table 6.1.

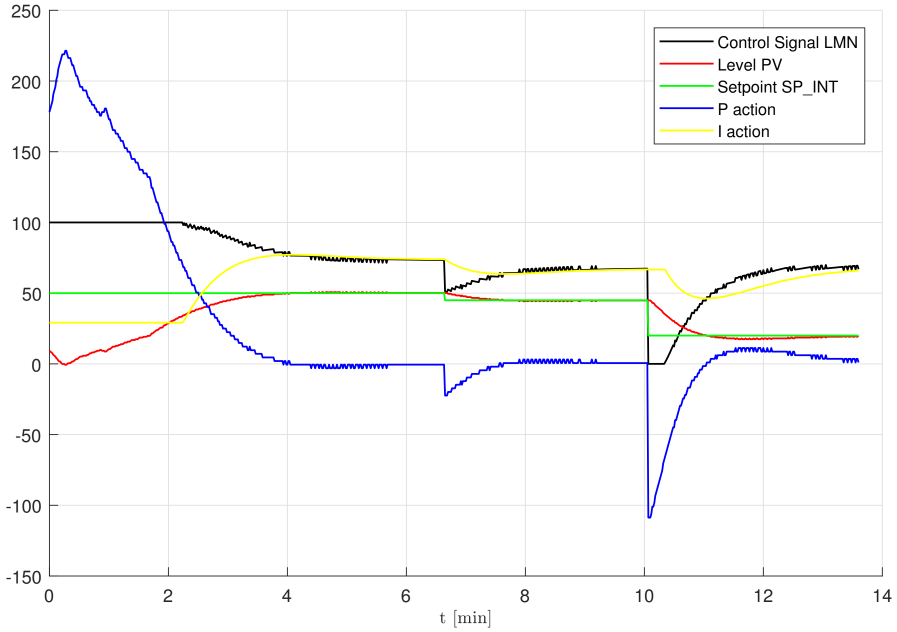


Figure 6.2: Various regulations of the water level

As output, the control signal LMN and the process variable PV have been read. In addition, also the proportional and integral actions have been plotted in order to analyze their behaviours. Figure 6.2 shows one of the first regulations where both P and I actions have been displayed.

- P action has a trend which tends to zero as the process variable approaches the setpoint, exactly what was expected to be.
- I action has a trend which tends to a constant value as the process variable approaches the setpoint. Also here the behaviour is very good and it occurs according to the high and low saturation limits which have been imposed on the control signal.

Table 6.1: PI controller set up using 'CONT_C' instruction

Parameter	Data type	Set up	Description
MAN_ON	Bool	False	If it is set the control loop is interrupted. A manual value (MAN) is set using the SCADA process screen.
PVPER_ON	Bool	True	If it is set, the control loop takes as input the PV_PER variable which comes directly from the pressure sensor.
PV_PER	Word	DB4.DBW4	Peripheral input process variable. It is the water level value which comes directly from the pressure sensor measuring.
PV_FAC	Real	1.261	Process variable factor. It is multiplied by the process value. The input is used to scale the process value range.
PV_OFF	Real	-36.277	Process variable offset. It is added to the process value. The input is used to scale the process value range.
PV	Real	DB9.DBD14	Process variable. It is the water level normalized and in percentage.
SP_INT	Real	DB9.DBD2	"Internal setpoint", used to specify a setpoint. This value is selected through the SCADA screen.
LMN	Real	DB9.DBD18	Control signal. It is the motor speed information in % which goes to the inverter.
LMN_HLM	Real	100	High limit restriction for the control signal.
LMN_LLM	Real	0	Low limit restriction for the control signal.
P_SEL	Bool	True	Proportional action is active when P_SEL is true.
I_SEL	Bool	True	Integral action is active when I_SEL is true.
D_SEL	Bool	False	Derivative action is active when D_SEL is true.
GAIN	Real	4.37	Proportional gain K_c
TI	Time	78.3	Integration time T_i

Despite the strong approximation of P(s), the design of the controller has been effective and highly simplified. According to Figures 6.2 and 6.3, the control is able to regulate the level of the water in a very satisfying way, both for increasing and decreasing the amount of water in the tank.

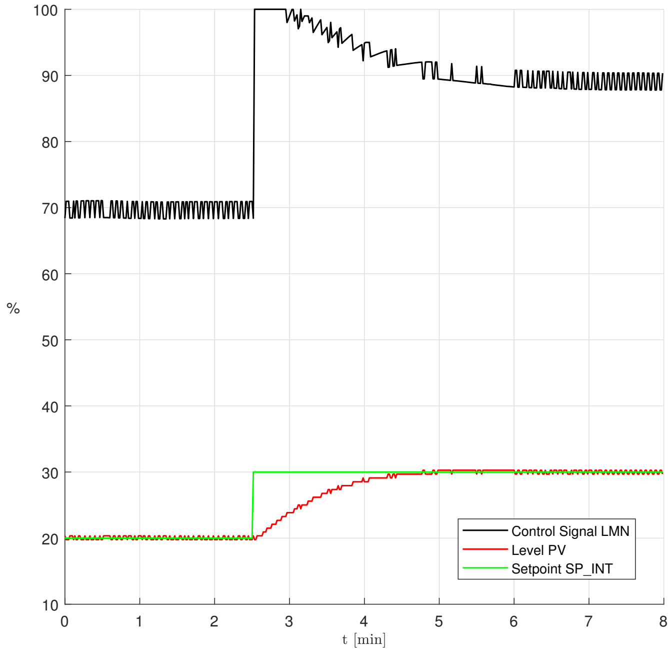


Figure 6.3: Step response

In addition, always from Figure 6.2, a small undershoot can be noticed when the setpoint forces the system to a high-level jump. This behaviour could be expected since the controller has been designed for a maximum setpoint difference of 20%.

Final considerations about the whole plant functioning have been listed in order to propose improvements which were not possible to implement due to lack of time.

1. Wireless connection was very stable but with low power (average 25% of signal strength according to the access point data statistics which regard the communication). In this condition, sometimes (rarely but it happened) the connection was missed for seconds. This is not permissible, especially in remote control situations. The communication can be improved simply using external antennas for both Scalance W since in this way the presence of the walls, which are the principal source of disturbance, is avoided.

2. For how P(s) has been modeled, it depends on the valve position. With small position changes of the drain valve the system becomes a completely different one and, thus, the controller is not able anymore to regulate the level.

3. Cavitation of the pump is a problem which decreases the hydraulic characteristics and affects the behaviour of the entire system. It is due to the fact that the tank which

collects the water and closes the circuit is at the same height of the motor-pump. According to the literature, suction cavitation can be a very dangerous phenomenon. In this case, it is mild but, in my suggestion, this part of the system has to be modified to permit the pump to operate in perfect suction conditions.

4. Air presence inside pipes has been a heavy issue during the entire work. However, the suction cavitation is in small part responsible for this problem. The real cause is shown in Figure 6.4: the pump output becomes with the same diameter of the pipe in few centimetres. This situation does not allow the flow to expand linearly inside the pipe and causes a remarkable pressure loss. However, it has been noticed that the amount of air increased when the motor was at maximum speed, obviously because the flow speed was greater and it had less time to adapt to the new diameter. A possible solution, instead of changing the entire system, is to impose a lower saturation of the control signal for not allowing the motor to rotate at 100% speed.

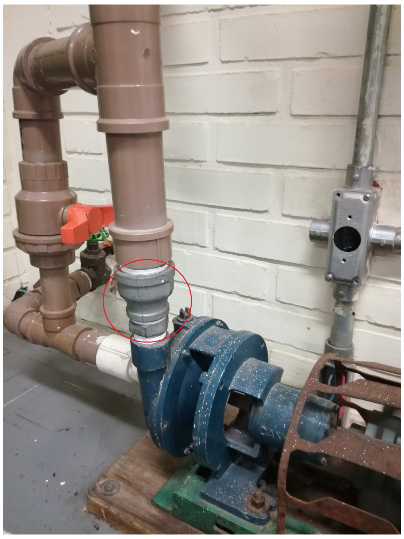


Figure 6.4: Pump output

5. The motor speed was set to range from 1280 rpm (LMN = 0%) to 1800 rpm (LMN = 100%). However, when the valve was open at 30°, the maximum water level was not reachable even with maximum motor speed. In addition, if the valve was set closer (15°), the minimum speed was not able to bring the level to zero. From these simple tests, it has been noticed that the system was very sensible to the drain valve position and a better design of the plant must be done. A solution may consist in setting the motor speed to range within other values, decreasing the minimum speed to reach the zero level in almost any conditions.

Appendix

The list of the devices used in laboratory n. 201, together with their firmware version and the description, is shown in Table 6.2. As it emerges, 23 devices have been utilized without taking into account the I/O modules installed in the various racks. Table 6.3 lists the adopted I/O modules and, thus, all the I/O points available. Considering everything, the system has 35 devices which have been subdivided into 15 stations. However, as it is clear in Chapter four, not all the I/O points have been used in the mineral crushing system.

In addition, Table 6.4 has also been inserted, it shows some network characteristics, from the used protocols until the meters of cables, in order to have a further idea of the size of the work.

Table 6.2: Devices used in laboratory n. 201

Model	**Siemens code**	**FW version**	**Description**	**Nr. used**
PS 307 5A	6ES7 307-1EA01-0AA0	-	Power supply	5
CPU 315F-2 PN/DP	6ES7 315-2FJ14-0AB0	3.1	PLC S7-300	2
CPU 1212C AC/DC/Rly	6ES7 212-1BD30-0XB0	2.2	PLC S7-1200	1
IM 154-6 PN HF IWLAN	6ES7 154-6AB00-0AB0	1.0	Remote CPU ET200PRO	1
IM 153-4 PN	6ES7 153-4AA01-0XB0	2.0	Remote CPU ET200M	1
SCALANCE X 308-2	6GK5 308-2FL00-2AA3	3.0	Industrial switch with electrical and optical interfaces	2
SCALANCE W 788-2 PRO	6GK5 788-2AA60-2AA0	4.3	IWLAN dual access point	1
SCALANCE W 744-2 PRO	6GK5 744-1AA60-2AA0	4.3	IWLAN client module	1
PROFIBUS OLM/G12	6GK5 1503-3CB00	-	Optical Link Module	2
DP/AS-i Link 20	6GK1415-2AA00	Z1.0	Converter DP/AS-i	1
MICROMASTER 440	6SE640X-1PB00-0AA0	1.0	Inverter	1
METALCORTE 84-2364	-	-	Three phase induction motor	1
KTP600 Basic color PN	6AV6 647-0AD11-3AX0	12.0.0.0	Wired HMI	1
SIMATIC Industrial Field PG	-	WinCC Flexible	Indutrial notebook	1
SCADA WinCC	-	7.3	SCADA system	1
Mobile Panel 277 8” IWLAN	6AV6 691-1DM01-2AD0	1.4.0.0	Wireless HMI	1
Total				23

Table 6.3: Inputs/Outputs available in laboratory n. 201

Rack	Siemens code	Module	Digital points	Analog points
AS-i	3RG9001-0AA00 3RG9001-0AB00 3RG9001-0AC00	AS-i module AS-i module AS-i module	8I 8O 4 I/O	- - -
ET 200M station	6ES7 323-1BL00-0AA0	DI16/DO16 x 24VDC/0.5A	16 I/O	-
ET 200PRO station	6ES7 141-4BF00-0AB0 6ES7 142-4BD00-0AB0 6ES7 144-4JF00-0AB0	8DI x 24VDC 4DO x 24VDC/2A 4AI x RTD	8I 4O -	- - 4I
S7-1200 station	-	Embedded in PLC	8I/6O	2I
S7-300 station	6ES7 334-0CE01-0AA0 6ES7 323-1BL00-0AA0	AI4/AO2 x 8BIT DI16/DO16 x 24VDC/0.5A	- 16 I/O	4I/2O -
Total		12 devices	60I/54O	10I/2O

Table 6.4: Network characteristics of laboratory n. 201

Protocol	Transmission medium	Length [m]
PROFIBUS DP	Electrical Optical fiber	9 5
PROFInet	Electrical Optical fiber IWLAN	60 5 4
AS-i	Electrical	0.5
Total		$\simeq 85$

Bibliography

[1] Karl Johan Åström and Richard M. Murray. *Feedback Systems.* Princeton University Press, 2010.

[2] William Bolton. *Programmable Logic Controllers.* Elsevier, 2009.

[3] Plinio Castrucci and Cicero Couto Moraes. *Engenharia de Automação Industrial.* Rio de Janeiro: L.T.C., 2007.

[4] International Electrotechnical Commission. *Digital data communications for measurement and control – Fieldbus for use in industrial control systems.* IEC 61158. Technical report. 2002.

[5] Ebel, Idler, et al. *Fundamentals of automation technology.* Reinhard Pittschellis, 2008.

[6] Max Felser. "The fieldbus standards: history and structures". In: (2002).

[7] Loureiro Alves José Luiz. *Instrumentação, controle e automação de processos.* Rio de Janeiro: L.T.C., 2005.

[8] Steve Mackay, Deon Reynders, and Edwin Wright. *Practical industrial data communications: best practice techniques.* Practical professional books from Elsevier. Elsevier, 2005.

[9] Luigi Mazza. *Notes on PLC programming.* Lecture notes. Torino: Politecnico di Torino, 2016.

[10] Paolo Mazzoldi, Massimo Nigro, and Cesare Voci. *Fisica vol. 1 - Meccanica e termodinamica.* EdiSES, 2002.

[11] PROFIBUS Nutzerorganisation e.V. PNO. *PROFIBUS System Description. Technology and Application.* White paper. 2016.

[12] PROFIBUS Nutzerorganisation e.V. PNO. *PROFInet System Description. Technology and Application.* White paper. 2011.

[13] PROFIBUS Nutzerorganisation e.V. PNO. *PROFInet - The Solution Platform for Process Automation.* White paper. 2015.

[14] AG Siemens. *Actuator-Sensor-Interface: System Description.* System manual. 1994.

[15] AG Siemens. *Basics of Setting up an Industrial Wireless LAN.* White paper. 2016.

[16] AG Siemens. *Communication with SIMATIC.* System manual. 2006.

[17] AG Siemens. *Industrial Ethernet Switches Scalance X-300.* Operating instructions. 2016.

[18] AG Siemens. *MICROMASTER 440. Lista de Parâmetros*. Operating instructions. 2013.

[19] AG Siemens. *PROFInet System Description*. System manual. 2012.

[20] AG Siemens. *SCALANCE W744-1PRO (Client Module)*. Operating instructions. 2005.

[21] AG Siemens. *SIMATIC NET PROFIBUS. Optical Link Module*. Operating instructions. 2013.

[22] AG Siemens. *Step 7 Professional V13 SP1*. System manual. 2014.

[23] AG Siemens. *WinCC V7.3: Working with WinCC*. System manual. 2014.

[24] Richard Zurawsky. *Industrial communication technology handbook, Second edition*. Industrial Information Technology. CRC Press, 2015.