POLITECNICO DI TORINO

Master of Science in Mechatronic Engineering

Master's degree thesis

Analysis and design of automation strategies of industrial processes

Supervisor

Prof. Alessandro Rizzo

Author

Agostino Palomba

October 2019

Contents

1 Abstract 1

2 Introduction 2

2.1 History of automation 2

3 Industrial process control 4

3.1 Organization of an industrial process 4

4 Hardware architectures of automation systems 7

4.1 Electric drives in the industries 7

4.1.1 Electric drives in the industrial processes 9

4.2 Control systems 10

4.2.1 Programmable logic controller (PLC) 11

4.2.2 Distributed control system (DCS) 14

4.2.3 Programmable automation controller (PAC) 15

4.2.4 SCADA 16

4.2.5 IIoT 20

4.2.6 Industry 4.0 20

4.3 Communication systems 23

4.4 Network in the industries 25

4.5 4-20mA transmission standard 26

4.6 Fieldbus 27

4.6.1 HART 28

4.6.2 Profibus 29

4.6.3 Profinet 31

4.7 Language programming for Programmable Controllers 33

4.7.1 Ladder logic programming 33

4.7.2 Sequential Function Charts . . . 34
4.7.3 Function Block Diagram . . . 34
4.7.4 Instruction List and Structured text languages . . . 35

5 Safety and Risk Analysis of industrial processes 37
5.0.1 Consequences Analysis in the field of industrial process . . . 41
5.0.2 IRIS tool for Risk Identification in the industries . . . 43
5.1 RAMS Analysis . . . 44
5.1.1 Relayability . . . 45
5.1.2 Availability . . . 48
5.1.3 Maintainability . . . 53
5.1.4 Safety . . . 56

6 Practical case study of automation of an industrial process 61

7 Future developments and conclusions 67

Bibliography 69

Chapter 1

Abstract

This thesis work aims to present and describe the main automation architectures adopted in the field of industrial process, starting from a brief description of the history of industrial automation and its evolution up to the present day, with the advent of Industry 4.0 and its various software technologies which allowed the various levels of the process industry to be linked together through dedicated communication networks. Furthermore, it was possible to implement solutions related to the remote management of the whole industrial process plant, such as Supervisory Control And Data Acquisition systems.

The automation itself is possible thanks to the use of components such as programmable logic devices, which through the configuration made by writing high and low level code languages or through the use of ladder logic programming, becomes possible to manage a certain number of input interfaces dedicated to the acquisition of information from various sensors available in the automation system and from the output interfaces to which will be connected the devices that must be automated such as electric, hydraulic or pneumatic actuators..

This kind of programming languages has been described and compared in order to better understand the programming logic adopted in the field of industrial automation systems.

In fact, industrial automation has led to a reduction in terms of human error, but caused the needed of redundant implementation and security mechanisms connected to the system and to each component of the process industry, with the aim of reduce or avoid the risk of accidental damage due to machine malfunction and also in order to reduce the costs and time in terms of production.

It was mentioned and described the solutions related to risk assessment and safety management.

Furthermore this kind of solutions has been efficiently explained through the application of specific analysis or mechanisms that allow us to evaluate a priori the reliability, availability, maintainability and safety of the production systems present in the process industries.

Before the conclusion, was taken into account an example of industrial process automation system, in order to explain how the process itself works and the purpose of each component of the plant. Subsequently, risk analysis was evaluated in order to apply an appropriate security mechanism dedicated to the whole industrial system. Furthermore, was evaluated the maintainability of the system taken as case study as well as possible maintenance solutions to it related.

Finally, possible future solutions applicable in the field of industrial automation, such as the use of artificial intelligence in the Industry 4.0 sector, have been evaluated.

Chapter 2

Introduction

In this chapter will be introduced the history of automation, in particular way the automation applied in the industries and it was explained the effects related to the automation of processes inside a factory. Automation term rise in order to identify everything is necessary to make work a machine or a process in an automated way. In other words, this term define a set of technologies that will replace the presence of humans in the industries [1]. In particular, the industrial automation, exploits mechanical, electronic, electrical and computer technologies, in order to manage the productive processes of the industries with the flux control of energy, materials and informations.

2.1 History of automation

From the historical point of view, automation was born with the main purpose of replacing man in repetitive or harmful tasks, with equipment capable of operating autonomously or with minimal intervention by the human operator. By merging industrial technologies typical of production processes and information technology, it aims to enable efficient information management, placing itself as a branch of modern engineering that aims to reduce or eliminate human intervention in the production of assets and services.

The forerunner of automation systems can be considered the speed regulator by J. Watt 2.1 (late eighteenth century) for steam locomotives, whose initial aim was to maintain constant speed regardless of weight towed or from the slopes of the railway. The regulator, based on the actual speed and comparing it mechanically with the predetermined one, was able to obtain the power necessary to vary the speed.

The "modern" automatic systems born at the end of the century, at the time of the industrial revolution and of the steam engines, due to the needed to have always faster and more precise machines. However, becomes also necessary mechanisms able to correct in an automatic way the factors of disturbance that altered the correct working of the machines. From the half of the twentieth century the controllers was mechanical or pneumatic devices, able to perform quite limited processing algorithms and their connection to the sensors and actuators was a complex problem of engineering. Subsequently, the mechanical and pneumatic control systems were progressively improved. In fact they have established the basis of chemical and thermal industrial control systems, using real pneumatic signals for their operation. At the beginning of the Seventies, the evolution of the electronics allowed the development of low-cost electronic devices, of reduced dimensions and

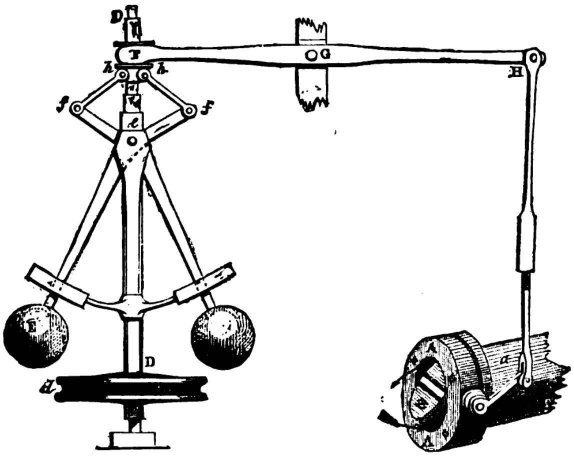

Figure 2.1. J. Watt Speed Regulatar [1]

simple replacement for the regulation and control of valves and actuators. The most important innovation was that become possible to build a single hardware product that could be adapted to different applications only modifying the software. In order to manage analog signals such as pressure, temperature and also for the regulation of chemical and thermal processes, was created the Distributed Control System (DCS) 4.2.2. Instead, for the control of electrical machines was developed the Programmable Logic Controller (PLC) 4.2.1 which are devices able to process digital signals. The purpose of the PLC, was to replace the traditional electromechanical panels which are composed by relays, timers, pulse counters or similar devices.

The increasing in terms of availability of powerful systems, versatile and at a lower cost, give rise the possibility to perform in an increasingly way advanced control functions. On the other hand, the simplification in terms of exchanging of information between the various devices of an automation system, allowed by the communication networks and by the availability of sensors and actuators able to be directly connected on a communication network, has allowed to simplify the problems of design, construction and management of an automated system and, consequently, to reduce costs.

Over the decades, the development of information technology and the advent of the Internet have brought about a very proper revolution in the automation systems. In fact, nowadays, an essential part of the world of automation and control is composed by advanced technologies such as those that oversee SCADA systems 4.2.4, fieldbus 4.6, wireless sensors, Internet of things (IOT), Cloud, virtual instrumentations, cyber-physical systems, smart sensor and solutions for the plant intelligence.

Chapter 3

Industrial process control

In this chapter will be described how the automatic process control works in the continuous production processes, and how the industrial control systems are used in order to achieve a good level of production consistency, economy and safety, that could not be achieved in case of manual human control.

3.1 Organization of an industrial process

An automation system can be described through the Computer Integrated Manufacturing (CIM) Pyramid [8] that represent a theoretical model of a production system which provide the integration of production processes, thogeter with automation systems and management information systems. As illustrated in the picture 3.1 and described in the Automation-CIM-Architecure document [3], one of the most common pyramid model provides 5 levels:

- Field level
- Control level
- Supervisory level
- Planning level
- Management level

In the modern industrial automation systems, the main advantages becomes the integration of Information Technologies in the production plant, in order to obtain the following results:

- an improvement of the production quality
- reduction of time and costs
- increasing in terms of production flexibility
- reduction in terms of waste

- compliance with laws and regulations of safety in the production processes.

So, the CIM model it's a typical hierarchic model in which provides:

- support activities at a higher level than those of production
- hierarchy within support activities
- hierarchy also within production activities. In fact, a particular mechanical processing influences the movements of the individual parts of the machine tool.
- automation of a production step such as rotation of a spindle. This is at the lower level than the automation of the whole machine (sequences of actions)

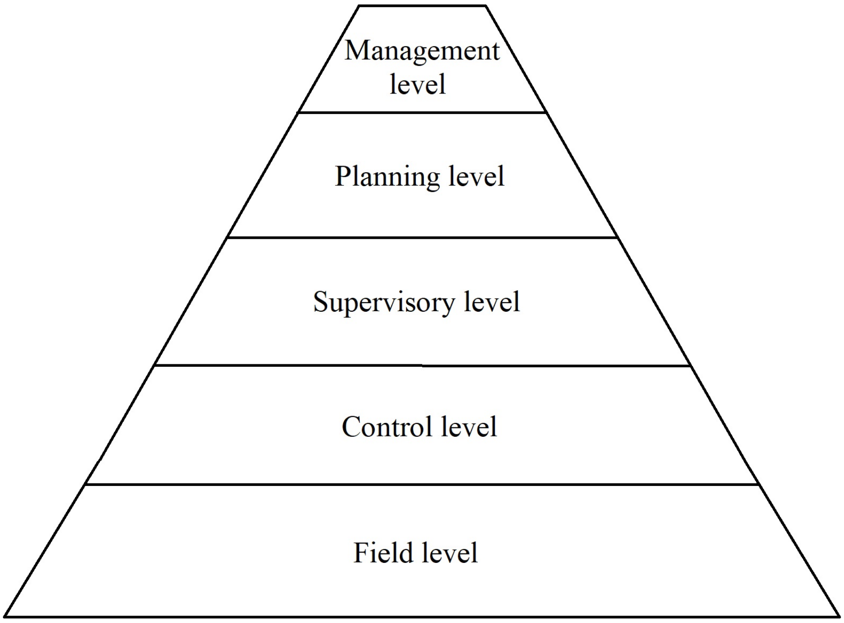

Figure 3.1. CIM hierarchy pyramid [2]

Even the control systems that implement the automation of the various levels are composed by a hierarchical structure. Furthermore, each level of this model involves in specific functions such as:

- acquisition, manipulation and information transfer
- strategies elaboration
- implementation of the developed strategies.

This architecture is defined as modular, in fact communication is allowed in either ways horizontal and vertical. As described in the CIM Domcumentation of UNIRO [3], for the field and machine level becomes necessary a specific dedicated hardware that allows a direct control by using digital systems able to solve tasks in real time. On basis of the absolved functions in the production systems, becomes possible to identify 3 fundamental kinds of automation system components, such as:

- sensors - which the main purpose is to measure and evaluate the advancement and/or the correct course of the work in progress of the industrial process.
- controllers - which on bases of information obtained from the sensors and on the basis of the objectives of the work in progress, decides the actions that must be taken.
- actuators - which are able to perform the actions controlled by the controllers.

So, the instrumentation adopted to design in abstract and in formal terms, the control algorithms used to perform the action or movement in the industrial process, are identified as Automation methods. Instead, the development of physical devices used to build sensors, actuators and controller, is identified as Automation techniques.

Chapter 4

Hardware architectures of automation systems

This chapter aim to describe the automation architecture adopted in a hierarchical structure such as that of industrial automation systems. Furthermore will be described the essential functions at each level of the CIM pyramid, the communication systems adopted in the industries and will be described the main functionality of the control devices and their language programming. Will be also mentioned the differences between automatic control and supervisory control. Moreover, this chapter also provides an exposure to the technologies that enable operation and control of modern industrial machines and systems.

4.1 Electric drives in the industries

On basis of Automation technologies, there is the drive which is typically electric and its located on the level 0 of the CIM Pyramid said field level and connected with the section immediately above, where it depends on the process control units, from which it receives the command signals and reference and to which it sends the measurement signals and other kind of alerts.

This device is capable to convert electric energy in mechanical energy with the characteristics of rotation speed and torque selected by a command signal in according to the CEI C.642 standard. The main purpose of a drive is to move or actuate a certain mechanical load in a controlled manner. The drive consists of an electric motor, which converts the electrical power supplied by a controlled power supply into mechanical power. The power supply is composed by a power unit, which provide to transfer electrical energy from the network to the motor, and a conversion and control unit that allows to regulate the electric power necessary to the electric motor to maintain the desired speed and torque. The conversion and control unit usually operates through a feedback which is based on the measurements that coming from the motor. So, the unit increases or decreases the electrical power supplied by network so that, independently of variations in terms of mechanical load moved by the drive, the motor deliver speed and torque, as close as possible to the values selected by the command signal. The measurements taken by the motor and used used as a feedback for the control system, can be either mechanical such as the rotation speed and the position of the motor shaft, or electrical, like the motor power supply voltage and the current absorbed from the motor. In alternative way, there are drives which are regulated without no feedback where the mechanical quantities are estimated starting from the electrical quantities using mathematical models rather than using sensors. The drives can be classified in according to the type of power supply such as direct or alternate current, with control feedback or without feedback and by the motion, such as linear or rotational.

In the industrial processes, the drive represents only one of the components of a system, in which includes other devices and drives that require coordination of operations. In this case, the exchange of information becomes crucial and it is essential to define the characteristics of the data to be exchanged and the ways in which they are processed, in order not only to allow the process to works correctly, but also to guarantee compliance with any rules and compatibility for future upgrades also in case of products with different brand. Notice that in the automation processes, drive systems perform different tasks with different levels of performance and coordination, in relationship to the different applications described below.

Drives controlled by motion controllers

These are single-axis or multi-axis servo drives, equipped with configurable and programmable boards, adopted to achieve a predetermined sequence of movements within a given work cycle. Typical functions are considered all the general applications in which the coordinated movement between crankshafts must be guaranteed. These drives do not require a particular precision in terms of speed, such as is needed in machine tools or industrial robots.

Continuous industry automation

Continuous industry automation identify the continuous and large-scale production lines like rolling mills, paper mills or textile fixing lines, in which a large amount of motors and drives are adopted to determinate a continuous and regular product flow. For this reason, will be introduced different kinds of motors with different sizes, depending on what kind of material will be treated such as conveyor belts, winders and unwinders, compression rollers or mixers and the control system must guarantee the synchronism of the various actuators with respect to the reference speed of the line. Each electrical drive is generally controlled by controlling the speed or the torque and the precision of this kind of control only depends on the quality of the required product.

Discrete production lines

The discrete production lines are identified as machines adopted for the regular and continuous production of objects that require a higher level of handling such as packaging machines, packaging machines or food industry machinery or are also identified as medium-small power plants. So becomes necessary an higher flexibility, a good coordination of actuators and a synchronism of phase speed achievable by gear systems or shafts and electric cams. The production speed and its quality are considered as critical elements, as well as the processing flexibility, that is the possibility to easily modify the parameters and the coordination of the actuators in order to manage to tolerate the frequently production variations. So, the coordination level required is high and this means that will be necessary an higher level of computation.

Machine tools

In the Machine tools the axis movements are characterized by increasing demands in terms of movement speed and in terms of precision of positioning also correlated to the correct use of the sensors and to the better exploitation of the machines also in terms of dimensioning in according to the work cycles. Instead in terms of processing quality, the general requirement identified by the production speed increment, needs a good coordination between axis and spindle movements and a coordination between spindle and devices in order to change the tool. Compared to the previous case, becomes necessary further processing capabilities in order to determinate the trajectories with the use of interpolation systems.

Industrial robots

The considerations made for the machine tool regarding the speed requirements and the problems of defining the trajectories, are further complicated by the possible needed of a greater number of degrees of freedom and by the needed to compensate the variation of the load and of the inertias.

Work cells

In this case, one or more of the components described in the last three points are used in order to carry out a complete processing in which includes, as well as the individual processing machines, also additional transport, positioning and unloading elements for the machined pieces. The number of actuators increases accordingly, and in addition to the coordination elements already provided for the individual machines will be added a supervision level.

4.1.1 Electric drives in the industrial processes

Electric drives adopted in the industrial applications performs the function of speed and torque with a suitable structure and signal management. In terms of hardware, these devices are composed by a power module, which includes in addition to the motor also the static converter, the sensors and a control board that implements both the regulation functions (in analogic or digital form) and the functions of user interface, signaling, protection and diagnostics. The actuators are asynchronous or synchronous alternating current motors with permanent magnet on the rotor structure, powered by power converters based on solid state static devices. These components belong to the thyristor family with regard to the highest power band like GTO, or to the transistors family like IGBT. This devices are composed by modules diodes in parallel, starting circuits and operating sensors. For their modulation, the Pulse width modulation (PWM) technique is used in order to reduce the harmonics generated in the converter output voltage. However, in order to exploit more voltage at the ends of the inverter, was adopted the Space Vector Modulation (SVM) technique which uses the Park's transformation [38]. For the sensors, the mostly used systems are tipically optical or ultrasonic, in which are used to obtain information without any kind of contact with the part that must be measured, with the possibility to directly use the digital signal and transmit this through optic fiber, in order to reduce the problems due to the electromagnetic fields. Their current development is mainly based on modularity, in fact this allows them to be easily modified, either by separating the part dedicated to the detection from that relative to the amplifier (which takes care of analyzing the detected quantity), or by simplifying the structure as much as possible in order to allow easily modification. The input or command signals of the electric drives, such as references, set points of speed, torque or current must be strictly related to the type of application and can be supplied in analog or digital form for general use. In the latter case they may have a numerical form or can be a sequence of pulses, where in this case an additional circuit is required for the counting.

As we can see in the picture 4.1, a typical control scheme adopted for the electric drives is composed of 3 regulation rings which defines the speed, position and torque regulators.

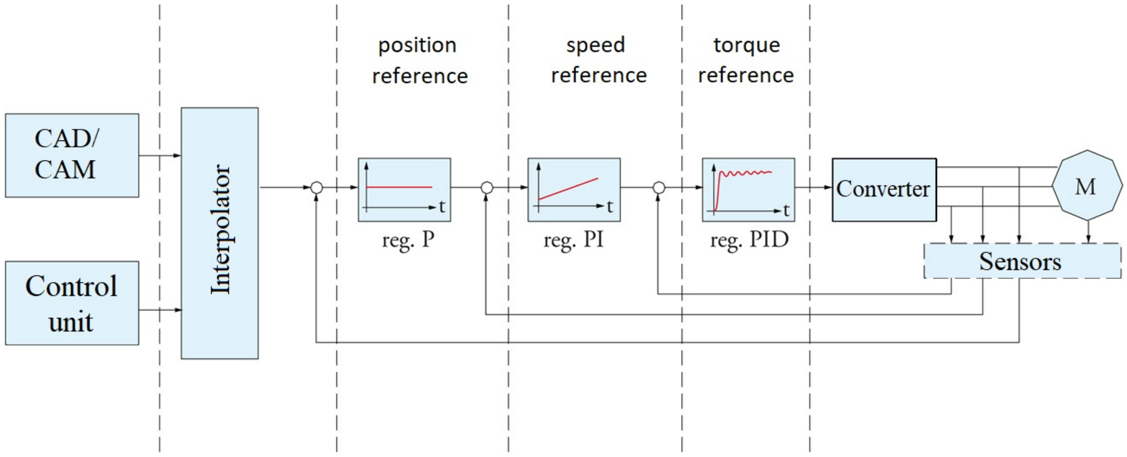

Figure 4.1. Control scheme [4]

Each of the loops described in the picture 4.1 is adjusted and activated in according to the needed and type of quantity reference. The figure 4.1 also shows the regulators, which can be either analog or digital. Their structure is typically composed by a Proportional-integral-derivative (PID) regulator with a configurable gain, compensation term, in addition to the self-calibration techniques. Regulation of axis position of the motor is not provided in the standard versions, due to the fact that this is a requirement needed for applications with either sophisticated coordination level and external interface. However, this option is often present in order to satisfy the simplest positioning requirements such as allow the inclusion of the single drive in a multi-axis movement system. The function dedicated to the position regulation, which is identifiable in the outer ring of the picture 4.1 is generally saved inside an additional electronic card. In this way becomes necessary a further ring inclusion and an additional interface situated between the output of the position ring and the speed reference. Notice that the different rings must have characteristics linked to each other. In fact, the inner loop must be faster thus with a shorter response time than the last one situated in the outer position, while the bandwidth must decrease. The consideration of a system with more rings with respect of that composed of a single feedback ring, imply that this system will be slower, making difficult to respect of the design specifications. In the picture 4.1 is shown also the control unit such as PLC 4.2.1 or something similar like DCS 4.2.2 or 4.2.3.

4.2 Control systems

In industrial automation, the Control System provide several devices adopted for the automation control process. These kind of systems, can be composed of modular controller and directly interconnected (or through a dedicated network), with thousands of field devices. As described in the Industrial control system document [7], there are different kind of control systems such as the Supervisory Control and Data Acquisition 4.2.4 systems, or Distributed control systems 4.2.2, and programmable logic controllers 4.2.1. Such devices, are extensively used in the industries such as chemical or oil and gas processing, paper manufacture, power generation, and telecommunications.

4.2.1 Programmable logic controller (PLC)

Programmable logic controller (PLC) is a particular kind of computer adopted in the industries for process automation. The PLC through the execution of an algorithm provides to elaborate analog and digital signals that coming from sensors and directed to actuators present in the industrial system. The main difference with respect the most other computing devices is that the PLC are developed and adopted for more severe conditions such as dust, heat, cold, while offering extensive input/output (I/O) to connect the PLC to sensors and actuators. PLC input can also include simple digital elements such as limit switches, analog variables from process sensors such as temperature and pressure, and more complex data such as that from positioning or machine vision systems. The PLC output can also include elements such as magnetic relays, electric motors, pneumatic or hydraulic cylinders, solenoid valves, or analog outputs. The input/output arrangements can be built into a simple PLC, or the I/O modules can be external and attached to a fieldbus or to a computer network that plugs into the PLC device.

Over the time and with the progressive miniaturization of electronic components and with the decreasing in terms of costs, the programmable logic controller also entered into the domestic use, installing a PLC inside the electrical panel after the Differential thermal magnetic circuit breaker. This kind of device, adopted for the domestic use, permit the automatic management of the multiple systems and systems installed in the house such as LAN, lights or heating, alarm and irrigation systems. So, as I have introduced above, the PLC is composed of modular hardware and its extreme robustness guarantee the possibility to normally place it in electrical panels with a lot of electrical interference, with high temperatures or with a big level of humidity. In some cases the PLC operates for 24 hours a day, 365 days a year, on industrial systems that can never stop. The structure of the PLC is adapted in according to the process that mast be automated. In fact during the design of the control system, are chosen the electrical devices suitable for the electrical quantities involved in the system that must be automated. Then, the various cards are inserted on the BUS or through the installation into a PLC rack. The first PLC was created by Dick Morley in the 1968 under the *Modicon* brand and now is owned by the Schneider Electric Company. The first action that the PLC takes, is to read the signal form the input ports which can be digital or analog, on board or field bus inputs. This signals becomes from the sensors which are needed to get information from the automation system. After reading all the inputs, their status is stored in a memory which is called *Input image register*. At this point the command instructions are processed sequentially by the CPU and the result is stored in the *Output image register*. Finally, the content of the output image is used to activate the outputs or is written to the physical outputs. Since the processing of the instructions is continuously repeated as a cyclic process, the time that the controller takes for a single processing is called cycle time in which is usually included between 10 and 100 milliseconds.

The PLC architecture 4.2 is composed by a power supply unit, the CPU that in some cases can be composed of an internal or external RAM, ROM, EPROM or EEPROM memory, a certain number of digital input cards and digital outputs 4.3. Moreover, in case becomes necessary to manage analogue quantities, the PLC can host both, analogue and digital input or output card devices. If the PLC operates in a network with other PLCs, communication card devices are needed and that must be suitable for the network protocol already implemented on the other PLC, in order to allow the correct communication between them. Instead, in case of handling operations, such as in the field of robotics, the PLC needs to host also the axis control devices, that are boards designed to manage displacements and positioning of an industrial manipulator.

The power supply unit, is a device necessary for PLC operation and it's used to supply electricity to all PLC boards. It supplies the 5V voltages required for the boards, the voltages at + or - 12V, the other necessary voltages, always in *direct current* (DC). This unit, can be internal or external to the PLC, and usually in the industrial automation field, the power supply is 24 V DC, which is also compatible with most of the sensors adopted in the industries.

The main component of the PLC is the *Central Process Unit* (CPU) or main processor, which is an electronic circuit based on a programmable logic, which carry out the instructions of a specific algorithm, in order to perform the basic arithmetic, logic, control, and input/output (I/O) operations specified by the instructions, Furthermore, this component also provides additional functionality such as a boot-loader and an additional memory dedicated to the user program, that is the automation program.

As I have mentioned before the user memory can be often external, such as in the case of EPROM memory. One of the main advantages of an external memory is due to the simplicity in terms of programming and upload of the source code. During normal operation, the CPU communicates with all the boards connected to the PLC BUS, transferring data and commands to and from the outside world (input and output).

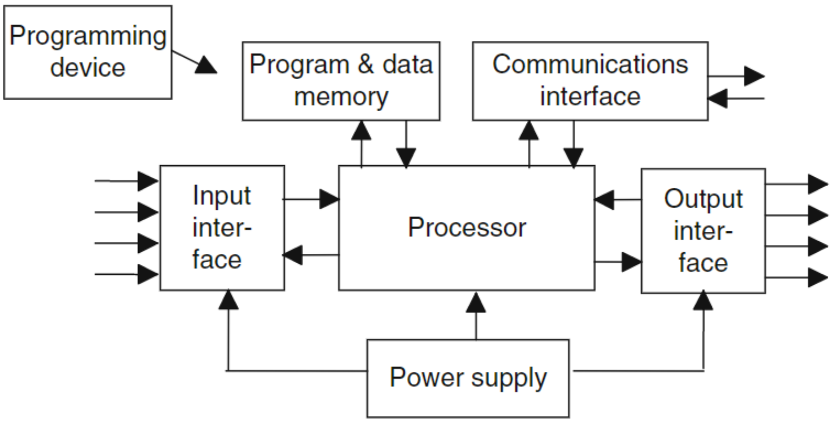

Figure 4.2. PLC Hardware Architecture [10]

One of the peculiar characteristics of many CPU is the ability to handle changes in the process management program, during normal operation. This possibility could be extremely useful in the case of systems that must always be active, such as in process control and in industrial mass production.

The functionality of the PLC has evolved over the years in order to include sequential functionality such as distributed control, motion control or process control systems. So, the most basic functions provided by the programmable logic controller are used to emulate the functions needed to drive electro-mechanical relays. Instead, the discrete inputs are provided with a unique address, and a PLC instruction can test if the state of the input is turned on or set to off. Just as a series of relay contacts the PLC is able to perform a logical AND function, not allowing current to pass unless all the contacts are closed. So a series of instructions able to examine if the status is on, will energize its output storage bit if all the input bits are on. In a similar way, a parallel set of instructions will perform the logical OR. In an electro-mechanical relay wiring diagram, a group of contacts controlling one coil that is called a “rung” of a “ladder diagram”, and this concept is also used to describe the PLC logic.

Some models of PLC limit the number of series and parallel instructions in one “rung” of logic,

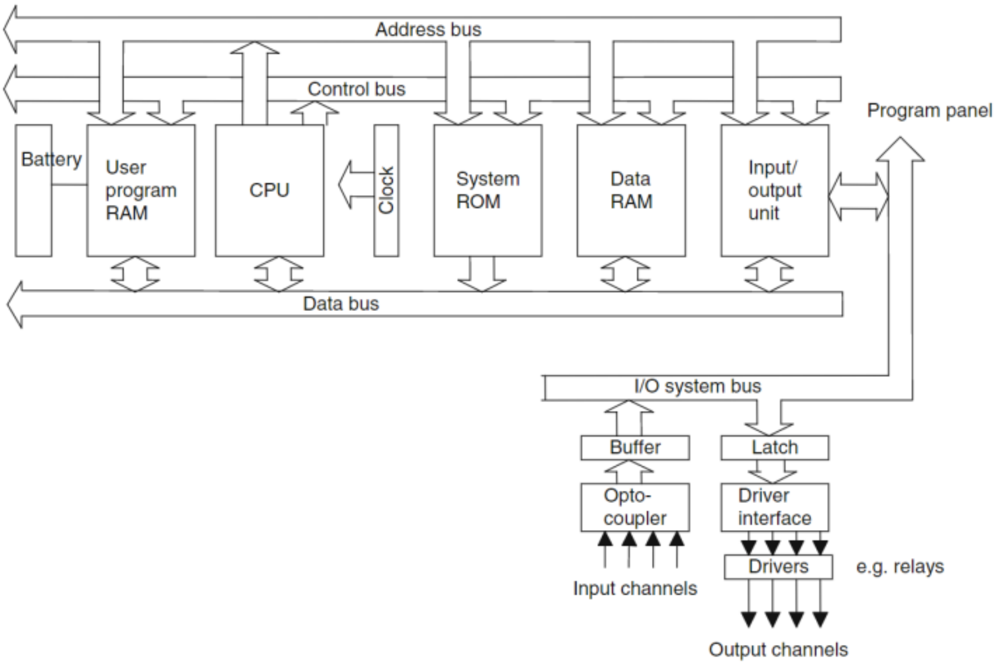

Figure 4.3. PLC Internal Architecture [10]

and the output of each rung sets or clears a storage bit, which this can be maybe associated to a physical output address or which can be an “internal coil” with no physical connection. Such internal coils can be used, for example, as a common element in multiple separate rungs. Unlike physical relays, usually, there is not a limit for the number of times in which the input, output or internal coil can be referenced in a PLC program. Furthermore, some PLC are able to enforce a strict left-to-right, top-to-bottom execution order for evaluating the rung logic. This is different from electro-mechanical relay contacts, in which in a really complex circuit may either pass current left-to-right or right-to-left, depending on the configuration of the other contacts placed around. The elimination of these “sneak paths” can be interpreted either such as a bug or a feature, depending on programming style. More advanced instructions of the PLC can be implemented as a set of functional blocks, which carry out some operation when enabled by a logical input and which produce outputs to signal, such as completion or errors, while manipulating variable internally that maybe, could not correspond to a discrete logic. Besides, the PLC can be programmed not only in elementary logic “relay” but also in advanced language such as C, C++ or even in the dedicated *State Logic* language.

4.2.2 Distributed control system (DCS)

A DCS is a control system designed for industrial process automation and which usually provide a large number of control loops, in which autonomous controllers are distributed through the whole system, with a central operator that provide a supervisory control. This is in contrast to systems that use centralized controllers such as discrete controllers located at a central control room or into the main computer. So, DCS devices increases the reliability inside the industries and reduces installation costs due to the fact that control functions are located near to the process plant, with the possibility to remote monitoring and supervision.

So, Distributed control systems was adopted for the first time, into safety critical process industries. These kind of devices was a good attractive for the industries, because its manufacturer would supply both the local control level and central supervisory equipment as an integrated package, thus reducing design integration risk. Today the functionality of DCS can be easily compared to the SCADA 4.2.4 systems, but DCS tends to be used on large continuous process plants where becomes necessary an higher level of reliability and safety, and in case of the control room cannot be remotely located.

The main feature of a Distributed Control System is its reliability due to the distribution of the control processing around the nodes of the system. This characteristic allow to mitigates a single point of failure. In fact, thank to this approach, if a processor fails, it will only affect one section of the plant process. This is different in case to a failure of a central computer which would affect the whole process. This kind of local computing power distribution to the racks that host the Input/Output (I/O) connection also ensures fast controller processing in terms of time, by removing possible network and central processing delays. The processor nodes and operator graphical displays are connected over proprietary or industry standard networks, and network reliability is increased by dual redundancy cabling over diverse routes. This distributed topology also reduces the amount of field cabling by using the I/O modules and their associated processors close to the process plant.

The processors able to receive information from the input modules, have the main purpose of process information and to decide the control actions that must be signaled by the output modules.

The field inputs and outputs can be analog signals such as 4 to 20mA or 2 state signals that switch either “on” or “off” such as relay contacts or a semiconductor switch.

DCSs are connected to sensors and actuators and they adopt a set-point control useful to control the flow of material through the plant. A typical application is related to a PID controller which is powered by a flow meter and that use a control valve as the final control element. The DCS sends the set-point required by the process to the controller which allow a valve to operate. So that the process reaches and stays at the desired set-point.

Large oil refineries and chemical industries have several thousand of I/O devices and employ a very large Distributed Control System. However, processes are not limited to fluidic flow through pipes, in fact its also possible to include things like paper machines and their associated quality controls, variable speed drives and motor control center, cement kilns, mining operations, mineral processing facilities, and many others.

This kind of control system for industrial process automation provides very high reliability applications that can have dual redundant processors with “hot” switch over on fault, in order to enhance the reliability of the entire control system.

Although 4 to 20mA has been the main field signalling standard, in the modern DCS systems its allowed also the fieldbus support digital protocols such as fieldbus 4.6, profibus 4.6.2, HART

4.6.1, profinet 4.6.3 and other digital communication protocols adopted in the process industries. In fact, the modern DCS also support neural networks [20] and fuzzy logic [19] applications.

4.2.3 Programmable automation controller (PAC)

With the PAC term, which is the acronym of Programmable Automation Controller, are identified compact or modular hybrid controllers that combine the features and capabilities of a PC-based control system with that of a typical programmable logic controller. The PACs are particularly suitable for communications that use standard protocols and network interfaces and are usually enclosed in boxes that are no larger than the PLC boxes. In this space is possible to identify an advanced microprocessor, several memory modules (both volatile and permanent), axis control modules and different communication interface models. The on-board intelligence is provided by the tools of an operating system, which is typically in real time and that is able to offer low latency times and a suitable determinism for the critical tasks use. This kind of on-board intelligence provide also an advanced application software that is usually realized on platforms of PC development and that can be subsequently downloaded to the device. The PAC devices were born when Internet was already a reality, and therefore was characterized by the fact of having already integrated networking features such as TCP/IP, SMTP and other kind of network protocols. PACs are mainly used for the same PLC applications. However they provides a more open and modular architecture. At the contrary, in general they do not have the possibility of being programmed in the “old” sequential logic typical of the PLC.

Programmable Automation Controller was founded by the ARC Advisory Group, in which this company provided five characteristics to define the PAC and that are described as follow:

- Multi-domain functionality.
- Multi-disciplinary development platform.
- Flexibility in terms of software tools able to maximize the flow process across machines or processes.
- Modular and open architecture.
- Network enterprise compatibility.

Notice that as quoted into an article written by Danielle Collins [12]:

> *“PACs can operate in multiple domains simultaneously - such as motion control, process control, sequential control, logic, data management, and communication - using a single platform. Furthermore, PACs are often used in Cartesian, SCARA, and 6-axis robot applications, which require coordinated motion across multiple axis as well as integration with other motion and data systems.”*
>
> When to use a programmable automation controller (PAC), *Danielle Collins* [11].

The PAC is able to collect, store and track a large amount of information and permit to manage the predictive maintenance and monitoring operations, storing data through ethernet network into storage devices. These devices adopt IEC 61131-3 programming languages such as sequential functional diagram, ladder diagram, function block diagram, instruction list or structured text, and some include standard PC programming languages such as C or C++. In this way, the familiarity is maintained and the learning curve for programming is low. The PAC Programming is performed in an integrated development environment called IDE in which this uses a single tag-name database, with the meaning that all defined variables are stored into a single database, which is used by all software applications, such as *Human Machine Interfaces* (HMI), ERP systems and vision applications. This method simplifies and reduces the programming work and also simplifies in terms of scaling of larger systems. So, the PAC with respect the other control systems such as PLCs are better suited for applications that requires complex controls in industrial automation such as multi-axis, coordinated motion or circular interpolation. Instead PLC are suitable for more simple applications such as of single-axis motion control.

4.2.4 SCADA

SCADA acronym stands for supervisory control and data acquisition. This definition clarifies very well the functions and objectives able to regulate the SCADA systems and which are namely referred as supervision, control and data acquisition.

Each SCADA system, in its generality, is part of an architecture that includes:

- One or more computers interconnected to each other, to which supervision and, in particular, a man-machine interface are assigned
- A series of connected units such as PLCs that are able to interface directly with the process through sensors and actuators.
- A communication network, described by a variety of transmission media and communication protocols, able to guarantee the correct exchange of information between supervisory computers and integrated units.

Instead, SCADA software means the integrated development environment, which provides all the tools needed for the implementation of a SCADA system, providing operation on supervisory computers, as well as performing the functions of SCADA systems such as supervision, control and data acquisition.

Supervision functionality is the function that selects the whole operator in order to observe the state in which a process is found and to acquire evolution by analyzing the succession of the states.

In fact, supervision is achieved through a man-machine interface such as HMI which have the main advantage to provide to the operator an immediately representation of the process, its evolution and exceptions with respect to the development of the wait.

In this sense the graphic representation is of great importance, which in fact translates the information on the state of the process into a visual language of immediate understanding for the operator.

For example, is possible to consider the status of a pump which can be represented by a graphic symbol that changes color, while the time dedicated for a specific pressure can be represented through a graphic trace and finally the occurrence of an alarm through a pop-up window.

Moreover, about the control function of the SCADA system, this essentially consists in the ability of control the system to attend in the controlled process in order to modify the evolution of the bases of some pre-established rules or decisions that are provided a “priori” by the operator.

It is important to underline how the control of a SCADA system does not means the real-time process control, normally managed by the PLC, rather than aimed at modify the same process, such as for example by sending a specific processing “recipe”.

In order to better clarify the concept is possible to say that, with as a reference to a particular process temperature, the task of real-time control becomes to guarantee that the temperature of the process remains constant by acting on the appropriate actuators, while the task of the SCADA control is to set the temperature at which the process is to be managed such as considering the set point and sending the appropriate one.

To acquire data we mainly mean the transfer of information from the peripheral devices to the supervisory computer, but also the transfer of information in the opposite direction, without which it would not be possible for the process control supervision system, or to address the purchase by operating on the values of the variables that use it.

So, for SCADA systems the acquisition of data is the main functionality, due to the fact that the process is in communication with the supervision level, supplying it with all the information on the state of the process, and also supplying a possible return for observation.

The task of data acquisition is to ensure the precise transfer of information between process and supervision, in a context characterized by a multiplicity of transmission media and different communication protocols.

SCADA software is a development environment that allows the creation of Human Machine Interface supervision applications. There are different kinds of SCADA software, offered by various manufacturers, with significant differences in terms of price and performances. The choice of which software is needed depends on various factors, as well as on own preferences, but in general it is conditioned by the complexity of the application to be used, the performance required, any constraints imposed by the customer and the availability in terms of budget.

Must also be taken into account the learning time, which is much longer, and more complex as much as more complex the SCADA software is. In general we can say that the use of complex SCADA software is justified when dealing with large and costly plants that make the cost of licenses and development times almost irrelevant. Instead, in the case of small or medium-sized plants and of a not particularly high cost, it is advisable to move towards lower cost SCADA software that requires lower learning times.

However, all SCADA software, regardless of complexity, have common features that cover the following aspects:

- Communication: development tools and driver library to communicate with electronic devices such as PLCs, regulators or multimeters, produced by the various manufacturers operating in the Industrial Automation market. It allows to define the variables to be exchanged with the devices and includes the most widespread communication protocols such as OPC, Siemens, Omron, Allen Bradley, Modbus RTU, Modbus TCP or KNX.

- Human Machine Interface (HMI): development tools and graphic libraries for building static and animated synoptics. It is important to underline the importance of graphics in the development of a SCADA application. The man-machine interface (HMI) is all the more effective, the more it is able to immediately provide the operator with a representation of the process, its evolution and exceptions with respect to the expected evolution.

- Process information: development tools to provide the operator with all the information describing the current status (online data) of the process and its evolution over time (historical data). Particularly important are the alarm management and the graphic representation of the trend of the monitored and recorded process variables over time.

- Reports: development tools to order and process the information acquired by the plant in order to generate reports for production and quality managers. The reports usually refer to a specific production lot, highlighting the characteristics and certifying compliance with the required requirements.
- Architecture: set of tools and rules for building complex architectures that provide for the existence of multiple applications interacting with each other through local (LAN) or public (Internet) networks and capable of interfacing with more local and remote operators via browser.

SCADA applications are now present in most industrial companies and represent an indispensable solution for all companies, regardless of their size and the sector of activity. The SCADA software is the ideal development environment for creating complex SCADA applications into an easy and intuitive way.

The benefits that the SCADA applications bring are different, but having to highlight one in particular we can say that they replace the man in performing many repetitive and boring tasks, with a consequent increasing in terms of productivity, better and more rapid management of alarms and drastic reduction of the risk of potentially dangerous situations for the environment. More generally we can say that the SCADA applications:

- They provide a huge amount of information. All information on the state of the plant, partly acquired directly through the sensors and partly provided by the real-time control devices (PLC), is collected, stored and made available for subsequent processing aimed at quality control, increasing efficiency and optimization of the production process.
- They offer a synthetic and intuitive view of the system. Thanks to a series of synoptics, which constitute the human-machine interface (HMI), the operator is offered a graphic representation of the entire process, its evolution and exceptions with respect to the expected evolution. In this way the information on the state of the process is translated into a visual language of immediate understanding for the operator.
- They grow and adapt easily as the company grows. The modular and flexible structure of the SCADA software makes it easy to adapt to the different situations that arise when the company needs to grow or change, to respond promptly to the challenges of a globalized market. The SCADA software offers, in particular, all the development tools that allow to intervene on the SCADA application to ensure the precise transfer of information between process and application, in a context characterized by a multiplicity of transmission media and different communication protocols.
- Allow centralized control of distributed realities. Many business realities and, in particular, public utility networks such as water or electricity systems infrastructure, are characterized by a structure distributed over the territory, which traditionally requires the permanent presence or the periodic sending of technical personnel for operating operations and maintenance. The SCADA application ensures remote control of peripheral equipment and allows technical personnel, to get access of all informations through a browser and wherever they are.

The development of SCADA applications was born in the field of Industrial Automation, as a response to the request to centralize in a single control station all the information concerning the industrial process, with particular attention to aspects concerning the proper functioning of the plant (alarm management and maintenance).

In the field of Industrial Automation, supervision finds application in the most varied sectors, from plastic to wood, from ceramics to food, from textiles to packaging, providing a series of automatic supports aimed at optimizing the production process (quality control, regulatory compliance, returns, production ratios).

In a short time the development of SCADA applications goes beyond the boundaries of Industrial Automation to extend to the Remote control of public utility networks (electricity networks, water networks, railway networks, etc.), to Business Automation (building supervision), and finally to home automation (housing supervision).

Below are mentioned a series of examples of SCADA applications.

- Supervision of low and medium voltage switchboards: the liberalization of the energy market together with the possibility of choosing differentiated and targeted tariffs make the use of a supervision system to monitor consumption and energy costs of the electrical panels of low and medium voltage.

- Quality control in heat treatment of metals: ensures quality control on heat treatments performed in a department consisting of heterogeneous furnaces (multi-chamber furnaces, tempering, well furnaces, tempering and annealing furnaces), replacing traditional paper recorders and generating reports of production.

- Testing system for wood stoves: it allows performing comparative tests on the functioning of wood stoves according to different environmental parameters, the spatial diffusion of heat is visualized through thermographic maps.

- Supervision of a spinning plant: it allows the processing of polypropylene yarns in order to guarantee that all the characteristics of the product (torsions, stabilization, title, toughness or color, perfectly correspond to the technical specifications required by the customer and can be reproduced even months later.

- Monitoring of dedicated devices for hospital environment: installed in numerous hospital and research institutes, it ensures the continuous monitoring of local or remote equipment used for the conservation of organic material and produces periodic reports for Quality Certification, in compliance with the laws in force.

- Monitoring of the level of dust pollution: it ensures continuous monitoring of the level of dust pollution detected by dedicated sensors, thus allowing intervention on the plant before the concentration limit values are reached.

- Supervision of a film production plant: applied to a plant for the production of films with a gas barrier that combines the “cast film” and “extrusion coating” technologies, it allows to control all the features of the line from a single point, characterized by by the presence of different machines and multiple control devices.

- Quality control in food production: the quality standards require that the production and preservation processes in the food industry be certified and meet specific criteria such as the system makes it possible to adapt to the legislation, limiting intervention costs and consequences on production to a minimum.

- Supply chain control in a plant for the production of ice cream: in order to comply with the regulations and protect the safety of the consumer, the system guarantees the quality of the pasteurization process, also providing a capillary control on the state of processing of the mixtures in the aging vats and ensuring the effectiveness of washing and sterilization of the same.
- Supervision of continuous and intermittent kilns for firing ceramics: guarantees repeatability and quality of production through the management of production recipes and the construction of reports at the end of the batch as well as displays the actual and theoretical cooking curves in continuous ovens and allowing to construct the cooking and air dilution curves in intermittent ovens.
- Supervision of an automatic island for heat treatments: the material to be treated is combined with its processing recipe and placed on one of the waiting benches. Then it is sent to the reclamation, cementing and tempering processes, optimizing the charges based on the availability of ovens.

4.2.5 IIoT

The IIoT acronym of Industrial Internet of Things refers to all those technologies that make it possible to transform any object adopted in the industries, such as sensors, actuators and also automation devices like PLC, into devices connected to Internet and in which they are able to send its data or informations to the cloud through the use of light and fast protocols like the *Message Queue Telemetry Transport*(MQTT) [18].

The increasing in terms of necessity to adopt cloud applications has allowed SCADA technologies a further evolution, in particular way allowing these systems easily to integrate with the Internet of things in the industries. In fact, SCADA systems can increase the potential of the Industrial Internet of Things.Moreover, through the integration of these two technologies, becomes possible to collect and verify the informations acquired in the industrial process in a faster way and through safer mechanism granted by the cyber security protection.

Due to their architecture, these systems are particularly suitable for managing:

- Remote maintenance, control and diagnostics.
- Monitoring and control of machine in terms of working conditions.
- Monitoring in terms of energy and water consumption and with the aim of reduce emissions.
- Quality control at the level of the production system and related processes.

These systems include the main enabling technologies known as KET [17] of Industry 4.0 in which are SCADA, IoT, cloud, big data and cybersecurity features. These technologies are able to perfectly meet the guidelines approved in the National Industry 4.0 Plan.

4.2.6 Industry 4.0

As described in the *"Industria 4.0: storia, significato ed evoluzioni tecnologiche a vantaggio del business"* [13], *"Industry 4.0: The Digital German Ideology"* [15] and in the *"Industria 4.0: cos'è e quali sono i vantaggi"* [14] articles, the Industry 4.0 term was chosen to indicate the integration of some new production technologies adopted to improve working conditions, create new business models and increase the productivity and the quality in terms of production of the industrial systems. This term, was firstly adopted by Henning Kagermann, Wolf-Dieter Lukas and Wolfgang Wahlster in a meeting of the 2011 in Hannover, in which they announced the Zukunftsprojekt Industriy 4.0 as a German government project, that was an inspiration for an *european initiative* in the industries. Starting from the first Industrial Revolution, will be mentioned all the evolutionary steps in the industrial field up to the present day, in particular way, focusing on industry 4.0 4.4.

The first Industrial revolution corresponds to a revolution in terms of manufacturing with respect to the use of energy such as the invention of the steam engine, that has allowed the factories to introduce a mechanization of production in the name of greater speed and power.

The second Industrial revolution has represented the second generation in terms of energy, linked to the use of electricity as first and then of oil making it possible a further increasing in terms of levels of mechanization and production. In fact, thanks to this kind of "renewed power" that the manufacturing gradually establishes the assembly line that inaugurates the era of mass production.

The Industry 3.0 instead, summarize the entry into the factory of the first generation of ICT such as information technology and electronics that had allowed a further increasing of automation levels not only in terms of production but also in terms of organizational. Moreover, the infrastructures are diversified and new processes are started thanks to the progressive digitalization, which has diversified and facilitated the work of people also improving the production quality.

Starting from 2011, begins the fourth Industrial revolution, that with the inclusion of a technological mix of robotics, sensors, connection and programming, represents a new revolution in terms of production and working organization. This append tanks to new models of production that are increasingly automated and interconnected between them, intelligent and communicating assets and products, traceability and traceability of processes that lead a collective information management, new service logics aimed for cloud and mobility technologies. All focused on a last generation Internet such as the Industrial Internet, which is capable of bringing more information inside and outside the factories, moreover allowing also more integration, interaction and efficiency, renewing processes and systems but also bringing new rules of communication and service. So, this new generation software on the one hand and Big Data Management on the other, is how production in the industries can reach a mass customization.

This revolution, if compared with the previous ones, introduce the use inside the industrial production systems of the "enabling technologies" such as KET [17], that was mentioned in the previous section and which is the acronym of *"Key Enabling Technologies"*. This kind of technological solutions or improvements, contain a lot of research and development activity and are able to "revitalize" the industrial production system, with the meaning that by exploiting these solutions the processes related to the industry will be equipped with a fast, clear and direct interconnection between all company assets, moreover with a huge increasing of productivity and a decreasing in terms of waste.

The enabling technologies that conventionally characterize the Industry 4.0 are:

- Advanced robotics - like interconnected machines, rapidly programmable and equipped with artificial intelligence.
- Additive manufacturing as well as 3D printing and digital manufacture.
- Augmented reality such as wearable devices through which to experience a plan of reality superimposed on ours.

- Horizontal/vertical integration which is referred to all the steps of the value chain, from the producer to the consumer, communicate with each other.
- Simulation, which means the possibility to simulate new processes related to productive activity before putting them into practice in reality.
- Internet of things applied to industry as well as recognizable and intelligent objects *"things"* that are able to communicate data about themselves.
- Cloud, which is referred to the management of large amounts of data directly through the network.
- Cyber-Security, that guarantees the security during all the network operations and on cloud systems.
- Big Data and Analytics, that consist of analyzing a large amount of data stored into specific databases and which are used for real-time production of information and that are useful for optimizing products and production processes.

The implementation of these new technologies requires a paradigm shift. We are facing a transition from the old factory concept to the new intelligent factory (smart factory), characterized by a digitalized production, which works in a dynamic and smart way, composed of more fluid and interconnected processes, and from production systems adapted to modernity and its needs, capable of making the best use of available resources.

As it was mentioned before, it is possible to say that the fourth industrial revolution is characterized by the introduction into the production system of intelligent machines, interconnected with each other and connected to the internet, which allow complex analysis through Big Data and real-time adaptations. In concrete terms, the benefits of the revolution that is sweeping the productive ecosystem are described below:

- Greater flexibility through the production of small lots at large scale costs.
- Greater speed from prototype to mass production through innovative technologies.
- Increasing in terms of productivity through shorter set-up times, reduced errors and downtime.
- Better quality and less waste through sensors that monitor production in real time.
- Greater competitiveness of the product thanks to greater functionality deriving from the Internet of things.

By connecting all the assets involved in the logistics-production chain, the primary advantage of the Industry 4.0 paradigm is certainly the availability of all relevant information in real time. Obtaining reporting from the data at any time and the support necessary to overcome any production bottlenecks is not an aspect to be underestimated. The connection between people, things and systems, creates a huge added value in terms of cost reduction, availability of information in real time and interaction between resources. Not surprisingly, the companies that have already introduced enabling technologies within their plant, estimate a relative percentage in terms of increasing in production efficiency due to the use of these new technologies. In fact, to realize the advantages derived from the fourth industrial revolution, participates also the government, which takes care of promoting the innovation process and that has launched a huge amount of money in favour of those companies, who have decided to invest in the industry of the future.

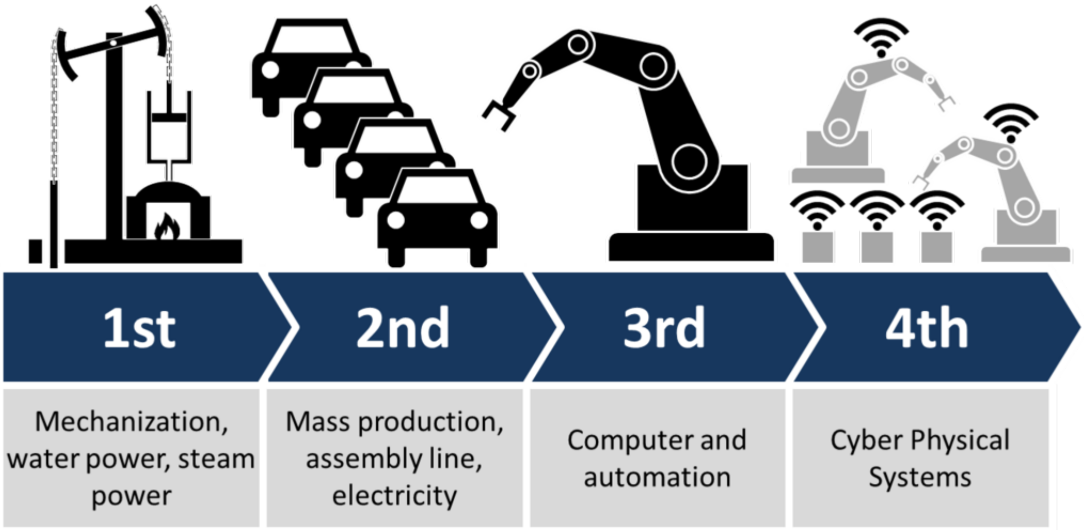
1st
2nd
3rd
4th
Mechanization, water power, steam power
Mass production, assembly line, electricity
Computer and automation
Cyber Physical Systems

Figure 4.4. Industry 4.0 By ChristophRoser, AllAboutLean.com, via Wikimedia Commons [15]

4.3 Communication systems

As mentioned in the SIMATIC Siemens documentation [36], the communication networks are the main component of the modern solutions in the industrial automation. In this regard, the Industrial networks must be able to respect specific requirements:

- Becomes necessary the connection between actuators, PLC, sensors and other devices.
- Data informations must be transmitted correctly and at the right time.
- Protection against electromagnetic interference, mechanical stress and dirt must be present.
- Flexible adaptation to production requirements is necessary.

The industrial networks are part of a Local Area Network (LAN) and it's allowed the communication between other environments only in a limited way. Moreover, the industrial networks are able to respond to the following communication functions only:

- Process and field communication between sensors and actuators.
- Data communication between automation systems.
- IT communication for integration into the modern information technology.

In the process industries the pyshical part of the communication system is selected by choosing specific cable for the signal transmission in according to the type of signal that can be digital or analog. Typically analog signals coming from sensors and digital signals are used to control field devices such as actuator, motor or solenoid valves. The choice of the physical communication for the devices, also imply to consider in a right way the bandwidth needed for the data transmission, the immunity to disturbances, the maximum length needed without the necessity of additional repeater, reliability and costs. In we consider the transmission mode in wired logic, the connection will be direct between the command and the component that must receive or send a or send the signal, such as sensors. Another way is to replace the anolog signal into a digital signal. In this case, the informations are encoded in groups of bytes and transmitted through a physical connection. The transmission mode or protocol, can be sequential or parallel. In the first case, the original byte, to be transmitted along the serial line, must be treated in such a way that each bit that composes it is methodically arranged in a sequence, to which the control bits will be added in the correct order. At the other end of the line, the bits that arrive in serial mode must in turn be decoded, in order to identify the significant ones and arrange them in the correct order, so as to reconstruct the original data. These operations are carried out by serial ports, that is devices mounted on specific cards present both on the unit that sends the data and on the one that receives it. The most used protocol is called RS-232 or its most updated and powerful version, the RS-422. Although these protocols allow the use of a large number of signals, for the applications under examination reduced versions are used with only 3 connection lines comprising at least the transmission signal, the reception signal and the ground. It is therefore a two-way communication that takes place via a shielded cable. The RS-232 interface, supplied to most of the instruments and electronic devices used in the sector, reaches a transmission speed of 19.2 kbit/s and is preferably used for point-to-point communications. The maximum allowed distance is 15 meters, although theoretically, under particular conditions, better performance can be obtained. The voltage signal is transmitted on a single line and refers to a common mass. The RS-422 version differs from the previous one in that the transmission takes place in a differential manner on two lines, and allows higher performances (up to 10 Mbit/s and distances up to 1200 meters) because there is a greater immunity to common mode disturbances. In fact, this protocol can be used for serial connections from a transmitter to multiple receivers. In the case of a parallel transmission, the bits that constitute the elementary word (from 8 to 32) are transmitted simultaneously to a corresponding number of conductors, combined in a flexible cable which is called the system bus. This bus allows the multiplication of the equivalent speed of transmission compared to serial communication. Considering the needed to maintain the parallelism of data in order to avoid a phase shift of bits of the same word, this type of transmission is reserved for the exchange of data within single devices. Taking into account the system architecture, becomes necessary to make a further distinction between point-to-point and multipoint connections. In the first case, there is a specific connection between each drive and the steering unit, through a specific cable, coupled to the two components through a serial port. Since these are point-to-point communications, as many control ports are required on the control unit. However, from a mechanical and electrical point of view, there is a limit referred to the maximum number of connections. In case of multipoint connections, the control unit and the various drives or devices are connected to a single serial communication cable, which together constitute a local network, of which the field bus represent a typical application for process automation. Different network control and management modes are possible, depending on whether it is concentrated in the control unit or distributed between the different devices. In any case, the device that get the access to the network must have a specific interface and also the ability to recognize and manage the signals that interest it. The local networks adopted as field bus are characterized by the kind of pyshical transmission, the topology and the structure of the protocol. Notice that the topology of the network can be as a tree, a star or a ring. Instead, taking into account the structure of the protocol and the access priority of the devices to the network, it's possible to obtain different modality such as Master and Slave mode, where the control of the network is centralized and concentrated in the master unit which is able to grants the access to the various slave devices in order to permit them to send or receive signals, providing also to send signals to the correct destination. The network access is given to the nodes in according to priority and timelines established by a pre-established query list. Only the nodes that has received a specific token are able to access access to the network. Than, each enabled node, at the end of this operation, delivers the token to a subsequent station in according to a previously fixed schedule which is defined a priory by the network administrator.

The protocols adopted in the industrial automation are many and different for each level of the CIM Pyramid 3.1 and are described in the next sections.

4.4 Network in the industries

As mentioned in the section before, each level of the automation CIM Pyramid [3], should provide:

- Acquisition of information.
- Control strategies developing.
- Correction strategies implementation.

Another fundamental thing consist in the fact that the whole automation system must be interconnected in order to guarantee the correct flow of information. Communication must be horizontal and vertical, in which in the first case the field devices present in the field level, must be able to communicate between them such as sensors and actuator, or PLCs must be connected with each other in the control level of the process automation. In the second case, devices of the field level must be able to communicate with the devices of the control level, and so on, until all the levels of the CIM Pyramid 3.1 will be interconnected with each others. In order to guarantee the correct flow of information becomes also necessary to take into account the different characteristics of each level such as:

- Kind of data that must be transferred over the network.
- Network communication constraints.
- Interoperability [37].

As described in the Network Automation Document of Università la Sapienza [37], Field, Control and Supervision levels have 3 different network 4.5 that allow the communication between each others and a dedicated bus for each level guarantee the communication between devices of the same level.

Field and Control network

Field and Control networks [37] are dedicated to management and transport of informations between field, control and supervisory level of the CIM pyramid in the process automation of the industries. The client in this system typically is not standard, in fact could be something like a PLC or an embedded controller, due to the fact that flexibility becomes an important aspect to consider. Informations are transferred such as small and not structured data and with an higher frequency level. Moreover, must be taken into account also the real-time constraints, in fact, becomes necessary ad-hoc solutions. Another important aspect to consider is the needed of determinism, due to the fact that the transmission delay, introduce a delay in the control loops leading to a performance degradation.

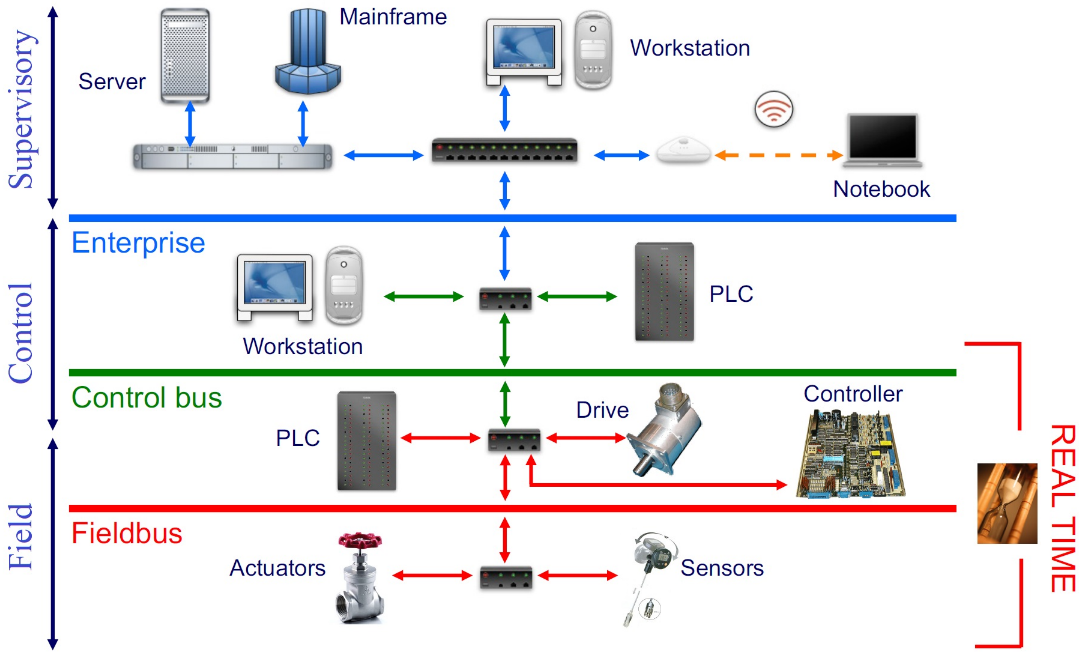

Figure 4.5. Industrial network scheme [37]

Enterprise Network

Enterprise network instead, is dedicated to management information between client and server devices connected to the industrial network. This kind of devices are typically chosen as standard network systems. In this network are not necessary ad-hoc solutions for the network systems, due to the fact that the real-time constraints are not required. Instead, the information safety, is an important aspect that must be considered, but not the robustness with respect the environmental disturbances [37]. Moreover, due to the fact that in general, ethernet network does not guarantee the retransmission of data, is adopted the TCP/IP protocol in case of lack of acknowledgement signal related to the single packet.

4.5 4-20mA transmission standard

Before HART Protocol 4.6.1, 4-20mA current loop [5] has been the standard in industrial process control for the analog signal transmission and electronic control adopted in the control systems, with the two values of 4mA and 20mA that corresponding to 0In fact, in a current loop 4.6, the signal is drawn from a dc power supply and flows through the transmitter into the controller, then back to the power supply in a series circuit. The main advantage was that the current value does not degrade in case of sensors situated in long distances. So the current signal remains constant through all components in the loop, with the result of accuracy of the signal which was not affected by a voltage drop in the interconnecting wiring. As mentioned before, the use of 4mA as a "Live Zero" enhances the signal-to-noise-ratio at low levels, making a loop failure more apparent. Instead a non functioning current loop with an open termination or connection means zero current flow, which is outside the valid 4-20mA signal range. In order to verify the 4-20mA current loop, was introduced a milliamp loop calibrator that was typically used in order to test loops that measure pressure, temperature, level and flow. So, the verification of the 4-20mA loop becomes a crucial step in any instrument calibration. Moreover, the full loop verification includes testing the output of the transmitter, the wiring, input to the control system as well as the control input system card and the return wiring back to the transmitter.

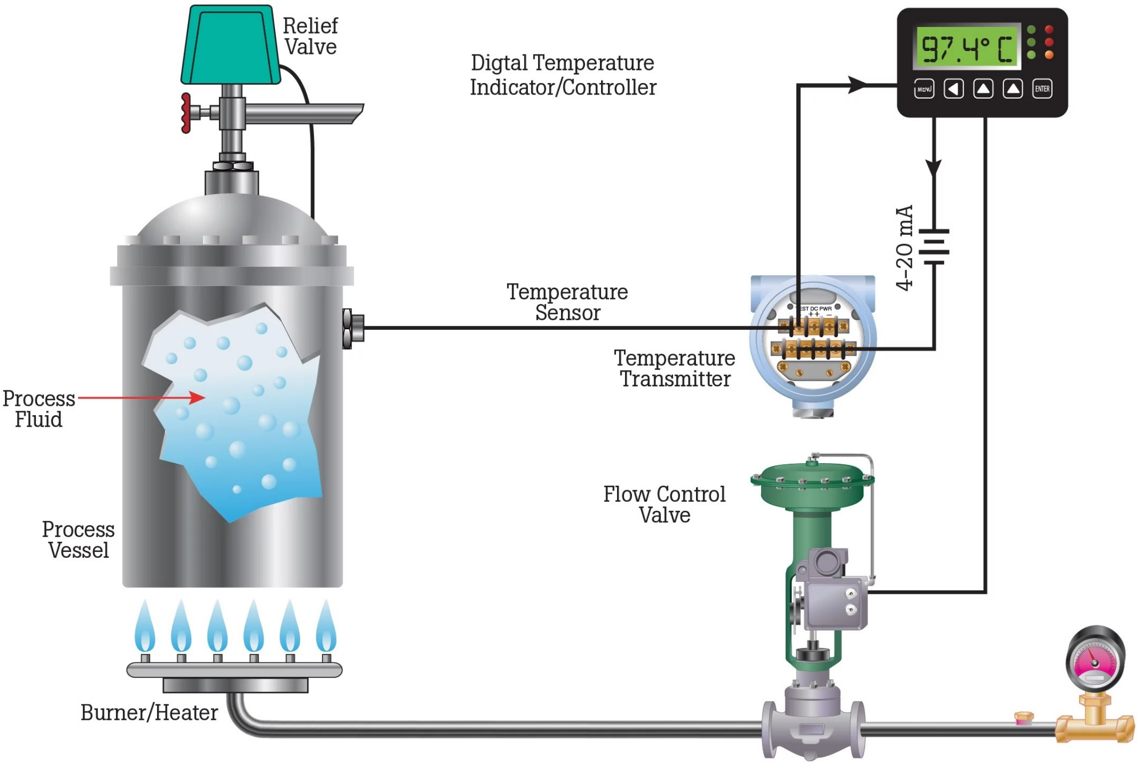

Figure 4.6. 4-20ma current loop [5]

4.6 Fieldbus

After the 4-20mA transmission signal, the main purpose in the industrial automation was to replace traditional control schemes in which each device has its own control wiring with bus systems that link a number of devices via the same cable. One of the advantages of the bus networks is that they require far fewer cables and wires, in order to connect devices with controllers. One of the most popular and widely used solution for the process industries is the Fieldbus architecture. So, *Fieldbus* indicates the name of an industrial computer network protocols family used for real-time distributed control and standardized as IEC 61158. A complex automated industrial system, such as manufacturing assembly line, usually needs a distributed control system and an organized hierarchy of controller systems to work. In the section below are described the main differences between the *Fieldbus* architecture with respect the traditional architecture.

Traditional architecture

The kind of topology is centralized with point-to-point connections.

Advantages:

- reliable and proven system
- availability for all kinds of instrumentation

Disadvantages:

- high number of connections
- expensive wiring
- critical wire drawing and protection

Fieldbus architecture

The kind of topology is defined as digital transmission on bus.

Advantages:

- savings in installation and error reduction
- easy to add or remove devices
- fault tolerance
- resorce sharing

Disadvantages:

- standard access protocols are needed
- difficulties of application in hazardous areas

4.6.1 HART

Highway Addressable Remote Transducer (HART) is a communication protocol adopted in the field level of the automation industries. This protocol adopt the Frequency Shift Keying (FSK) [26] standard in order to superimpose digital communication signals at a low level on top of the 4-20mA. This kind of procedure, enables two-way field communication to take place and makes it possible for additional information beyond just the normal process variable to be communicated to or from a smart field instrument. Moreover, the HART Protocol is able to communicates at 1200 bps without interrupting the 4 to 20mA signal, and allowing an host application such as master, in order to get two or more digital updates per second from a smart field device. Due to the fact that the digital FSK signal is continuous in phase, there is no interference with the 4 to 20mA signal. So, the HART communication protocol also provides two simultaneous communication channels which are the 4 to 20mA analog signal and a digital signal. Taking into account the field instrumentation, the first signal communicates the primary measured value through the 4 to 20mA current loop and the additional device informations are communicated with the use of a digital signal that as I have above mentioned before, is superimposed on the analog signal. The digital signal contains information the comes from the field devices, including also the device status, diagnostics and additional measured or calculated values. So, this two communication channels provides a low-cost and very robust solution for field communications with the additional advantage related to the easy configuration. Furthermore, the HART protocol permits all digital communication with field devices in either point-to-point or multi-drop network configurations. There is also an optional communication mode which is called *burst mode*, where a single slave device can continuously transmit a standard HART message as response to the master. Moreover, for this kind of communication mode are possible higher update frequencies [6].

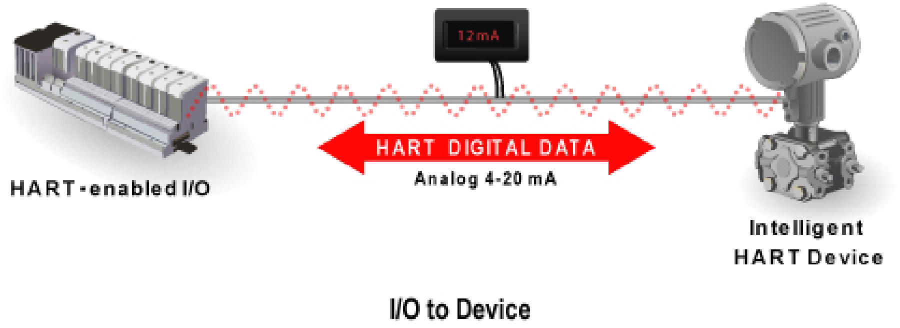

Figure 4.7. Two channel HART communication protocol [6]

4.6.2 Profibus

Profibus protocol which is the acronym of *Process Field Bus* is one of the fieldbus standard adopted for the communication in the industrial automation technologies and is openly published as a part of the IEC 61158. In principle, profibus protocol was promoted by the *German Department of Education and Research* and then, adopted by *Siemens*. This protocol provides 2 variations which are:

- PROFIBUS DP
- PROFIBUS PA

The first variation, PROFIBUS DP which is the acronym of Decentralized Peripherals, is adopted to operate actuators and sensors and via a centralised controller in the factory production for automation applications. The main advantages of this protocol are:

- Most used field bus in production environments for all over the world
- Faster data transfer - 12 Mbps
- Plug-and-play

Typically, the industrial automation applications are usually realized by creating a network composed of remote I/O, frequency converters, sensors and actuators. If the power supply and wiring are not a problem in the field, reliable installations can easily be carried out. Due to the fact that the PROFIBUS DP protocol can be used in so many ways, this becomes an excellent solution for many automated environments 4.9. Other field buses only work in limited application environments, so the user administrator is often forced to use multiple protocols in the same system. Furthermore, due to the fact that PROFIBUS DP complies with the IEC 61158 standard, it is possible to use devices produced by different suppliers, without binding to a single manufacturer.

This digital communication system, allows to share a two-wire copper cable such as a bus system with many components [22]. This saves the wiring and installation costs enormously compared to conventional and non-digital systems also allowing to:

- Decrease in components.
- Simpler schemes.
- Test time and subsequent shorter purchase.
- Simple maintenance.

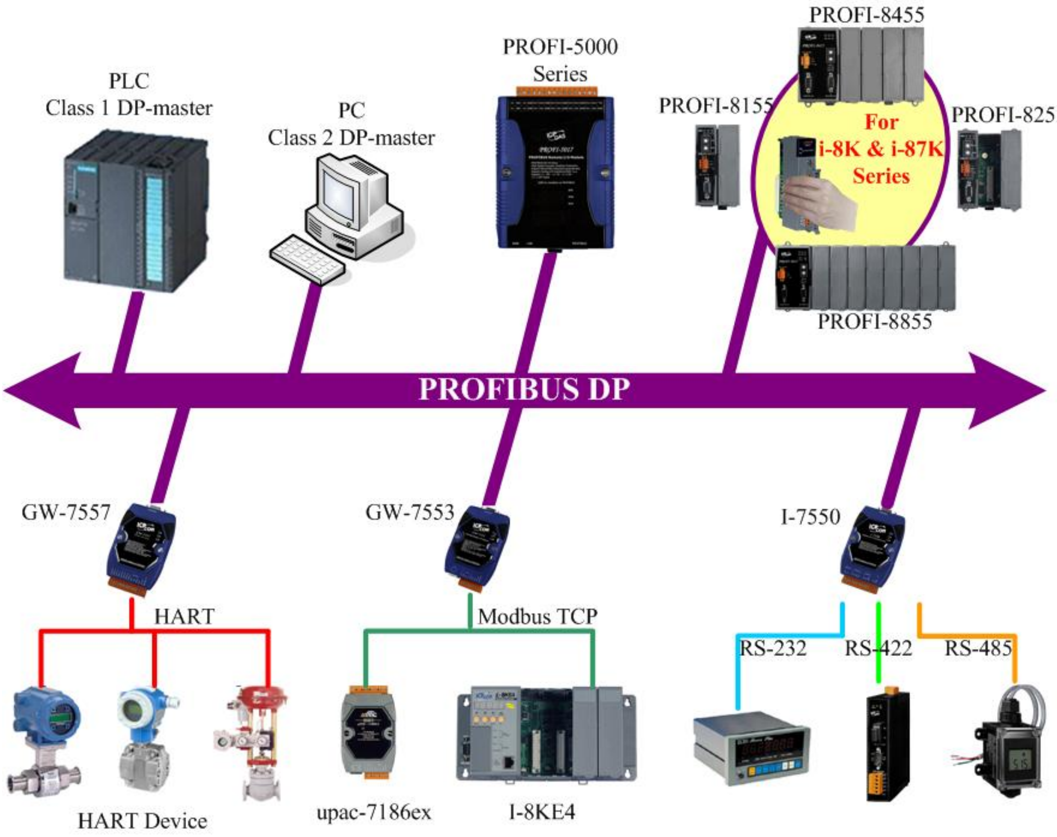

Figure 4.8. PROFIBUS-DP network [23]

As described in the Prontec article [24], PROFIBUS PA instead, is a variant of PROFIBUS DP. In fact, this protocol is specially designed for improvement and replacement of conventional systems such as 4 to 20mA and HART protocols, for process automation in the industries. The main differences with respect PROFIBUS DP protocol, consist in the fact that data and power supply are transported over the same two wires. In fact, this variant is designed for the use in explosion or hazardous areas, also allowing power to be delivered over the bus to field instruments, while the current flows in a limited way so that explosive conditions are not generated, even if in case of malfunction. Notice that, in terms of protocol and use, the two types of protocol are practically the same. One of the main advantages of PROFIBUS PA protocol is that it can be seamlessly connected to PROFIBUS DP, with the meaning that becomes possible to equip a production environment entirely with PROFIBUS. This optimizes knowledge as well as spare parts, and everything can be equipped with an only one type of control system. PROFIBUS PA is linked via coupler to PROFIBUS DP. The coupler translates the DP signal that come from the master to PA signal (data and power supply) on the same two wires. The answers of the PA instruments are translated back to PROFIBUS DP. The translations are electrical, because the protocol remains intact. Moreover, due to the low transmission speeds of 31.25 kpbs, becomes possible to flexibly create an infrastructure, and branches can be very long compared to PROFIBUS DP where the cabling rules are very narrowly defined. That is the main advantages with respect to the conventional 4 to 20mA communication system, in which the cable that connect a device with the control system, is a non-shareable element. Instead with PROFIBUS, only one shared cable comes out from the coupler, which can be linked to a star network. As mentioned before, this kind of protocol provides a protection against explosions in the process industries, due to the fact that the are dedicated devices which allow a low consumption of electrical energy. Moreover, these dedicated devices must be satisfy specific requirements in terms of protocol to which the producer must comply.

4.6.3 Profinet

Profinet which is the acronym of Process Field Network is the industry standard for data communication over Industrial Ethernet. This protocol give the possibility of an interconnection between devices of whole levels of the CIM pyramid, with a particular strength in delivering data under tight time constraints approximately on the order of 1ms. This standard is maintained and supported by PROFIBUS and PROFINET International (PI) [29]. The peripherals interfacingis implemented by the PROFINET IO [?], which defines the communication with field connected peripheral devices. In fact, PROFINET IO defines the entire data exchange between controllers such as the IO Controllers and the devices that are defined as IO Devices, as well as parameter setting and diagnosis. Typical examples of IO Controllers could be PLC, DCS, or PAC. Instead the IO Devices can be something like I/O blocks, drives, sensors, or actuators. The PROFINET protocol is designed in order to obtain a faster data exchange between Ethernet-based field devices and follows the provider-consumer model. An important aspect to consider is the possibility to integrate field devices connected to a PROFIBUS line with a PROFINET system seamlessly via an IO Proxy. Functionality supported by PROFINET applications can be divided in three conformance classes 4.10, in according to the international standard IEC 61784-2:

- *In Conformance Class A (CC-A), only the devices are certified. A manufacturer certificate is sufficient for the network infrastructure. This is why structured cabling or a wireless local area network for mobile subscribers can also be used. Typical applications can be found in infrastructure such as motorway or railway tunnels, or in building automation.*

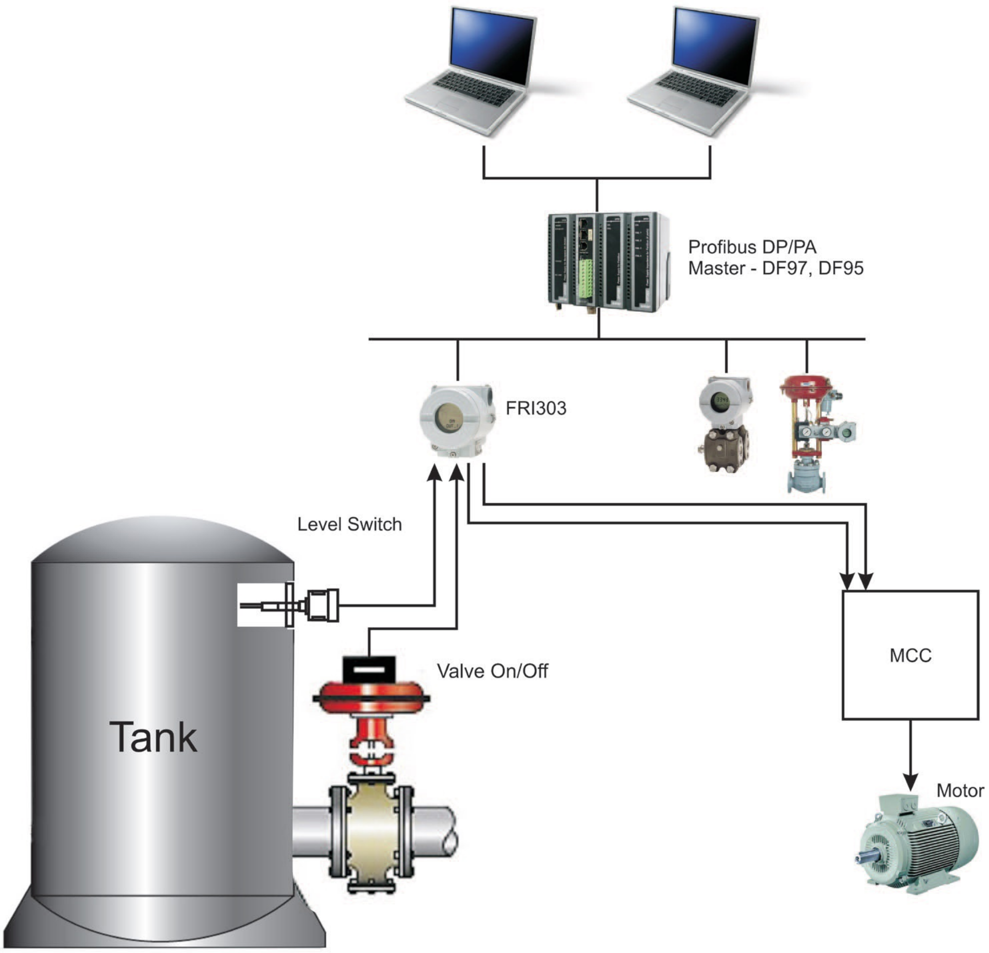

Figure 4.9. PROFIBUS-PA network [25]

- *Conformance Class B (CC-B) stipulates that the network infrastructure also includes certified products and is structured according to the guidelines of PROFINET IO. Shielded cables increase robustness and switches with management functions facilitate network diagnostics and allow the network topology to be captured as desired for controlling a production line or machine. Process automation requires increased availability, which can be achieved through media and system redundancy. For a device that respect the Conformance Class B, it must be necessary that is able to communicate successfully via PROFINET RT, have two ports (integrated switch), and support SNMP.*
- *With the Conformance Class C (CC-C), positioning systems can be implemented with additional bandwidth reservation and application synchronization. Conformance Class C devices additionally communicate via PROFINET IRT.*
- *As of PROFINET V2.4 (June 2019), Conformance Class D (CC-D) was introduced which corresponds to CC-B and CC-C, except with communication via Time*

Sensitive Networking Ethernet being specified.

Conformance Classes (CC), *PROFINET*, Wikipedia [28].

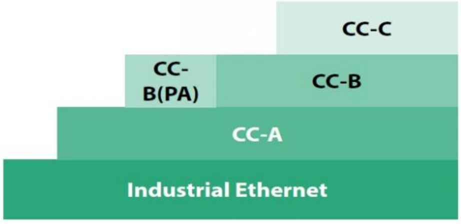

Figure 4.10. PROFINET Conformance Classes [27]

4.7 Language programming for Programmable Controllers

The languages adopted in the electronic devices which are present in the industries, allow to automate the industrial processes for which these devices are designed, in order to ensure the correct automation of the industrial process. Programs are usually written on a PC, and then transferred via cable or USB to the PLC or DCS itself. These kind of programs are stored in a non-volatile memory in order to ensure that the processes for what they are designed can be controlled and continues to works properly. Like any other machine that can execute programs, there are different kind of languages available. The languages described below have their use cases. Some of them are mainly chosen for their simplicity within the context of electromechanics while others are useful because of their complexity allow to develop more complex programs.

As described in a Codesmithdev aticle [32] five are the languages that are considered as standard languages for use on PLCs and other similar programmable industrial automation devices, in according to the IEC 61131-3 standard.

4.7.1 Ladder logic programming

Ladder Diagram is the oldest PLC language. This graphical programming language was modelled from relay logic to allow engineers and electricians to achieve a smoothly transition for the PLCs programming .

Within Ladder, rungs and rails represent the electrical connections of the device. In particular way, the vertical lines 4.12 represent the power supply of the PLC device, while the rungs that are connected to the rails 4.12 are equal to the amount of the control circuits.

The input conditions can be written in input terminals illustrated in the picture 4.12, which then impacts the output on the output terminals. The poor quantity of instructions which are present in the ladder logic language, makes it difficult to model the motion, due to the fact that the ladder logic strictly adheres to the on/off logic of the hard-wired relays.

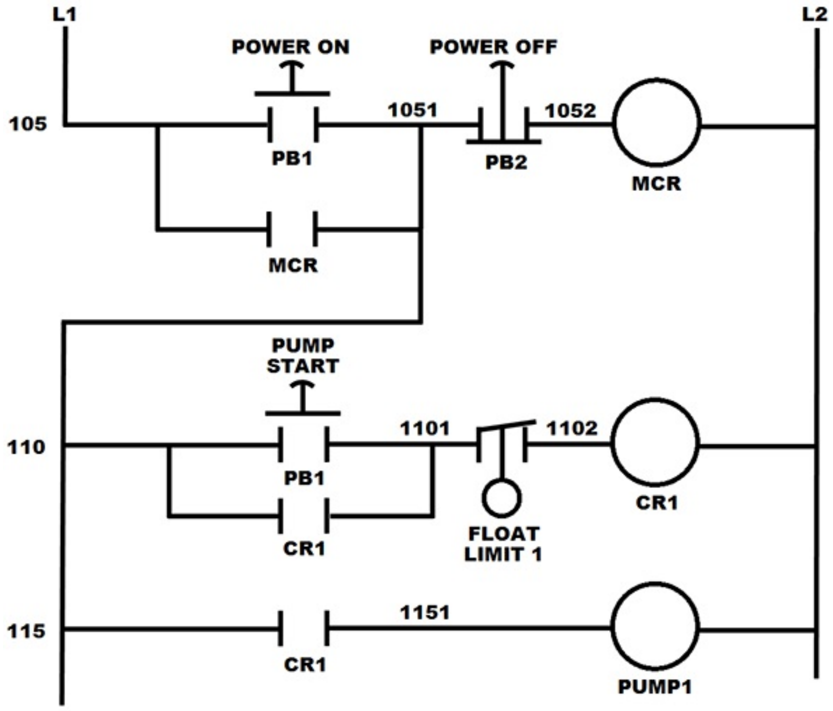

Figure 4.11. Ladder logic programming [32]

4.7.2 Sequential Function Charts

A sequential function chart [33] is defined as a graphical programming language that is similar to the flow chart. In this kind of language programming is possible to use the steps and transitions in order to get output.

Steps are referred as the functions within the program in order to activate the events on the basis of the state and other well specified conditions.

Instead, the transitions are defined as instructions which are mainly based on true/false values and that moves from one step to another.

Finally, branches are used in order to initialize multiple steps in the same amount of time. These branches in fact, act like threads where the functions can run concurrently.

All of the above mentioned steps such as transitions, and branches are hosted in a series of scripts that are being executed in a manner procedure. The visual nature of the language allows users to monitor the processes that both heavily use conditional logic and run parallel instructions. Devices like PLCs that are prone to suffering from bottlenecks can be more intuitively maintained and troubleshooted through the use of the chart, in order to follow the logic of the program.

4.7.3 Function Block Diagram

The block based programming languages [34] are mainly based on a kind of graphical language that minimizes code into blocks and which allows a simple way to create executable commands.

In particular way, the block based programming language describes a function between inputs and outputs which are connected by connection lines. The logic of the inputs and outputs are stored inside blocks. These blocks are programmed onto sheets and the PLC scans these sheets following a specific order or by specified connections between the blocks itself, as well as the procedural languages.

The I/O is similar to the ladder logic. However, the code that the blocks contain, allow engineers to develop more complex batch control tasks among other repeatable tasks.

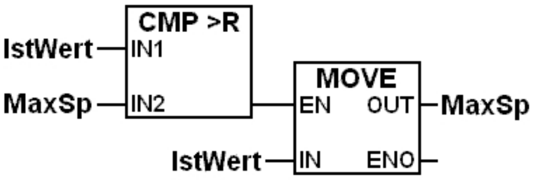

Figure 4.12. Function Block Diagram [34]

4.7.4 Instruction List and Structured text languages

The Instruction List [35] language programming adopted for the PLCs is equivalent to the assembly language. This kind of language, allow to immediately grant the direct access to the machine itself. Moreover, permit the programmer to write code that is compressed and faster if compared with the other kind of languages. The program control flow is achieved by jump instructions and function calls which are subroutines with optional parameters.

The Structured Text programming language is referred to an high level programming language. Due to the fact that the Structured Text language is based upon another high level programming language, which is known as Pascal, both languages bear strong resemblance syntactically. This kind of resemblance is adopted in order to clarify the syntax of the Structured Text by comparing the Pascal code to other equivalent pieces of program which was written in Structured Text. To be able to write pieces of Structured Text, the language constructs and the data types that these pieces are composed must be introduced as first. As I have introduced before, also this kind of language is designed to program the programmable logic controllers adopted in the field of industrial automation. With this kind of language, are also supported complex statements and nested instructions such as:

- Iteration loops like REPEAT-UNTIL and WHILE-DO.
- Conditional execution as well as IF-THEN-ELSE and CASE.
- Functions such as SQRT() and SIN() functions

Notice that unlike in some other programming languages, there is no fall through for the CASE statement. In fact, the first matching condition is entered, and after running its statements, the CASE block is left without checking other conditions.

A concept that occurs in the Structured Text language but not in the Pascal language, is referred to the notion of directly represented variables. In fact, the directly represented variables are variables that are not identified by name, but that are addressed by their position in the PLC data memory. This kind of concept has been adopted from programming languages, such as the Ladder Diagram programming language. Another reason why it has been included in Structured Text is due to the fact that it is commonly used in many PLCs. However, the kind of identification that directly represented variables is extremely implementation-dependent and therefore should have no place in a standard such as IEC 1131-3 that addresses implementation-independent issues.

Chapter 5

Safety and Risk Analysis of industrial processes

An important aspect that must be considered in the field of industry is to identify and analyze the risks related to equipment and plants, with the aim of managing safety in industrial plants. In order to better evaluate the risks throughout the plant's life cycle it is important to consider that the identification and risk evaluation are fundamental aspects that must be considered not only during the design phase of the plant, but also throughout its life cycle taking into account also the changes in terms of management. In particular way, the risk evaluation is not an activity that should be carried out once at time only, but it is a continuous process that follows the entire life cycle of the plant such as follow:

- In the planning phase the main hazards must be identified and eliminated or reduced with appropriate technical solutions.
- In the construction phase the consequences for the safety of the modifications in progress must be assessed.
- In the operational phase temporary or permanent repairs, plant modifications, changed operating conditions go to influence in various ways on risks, as well as organizational changes.
- in the closing phase the particular kinds of danger that characterize the final phase must be considered.

As described in the *La valutazione dei rischi negli stabilimenti industriali* article [30], in the next sections was explained two methods adopted in the field of industrial automation for risk analysis and which are known as HAZOP, which is the acronym of Hazard and Operability Analysis 5 and check list or Index method 5.0.1.

HAZOP method

This method provides to systematically review the process and operations in order to identify potential deviations from the design intent, examining their possible causes and assessing the consequences. So, the HAZOP analysis is conducted by a group of specialists in the various disciplines to it related and providing for a logical partition of the plant that is characterized by a design intent such as for example a line of process. Furthermore the potential deviations must be identified considering the characteristic parameters of the component which is examined, as well as temperature, pressure or level. In other words, this method is a systematic and structured kind of a complex planned examination, operation or existing process. This, with the aim of better evaluate and identify the problems that could represent risks to personnel or equipment. The intention of performing an HAZOP is to review the design to pick up design and engineering issues that may otherwise not have been found. This technique it is mainly based on breaking the overall design of the process into a number of nodes or sections allowing an easily and individually reviewed. As well as I have aforementioned before, this technique is carried out by a suitably and experienced multi disciplinary team. Moreover, the HAZOP technique allow the team to better identify potential hazards and problems in terms of operability in the industrial process. So, the HAZOP working group, carried out in sessions, with the aim of identify the existing dangers in the management of a specific work process. This analysis is conducted through a phase of defining the work environment and understanding the work processes that take place inside of them, in a subsequent examination of parameters, their deviations and their consequences, in order to come to conclusions of possible dangers and to better formulate useful recommendations for their management. The HAZOP team is composed by the leader, which the main task is to asks questions to the team and coordinates the work. Subsequently there is the secretary that takes note of the key points issued during the discussion and the attendant of each discipline of the system taken as a case study which are:

- Process.
- Exercise.
- Safety and maintenance.

The system taken as a case study, is defined at the beginning of the HAZOP method, normally using general planimetry, functional diagrams, travel diagrams, single-line wiring diagrams of the system and clearly identifying limits in terms of communication and connection with other industrial systems.

As taken from *“An Introduction to HAZOP” by R. Ellis Knowloton, Chemetics Int. Ltd, (1981)*, it was explained with a graphical example 5.1, how the HAZOP method works.

Unlike other methods of analysis of undesired events, which also lend themselves to studying such as a general case, HAZOP is in opposition to the other methods allows to forecast and analyse complex situations in particular way in the field of industrial automation of chemical processes since it applies to any minimum part of the plant provided that its intention is clearly defined. However, for this reason, the part of the plant that must be examined should be precisely defined. In the case of the diagram shown in the picture 5.1, the first analysis to be performed is the part of the plant delimited by the closed dashed line, or by the load pump of component A and by the section of pipe that connects it to the reactor. The shut-off valve sited in upstream of the pump is not included, furthermore, neither the one placed on a secondary pipe that is connected to the pump inlet section, but the shut-off valve downstream of the pump is included.

In the first step, the intention of the part of the plant that was being examined is clearly to transfer the A component into the reactor with a predetermined flow rate. In the second step, some guide words can be adopted, in order to identify possible deviations from the intention.

In order to denies the intention, like for example the case in which the A component is not transferred, or the flow rate is null, can be adopted the words “NO” or “NOT”,. This could be a dangerous condition since it could happen that the B component is fed up, in order to find itself in quantity higher than that of A component, a situation that must be absolutely avoided.

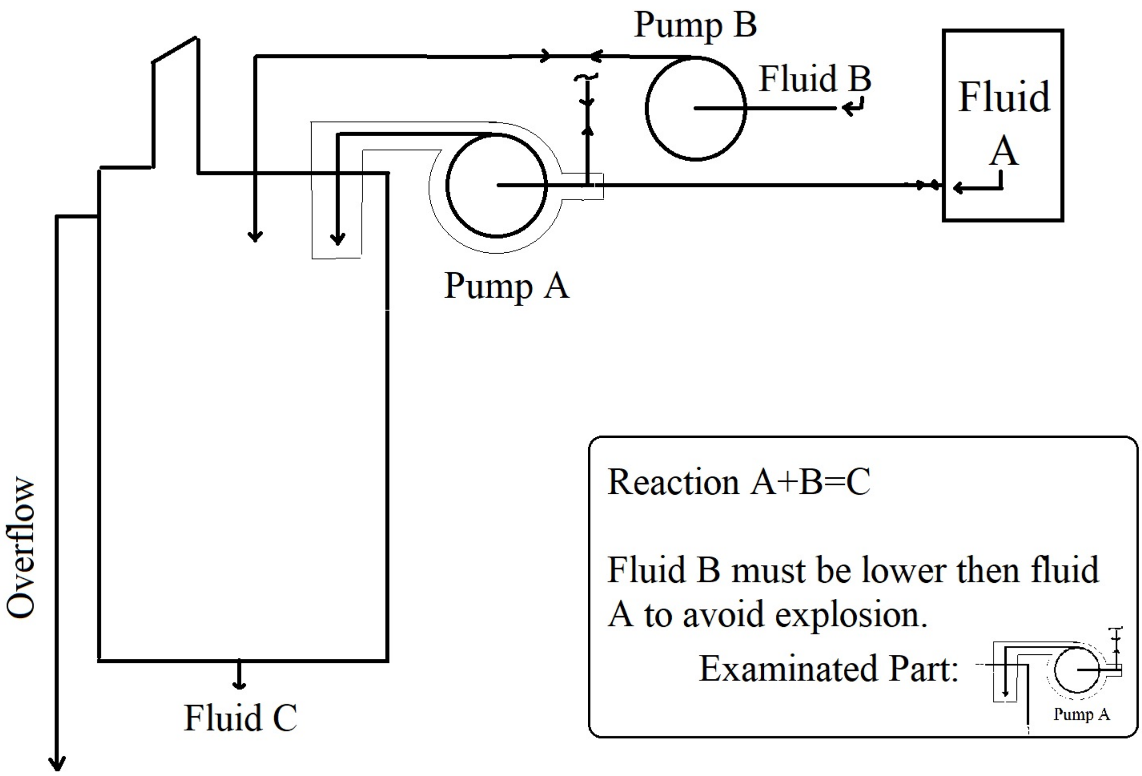

Figure 5.1. HAZOP example quoted by "An Introduction to HAZOP" by R. Ellis Knowloton, Chemetics Int. Ltd, (1981)

Therefore it is important to get to the bottom and understand the possible causes(third step) of this first form of deviation:

- The tank A is empty.
- The pump fails due to various causes which may be referred to:
  - mechanical breakage
  - failed power supply
  - accidental switching off
- The pipe section downstream of the pump is broken.
- The shut-off valve downstream of the pump is closed.

Also if in this part of analysis, some of these causes could be unlikely, at this level of analysis does not matter. The consequence of these causes which is defined as fourth step, is that sooner or later could append that inside the reactor will be an excess of B component compared with respect to A component and therefore in a condition of danger in terms of explosion. In fact, the same procedure from the second to the fourth step must be repeated with other guiding words.

The word “major” leads us to think of the case where for some reason the pump transfers the A component with a greater flow rate than the intention established in the project. In fact, if the cause can be considered realistic due to the fact that in some circumstances the pump could actually feed a greater flow, then becomes necessary to consider the consequences that are not referred to the explosion since we would have A component extremely larger than B component, but could be a contamination of the product C which it would be found with an excessive percentage of unreacted A, or it could be an excessive filling of the rector. At this point, must be evaluated if these possible consequences could constitute any kind of danger such as something similar to the initial one related to the explosion of the reactor and which in any case, must be avoided.

Instead, the word “minor” is referred to the case in which the reactor reach a lower(not zero) capacity of A with respect to the lower limit. Possible causes related to this can be expressed as follow:

- The shut-off valve downstream of the pump is partially closed.
- There is a loss of product due to small breakages on the pipe.
- Some fault append into the pump, due to fan erosion or other mechanical problems.

The consequence is again a condition of danger of explosion which sooner or later can be found in the reactor with an excess of B component with respect to A. In the picture 5.1, it is possible to observe that there is a pipe that is connected in upstream of the pump and presumably conveys a substance different from A. Therefore it is a situation in which becomes necessary a further investigation, due to the fact, that this let us thinking about the presence of something inside the tank, which could be different from A component. This can append in the case of after maintenance or cleaning operation of the tank there is a trace of something that can react with A and that can cause some kind of decomposition or polymerization. So, also these situations must be examined in a greater detail. This can be accounted by repeating the HAZOP analysis on the A component and so on on other well defined parts of the entire plant where for some reason dangerous conditions can be generated. Furthermore, in the HAZOP analysis can be adopted various kind of guiding words which could be helpful for the HAZOP team in order to better configure the different possible scenarios.

So, as described in the HAZOP example, the identification of the dangerous conditions and the related possible unwanted accidental events is the first and the most important step in the field of risk analysis, due to the fact that if danger is known becomes possible to reduce its risk, otherwise it remains a hidden threat. There is no general criterion of investigation that are capable of flushing out all forms of danger within a complex system. Instead, have been developed various methodologies that if applied to specific objectives are able to guarantee different levels of in-depth analysis of the problem in relation to the dangerousness and complexity of the situations. Therefore, it is also advisable to adopt more than one of these methodologies so that the different information and the different scenarios examined, suitably integrated with each other, are able to provide a sufficiently complete picture of the case in question. These methodologies derive substantially from three different approaches such as:

- Knowledge and experience of experts in the field (Safety Review, Check list, Preliminary Hazard Analysis, What-if Analysis).
- Indexed methods with which it is possible to make relative assessments with respect to known systems (Relative Ranking).
- More or less rigorous logical paths (HAZOP, FMEA, logical criteria for fault analysis).

A particular criterion of investigation consists in analyzes the man reliability in all his activities and functions, that are unavoidably present throughout the life cycle of the plant or process. This is referred to the Human Reliability Analysis [39].

5.0.1 Consequences Analysis in the field of industrial process

In according to the European Federation of Chemical Engineering (EFCE), safety in the process industry, is equivalent to loss prevention, whether it is products or energy. The analysis of the consequences tries to prefigure the possible losses scenario, also including physical effects and consequent damages. So, the situations can be absolutely various and difficult to predict. For example it is possible to consider a tank in which there is fluid in the presence of its steam at a pressure higher than atmospheric pressure. If an accidental breakage of small dimensions occurs in the upper part or in the lower part of the tank or on a connected pipe, a release of only steam or only fluid will occur. However, if the damage is not so small, or the internal pressure can be considered relatively high, a biphasic outflow can be generated. This is similar to what happens when a bottle of champagne is extremely agitated. These outflows can lead to different harmful consequences if the substance is flammable, unstable or toxic. An outflow of gas or steam leads to the formation of a cloud that will be subjected to a transport phenomenon or diffusion, depending on the local meteorological characteristics. So, it is presumable that, within a certain distance from the source within the cloud, high substances concentration will remain above the toxicity limits or the minimum flammability limit for a certain time. In the first case the passage or permanence of this cloud may cause human damages in terms of health if them are exposed, while in the second case it may ignite and accidentally explode in the presence of a source of ignition. In the case of release of a substance in the liquid state, this may partly form a cloud due to evaporation, due to the difference in terms of pressure, between that in the tank and and the atmospheric one, with the subsequently puddle creation. The latter will also be subjected to evaporation with the consequent formation of a cloud or it may catch fire or it may also leach into the ground, moreover causing an aquifers pollution. A particular case of simultaneous losses of product and energy occurs as a result of a large-scale which is also called as *catastrophic failure* of a container that contains a liquefied gas. The extreme but not so rare phenomenon is also known as *Boiling Liquid Expanding Volume Explosion* (BLEVE), or a very rapid phase transition with an expansion of the volume of the order of two hundred times the initial one, which could be able to produce a pressure wave equivalent to a chemical explosion. Then, if the gas instantaneously ignites in the expansion phase, as it is very likely for events of this type, a fireball can be produced due to the fact that the flame envelops the entire mass of the released substance before a mix up with the air. So, due to the fact that are many and different the hypothetical scenarios due to the release of substances or energy and these are not easily reproducible. Furthermore, there are many mathematical models developed to examine each of the possible physical phenomena such as, for example:

- Gas/vapor discharge.
- Outflow of liquids.
- Biphasic efflux.
- Flashes of liquids under pressure.
- Puddle evaporation.
- thermal radiation from open flames.

- Dispersion of toxic gases.
- Diffusion of heavy gases.

As in the case of the damages of an accidental event, also these physical phenomena can manifest themselves in various forms.

Check list method

An other methods is known as Check list method, which was developed by the Institute for Prevention and Occupational Safety in collaboration with the National Institute of Health. This method is a fundamental requirement for the risk establishments of a major accident in according to the *Seveso directive* (Legislative Decree No. 334/99). It does not require considerable detailed information on the operation of the plant and is also very suitable for guiding decisions regarding the choices of the plant.

This method starts with the subdivision of the plant into logical units, where each of these corresponding to a single processing of the production process. For each unit, based on the dangerousness characteristics of the most important substance among those present (key substance), will be obtained the "substance factor" in according to a specific table. Subsequently, the unit is examined using a check list of over 40 points that reviews in detail all the aspects that could have effects on safety by grouping them according to a logical path that looks first at the risks linked to the substance, then those related to the process. Finally those related to the structure of the plant and the plant itself. For each of these four groups a corresponding numerical factor is obtained. Furthermore, a combination of the factors derived from the check list and the "substance factor" calculates a general risk index and an intrinsic index of risk for fire, confined explosion, unconfined explosion and toxic release. Lastly, the lines of defense are examined through the use of another check list of more than 30 points.

The quantification of the risk for the system taken as case of study is the result of a series of assumptions, mathematical models, hypotheses related to possible scenarios in which it has the value of the order of magnitude rather than a certain parameter to be related to legal standards. For this reason the calculated risk needs to be "evaluated" or "weighed" before deciding whether it is acceptable or not and before taking measurements needed to improve the safety. The first evaluation is the comparison with alternative solutions or with systems similar to that under examination or with orders of magnitude of the risk that indicatively are considered acceptable. This comparison is legitimated and reasonable if the level of risk is obtained through the same methodology and with the same approximations.

Secondly, perception of the risk must be taken into account as the real risk that emerges a posteriori from statistical data on accidents which rarely corresponds to the detected risk.

So becomes necessary that everyone creates their own risk ranking which is completely different from that of people who may live in the same living or working environment. It is superfluous to remark that the same ranking may be change if repeated at different times and places, but always with a substantial discrepancy between real risks and detected risks. It is clear that in the cases where the perception is high, it is not sufficient to maintain the calculated risk is absolutely acceptable but it is also necessary to give different reassurances such as not theoretical or numerical and help the public opinion to remove the reasons of an excessive concern, also through additional prevention methods, protection and organization.

5.0.2 IRIS tool for Risk Identification in the industries

Through these two methods, a system adopted for risk identification, known as IRIS, is a support tool for the industrial plants manager, which aims to identifying and assessing risks in the process plants, through the Check list method and the HAZOP analysis. In particular way, the system has adopted an internal representation also called as "digital representation of security" which, in addition to describing the plant in detail, manages information relating to the risks identified and their evaluation. Furthermore, the system is a tool to support the operator of establishments at risk of major accidents in order to prepare some parts of the Safety Report, such as the risk assessment of each unit, in according to the Check list method, the identification of potential deviations, by means of the HAZOP study, and the identification of the main events also known as "top events" and of the critical components.

These are the modules that are included in the system:

- Plant descriptor, that contains useful functionalities for defining the plant in all its parts and its properties.
- Application of the Check list Method, with the procedures and automatisms needed for the determination of the intrinsic and compensated factors which are necessary for the computation of the risk indexes.
- HAZOP application, which contains the functionalities that are needed for the potential deviations analysis, the risk assessment and finally the identification of possible causes and consequences.
- The Generator of technical reports, with the automatic generation of documents.
- The Coherence Verifier, which is a tool that verifies if the results obtained from the identification and evaluation risks are consistent with respect the changes made to the plant.
- The Product configurator, which allows a system customization, such as for example by introducing new types of components, or by editing new rules related to causes, consequences or safeguards of the plants.

All these modules make use of a single database which contains both the establishment description and the information needed for the application of the risk identification, through the Check list and HAZOP Analysis.

Furthermore, is also remarkable to know that whenever a change is introduced in the plants, in the equipment, in the materials, in the procedures or in the organization, it is necessary to do a new evaluation of the risks, verifying which ones have been eliminated or reduced and which ones, possibly introduced or increased.

Notice that, if the permanent plant modifications are usually preceded by above mentioned evaluations, or continuously minor changes are made, an update of the risk assessment does not become necessary. A continuous review of risks is essential but it becomes more difficult to make, if the assessment has been completely outsourced, such as usually append in the case of small and medium-sized enterprises industries. In order to avoid the postponing assessments due to consultancy costs, becomes necessary that the manager has a minimum level of autonomy in the field of the risk analysis, in order to at least assess the impact of the "minor changes". Also in this sense the IRIS system can be considered useful due to the fact that the external analyst will be consulted only for the most important evaluations, but the manager, through the IRIS tool will be also able to follow the analytical work of the consultant and become independent at least if we take into account minor interventions.

5.1 RAMS Analysis

The sections just described are referred as a part of the procedure and methods adopted in the field of industrial automation, in order to guarantee Reliability, Availability, Maintainability and Safety of automation systems and industrial plant. These four procedures are identified and also known as RAMS analysis. With the development of industrial activities and with the growing complexity of the systems, the problems of reliability and operational safety of systems and their components have become the subject of systematic studies. The techno-economic implications connected to the development of civil aeronautics and military, space vehicles, computers, nuclear plants, have made it clear that redundant tools and safety factors were no longer able to ensure these reliability parameters for obvious problems in terms of size, weight and costs. The development of RAMS Methodologies, allow to evaluate in advance, the parameters connected to the systems reliability, through the identification of possible points of weak during the design phase and also allowing to better evaluate the appropriate changes. These methodologies allows the introduction of one instrument that could be able to guarantee reliability and system availability, also satisfying the requirements in terms of safety through the study of the laws that correlate the performances of the components and of the systems to the solicitations imposed on them. The study of these parameters, together with the maintainability of the system, lead to increase the probability of success of the mission, through the study of the laws that correlate the performance of materials into the production processes. So, RAMS analysis aims to guarantee an optimal result of an investment such as a new production plant or the modification of an existing one. Furthermore, any kind of these projects should be managed taking into account and considering the four ingredients of the RAMS analysis and which are commonly used in engineering to characterize a product or a system.

In fact, the quality in the industrial systems is expressed by features that are verifiable through deterministic and probabilistic techniques such as follow:

- *Deterministic Characteristics.*

  These kind of characteristics are represented by basic services or specification, the measurement usually takes place during the acceptance testing by verifying their degree of compliance.

- *Probability Characteristics.*

  These other kind of characteristics are represented by expected performance over the time of the system. The measurements was done through the use of probabilistic methodologies of the following parameters:

  - Reliability: which means of guarantee a continuity of the system service that is designed or managed. It is linked to a period of time. The reliability is practically defined as the probability that a component or a system performs its function correctly for an assigned amount of time, in well-defined operating and environmental conditions 5.1.1.
  - Availability: means reducing downtime to a minimum, optimizing production and at the same time ensuring the efficiency of safety systems during the standby condition. It is practically defined as the probability that a component or a system performs correctly its function at a predetermined instant of time, in well-defined operating and environmental conditions 5.1.2.
  - Maintainability: means to guarantee the rapid recovery of the faulty components 5.1.3. It is practically the probability that a component will be repaired within a set time.

This time considers both the detection of the fault and the repair such as the ability of the system to be quickly and easily maintained.

- Safety: means to produce by minimizing the risks for operators, peoples and the environment, but also the in terms of economic factor as well as direct and lack of production. In practical terms is the condition of least chance of incurring accidents to men, things or environment. The distance from the safety condition is measured by the concept of Risk, that is referred to the probability that an undesired event of an uncertain nature will occur. The most commonly used mathematical definition predicts the product between the frequency of occurrence of the event that produces the damage for the extent of the damage itself 5.1.4.

The result of a project done through RAMS analysis will surely bring a big benefit of production optimizing in terms of:

- Preliminary design;
- Losses in terms of production;

and the consequent optimization of the resources such as design, maintenance and warehouse.

A company must be able to invest in the RAMS analysis to ensure that it complies with all regulatory aspects concerning safety, the environment, energy and design.

For Maintenance Engineering, knowledge of the analysis becomes essential to be able to design and manage Maintenance through the use of the RCM logic.

The main difficulties of RAMS analysis are due to:

- Multidisciplinarity which is referred to the interaction problems between different functions such as Process Engineering, Safety, Maintenance and Production.
- Systemic approach which is an overview with different levels of detail.
- Conflictuality of RAMS requirements which consists of finding a good compromise between the four points.
- Methodological aspects as well as analyst training, analysis techniques and data coherence.

5.1.1 Relayability

As described in the *RAMS Analysis* [40] document, the reliability of a component is defined by the probability that it will work without any kind of failure and through a certain time period t and also referring to well-defined environmental conditions.

The elements that are necessary for the reliability definition are the following:

- A unique criterion needed to evaluate if a specific kind of element works fine or not.
- Becomes necessary an exactly definition of the environmental and employment conditions.
- Determination of the time interval t is needed.

After the establishment of the first two conditions, the reliability of an element becomes function only of time and the form of this function depends on the probabilistic law with which the malfunctioning conditions of failure may occur over time.

A broader definition of reliability can be referred as the science of predicting, analyzing, preventing and mitigating failures over the time.

It is a science that has a some kind of well-defined principles and theoretical bases which, in some way are all related to the study and fault knowledge. Reliability is closely linked to mathematics and in particular to statistics, physics, chemistry, mechanics and electronics. Since the human element is almost always part of the systems, often becomes necessary also the psychology and psychiatry. Reliability attempts to answer numerous questions in addition to how much the system will last such as:

- Availability of the system, which means how longer a system lasts between one fault and another, then the smaller will be the repair time and availability.
- Prevention in terms of breakdowns, such as potential failures, intervening on design, materials and maintenance.
- Life Cycle Cost (LCC) of a the system, which includes the initial cost, repair costs, management costs, spare parts warehouse, transport, opportunity costs and the end of service costs.
- Biggest risks, which are referred as the greatest risks such as those that have the worst consequences and that occur more frequently.

Reliability also concerns all that aspects related to the own of a specific asset such as:

- Management costs.

  Reliability involves both the purchase of an item and the maintenance costs of this, due to the fact that the adoption of more reliable materials often involves an increasing in terms of price. In other cases, it happens that the adoption of more reliable technologies implies a parallel decreasing in terms of costs.
- Customer satisfaction.

  If a component does not meet the expected reliability requirements, required by the customer, can happen that there is a disaffection related also to the other products of the same company.
- Resource management.

  Reduce the probability of a breaking down of a component and less resources will be needed to the management of inefficiency situations that are caused by failures.
- Ability to sell products or services.

  The greater reliability of the components allows an increasing of customer satisfaction and gain new market shares.

- Safety.

  Reliability is closely related to some security aspects.

- Quality.

  Is the capability to be relevant to a product's specifications, due to the fact that a poor quality can means a low reliability.

- Maintainability.

Three are the approaches that provides the possibility to better evaluate the reliability of an industrial machine:

- Use the information that comes over a long period of time by many identical machines in the same operating conditions.
- The use of the information that comes from the operation for a short time period of a few machines. Data can be provided as an estimation of the behaviour of a certain degree of confidence, or a certain probability that this data are being true.
- The reliability of the components can be useful to make predictions of the reliability of the whole machine.

Each of the system component has a precise function that must be performed. So, the component specification contains a huge number of data including the description of the function that must be performed, interactions with others components and the environmental conditions in which it operates. The behaviour of a component influences the system at various levels such as:

- Performing the function properly.
- Function performing is not provided.
- A partially fulfilling of the function is adopted.
- During the activity one component provides to disturbs another function or another component.

The period of a device in terms of regular operation ends when any physical-chemical failure phenomenal produced in one or more of its parts determinates a changes in terms of nominal performance such as to consider unacceptable the device behaviour. So, the device switches from the operating status to the failure status.

The causes of failure are due to:

- Solicitations, bump and fatigue.

  This is referred to function of temporal and spatial distribution of loading conditions and of the material response. In this case the characteristics take an important role in terms of structural components, in order to be assessed in the widest form, also incorporating possible errors design, realization errors and defects related to materials.

- Temperature.

  It is an operational variable that is mainly influenced as a function of specific characteristics of the material such as thermal inertia, as well as spatial and time distribution of heat sources.

- Degradation.

  It is a state of physical degradation related to a specific component. This can be manifest after aging phenomenal that appear during the normal activities such as friction between materials or exposure to harmful agents.

- Corrosion.

  It is a phenomenon that depends on the characteristics of the environment in which the component operate. These conditions can cause a physical and chemical degradation and which are capable of making the component no longer suitable.

Now will be considered the kinds of failure that can be append in the industrial process.

- Premature failure, which occur in the first phase of the system operation. The causes can be often related to structural, design deficiency or a installation defects. In terms of reliability of an installation subjected to the manifestation of childhood breakdowns, the reliability of the installation improves its status over time.
- Accidental or random failures, occur in unnamed nominal conditions which put a strain on the components, producing inevitable alterations with consequently losses of operational capabilities. This type of fault occurs during the useful life of the plant and corresponds to unpredictable situations. The probability the occurrence of a fault is independent of the accumulated operating period.
- Failures due to wear are referred to component alterations due to structural and material aging. The start of the wear period is identified by an increasing in terms of frequency of faults until to reach the maximum value. Faults due to wear, occur around the average age of operation.

5.1.2 Availability

In the case of Availability, it is important to make a distinction through two kind of systems, which can be:

- *Not Repairable Systems.*

  Taking into account not recoverable objects or components, the transition from the state of operation to that of failure becomes irreversible. In this case reliability is referred in the strict sense.

- *Repairable Systems.*

  Are considered repairable objects or components. In fact, in this case there is a random alternation of the time intervals with the system, starting from the state of operation until to reach the state of failure. In this case is possible to refers to availability. The availability of a specific component is the probability that it will work without failing in a given and well established time instant t, also referring to well specified environmental conditions.

In the field of process engineering, since the systems are mostly recoverable, due to the presence of a maintenance plan, becomes possible to better evaluate the availability parameter. In the cases of not repairable systems, these concepts coincide.

Taking into account electronic, mechanical and electromechanical components, becomes possible to adopt with good approximation, the negative exponential distribution, which corresponds to a constant failure rate. It is also remarkable to know that in this period o time the machine "has no memory" in the sense of that its behaviour is the same whatever his previous story was.

These are referred as failures which results from the combination of a huge number of random events and which are known as *Poisson faults.* For the mechanical elements which are subjected to fatigue and stresses, becomes no possible separate the external randomly event from an increasing in terms of internal damage, so that the relationship between life of the mechanical element and the damage parameter grows without know if there is any failure in the component.

A component is usually adopted to operate within a system and this involves its interaction with so many other elements that contribute at the completion of a mission. So becomes necessary a *combinatorial reliability analysis* in order to provide models for the study of different connection structures. The interaction of the component that are just being analysed with the rest of the system takes place through physical connections and logical connections.

- Physical connections depends on the structure of the system.
- The logical connections are based on the answers that the various components provide during the various operational phases. In this sense, to obtain the reliability of a system, becomes necessary to analyse the influence that a possible failure of each component has on the functionality of the boundary components and on the whole system.

It is possible to distinguish two models for the availability analysis, such as:

- Series Model
- Parallel Model

Series Model

Taking into account a system composed of only two elements 5.2, these will be connected in series if the failure of only one of them involves causing an instability of the whole system, as described in the *RAMS Analysis* [40] document.

So, the series connection can be represented through a flow chart known as *Reliability block diagram* (RBD) as shown in the figure 5.3 where xi indicates elementary components that work correctly and with x'i those out of service. In fact, if the events can be considered stochastically independent, a damage of a single component is independent with respect the damage of the other components. System reliability is lower than the reliability of the individual components. At the same cost, an action must be taken on the lowest reliability element.

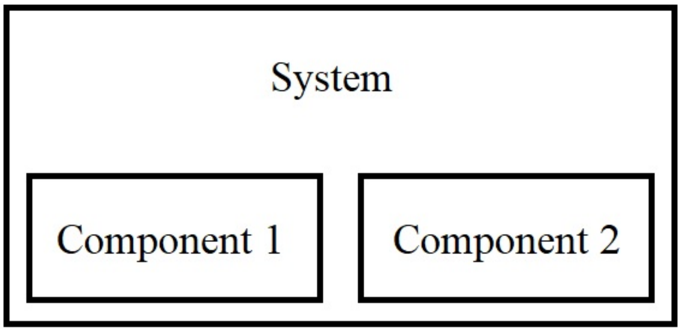

Figure 5.2. Series Model [40]

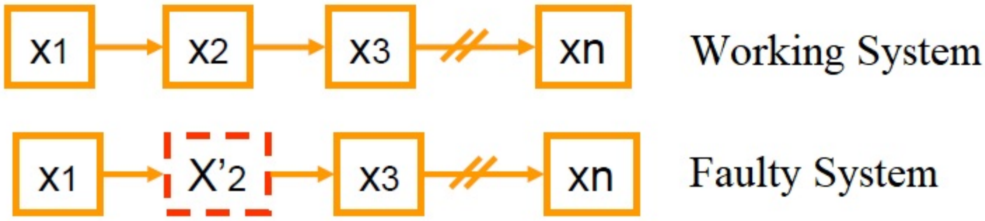

Figure 5.3. Series Model System Status [40]

Parallel Model

Also in the parallel model, is considered for simplicity, a system only composed of two elements 5.4. These components will be connected in parallel if the whole system functionality is guaranteed even when only one component is active.

A parallel connection can be represented through a flow diagram such as the *Reliability Block Diagram* (RBD) as illustrated in the picture 5.5, where xi indicates the elementary components that operate correctly and with x'i those out of service. If the events can be considered stochastically independent, a damage related to the single component can be considered independent with respect a damage of the other components.

Its remarkable to know that in the parallel model, the reliability of the system is greater than the largest reliability referred to the individual components.

Sometimes, there are situations in which it is not possible to apply the series or parallel models 5.6, but it is necessary to use other analysis tools.

Fault Tree Analysis

The *Fault Tree Analysis* (F.T.A) studies the causes of a significant failure that can constitute a risk. Each system is composed by a number of elementary components that can be more or less complex. If their behaviour is assumed to be on/off such as working/failure conditions, it is possible to assign to the single cell a binary value. The purpose of Fault Tree Analysis is to identify the

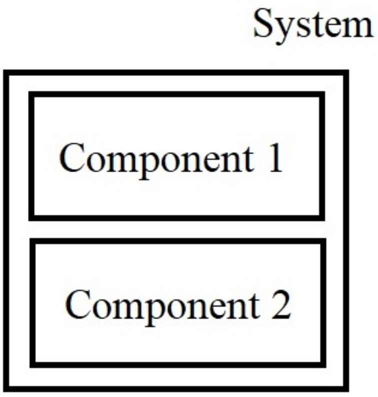

Figure 5.4. Parallel Model [40]

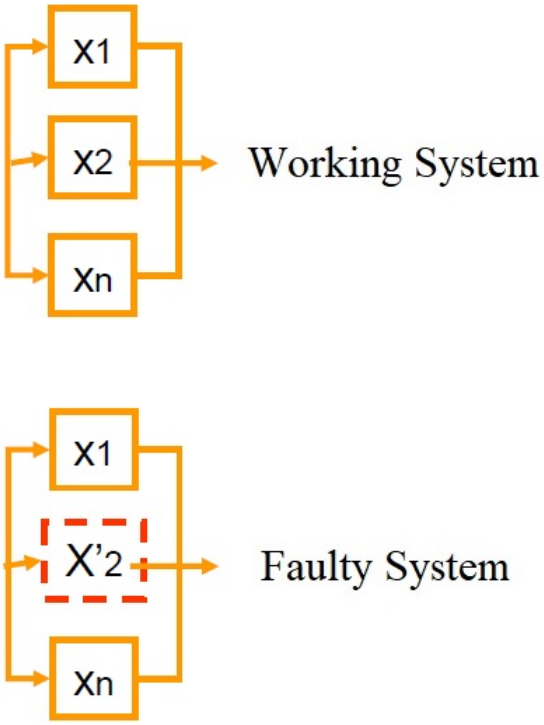

Figure 5.5. Parallel Model System Status [40]

basic events that involves in an accident which can be due by the top-event. These events can be classified as primary, secondary and intermediate faults. This is referred as a deductive method.

Through a symbolic representation [40] of the structure of a plant, or part of it, becomes possible to better highlight the logical interconnections that are present between the various components.

In this way it is possible to identify the structural connections that have caused the system malfunction or part of it. In this way a greater quantitative analysis is obtained. Also the process of transformation ensures that every single event that is repeated in different branches of the tree is properly counted.

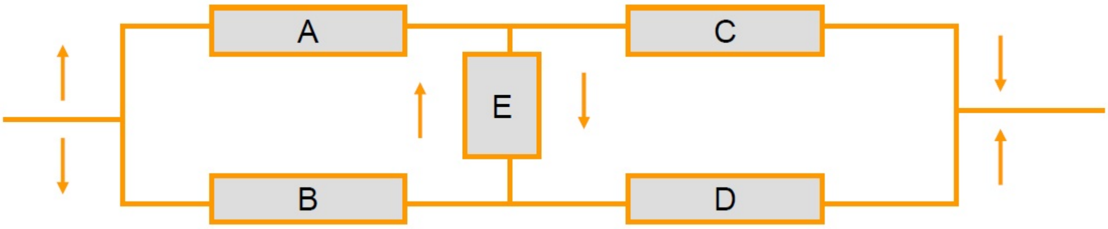

Figure 5.6. Series-parallel comination model [40]

Three are three steps that allow to solve the Tree of Fault:

- Problem definition:
  - Identification of the system.
  - Analysis of possible sources of risk.
  - Identification of the top-events (failures) causing risk.
- Construction of the Tree of Fault, starting from the top event, and going on level after level, until to identify the basic trigger event, in according to a top-down approach.
- Solution of the Tree of Fault, in which consist as first, in an estimation of the probabilistic parameters of each basic event, secondly will be evaluated the frequency of occurrence of the top-event. For this last step is possible to choose one of the two paths:
  - Analysis of *Minimal Cut Sets* (MCS), which is referred to all components that in case of failure causes a breakdown of the system in which they belong.
  - Gate by gate analysis.

Notice that the application of the MCS is possible when the following conditions are met:

- All faults are of binary type.
- The transition between the operating status and the fault status is instantaneous.
- The failures of all the components must be statistically independent.
- The failure rate of each component must be constant.
- The failure rate of a component remains the same before and after it was repaired.

Furthermore, its remarkable to know that by reducing the Failure Tree Analysis into an equivalent tree of Minimal Cut Set (MCS), becomes possible to adopt the Boolean algebra rules for the mathematical solution. So, the Failure Tree Analysis allow to obtain a system oriented quantitative analysis. Instead, for a quantitative analysis oriented to the component and not to the system, is possible to adopt the Failure Mode Effects, and Critical Analysis. This kind of analysis allows to determinates events and consequences, starting from a qualitative analysis such as the Failure Mode Effects Analysis, from which it is derived, through the elaboration of a matrix, the failure modes, the frequency of occurrence, risks and consequences of the failure of a specific component. So, FMECA analysis allows to better highlight and correct the weaknesses of a product at the design level. Furthermore, allow to highlight and correct also the process phases that can be generate some kind of defect of a product.

This kind of approach is sequential and the analysis starts from the bottom up. After the individuation of the critical, becomes possible to evaluate the resonances and the consequences on the whole system. From the analysis must be taken the following information:

- A description of all the fault modes and their consequences, furthermore the defects that are was contained or eliminated.
- Informations about:
  - Reliability analysis.
  - Availability analysis.
  - Maintenance analysis.
  - Security analysis.
- Information taken from the system and service manuals.
- Data for risk and security analysis, which mus be organized by topic and critical issues.

Finally, this kind of approach allow to obtain various types of failure of a specific component and the occurrence frequencies to it related. Furthermore, will also be adopted a database related to the history of the component, that mus be continuously updated and from which to derive the reliability parameters needed for the implementation of quantitative techniques related to reliability and availability of any complex system.

5.1.3 Maintainability

Before explain the maintainability attitude, becomes necessary to describe the maintenance procedure. Maintenance it is referred to the constant control of the plants together with the repair works and replacement that are needed to ensure that the system operate properly and to maintain the reliability standards of the plants. It is divided into a set of technical and administrative actions, including the supervision actions which aims to maintain or bring back the state of a component until this will be able to performs again the requested function. Maintainability consists in the probability that the operations of the reset of the functionality of a component are performed in a well established range of time t for given procedures and resources in terms of qualified staff and replacement parts. Maintainability also provides the properties of any component or system, which at the time instant t of the fault itself will be again able to works properly.

Between the 1950 and 1970 years, maintainability was referred to the fault system or component maintenance in case of fault only. Interventions were carried out only in presence of service interruptions by providing buffer solutions or through the replacement of the damaged component.

After 1970 and until 1980 was born a kind of maintenance philosophy which aimed to the damage system prevention. This kind of methodology was carried out through cyclical and diagnostic inspections technique through the adoption of process sensors. In the 1980, the maintenance becomes a function of the production process. It has allowed a continuous improvement of the process and therefore implementable through the continuous improvement procedures in terms of quality. In 1990 was born the outsourcing of the maintenance function also known as Global Service of Maintenance. In the new philosophy where the company is connected through the network, everything that is not considered as core business is outsourced, with the main purpose of reduce the complexity and the increasing in terms the flexibility.

About the methodological approach related to maintainability, it is possible to distinguish four methods:

- Fault maintenance, which is carried out following the survey of a failure and that the main purpose is to reset a component of a system in order to allow it to works properly again and absolve its specific functions.
- Preventive maintenance which is carried after one or more parameters measurement and the extrapolation of the remaining times before a system failure, in according to the adoption of appropriate models.
  - Cyclic maintenance which appends at a constant date or period.
  - Predictive maintenance, which is based on the evaluation of the residual life of a component that can be estimated in the measure of one of its operating parameters.
  - Maintenance in according to specific condition, which consist in the replacement of a component after the achievement of a measurable threshold, also taking into account its operating parameters.
- Improvement maintenance, which consist in a set of improvement or small actions changes that do not increase the asset value of the entity.
- Production maintenance, which is referred to a set of actions aimed to the system or component prevention, at continuous improvement and the transfer of elementary maintenance functions, through the use of data collection and diagnostics of the entity that must be maintained.

The main purposes related to maintainability are referred to:

- Maintenance of the plant assets, which causes a contrast between the productive and maintenance functions. An absence in terms of maintenance with timely interventions due to necessity, will lead to a gradual deterioration of the company's assets.
- Performance improvement, where the maintenance policies must aim at a continuous improvement and adaptation of the systems. In fact, maintenance must carry out all those small modifications and improvements that are useful to the productive function, in a compatibly way with the company budgets.
- Reduction in terms of cost: targeted and deep interventions must be provided to avoid the increment of global costs which are related to wrong and prolonged interventions or due to replacement of component which could be already reused.
- Growth in terms of availability: this allows to confirms the goodness of the maintenance intervention. On the basis of the reliability and economic analysis will be possible to proceed to the identification of critical assets. So, will be evaluated the failure or the preventive intervention.

In terms of maintainability must be evaluated also the design criteria and the maintenance policies. In fact, critical components must be selected through the adoption of reliability analysis, which are based on only two features:

- Maintainability
  - Class 1: low maintainability.
  - Class 2: high maintainability.
- Replacement costs
  - Class 1: low replacement cost.
  - Class 2: high replacement cost.

Through a scheme 5.7 that allows the comparison between Maintainability and costs in terms of production, becomes possible to make a better choice in terms of maintenance policy.

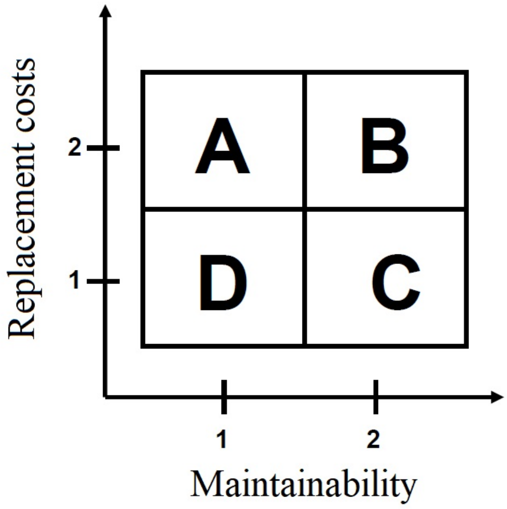

Figure 5.7. Maintainability vs Repalcement costs scheme. [40]

Each of the quadrants that has been illustrated in the picture 5.7, is described as follow:

- Quadrant A: depends on the affordability between intervention costs and replacement costs. However, must be an increasing in terms of maintainability.
- Quadrant B: it is convenient.
- Dial C: depends on convenience between intervention costs and replacement costs. Dial D: It is not convenient perform the maintenance.

The maintenance plan related to critical components is illustrated in a specific block diagram 5.8.

Maintenance have the main purpose, to making it possible the management in a competitive way, in order to allow as much as possible a low level of costs related to production. The overall maintenance management costs are indicated as follow:

- Preventive and Corrective maintenance costs.
- Loss of production in terms of costs;

So, becomes necessary to find the right compromise between the level of preventive and corrective maintenance, on the basis of the techno-economic and reliability consideration.

5.1.4 Safety

As described in the Safety and Risk Analysis slides of Andrea Carpignano course, Safety in the industrial automation is referred to the condition of minimum probability of incurring in accidents for men, property and for the environment. The distance from the safety condition is measured through the use of the concept of Risk, that is the possibility that there is an undesired event of uncertain character. The mathematics definition adopted involves the product between the frequency of occurrence of the event that produces the damage to the entity of the damage itself. The units of measurement that can be taken are several such as deaths per year, working hours lost per year or price per year. So, becomes necessary to analyse the Safety Life Cycle for the design of process systems.

For all the activities of the Safety Life Cycle of Electrical, Electronic, and Programmable Electronic Systems, was introduced the Standard IEC 61508, which is an international standard that sets a general approach for those activities related to the Safety life cycle of the industrial component, in order to perform Safety Functions. So, the Standard IEC 61508 provides a method for the development of specific safety requirements, as well as introduce and use the safety integrity levels also known as SIL.

Then, the functional Safety is referred as a part of the total safety, in which depends on a system, or a component, operating properly in response to one or more logic inputs. This part is strictly related to the process and to the Basic Process Control System also known as BPCS. This depend on the correct working of the Safety Instrumented System (SIS) and other independent Protection Layers. Then, a Safety Instrumented System is defined as a combination of one or more:

- Sensors such as Transmitters or Switches.
- Logic Solvers with E/E/PE technology, where:
  - E = Electric such as Electromechanical relay.
  - E = Electronic such as Logical solid state.
  - PE = Programmable Electronic such as PLC.
- Final elements such as Solenoids, Actuators or Valves.
- Input and output devices
- User interfaces.
- Feeders.

In addition to the SIS, there is also the Safety Instrumented Function (SIF), which is a function that has to be implemented by a Safety Instrumented System (SIS) and by other independent Protection Layers and which aims to maintain or restore the safety in the process, in relation to a specific dangerous event as well as in the cases when one or more predetermined conditions are not met.

The IEC 61508 considers two categories of systems/subsystems. A system/subsystem is defined as Type A if it meets the following requirements:

- Failure modes of all the constituent components are well defined.
- The behaviour of the system under fault conditions can be determined in a comprehensive and exhaustive way.
- There are sufficient data from the field or from a test to support the reliable data associated with different failure modes.

A system/subsystem is defined of Type B if not all of the above criteria are met.

Typical examples of components of Type A, according to the standard, are for example: switches, relays or solenoid valves. Typical components of Type B are: microprocessors and other electronic components that implement complex logics.

The Safety Integrity Level (SIL) is a discrete level, which corresponds to a set of safety integrity values, where SIL 4 is the highest and SIL 1 is the lowest. It is a complex parameter indicating a range of probability that an SIS run properly a safety instrumental function within a preset period of time and respecting defined technical, architectural, functional and design requirements. It is important to remark that the SIL is allocated to an independent Safety Instrumented Function (SIF), that can be implemented by one or more SISs, not directly to a SIS (that anyway inherits the SIL allocated to the implemented SIF).

Regarding the definition of Safety Integrity Level (SIL) instead, is possible to consider this as a discrete level, which corresponds to a set of safety integrity values, where SIL level four is referred to the highest and SIL level one is referred to the lowest. It is a complex parameter that allows to indicate a range of probability that a SIS run properly a safety instrumental function within a preset period of time and respecting defined technical, architectural, functional and design requirements. It is important to remark that the SIL is allocated to an independent Safety Instrumented Function (SIF), that can be implemented by one or more SISs, not directly to a SIS that anyway inherits the SIL allocated to the implemented SIF.

After these descriptions becomes possible to say that the Safety life cycle can be divided in 12 phases which are described as follow:

- Phase 1 General Conception of the Functional Safety Project.
- Phase 2 Definition of the overall objective of the Functional Safety Project.
- Phase 3 Risk Analysis.
- Phase 4 Allocation of the safety functions to the Independent Levels of Protection and SIL Allocation.
- Phase 5 Specification of the requirements of the Safety of SIS.
- Phase 6 Design and engineering of SIS and SIL Verification.
- Phase 7 Factory Acceptance Test.
- Phase 8 Installation and Commissioning Service of SIS.

- Phase 9 Site Acceptance Test.
- Phase 10 Operation and Maintenance.
- Phase 11 Modifications.
- Phase 12 Decommissioning of SIS.

So, the application of Safety Life Cycle IEC 61508 Standard is resumed through a block diagram illustrated in the picture 5.9. Furthermore, are adopted four steps that allow to better understand the meaning of the Safety Life Cycle block diagram.

- 1. Definition of SILs according to the risk analysis of the system.
- 2. Design of safety.
- 3. Checking of the level of SIL imposed.
- 4. Commissioning and management to maintain the level of SIL of the project.

Finally, its remarkable to know that other standards are derived from the IEC 61508, such as:

- STANDARD IEC 61511 Functional Safety: Safety Instrumented Systems for the Process Industry Sector.
- STANDARD IEC 61513 Nuclear Power plants - Instrumentation and Control for Systems important to safety - General Requirements for Systems.
- STANDARD EN 50402 Electrical Apparatus for the detection and measurement of combustible or toxic gases or vapours or of oxygen. Requirements on the functional safety of fixed gas detection systems.
- STANDARD IEC 62061 Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems.

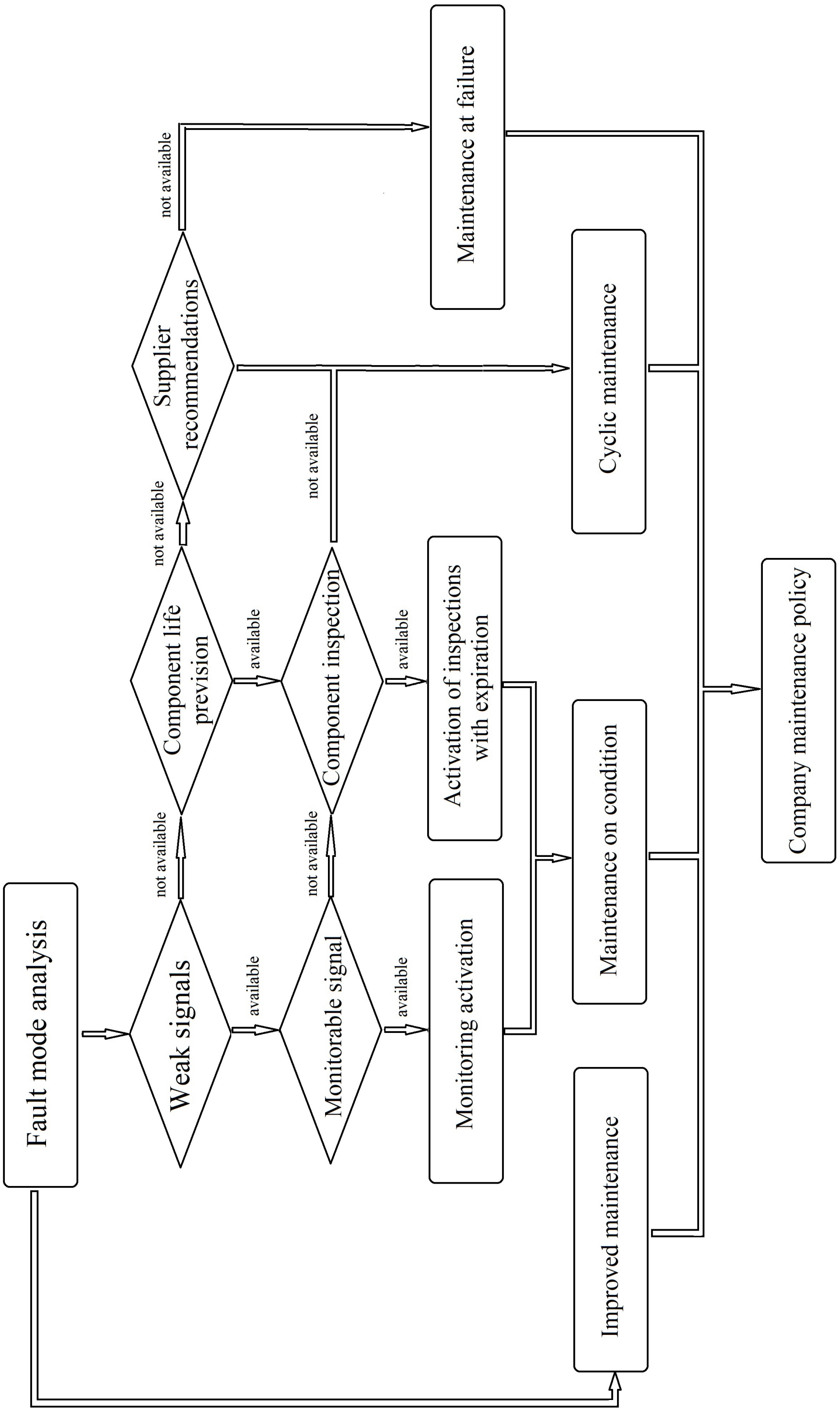

Figure 5.8. Maintainability blocks diagram. [40]

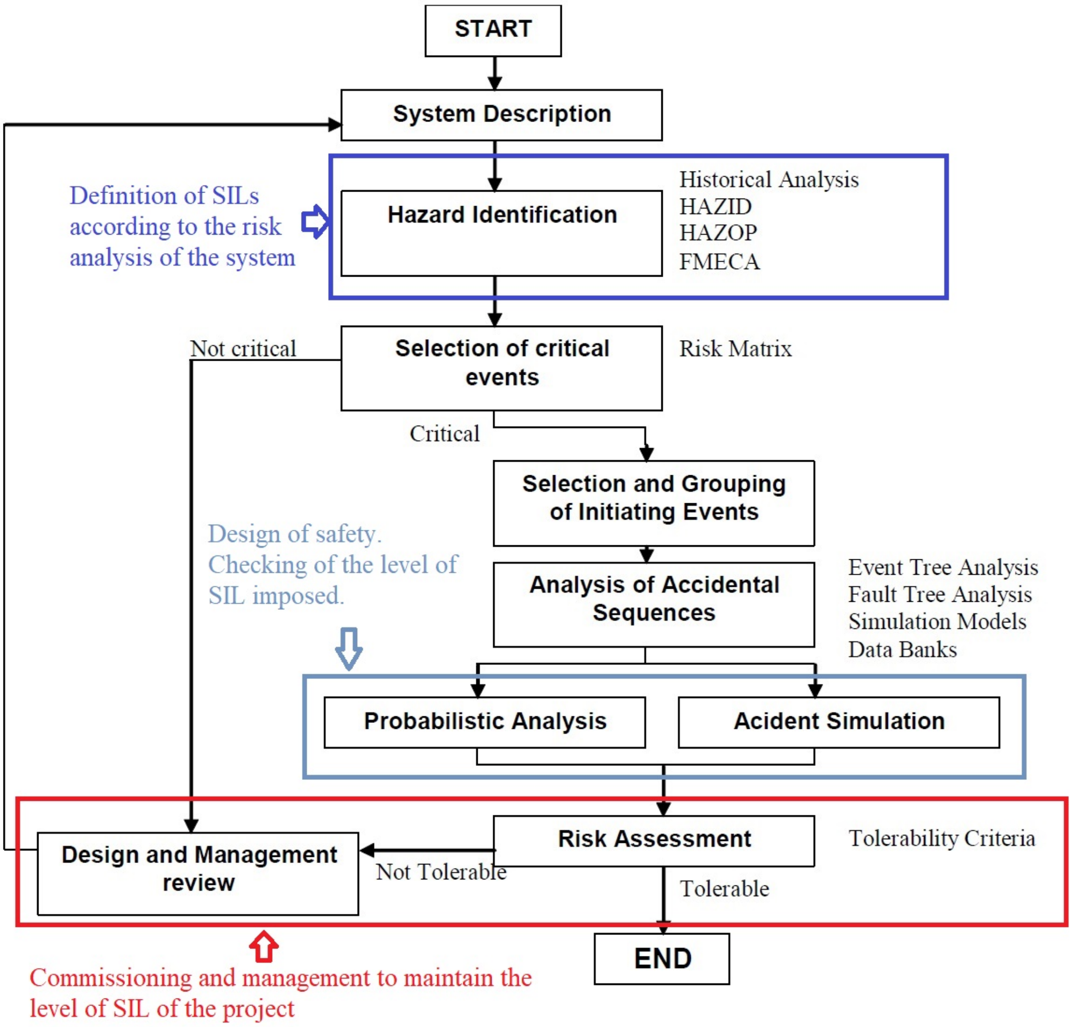
START
System Description
Definition of SILs according to the risk analysis of the system
Hazard Identification
Historical Analysis
HAZID
HAZOP
FMECA
Not critical
Selection of critical events
Risk Matrix
Critical
Selection and Grouping of Initiating Events
Design of safety. Checking of the level of SIL imposed.
Analysis of Accidental Sequences
Event Tree Analysis
Fault Tree Analysis
Simulation Models
Data Banks
Probabilistic Analysis
Acident Simulation
Risk Assessment
Tolerability Criteria
Design and Management review
Not Tolerable
Tolerable
END
Commissioning and management to maintain the level of SIL of the project

Figure 5.9. Safety Life Cycle IEC 61508 Standard blocks diagram. “Slides of Safety and Risk Analysis course” (Andrea Carpignano).

Chapter 6

Practical case study of automation of an industrial process

In this chapter, will be taken into account an example of automation of an industrial process, with the aims to describe its process, the functionality of each component or devices of the whole system and finally will be studied and evaluated the risks related to this industrial plant, in order to apply a safety solution that could guarantee to avoid damages in the factory or lost of production due to the system slow down.

In the figure ref fig:my-project is illustrated an industrial automation process which describe the process of a fluid transfer by means of a hydraulic pump to a container reactor. This process was automatized by two basic Process Control Systems, through the use of PLCs.

The first PLC system, whose task is to control the speed of the pump, through the measurement of the flow that coming out from the hydraulic pump, in order to better evaluate the necessity of reduce or not the speed of the pump 6.2.

The second PLC system takes care of measurement related to the fluid level which is inside the reactor, in order to avoid an exceeding in terms of fluid quantity, causing a damage to the entire system 6.2.

In case that the fluid level reach a dangerous level, the second PLC system must be able to close the reactor inlet valve as first, and open the reactor discharge valve, in order to reduce the level of fluid inside the reactor and consequently its temperature and pressure. The closure of the reactor inlet valve will result in a null reading of quantity of flow by the sensor connected to the first PLC system, thus leading to the shutdown of the hydraulic pump. Both basic Process Control Systems are connected via profinet bus to the *Supervisory Control And Data Acquisition System.* This SCADA system will then take care about the acquisition of the flow and level information, with the aim of sending the setpoints to the basic process control systems. With the SCADA system it is also possible to manage communications, analyse acquired data and display the alerts and events. Moreover, the Supervisory control system allow early identification of any kind of damage related to any component of the industrial process, thus guaranteeing a greater level in terms of safety, allowing to make safe the whole work environment and providing faster restoring times.

At this point becomes possible to perform the *Risk Analysis* related to the automation process that has just been described. For the risk assessment it was decided to consider the HAZOP 5

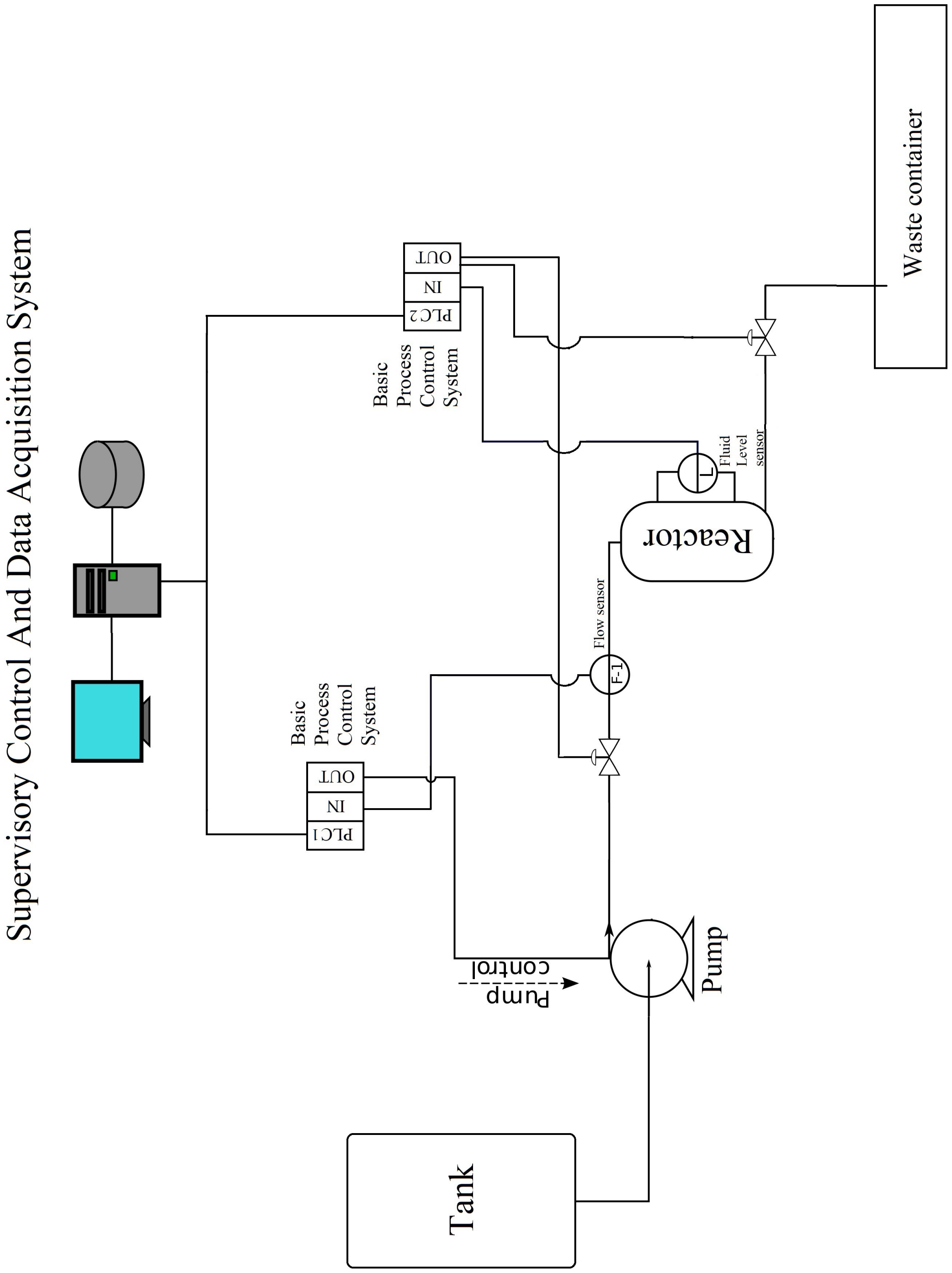
Supervisory Control And Data Acquisition System
Basic Process Control System
PLC1
IN
OUT
Basic Process Control System
PLC2
IN
OUT
Waste container
Fluid Level sensor
L
Reactor
Flow sensor
F-1
Pump control
Pump
Tank

Figure 6.1. Example of Automation of an Industrial Process.

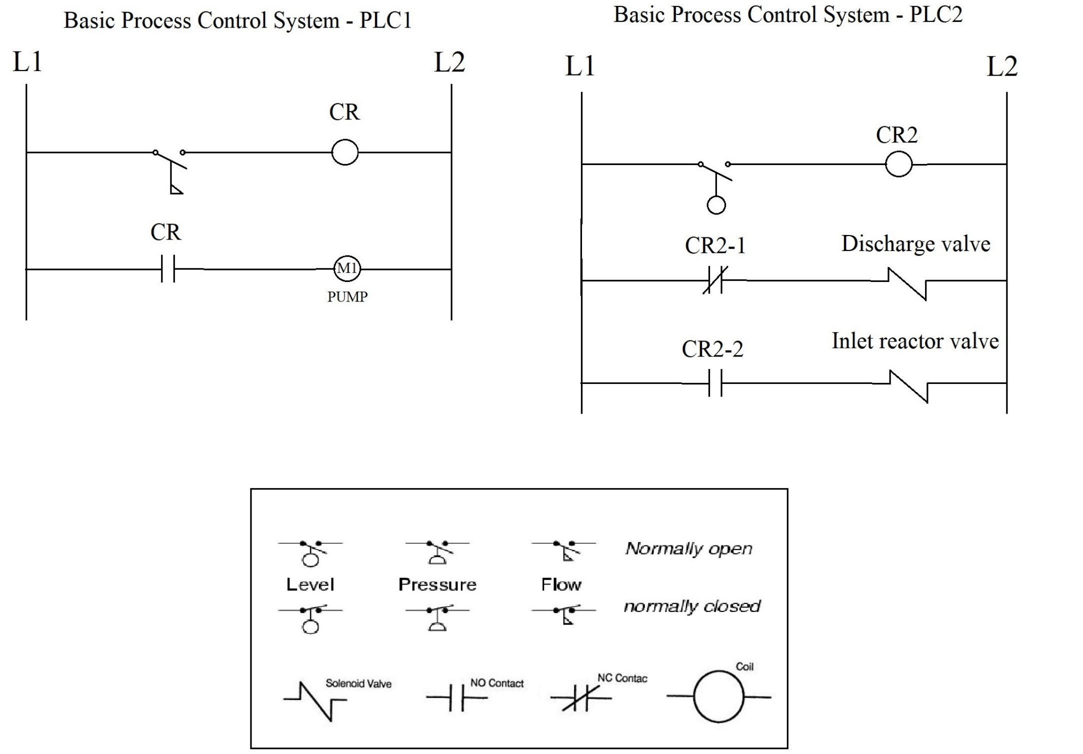

Figure 6.2. PLCs Ladder logic diagrams. In the PLC2, when the level of fluid inside the reactor exceeds the limit, the sensor will be closed and consequently the discharge valve will be opened, in opposition to the inlet valve which will be closed. Subsequently, due to the fact that the Programmable logic devices are connected through the PROFINET 4.6.3 network and sends sensor information to the SCADA system, the PLC1 will receive the status of the flow through the flow sensor, and the pump will be stopped for safety reasons.

method which has been previously described in this thesis work, in order to provide a systematically review of the process and operations in order to identify potential damages from the design intent, rather than examining their possible causes and assessing its consequences. So, was been identified the potential damages, considering the characteristic parameters of the component, as well as temperature, pressure and level of fluid. The intention of performing an HAZOP is to review the plant project in order to better identify the design and engineering issues that may otherwise not have been found. In a subsequent examination of parameters, was been possible to identify the consequences and dangers to it related. These conclusions were useful in order to obtain better management recommendations for their management. Thus, the possible causes can be related to:

- The pump works bad increasing the speed. This can be due to various causes which may be referred to:
  - Mechanical breakage.
  - Accidental switching.
- The control valve of the inlet flow to the reactor is damaged and remains open.

- The flow sensor is damaged by maintaining a constant flow reading or within the limits, with obvious cause of the speed increasing of the hydraulic pump.
- The level sensor does not detect an excess of fluid contained inside the reactor, causing an increasing in terms of pressure.
- When needed, the drain valve is not activated due to:
  - Mechanical malfunction.
  - PLC system malfunction.
- Communication system malfunction.

After evaluating the possible causes of risks, it was decided to implement a Safety Instrumented System such as that illustrated in the picture 6.4. This system will activate its safety functionality in case of which any component of the two Basic Process Control Systems, including sensors and valves that are no longer able to function properly, thus leading to a possible increasing in terms of pressure and temperature inside the reactor which would cause damages to the entire automation system of the industrial process 6.2.

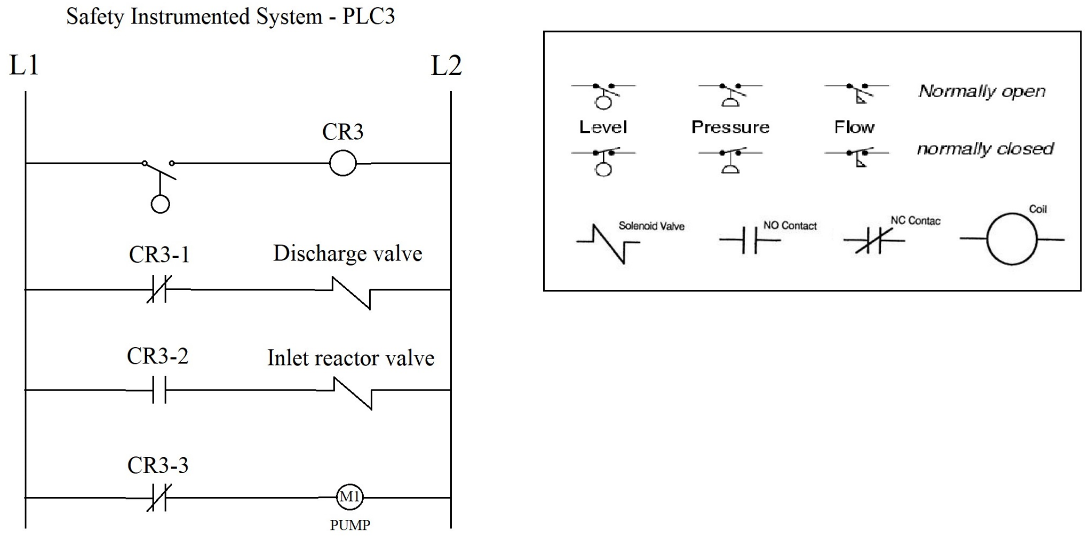

Figure 6.3. PLC3 Ladder logic diagrams. In case of pressure limit exceeding, the pump will be turned-off, the inlet valve of the reactor will be closed and the discharge valve will be opened.

So, the Safety Instrumented System read the information received from the pressure sensor connected to the reactor, and when the pressure limit is reached, the third PLC will send a signal to close the inlet valve of the reactor, subsequently a second signal will open the outlet valve of the reactor in order to reduce the pressure and the temperature inside the reactor. In order to avoid possible problems related to the speed of the pump, in case of which:

- the flow sensor does not work properly;
- the pump can not be stopped through the Basic Process Control System;

a safety line connected to the hydraulic pump and whose coming from the Safety Instrumented System, will be available to shutdown the pump.

Other possible safety problems could be also related to the presence of the SCADA system and to the fact that the whole system can be managed from the remote network. Since the presence of the Supervisory Control And Data Acquisition System, it is possible to guarantees management and supervision of the entire system even through remote network, but also leads to possible vulnerabilities related to external cybernetic attacks. In fact, since the management of these systems is guaranteed by systems connected to the network and possibly also through internet connections, a malicious user could be allowed to manage and control the entire industrial process systems, going to alter the parameters needed for correct functioning of the industrial process and thus causing serious damage to the entire system and to the people present in the factory. Furthermore, since the information of the sensor was stored into specific databases, it must not be allowed in any cases, the exposure of such databases through the remote network, but must be connected only through the local network. The exchange of credential and information must always take place through a secure and encrypted channel.

In the case that the industrial process is managed remotely it is important that the communication channel will be established through a *Virtual Private Network* (VPN) [42], possibly through security protocols such as IPsec [41]. Another import thing that must be taken into account is related to the safety of the IT devices adopted in the SCADA systems for the industrial process supervision. In fact, a proper choice of the Operating System can be useful to guarantee a good protection of the hardware resources.

Must be considered also the Operating Systems installed in the Supervisory devices in order to guarantee a good level of safety related to the hardware resources. A solution could be obtained through the adoption of unix base systems and the application of security mechanisms at the operating system level such as SELinux [43]. In fact, this kind of functionality allow the isolation of hardware resources dedicated to the industrial process management so that these resources can be accessible only from local and non-remote networks.

Furthermore, any software update must be made physically and never through remote network. This kind of approach substantially reduce the risk of information alteration, including the risk of alter the productive systems with malicious software. However, it should be noted that also in the case of software update without the use of remote connections, other kinds of vulnerability can be founded. In fact, also through a physical update adopted from qualified personnel, can be introduced malicious software, due to the fact that the qualified personnel could have received an infected update drive without know it. A possible solution could be related to the application of *Artificial Intelligence* (AI). In fact, AI aims to guarantee, on basis of well-known safety specifications stored inside of it, the possibility to independently manage and verify the reliability of each update of the entire automation system, without any external human intervention. Moreover, in the case of a malicious software try to infect the system, AI will be able to lock its attempt in a time extremely small with respect the time that will be spent by the human intervention.

Another aspect that must be considered is related to the maintainability 5.1.3 of the industrial plant and its components and devices. At this point, becomes necessary to consider a good level of redundancy for the automation system, in order to be able to avoid slowdowns in terms of production, which can lead substantial losses in terms of money. However, it should be noted, that the application of redundant components and any artificial intelligences would lead to a substantial increasing in terms of costs related to the design phase of the industrial plant. In my opinion this kind of costs, can be overthrow thanks to the maintenance interventions reduction and tanks to the reduction of probability that a serious failure may be append.

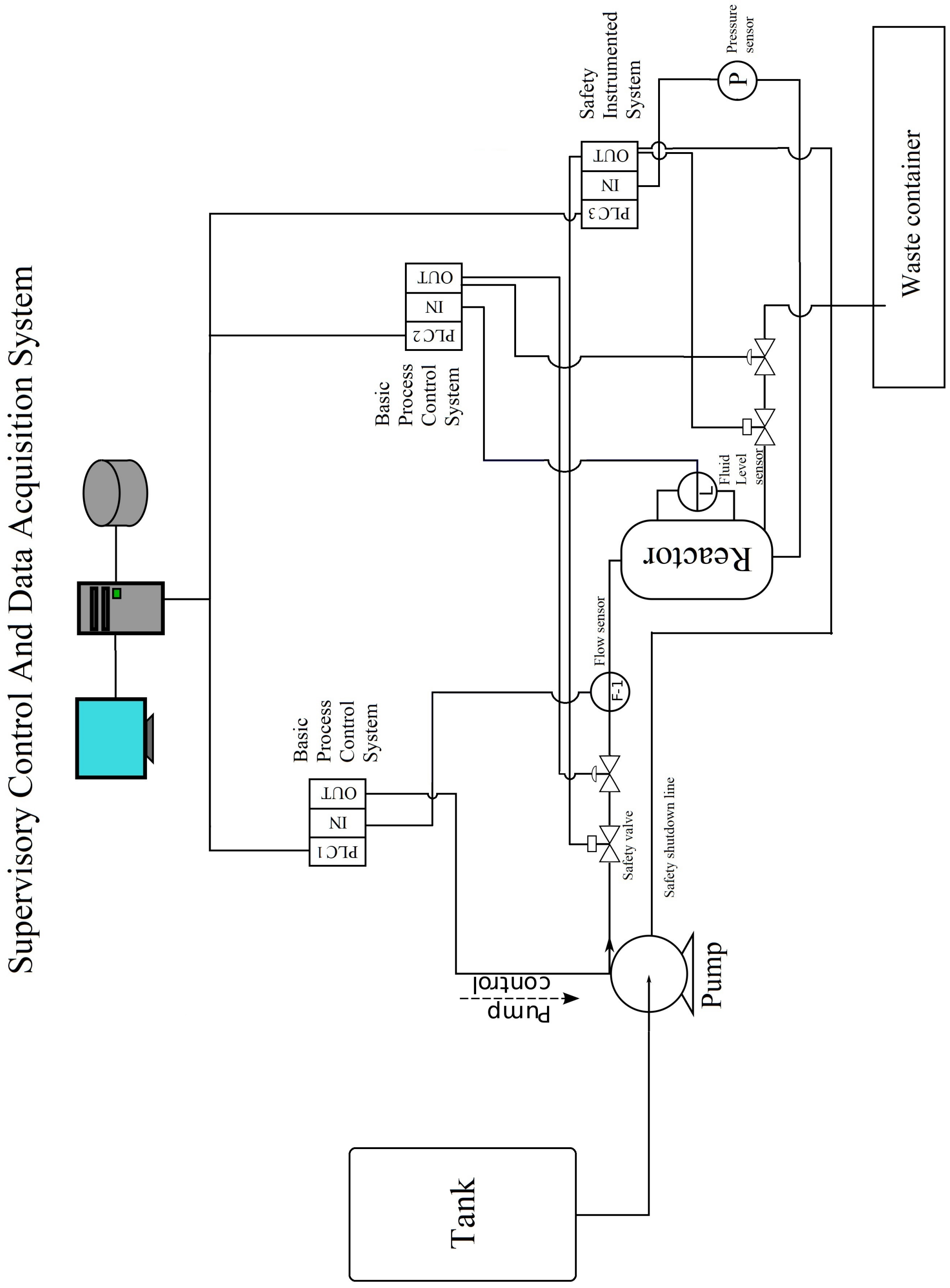

Figure 6.4. Safety mechanisms for an Industrial Process.

Chapter 7

Future developments and conclusions

With the advent of the Industry 4.0, the automation of industrial processes have reached a good level of evolution with respect the previous industrial revolutions, in terms of reduction of productivity costs, safety, management, production efficiency and as last but not the least in terms of importance, the remote control of the systems and of the component which are present inside process industry.

However, it is reasonable to think of further solutions that could improve the industrial process in all its requirements, including the prevention in terms of risks and the implementation of more efficient security mechanisms. A possible solution that was introduced in the previous chapter titled as *"Practical case study of Automation of an Industrial Process"* 6, is related to the application of the Artificial Intelligence in the industries. The reasons can be different and will be described below.

First of all, Artificial Intelligence can be adopted in order to manage a huge amount of data coming from the industrial devices and that are so called or also known as Big Data. This is such a large amount of information that the human mind cannot handle. On the contrary, artificial intelligence can succeed.

By analysing this kind of data, a company could be able to reduce its costs, but also immediately find design errors. In practice, in the industries, Artificial Intelligence will have the main task of monitoring the various processes and analyze the correct work of the industrial machines. So, Artificial intelligence will bring a synergy between the various tools and technologies adopted in the Industry 4.0.

In according to the experts, the implementation of this technology will allow news in some sectors on all that of energy, health care and safety. But, artificial intelligence actually help the IIoT 4.2.5 devices, such as for example an industry related to electricity. Some machines with high temperatures could risk an overloading. In fact, without the adoption of the artificial intelligence, industrial machines would send messages to the workers who must manually remedy the situation. But in this scenario, does not become always possible to actuate interventions without losses in terms of production time. On the contrary, with the support of Artificial Intelligence the systems would be automatically cooled after the first signal whose come from the safety sensor.

Even if there is no lack of criticism about the accuracy of these systems. Taking into account the network security, it is possible to think about human errors. In fact, most cybernetic attacks could be properly avoided by handling attachments, links and updates. For this reason, the application of artificial intelligence could be a proper solution in all major electronic devices of the future and will help users to avoid falling into various phishing or social engineering traps, in special cases of Industrial Internet of Things(IIot) 4.2.5 and IoT systems.

Bibliography

[1] Che cos'è l'Automazione http://automazione-plus.it/che-cose-lautomazione_71032/

[2] Automation Pyramid, Standard Computer-Integrated Manufacturing (CIM). https://www.researchgate.net/figure/Automation-Pyramid-Standard-Computer-Integrated-Manufacturing-CIM_fig1_331613336

[3] Automation-CIM-Architecture. https://www.google.it/Automazione-CIM-Architetture.pdf

[4] Automazione industriale. http://www.treccani.it/enciclopedia/automazione-industriale

[5] What is a 4-20 mA current loop? https://www.fluke.com/en/learn/best-practices/test-tools-basics/process-tools/what-is-a-4-20-ma-current-loop

[6] HART technology communication protocol. https://fieldcommgroup.org/technologies/hart/hart-technology-detail

[7] Industrial control system. https://en.wikipedia.org/wiki/Industrial_control_system

[8] Computer Integrated Manufacturing (CIM) https://www.google.it/url/Computer-integrated-manufacturing

[9] Fieldbus. https://en.wikipedia.org/wiki/Fieldbus

[10] The Architecture of PLC. https://mec6004suheyb.wordpress.com/2016/03/12/architecture-of-plc/

[11] When to use a programmable automation controller (PAC). https://www.motioncontroltips.com/when-to-use-a-programmable-automation-controller-pac/

[12] Danielle Collins Mechanical Engineer — Technical Content Marketing Authority— Product Management Expert — Queen of Linear Motion. https://sm.linkedin.com/in/daniellecollins

[13] Industria 4.0: storia, significato ed evoluzioni tecnologiche a vantaggio del business. https://www.digital4.biz/executive/industria-40-storia

[14] Industria 4.0: cos'è e quali sono i vantaggi. https://tecnologia.libero.it/industria-4-0-cosa-e-e-quali-sono-i-vantaggi-12664

[15] Industry 4.0: The Digital German Ideology. https://www.triple-c.at/index.php/tripleC/article/view/1010/1170

[16] Industria 4.0-Wikipedia. https://it.wikipedia.org/wiki/Industria_4.0

[17] Key Enabling Technologies. https://ec.europa.eu/growth/industry/policy/key-enabling-technologies_en

[18] Message Queuing Telemetry Transport. https://en.wikipedia.org/wiki/MQTT

[19] Fuzzy Logic. https://en.wikipedia.org/wiki/Fuzzy_logic

[20] Neural Network. https://en.wikipedia.org/wiki/Neural_network

[21] Distributed Control System. https://en.wikipedia.org/wiki/Distributed_control_system

[22] PROFIBUS DP. https://procentec.it/contenuto/cos%C3%A8-profibus-dp/

[23] PROFIBUS DP netwokrk scheme https://www.icpdas.com/root/product/solutions/industrial_communication/fieldbus/profibus/profibus_intro.html

[24] PROFIBUS PA https://procentec.it/contenuto/cos%C3%A8-profibus-pa/

[25] PROFIBUS PA netwokrk scheme https://www.google.it/url?profibus-pa

[26] Frequency Shift Keying. https://it.wikipedia.org/wiki/Frequency-shift_keying

[27] WHAT IS PROFINET PROTOCOL. http://www.eltra.it/encoderpedia-glossario-tecnico/cose-il-protocollo-profinet/

[28] PROFINET Wikipedia. https://en.wikipedia.org/wiki/PROFINET

[29] Profibus and Profinet International. https://de.wikipedia.org/wiki/Profibus_%26_Profinet_International

[30] La valutazione dei rischi negli stabilimenti industriali. https://www.puntosicuro.it/sicurezza-sul-lavoro-C-1/settori-C-4/industria-C-14/la-valutazione-dei-rischi-negli-stabilimenti-industriali-AR-11589/

[31] Safety in the process industries. http://ing.univaq.it/fumarola/page/analisi_rischio/esempio_hazop.html

[32] 5 Programming Languages Used To Program a PLC. https://codesmithdev.com/5-programming-languages-used-to-program-a-plc/

[33] Sequential Function Charts. https://it.wikipedia.org/wiki/Sequential_function_chart

[34] Function block diagram. https://en.wikipedia.org/wiki/Function_block_diagram

[35] Instruction list. https://en.wikipedia.org/wiki/Instruction_list

[36] SIMATIC Siemens. https://www.google.it/url/support.industry.siemens.com

[37] Reti di automazione. https://www.google.it/url/RetiAutomazione.

[38] Park's Transformation. https://en.wikipedia.org/wiki/Direct-quadrature-zero-transformation-Park

[39] Human reliability analysis methods and tools. https://www.sciencedirect.com/science/article/pii/B9780081018699000121

[40] RAMS Analysis. http://www.pjmsrl.it/site/images/Analisi-RAMS.pdf

[41] IPsec. https://en.wikipedia.org/wiki/IPsec

[42] VPN. https://en.wikipedia.org/wiki/Virtual_private_network

[43] SELinux. https://en.wikipedia.org/wiki/Security-Enhanced_Linux