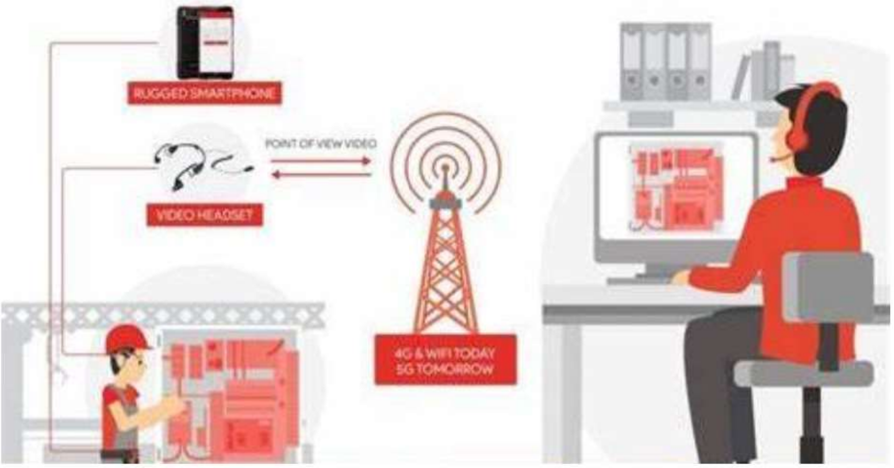
الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
جامعة وهران 2 محمد بن أ حمد
معهد الصيانة و الأمن الصناعي
Université d'Oran 2 Mohamed Ben Ahmed
Institut de Maintenance et de Sécurité Industrielle

Séminaire sur la télémaintenance

Seminar on Remote Maintenance

(Support de Cours)



Pour les classes : 2éme année Master : Maintenance des automatismes et de l'instrumentation industrielle

Présenté par : Dr AISSANI Nassima

2023

Summary

Figures List

Foreword

In an ideal world, it would be ideal if engineers were able to consistently and continuously uphold and rectify the functionality and operations of various products from their current locations, all the while avoiding any and all expenses and time committed to physically journeying to different locations. Although, this currently may not be feasible in numerous scenarios, there is a discernible trend within the industry that is moving towards this direction. What initially commenced over three decades ago as a method for vendors to provide assistance and support to users of mainframe computers has evolved and expanded to involve a wide range of applications, including but not limited to teleservice and remote maintenance. Consequently, this development has now branched out to cover a broader and more extensive realm, often referred to as remote repair, diagnostics, and maintenance.

the term "Remote repair, diagnostics, and maintenance" includes a wide range of technologies and applications, all of which are crucial in today's digital age. At its most fundamental level, information technology can refer to a simple phone call made to seek assistance in resolving minor technical issues. However, at its most intricate level, it comprises a comprehensive suite of computer and network applications that seamlessly integrate with one another. These applications are designed to continuously monitor the performance of various systems, identify any potential problems or faults, and automatically generate requests for attention from trained service technicians who possess the necessary expertise to address and resolve these particular issues.

To address the concept of remote maintenance, it's essential to understand the core principles of maintenance. This document will begin by providing an overview of maintenance and its fundamental aspects. Subsequently, the discussion will shift to remote maintenance, encompassing the nuances of remote communication and control, along with an exploration of industrial networks and their connectivity constraints. Valuable recommendations will be offered to tackle these constraints. Following this, the various facets of remote maintenance, such as teleservice, telediagnostics, and remote maintenance, will be elucidated, accompanied by insights into technological advancements in this domain.

Chapter 3 will introduce some prominent platforms designed for remote maintenance in industrial settings. Finally, in Chapter 4, we will delve into the details of an experimental remote maintenance platform that was developed within our laboratory at the Institute of Maintenance and Industrial Safety.

CHAPTER 1 : Maintenance basics

1. Introduction

Maintaining production equipment is a key factor in the productivity of companies where the notions of responsiveness, cost and quality are increasingly important, and where it is important to be able to rely on a high-performance production system at all times. Equipment availability at the right time is a prerequisite for smooth production. In this industrial environment, the constraints of technological realization costs, site accessibility and geographical distribution mean that data and maintenance processes have to be distributed. Access is remote, giving rise to remote maintenance [1].

2. Definitions

the activity of keeping a building, vehicle, road, etc, any system in good condition by checking it regularly and repairing it when necessary (Cambridge dictionary)

It is often talked about maintenance and optimization of the operation of the facilities. This mission is structured around the following areas:

1. Preventive maintenance: planning of maintenance operations, technical rounds and meter readings.
2. Corrective maintenance: quickly restoring the operation of failed equipment

2.1 Maintenance

Maintenance functions can be defined as repair, maintenance and overhaul (MRO), and MRO is also used for maintenance, repair and operations. Over time, the terminology of maintenance and MRO has begun to become standardized. The United States Department of Defense uses the following definitions:[2]

“Any activity—such as tests, measurements, replacements, adjustments, and repairs—intended to retain or restore a functional unit in or to a specified state in which the unit can perform its required functions.

All action taken to retain material in a serviceable condition or to restore it to serviceability. It includes inspections, testing, servicing, classification as to serviceability, repair, rebuilding, and reclamation.

All supply and repair action taken to keep a force in condition to carry out its mission.

The routine recurring work required to keep a facility (plant, building, structure, ground facility, utility system, or other real property) in such condition that it may be continuously used, at its original or designed capacity and efficiency for its intended purpose."

2.1.1 Maintenance objectives :

" Zero breakdowns is the main objective of maintenance."

The goal of the maintenance teams is to keep the production facilities in perfect condition and ensure maximum overall productivity while optimizing costs. It's why maintenance objectives can be classified into tow categories :

2.1.2 Financial objectives :

1. Cost Tracking and control

Strategic maintenance management requires smart budgeting. Lot of software enables to budget for maintenance more accurately. Software can help track maintenance costs by tracking the costs of maintenance work and MRO inventory purchases. Many indicator can be used such as equipment cost history, inventory cost history, work order cost history, and YTD (year to date) and LTD (life to date) equipment cost history.

2. Comply with Regulations

Many industries might follow many safety norms regulations, for example, oil and gas industry must follow ISO (an International Organization for Standardization) and national regulation (Ministary of energy and mines). Achieving these objectives will reduce the costs of insurance contracts.

2.1.3 Operationals objectives:

1. Minimize Equipment Failure and Production Downtime

Maintenance teams strive to maximize equipment availability, and they are better able to do so when preventive maintenance jobs are managed well. Maintenance technicians must be able to stay on top of preventive maintenance to keep machines running so that failure and production interruptions are minimized. At the same time, downtime cannot be avoided entirely, so when machines do need repairs, they must be done quickly and efficiently.[3]

2. Increasing machine useful life

When machine is properly and quickly maintained it lasts longer. Over time good maintenance practice improves reliability, availability, and maintainability. This is done through proactive maintenance work, which can include preventive, predictive, and condition-based maintenance.

3. Product quality

When machine is well maintained produced parts corresponds to the original design a decrease in the number or products that need to be scrapped or reworked. And more products are good quality, more customers are satisfied and more sales are made.

2.2 Maintenance types

According to the adopted strategy, six type of maintenance actions are defined. They are a range of proactive and reactive methodologies. In [4] an exhaustive overview was made to present different classifications of maintenance strategies, but had confirmed this classification :

1. “preventive maintenance”,
2. “corrective maintenance”,
3. “predictive maintenance”,
4. “condition based maintenance”
5. “proactive maintenance”

2.2.1 preventive maintenance:

Until 2019, 21084 research paper was dedicated to preventive maintenance. preventive maintenance tries to anticipate equipment failure and take corrective action before mechanical breakdown occurs. It is based on inspection schedule to find and fix small issues before they have a chance to develop into big problems “An ounce of prevention is worth a pound of cure.”. “scheduling” comes in two forms: based on time or use. It can be done according to a calendar dates for example every week, every month… or according a number of using cycle. [5]

Preventive maintenance avoids the waste of time and breakdown of the production line. The consistent practice of Preventive Maintenance improves the performance and safety of the machine or equipment used in any process. And finally, Preventive Maintenance tackles the cost affair from the very initial stage of operations.

2.2.2 corrective maintenance:

Less cited type with 3944 research paper, Corrective maintenance is often associated to breakdowns or reactive maintenance and can include troubleshooting, disassembly, adjustment, repair, replacement and realignment. Corrective maintenance tasks can be either planned or unplanned and occur for three different reasons:

1. When condition monitoring highlights an issue
2. When a potential fault is detected through routine inspection

3. When a piece of equipment breaks down

Corrective maintenance is often unavoidable, with maintenance teams having to respond to equipment breakdown or failure. However, it can be a bad idea to rely solely on corrective maintenance over other types of maintenance such as preventive maintenance [6].

Corrective maintenance can offer a range of advantages when used as part of a broader maintenance schedule. These advantages include:

Reduced Planning: Corrective maintenance requires less planning than preventive maintenance, even when scheduling repairs

Simple Process: Corrective maintenance is a simple process that is need-based, allowing maintenance teams to focus on other areas until required

Lower Short-Term Costs: This type of maintenance can be more cost-effective in the short term as work is only done when needed. This is true for simple repairs or replacements, such as a blown lightbulb that can be fixed quickly without the time and expense of a preventive maintenance plan

Improved Resource Planning: If corrective maintenance work orders are prioritized and scheduled they can allow for labor and financial resources to be optimized. This can lead to fewer service interruptions as maintenance teams can resolve problems before production is impacted or services are interrupted

Reduced Downtime: If a maintenance technician notices a worn component while performing routine maintenance, a corrective action can reduce the chance of later downtime due to failure

Extended Asset Lifetime: Corrective maintenance can extend the lifetime of critical assets if parts are repaired or replaced before they impact other parts of a machine

Corrective maintenance is fine for when an asset can be easily repaired or replaced and parts are freely available but, in some instances, it can lead to unexpected and costly downtimes. Experts tend to agree that 80% of your maintenance should be preventive and just 20% corrective.

Despite the advantages of corrective maintenance, there are also some disadvantages with this method, especially where there is no supporting preventive maintenance strategy. These disadvantages include:

Higher Long-Term Maintenance Costs: Simply running assets until they break can lead to higher long-term maintenance costs as the condition of equipment deteriorates before problems are discovered. This can lead to other components being affected and more parts requiring repair or replacement along with the associated labor costs.

Safety Issues: Pressure to reduce unexpected maintenance costs can also create safety issues as repair work may be rushed and not completed correctly. Also, running a machine until it breaks can cause potential hazards for staff using the machine.

Unpredictable: The biggest single disadvantage is the unpredictable nature of corrective maintenance. If an asset unexpectedly fails, it can cause disruption to other maintenance work as well as unforeseen downtime. Maintenance can be slow and expensive, as the cause of the failure needs to be located and spare parts ordered to effect a repair. Because of the reactive nature of corrective maintenance, equipment is not maximized and production can drop. Unpredictability is not a problem in the case of small repairs (such as replacing a blown lightbulb), but can be a problem with larger failures. This can be prevented with a more proactive and predictive maintenance strategy.

2.2.3 predictive maintenance

Predictive maintenance is an approach to asset management that relies on operational data to determine when a physical asset requires service. An important goal of predictive maintenance is to minimize maintenance costs by preventing equipment failures before they occur.[7]

Predictive maintenance plays an important role in industries that requires high availability for machine parts.

Predictive maintenance software uses data produced by Internet of Things (IoT) and Industry 4.0 edge nodes to monitor the condition of mechanical assets as they are operating, it is extremely related to remote maintenance concept. Consumer-grade predictive maintenance software apps will typically issue an alert when data suggests a replacement part or maintenance appointment is needed.

With predictive maintenance, organizations can monitor and test various indicators such as slow bearing speed, lubrication, or temperature. Using condition-based monitoring and IIoT technology, these tools detect abnormalities during normal operations and send real-time alerts to the machine owner that indicate a potential future failure. More specific types of predictive maintenance including:

Vibration analysis: This is a common type of predictive maintenance used inside manufacturing plants with rotating machinery. It can detect imbalance, misalignment, or loose parts of equipment.

Infrared analysis: Using temperature as an indicator, issues related to airflow, cooling, and motor stress can be identified.

Sonic acoustical analysis: Sounds can be converted to an auditory or visual signal that can be heard or seen by a technician, indicating conditions such as worn or under-lubricated bearings in both low and high-rotating machinery.

A predictive maintenance program associated with modern software is the best way to increase cost savings in a building or manufacturing plant. Automation is key when it comes to maintenance management.

According to the Department of Energy, maintenance teams can expect an increase in production of 25% after implementing a Predictive maintenance strategy.

Even with higher implementation costs than the other maintenance strategies, it tends to pay off in the long term.

Figure 1 Illustration of vibration analysis

2.2.4 condition based maintenance

Condition-based maintenance (CbM) is a proactive maintenance technique that uses real-time data (collected through sensors) to identify when an asset's performance or condition reaches an unsatisfactory level. By observing the state of an asset, a practice known as condition monitoring, maintenance professionals can identify when an asset is about to fail or has failed. With CbM, maintenance work is performed only when needed in response to the asset's real condition, preventing un-necessary maintenance tasks [8].

In this contemporary period of digital transformation and interconnectivity, diagnostic and analytical information is frequently accessible in real time to all stakeholders in asset information systems. This digital advantage significantly enhances the planning and scheduling of maintenance. Consequently, this expeditiously leads to gains in efficiency and effectiveness that contribute to the financial success of modern, quality-driven organizations. With the introduction of permanently installed sensors on our physical assets, the Industrial Internet of Things (or Industry 4.0, if you prefer) is revolutionizing our perspective on maintenance. It can almost be conceptualized as "maintenance 4.0." Whichever terminology one chooses to employ, these designations share a commonality: they signify nothing less than a revolution that is currently unfolding in the realm of industrial equipment maintenance. We are witnessing a transition from outdated and inefficient methodologies to a new approach of continuous and digital monitoring of the health and condition of assets.

This involves the real-time transmission of information to the cloud through Bluetooth connections, Wi-Fi, and gateways.

Given the prevailing trend of digitization in the manufacturing sector, as well as in other major industries that constitute the global economy, Condition-Based Maintenance (CBM) emerges as the most cost-effective and efficient method of asset maintenance. CBM relies on ongoing evaluation of an asset's actual deterioration, or lack thereof. It is important to acknowledge that CBM entails higher monitoring costs compared to reactive maintenance. However, it also offers considerable benefits, such as reduced asset repair expenses and minimized instances of unscheduled downtime, when compared to both reactive maintenance and time-based maintenance.

Other advantages realized through CBM in the context of its connection to the IIoT include:

Increased production output: If you can conduct real-time condition analysis and quickly spot any troubling patterns, you'll be able to plan and schedule maintenance more effectively. In the long run, this means your asset availability and performance levels will be higher — which can easily manifest as a notable uptick in production output.

Longer asset life cycles: A reactionary maintenance strategy can be detrimental not only to individual assets that fail and necessitate emergency repair or replacement, but also to the many components to which the malfunctioning asset is connected. Sudden failures are stressful on any system. You may soon find yourself fixing not one component but several — or perhaps even an entire set of interconnected machines. CBM strategies that allow ongoing equipment monitoring extend the life cycles of your assets, potentially facilitating reductions in operational and capital expenditures.

Enhanced planning, scheduling, and spares projection: When one possesses authority over asset maintenance, as opposed to being subject to it, one can meticulously strategize and arrange the distribution and implementation of resources. This not only allows for the advanced planning and projection of spares, but also permits the anticipation and corresponding planning of human resource levels.

The enhancement of dependability: One of the notable advantages of this is the capability to employ condition monitoring and asset health data for the eradication of defects and the execution of diverse root-cause analysis procedures. Although asset reliability cannot be directly enhanced by condition-based monitoring (CBM), the knowledge acquired can subsequently be utilized to heighten the likelihood of mission success. When employed in conjunction with a reliability program, the invaluable information obtained regarding our pumps, motors, fans, gearboxes, and a variety of other components proves instrumental in diminishing the probability of future defects and asset failures.

2.2.5 proactive maintenance

Proactive maintenance stands in stark contrast to the reactive approach. Each proactive maintenance strategy prioritizes the prevention of machine failure and downtimes to the greatest extent feasible. Rather than merely addressing the outward indications, proactive maintenance endeavors to discern the root causes of malfunctions and breakdowns, subsequently rectifying or averting them beforehand. Proactive maintenance is based on the idea that machine failures can be anticipated and eliminated before they develop.

Shifting to proactive maintenance can bring the following key advantages to an organization:

1. Reduced downtime due to fewer instances of malfunctions and breakdowns.
2. Improved equipment reliability, availability, and uptime.
3. Reduced long-term maintenance costs – both in repair costs and labor costs.
4. Fewer productivity and safety issues.
5. Increased longevity of equipment, resulting in further savings.

In the long term, proactive maintenance can result in significant advantages to a business, with increased productivity, savings, and reduced maintenance costs.

The main downside of proactive maintenance strategies is that it does take some planning, effort, and investment to implement them. Different proactive maintenance strategies have vastly different implementation requirements.

In Figure 2, these types of maintenance strategies are summarized:

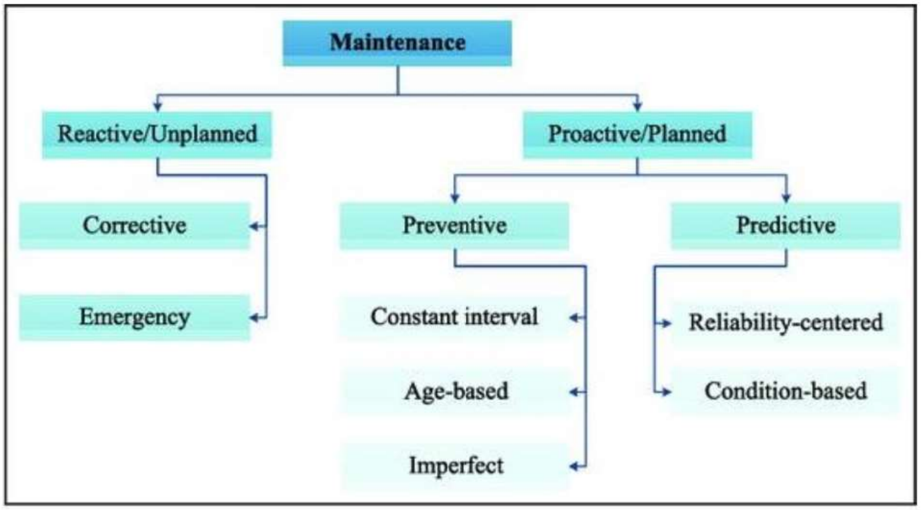


Figure 2 Overview of different types of maintenance strategies

Maintenance, with all its type, deals with system malfunction which is caused by Failure, Fault, Error.

2.3 Failure

The fact of something not working, or stopping working as well as it should [9].

Failure is the termination of the ability of an item to perform a required function. A failure is always related to a required function. The function is often specified together with a performance requirement. A failure occurs when the function cannot be performed or has a

performance that falls outside the performance requirement.

Example : *The shutdown valve: valve must adhere to the performance criteria, which dictate that the duration of closure should not exceed 15 seconds. Should the closure time surpass this limit, it would indicate a malfunction in the closing function.*

A failure may:

- Develop gradually
- Occur as a sudden event

The manifestation of failure may occasionally be revealed:

- On demand (i.e., when the function is needed) ("hidden")
- During a functional test (also "hidden")
- By monitoring or diagnostics ("evident")

2.4 Fault

The state of an item characterized by inability to perform a required function while a failure is an event that occurs at a specific point in time, a fault is a state that will last for a shorter or longer period.

When a failure occurs, the item enters the failed state. A failure may occur:

- While running
- While in standby
- Due to demand

.

2.5 Error

Discrepancy between a computed, observed, or measured value or condition and the true, specified, or theoretically correct value or condition.

An error manifests itself when the execution of a particular function diverges from the expected performance, which is the performance that is theoretically deemed correct, yet still manages to meet the criteria for performance. An error has the propensity to transition into a failure, although this is not always the case.

A failure may originate from an error. When the failure occurs, the item enters a fault state.

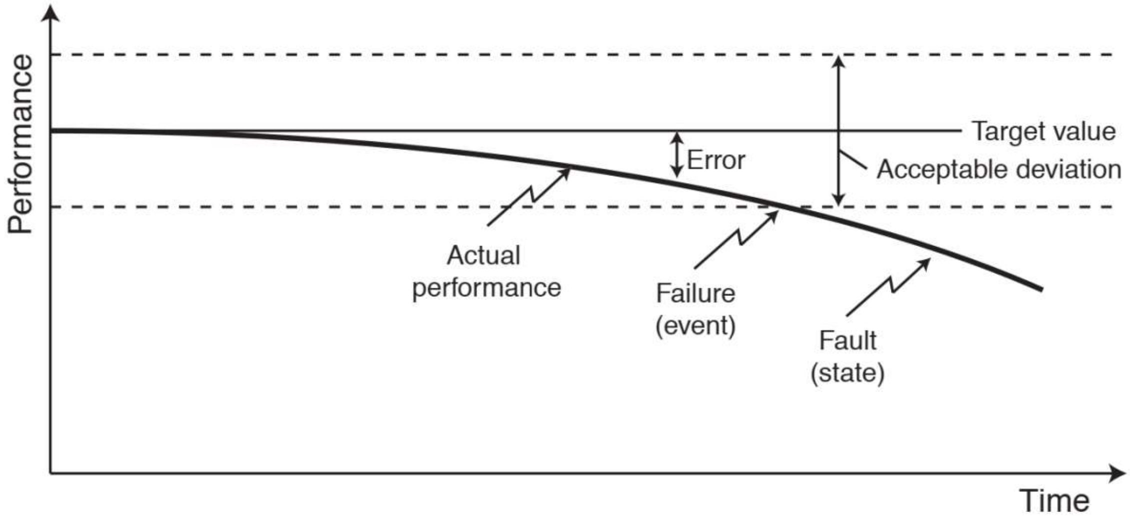


Figure 3 Fault apparition in performance evolution time

3. Failure modes, cause, effect

'Mode,' 'cause,' and 'effect,' when used with the word 'failure,' have different meanings.

- When we are focusing on the present, we use failure mode.
- Failure cause describes why a failure happened, i.e., it focuses on the past.
- Failure effect is all about the consequences of the failure, i.e., it focuses on the future.

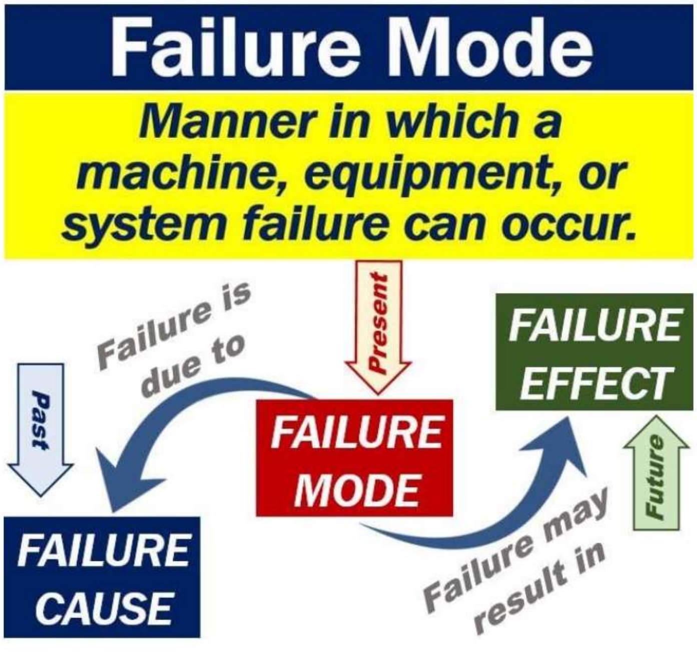


Figure 4 Failure mode

Failure mode the way a failure is observed on a failed item.

An item can fail in many different ways. A failure mode is a description of a possible state of the item after it has failed.

A failure mode can potentially exert a substantial or a negligible influence on the functioning of the constituent. A failure mode essentially entails a depiction of the manner in which the failure is discerned. Nevertheless, numerous data sources categorize failure causes as failure modes.

Failures may be classified according to their (IEC 61508 [10]):

Causes: To avoid future occurrences and make judgments about repair

- Random (hardware) faults
- Systematic faults (including software faults)

Effects: To rank between critical and not so critical failures

- Safe failures
- Dangerous failures

Detectability: To distinguish failures that may be revealed “automatically” (and shortly after their occurrence) and those that may be hidden until special effort is taken, such as proof tests.

- Detected - revealed by online diagnostics
- Undetected - revealed by functional tests or upon a real demand for activation

3.1 Random Hardware Failures (Faults)

Failure, which takes place at an unpredictable moment, is the consequence of one or more of the potential deterioration processes in the hardware. According to IEC 61508, random hardware failures can be identified by a failure rate that can be either constant or non-constant. A constant failure rate implies that the component is currently in its useful lifespan, where the impact of aging is insignificant. On the other hand, a non-constant failure rate indicates that the component is in either the burn-in phase or the wear-out phase.

3.2 Systematic failure

Failure, when associated with a determinable cause, can only be eradicated through a modification of the design, manufacturing process, operational procedures, documentation, or other pertinent factors [IEC 61508]. Systematic faults, which are not rooted in physical causes, exhibit the following characteristics:

- A systematic fault will invariably recur when the triggering condition is present.
- Systematic faults can be introduced at any stage of the lifecycle.
- In theory, if the necessary corrections are made, the failure should never resurface.

3.3 Safe Failure

According to IEC 61508 a Safe failure is a failure of an element, subsystem, or system that is involved in putting the safety function into place that:

a. causes the safety function to operate spuriously to put the EUC (or a part of it) into a safe state or maintain a safe state; or
b. increases the likelihood that the safety function will operate spuriously to put the EUC (or a part of it) into a safe state or maintain a safe state.

Loss of service or output may follow a safe failure, but not a loss of safety.

APPLICATION: Present a Scenario and ask students to identify failure, faults…

3.4 Detected and Undetected Faults

IEC 61508 distinguishes between detected and undetected failures. The most suitable definition is, however, identified in ISO TR 12489 [10]:

- Detected: Failure that is readily obvious to operation and maintenance staff when it happens. Failures that are reported as diagnostic faults or alarms are a common example.
- Undetected: A failure that operations and maintenance staff do not immediately notice. An example of this kind of failure is one that is hidden until the component is required to perform its function.

Detected, Undetected, safe and dangerous failure are combined to classify failure when comes to reliability systems analysis methods, here are some examples:

- Safe undetected (SU): A spurious (untimely) activation of a component when not demanded
- Safe detected (SD): A non-critical alarm raised by the component
- Dangerous detected (DD): A critical diagnostic alarm reported by the component, which will, as long as it is not corrected prevent the safety function from being executed
- Dangerous undetected (DU): A critical dangerous failure which is not reported and remains hidden until the next test or demanded activation of the safety function

3.5 Diagnosis

Diagnostics in industrial processes that deals specifically with the on-line, real-time, fault detection, isolation, and diagnosis of process defects is the diagnostics. As a result, industrial diagnostics concentrates on the process itself as well as the parts of technological installation, including its equipment (actuators and instrumentation) [10]

The diagnosis system is based on state estimators, namely dynamic observers.

3.6 Detection

Fault detection in industrial systems endeavors to ascertain the erroneous state of a procedure and undertake suitable measures against future malfunction or unfavorable incidents.[11]

For example, On PLC leds on the front indicate a faulty situation which allow user to detect a fault.

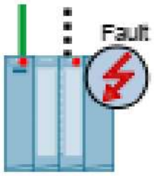


Figure 5 Fault indication led on PLC

3.7 Isolation

There could be lot of faults at the same time, identify theme separately is the isolation process.

Fault isolation is the process of determining the cause of a problem. It may refer to hardware or software, but always deals with methods that can isolate the component, device or software module causing the error. Fault isolation may be part of hardware design at the circuit level all the way up to the complete system. The goal of the fault isolation process is to localize the fault to the lowest component that can be replaced. Fault isolation aims at the location of a detected fault occurring on the actuators, sensors, instrumentation, control or system controlled by specifying which organ or component is affected by it.

3.8 Diagnosis

Diagnosis is the reasoning leading to the identification of the cause (the origin) of a failure, problem or disease, from symptoms identified by observations, controls or tests. Diagnostics serves to diminish periods of inactivity and consequently aids in the augmentation of the efficiency of the apparatus. Diagnostics provides assistance throughout the entirety of the existence of a machine, commencing with the initial design and extending to its operation and maintenance. Diagnostics fundamentally encompasses the determination of any faults within the system's components, the surveillance of procedural sequences, and the diagnosis of programmatic malfunctions.

In industrial system, diagnosis could be made in different levels:

3.8.1 System diagnostics (diagnosis of faults of electrical controller components)

The phrase "system diagnostics" is employed to elucidate the process of diagnosing devices and modules. The anomalies can be exhibited in plain language, thus facilitating maintenance personnel in swiftly identifying and rectifying the error. Defective devices and modules can be identified through diagnostics utilizing the user program. Consequently, replies to diagnostic messages can similarly be programmed within the user program, undesired machine behavior can be prevented.

3.8.2 Machine and system diagnostics (diagnosis of faults in the production process)

Many faults in the operational functioning of a plant can be attributed to errors in the production process that stem from mechanical or electrical components. By implementing a highly efficient plant-specific diagnostic system for process faults, combined with comprehensive knowledge regarding the location, cause, and troubleshooting information of these faults, it becomes possible to swiftly identify and rectify any such issues. The user program allows for the retrieval of error bits from both the machine and system diagnostics, enabling the machine to be promptly halted in the event of specific faults, for instance.

3.8.3 Diagnostics of program errors (analysis and elimination of programming errors)

Programming errors can arise not only during the commissioning phase, but also during the operation phase in the event that array limits are surpassed as a result of erroneous parameters. By utilizing a development environment that provides opportunities for dissecting programs, errors within the program can be expeditiously localized and eliminated.

3.8.4 Hardware API diagnosis

On industrial systems, primary diagnosis is made on its control unit or API. On every API there some Leds to indicate the API state:

S7-300:

SF : System fault: it shows there is an error in the system, this error could be software like an error in programming or hardware like a power loss in input modules

BF: Bus Fault: indicates that there is an error in the system network, like a bad contact in one of the communication connectors, or there is an overlap between the addresses in the network

MAINT: Maintenance: Indicate that the CPU is not working anymore and needs a service, but this is rarely happening.

DC5V: This led indicates that there is a 24 Volt DC delivered to the CPU.

FRCE: Force: it indicates that at least one of the PLC inputs or outputs is forced to on or off.

Run: The run mode is activated when the central processing unit (CPU) operates smoothly and without any issues, and it is indicated by a flashing signal during the startup process of the CPU.

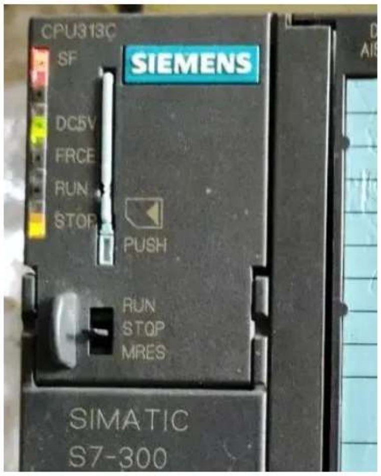


Figure 6 Siemens S7-300 Leds

<u>S7 – 400</u>

NTF red Lights up in the event of an internal fault

5 VDC green Lights up as long as the 5 V voltage is within the tolerance limits

24 VDC green Lights up as long as the 24 V voltage is within the tolerance limits

BAF Red Lights up if the battery voltage on the backplane bus is too low and the BATT INDIC switch is at the BATT position

BATTF Yellow Lights up if the battery is empty, or the polarity is reversed, also when the battery is missing, and the BATT INDIC switch is at the BATT position

<u>S7 – 1200 </u>[12]

STOP/RUN

– Solid yellow indicates STOP mode

– Solid green indicates RUN mode

– Flashing (alternating green and yellow) indicates that the CPU is in STARTUP mode

ERROR

– Flashing red indicates an error, such as an internal error in the CPU, an error with the memory card, or a setup error (mismatched modules)

– Defective state:

- Solid red indicates defective hardware

- All LEDs flash if the defect is detected in the firmware

MAINT (Maintenance) flashes when a memory card is inserted. The CPU then changes to STOP mode. After the CPU has switched to STOP mode, perform one of the next functions to initiate the evaluation of the memory card:

– Change the CPU to RUN mode

– Perform a memory reset (MRES)

– Power-cycle the CPU

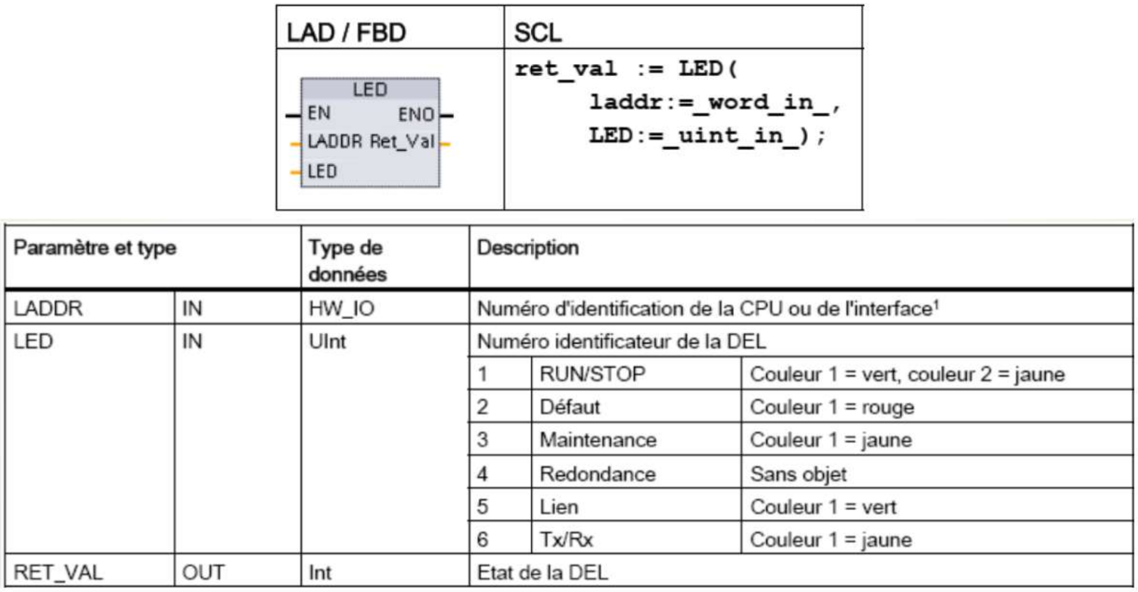
3.8.5 Software API diagnosis

The previous API state Leds can be used in the API program to show them on the "Human Machine Interface" or on remote control system.

A specific function is used for that:

1. LED instruction

(figure 7) is used to read the state of the LEDs on a CPU or interface. The specified LED state is returned by the RET_VAL output.



LAD / FBD	SCL

LED
EN ENO
LADDR Ret_Val
LED
	`ret_val := LED(`
	`laddr:=_word_in_,`
	`LED:=_uint_in_);`

Paramètre et type		Type de données	Description		
LADDR	IN	HW_IO	Numéro d'identification de la CPU ou de l'interface[1]		
LED	IN	UInt	Numéro identificateur de la DEL		
			1	RUN/STOP	Couleur 1 = vert, couleur 2 = jaune
			2	Défaut	Couleur 1 = rouge
			3	Maintenance	Couleur 1 = jaune
			4	Redondance	Sans objet
			5	Lien	Couleur 1 = vert
			6	Tx/Rx	Couleur 1 = jaune
RET_VAL	OUT	Int	Etat de la DEL		

Figure 7 Led Instruction

In the figure 8 an example of the use of Led instruction is illustrated, figure a the target PLC doesn't exist and in figure b the Led is red and then the PLC is stopped.

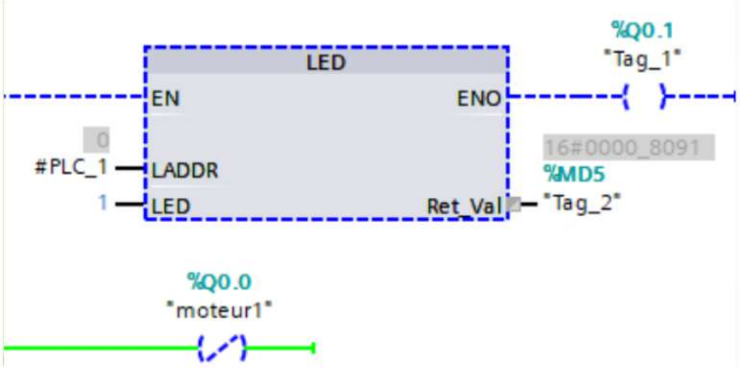


Figure a

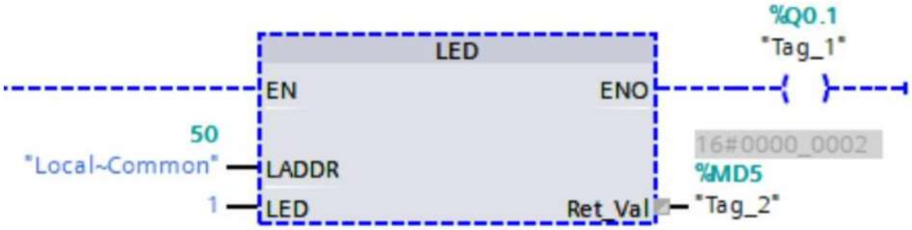


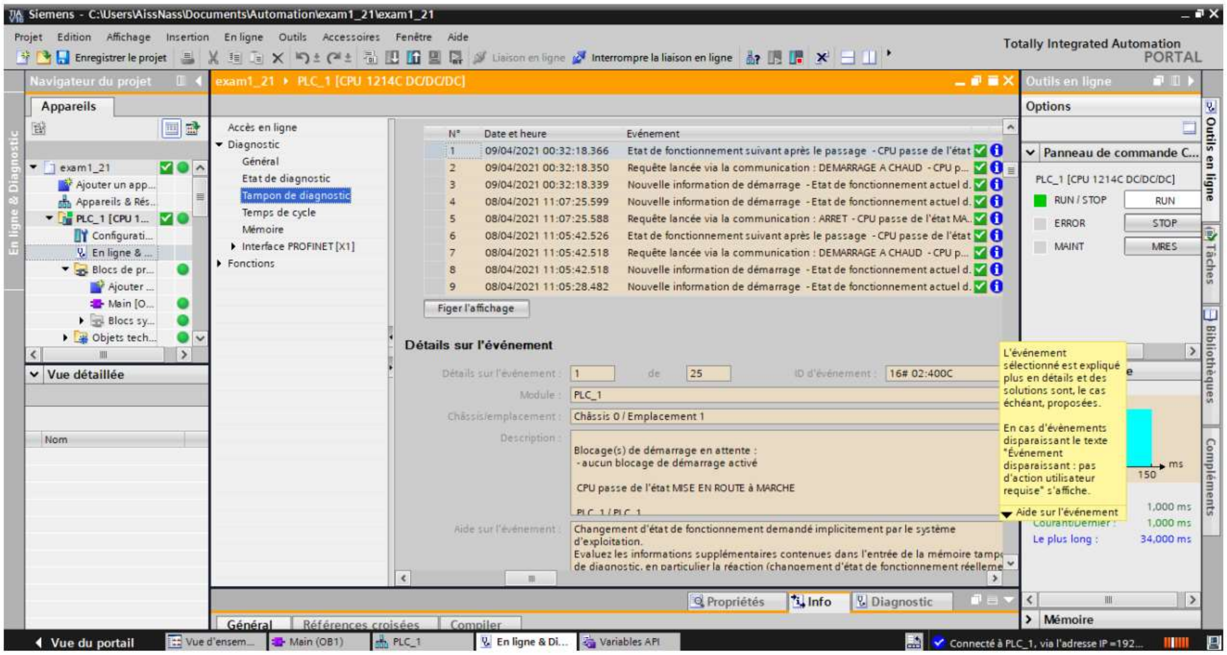
Figure 8 b Led Instruction use

2. Display of diagnostic events in the CPU

Every control unit within an industrial system diligently preserves its previous occurrences within a log, which can be referenced whenever the need arises.

The page presenting the diagnostic buffer showcases events of a diagnostic nature (see figure 9 as an example from PLC S7-1200). By using the selection tool provided on the left-hand side, users can opt to display a specific range of diagnostic buffer entries, with options including the range of 1 to 25 or 26 to 50. On the right-hand side, another selector enables users to choose between displaying the times in UTC format or the local time of the Programmable Logic Controller (PLC). The upper section of the page exhibits the diagnostic entries along with their respective time and date of occurrence.

Moreover, from the aforementioned upper section of the page, users have the ability to select any individual entry, which in turn will display detailed information pertaining to that particular entry in the lower section of the page. It is important to note that the language in which the diagnostic buffer entries are displayed is contingent upon the configuration setting for multilingual support on the user's device.



N°	Date et heure	Evénement
1	09/04/2021 00:32:18.366	Etat de fonctionnement suivant après le passage - CPU passe de l'état
2	09/04/2021 00:32:18.350	Requête lancée via la communication : DEMARRAGE A CHAUD - CPU p...
3	09/04/2021 00:32:18.339	Nouvelle information de démarrage - Etat de fonctionnement actuel d.
4	08/04/2021 11:07:25.599	Nouvelle information de démarrage - Etat de fonctionnement actuel d.
5	08/04/2021 11:07:25.588	Requête lancée via la communication : ARRET - CPU passe de l'état MA..
6	08/04/2021 11:05:42.526	Etat de fonctionnement suivant après le passage - CPU passe de l'état
7	08/04/2021 11:05:42.518	Requête lancée via la communication : DEMARRAGE A CHAUD - CPU p...
8	08/04/2021 11:05:42.518	Nouvelle information de démarrage - Etat de fonctionnement actuel d.
9	08/04/2021 11:05:28.482	Nouvelle information de démarrage - Etat de fonctionnement actuel d.

Figer l'affichage

Détails sur l'événement

Détails sur l'événement : 1 de 25 ID d'événement : 16# 02:400C

Module : PLC_1

Châssis/emplacement : Châssis 0 / Emplacement 1

Description :

Blocage(s) de démarrage en attente :
- aucun blocage de démarrage activé

CPU passe de l'état MISE EN ROUTE à MARCHE

PLC_1 / PLC_1

Aide sur l'événement : Changement d'état de fonctionnement demandé implicitement par le système d'exploitation.
Evaluez les informations supplémentaires contenues dans l'entrée de la mémoire tamp de diagnostic, en particulier la réaction (changement d'état de fonctionnement réelleme

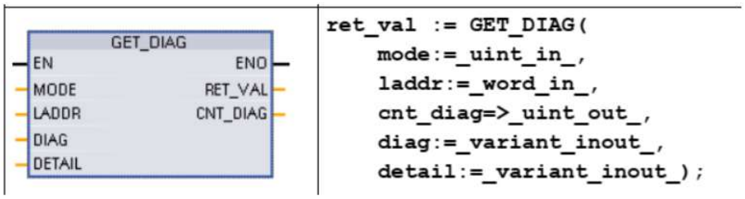
L'événement sélectionné est expliqué plus en détails et des solutions sont, le cas échéant, proposées.

En cas d'évènements disparaissant le texte "Événement disparaissant : pas d'action utilisateur requise" s'affiche.

Aide sur l'événement

Figure 9 Diag Buffer

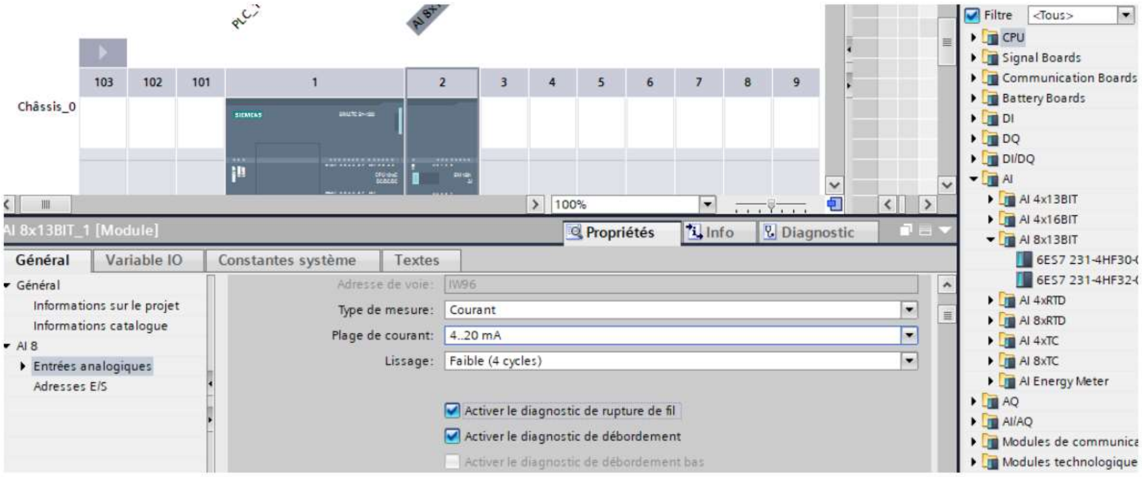
"GET_DIAG" is an instruction used to read out the diagnostic information of a hardware device. The hardware device is selected with the LADDR parameter. With the MODE parameter, you select which diagnostic information to read.



```
ret_val := GET_DIAG(
    mode:=_uint_in_,
    laddr:=_word_in_,
    cnt_diag=>_uint_out_,
    diag:=_variant_inout_,
    detail:=_variant_inout_);
```

Figure 10 Diag Instruction

In some PLCs there are some options available to allow performed diagnosis especially for inputs (figure 11) , for example : Activate wire break diagnostics. It flashes error led when there is no signal on input connexion.



Adresse de voie: IW96
Type de mesure: Courant
Plage de courant: 4..20 mA
Lissage: Faible (4 cycles)

☑ Activer le diagnostic de rupture de fil
☑ Activer le diagnostic de débordement
□ Activer le diagnostic de débordement bas

Figure 11 Diag parameters

<u>APPLICATION: Student are asked to experiment Diagnostic functions on Tiaportal</u>

CHAPTER 2 : Remote Maintenance constraints

Remote maintenance refers to the remote control of a system, via a communications network (telephone, intranet, internet), with the aim of firstly diagnosing, from a distance, problems and the nature of faults, and secondly suggesting corrective and preventive actions to be taken, taking into account the results of the analysis of the causes of the problem encountered.

Secondly, it is important to propose and recommend appropriate measures of correction and prevention that should be implemented, while considering the outcomes of the comprehensive investigation conducted on the root causes of the encountered problem. In essence, the objective is to execute all the necessary actions that will ensure the proper functioning and operation of the system. Notably, the possibility of remotely accessing the Programmable Logic Controller (PLC) through the Internet has become a tangible reality, facilitating various tasks such as PLC programming, control, supervision, plant maintenance, and remote management.

1. Teleservice, remote diagnosis and remote maintenance

The arrival of exceedingly intricate and costly capital machinery, exemplified by the implementation of flexible manufacturing systems (FMS), has generated a compelling need to operate these machines at elevated levels of utilization. This requirement arises from the fact that the complexity and cost associated with FMS necessitate their deployment in a manner that maximizes their productive output and minimizes any idle time. The advent of FMS, with their multifaceted capabilities and advanced functionalities, has engendered a scenario wherein the efficient and effective operation of these machines is imperative. This is due to the fact that FMS represent a substantial investment and their optimal utilization is crucial in order to achieve a satisfactory return on investment [13]. Consequently, in order to ensure a high degree of productivity and profitability, it is imperative to operate FMS at high utilization rates. In 1980, to improve performance, data links were set up between the FMS and the FMS manufacturer so the latter could quickly troubleshoot malfunctioning machines. The increasing computerization of manufacturing environments further drove the development of Remote diagnosis and maintenance. Predominant application areas include office equipment, building and facility maintenance, computer maintenance, and control of IT and telecommunications networks. For example, Xerox has developed a technology that sends data from high-end copiers to a central service center via phone lines [14]. At the service center, the copier’s status is monitored and maintained by an expert system. Other application areas include PC and computer networks. A popular example software includes Symantec’s System Works, which alerts users to suboptimal performance and major problems of their computer systems.

1.1 Teleservice

TeleService enables the operation of control systems through telecommunication connections. It provides a centralized approach to managing, controlling, and monitoring decentralized plants using remote connections. By utilizing a phone network, TeleService grants access to the functional capabilities typically accessible through an Adapter. Consequently, remote sections of plants can be conveniently accessed and integrated into the broader system.

TeleService offers the following functionality:

1. Access to remote plants (teleservice): centrally manage, control, and monitor decentral plants by means of remote connections.

2. Establishing connections from remote plants (programming-device to automation-system remote link)

3. Data exchange between plants (automation-system to automation-system remote link)

APPLICATION: Student are asked to experiment Teleservice setup on Tiaportal [15]

1.2 Remote diagnosis

It could be done on teleservice services

The act of diagnosing an issue or problem from a distance, commonly known as remote diagnostics, entails the analysis and identification of potential complications without physically being present at the site. Within a manufacturing environment, this practice is particularly relevant as it allows for the efficient monitoring and evaluation of various assets scattered across the plant. By employing an intricate network: sensors like infrastructure, motion, temperature, and pressure … are strategically connected to these assets, enabling the continuous transmission of data to a centralized system for further analysis and decision-making.

1.3 Remote Maintenance

Nuclear fusion constitutes a paramount method to address the pressing issues of energy scarcity that humanity faces. In light of the potential hazards associated with ionizing radiation, the nuclear fusion reactor will rely upon remote handling maintenance as a means to fulfill its scientific objectives. With the rapid advancement of technology in recent years, the Internet of Things (IoT) has emerged as a pivotal and indispensable means of enhancing maintenance efficiency in various industries. As a result, IoT has now assumed a paramount role in optimizing the maintenance processes of organizations, thereby leading to significant improvements in overall operational performance.

By seamlessly connecting devices and systems, IoT enables real-time data acquisition and analysis, facilitating the timely identification of potential issues and the proactive implementation of maintenance measures to prevent any disruptions or downtime.

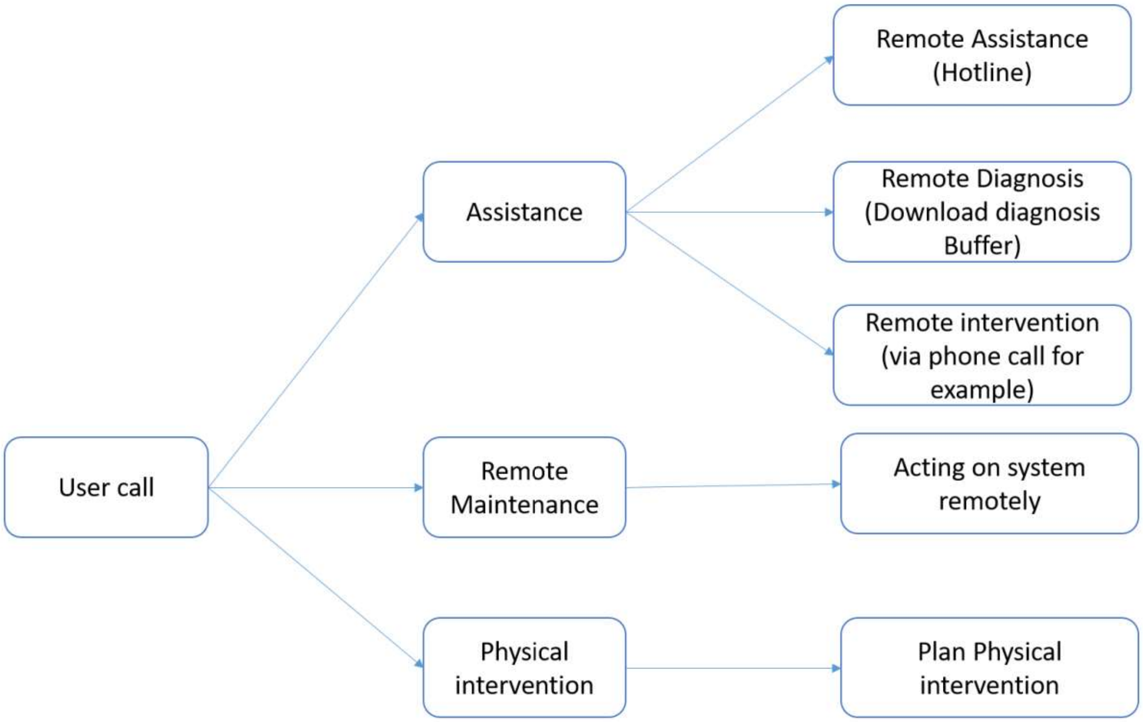

Remote Assistance (Hotline)
Remote Diagnosis (Download diagnosis Buffer)
Assistance
Remote intervention (via phone call for example)
User call
Remote Maintenance
Acting on system remotely
Physical intervention
Plan Physical intervention

Figure 12 Remote Intervention possibilities

A remote intervention has the potential to begin with the presence of an onsite operator, as illustrated in Figure 12. This operator has the capability of both identifying failure as well as requesting updates or the integration of new functionalities. As a first step, the operator can seek assistance by reaching out to the "after sale services" department. During this interaction, the operator is able to articulate the problem at hand and provide some initial diagnostic elements, which in turn allows the assistant to gain a clearer understanding of the issue and subsequently offer advice and recommendations for resolving the problem. In order to facilitate a more accurate diagnosis, the remote assistant also has the option of requesting or downloading a "Diagnosis Buffer". Additionally, the remote assistant can engage in further investigation and experimentation, facilitated through a transition process with the onsite operator, in order to effectively address and resolve the problem at hand.

Certain software applications provide the capability for users to manage and control processes remotely. This remote handling functionality enables a remote assistant to gain access to the system and execute various maintenance tasks, such as updating, configuring, and modifying settings.

Through this remote access, users are able to conveniently and efficiently manage the software and its associated processes from a distance, enhancing productivity and flexibility in handling maintenance activities.

2. Remote maintenance constraints

The advent of remote maintenance is closely linked to the establishment of a reliable connection, which is why the primary challenge revolves around ensuring a stable internet connection and safeguarding the integrity of data exchanged between the client and the maintenance operator. As a result, the key constraints in remote maintenance encompass securing the data transmission, ensuring a dependable connection, verifying the qualifications of personnel on both ends, and lastly, developing the requisite software to facilitate remote maintenance procedures.

2.1 Remote Maintenance architecture

The architecture of remote maintenance includes the configuration of two or more distinct systems or subsystems, which operate independently and engage in the exchange of data between them. Within this framework, one of the systems serves as a data acquisition system, effectively functioning as the source of structured data. On the other hand, the second system assumes the role of a data processing system, responsible for receiving and processing the data. The transmitting system can either autonomously send data or respond to requests for data from the receiving system.

The results of this data processing, in the form of output, can be utilized by human operators or may be directed towards the procurement system for the purpose of coordinating data acquisition. For effective communication between the systems, the data must adhere to a standardized structure to ensure mutual understanding and acceptance.

Considering the factor of geographical distance, remote maintenance can be configured in a manner where it is established at a single production site or distributed across various production or maintenance sites (figure 13), and potentially coordinated from a central maintenance center. The flexibility of this architecture allows for adaptability in diverse operational scenarios.

2.2 Internet connection for remote maintenance

The accessibility of the internet for the general population has been in place since the 1970s[16] However, it is crucial to note that the tools and mechanisms employed for communication may vary significantly depending on the type of data being exchanged and the specific end-users involved. For industrial sites seeking to implement remote maintenance procedures, it is imperative that they establish a connection to the internet. This connection serves as the foundational link that enables the exchange of data, but the methods and technologies employed may vary depending on the nature of the industrial operation and its specific requirements.

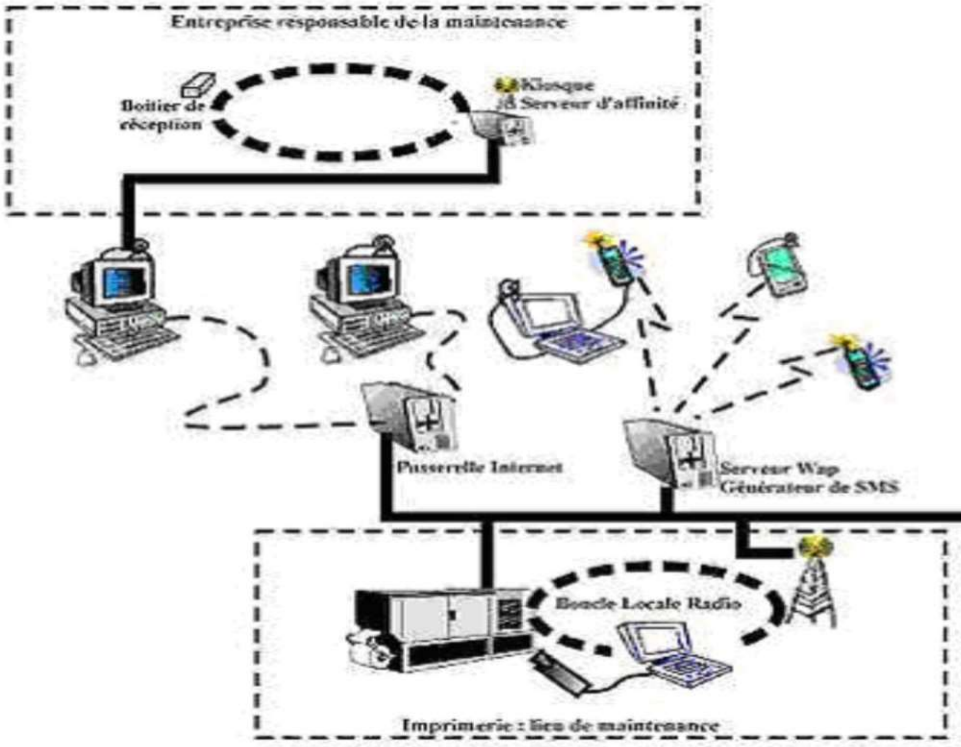


Figure 13 Example of remote maintenance architecture [17]

The internet connection for industrial sites differs from home or office connections, as it necessitates specific devices capable of connecting to technological equipment. These unique requirements for internet connectivity in industrial sites are often associated with industrial networks.

2.3 Industrial Networks as framework for Remote Maintenance

An industrial control network refers to an interconnected system of equipment designed for overseeing and managing physical machinery in industrial settings. These networks stand apart from conventional enterprise networks due to their specialized operational needs. Notably, industrial networks are increasingly adopting Ethernet and web standards, particularly in the upper echelons of network structure.

This evolution means that professionals involved in the design and upkeep of control networks must possess knowledge spanning both conventional enterprise considerations like network security and industrial necessities such as determinism and response time. As seen in figure 14, In manufacturing or process industries, information and data move both from the field level to the enterprise level (bottom-to-top) and from the enterprise level to the field level (top-to-bottom).

Each level has its own unique set of requirements to meet, and it's evident that a single communication network cannot supply to the diverse needs of every level. As a result, different levels may utilize distinct networks designed to their specific requirements, including factors such as data volume, data transmission speed, and data security, among others.

Industrial communication networks are typically categorized into three broad levels based on their functionalities.

2.3.1 Device Level:

The lowest tier comprises field devices, including sensors and actuators used in industrial processes and machinery. The primary role at this level is to facilitate the exchange of information between these devices and technical process elements like PLCs. Information transfer can take various forms, including digital, analog, or hybrid, and the collected data may have both short-term and long-term significance.

For field-level communication, conventional methods like the 4-20 mA current loop and serial point-to-point communication are commonly engaged. These methods often utilize multi-wire cables as the transmission medium. Several standard serial communication protocols, including RS232, RS422, and RS485, are established at this level. Numerous other field-level communication networks are available, each characterized by factors like response time and message size.

In the contemporary landscape, fieldbus technology stands out as a sophisticated communication network for the field level, enabling distributed control among intelligent field devices and controllers. This bidirectional communication system consolidates multiple variables within a single transmission. Examples of fieldbuses include HART, ControlNet, DeviceNet, CAN Bus, Profibus, and Foundation Field Bus.

2.3.2 Control Level:

The control level covers industrial controllers, such as PLCs, distributed control units, and computer systems. Responsibilities at this level involve configuring automation devices, loading program data and process variable information, adjusting set variables, supervising control processes, displaying variable data on HMIs, and archiving historical data. Consequently, the control level requires features like fast response times, high-speed data transmission, short data lengths, machine synchronization, and continuous utilization of critical data.

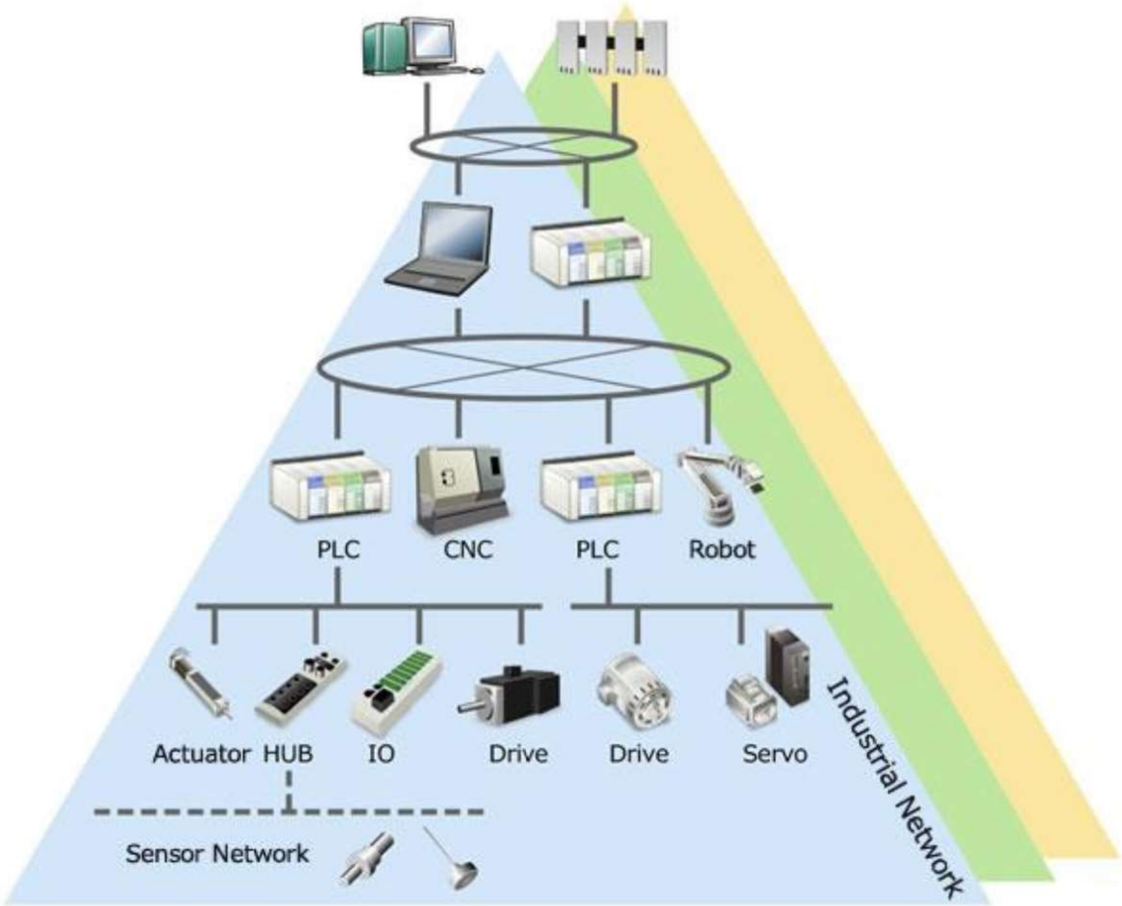


Figure 14 Industrial Networks pyramid [18]

Communication networks, including Local Area Networks (LANs), are widely utilized in this tier to meet the specific requirements. Ethernet with the TCP/IP protocol is the preferred network type for connecting control units with computers. Additionally, this network serves as a control bus to coordinate and synchronize operations among various controller units. Some fieldbuses, such as Profibus and ControlNet, are also used as control buses in this tier.

At this level, specific devices are employed to enable remote access. Siemens offers various communication extensions for its PLCs. TS module adapters are the electrical interface to the telephone network. The TS Modules are supplied with electricity from the basic unit over the shared connector [19].

The following TS Modules exist (figure 15):

● TS module modem: The TS Module Modem contains an analog modem for the connection to the analog telephone network.

● TS Module ISDN: The TS Module ISDN contains a terminal adapter for the connection to the ISDN network.

- TS Module RS232: The TS Module RS232 has a RS232 interface for the connection of an external modem.

- TS Module GSM: The TS Module GSM contains a radio modem for connection to the GSM/GPRS network.

Figure 15 TS adapter

2.3.3 Information Level:

The topmost layer of the industrial automation system collects data from the lower control level. At this level, the emphasis is on managing large volumes of data that are neither in constant use nor time-sensitive. Consequently, extensive networks are established in this tier. Ethernet Wide Area Networks (WANs) are the prevailing choice for information-level networks, facilitating data exchange for factory planning and management. In some instances, these networks may connect to other industrial networks via gateways. This kind of connection is used to connect to remote maintenance site.

2.4 Security, data integrity and privacy

Arriving at the stage of information exchange and data sharing entails the journey of data through the internet to reach the maintenance site. This means that the data can be exposed to the risks of disclosure and attacks by intruders.

Security in industrial networks shares many similarities with commercial networks due to the increasing convergence of technologies used in both contexts. While both networks face many of the same threats, the unique requirements and considerations of industrial networks can make security implementation more challenging. The primary objective of network security is to ensure confidentiality, data integrity, information availability, authentication, authorization, auditability, non-repudiation, and protection against third-party intrusion [20].

The absence or compromise of these features can lead to network failures and the maintenance operation unfinished. When the network is unable to or has not resolved interconnection issues through its inherent reliability measures, supplementary actions must be taken to obstruct access to these issues and enhance the system's security. The act of securing industrial networks is now a fundamental requirement for protection critical national infrastructure. This holds true for all industrialized countries, as the growing reliance on the advancement and execution of industrial network security is increasingly recognized with the greater integration of automation and computer-dependent processes in chemical processing, utility distribution, and discrete manufacturing [21].

With the rise of Ethernet as the prevailing technology in automation systems at higher levels, accompanied by an anticipated increase in the number of external connections to industrial networks, the importance of security became evident. Initially, the primary concerns revolved around the potential risks associated with the employed technology, and efforts were primarily focused on safeguarding the industrial network against inadvertent exposure to conventional threats.

2.4.1 Firewall Protection

Firewalls assume a crucial function in upholding network security by erecting a protective barrier that separates internal networks from potential external hazards. This discourse will delve into the fundamental aspects of firewall protection, encompassing its diverse classifications, and elucidate how it effectively fortifies network perimeters against unauthorized infiltration [22].

Functioning as a vigilant sentry, a firewall assumes the role of a gatekeeper for network traffic, diligently scrutinizing and regulating the movement of data between networks in accordance with pre-established security regulations. It meticulously inspects both incoming and outgoing traffic packets, employing a filtering mechanism that takes into account various parameters such as IP addresses, ports, and protocols.

Firewalls play a vital role in establishing a secure network perimeter, safeguarding organizations against unauthorized access attempts, malware, and network-based attacks. They serve as a fundamental element of network security, acting as the initial defense line against potential intrusions.

In summary, the implementation of firewalls is imperative for constructing a secure network perimeter. Through the deployment of firewalls, organizations can effectively monitor and regulate network traffic, thereby filtering out potential threats and unauthorized access attempts. It is crucial for organizations to comprehend the various types of firewalls and their capabilities in order to establish robust network security and protect their digital assets.

2.4.2 Intrusion Detection Systems

The active monitoring of network traffic for potential security breaches is a crucial aspect of network security, and Intrusion Detection Systems (IDS) play a vital role in this regard. IDS is a network security tool that detects and alerts administrators about suspicious activities or potential security breaches within a network. It works by analyzing network traffic, looking for patterns, anomalies, or known signatures of attacks [23].

There are two main types of IDS: host-based IDS (HIDS) and network-based IDS (NIDS). HIDS monitors activities on individual hosts or devices within the network, while NIDS monitors network traffic. IDS can also be classified into signature-based and behavior-based systems, with the former relying on a database of known attack patterns or signatures to identify threats, and the latter looking for deviations from normal network behavior to identify potential attacks.

By deploying IDS, organizations can proactively detect and respond to potential security breaches. IDS provides real-time alerts, enabling administrators to take immediate action, investigate incidents, and implement appropriate countermeasures. It helps in minimizing the impact of attacks, preventing data breaches, and maintaining network integrity.

In conclusion, IDS is an essential component of network security, and understanding the different types of IDS and their capabilities is crucial for organizations to improve their network security posture, detect and respond to attacks in a timely manner, and safeguard their digital assets.

2.4.3 Virtual Private Networks (VPNs)

In the current era of remote work and the imperative for secure communication, the significance of Virtual Private Networks (VPNs) has grown significantly. The aims here is to delve into the core principles of VPNs, elucidate their advantages, and expound on their ability to establish secure connections in order to safeguard sensitive information [24].

By establishing a secure and encrypted connection over a public network, such as the internet, a Virtual Private Network (VPN) ensures the confidentiality and integrity of data transmission. It empowers users to securely access private networks, even when connected to an untrusted or potentially insecure network.

VPNs offer a multitude of benefits in terms of network security and data privacy.

1. Confidentiality: By encrypting data traffic, VPNs ensure that information transmitted over the network rests confidential and safe from eavesdropping or interception by unauthorized parties.
2. Data Integrity: VPNs use cryptographic protocols to verify the integrity of data, ensuring that it remains unchanged during transmission. This protects against interfering and unauthorized changes.

3. Authentication: VPNs often necessitate user authentication, ensuring that only authorized entities can access the private network. This helps avoid unauthorized access and protects against potential breaches.
4. Bypassing Geo-Restrictions: VPNs can allow users to bypass geographical restrictions and access resources or content that may be restricted in their position. This can be principally useful for remote workers or individuals traveling abroad.

To ensure secure access to company resources and protect sensitive data, VPNs have become indispensable tools for remote workforces. Additionally, individuals who are concerned about online privacy can benefit from VPNs as they mask their IP addresses and maintain anonymity while browsing the internet. Virtual Private Networks (VPNs) provide secure and private communication over public networks by encrypting data traffic, ensuring data integrity, and providing user authentication. It is essential for individuals and organizations to understand the benefits of VPNs and their role in network security to maintain privacy, access resources securely, and protect valuable data.

In [25] the security assessment and quantification of VPN configurations are conducted by authors through the utilization of a probabilistic model. In order to explore the trade-offs and parameter dependence within different VPN configurations, simulations of the VPN model are performed. According to those results, some recommendations are given, for example: Long alphanumeric passwords or PSKs should be used to attain tolerable security. Less populated VPNs are more secure…

APPLICATION: Students are asked to search about VPN and available VPNs for industrial applications

2.4.4 Resilient Infrastructure

Implementing best practices is crucial for maintaining a robust and resilient infrastructure. Here are some key best practices that can enhance the security posture of an industrial network and mitigate the potential risks of cyber threats [26].

One important practice is to regularly update network devices, operating systems, and applications with the latest security patches. These updates help address vulnerabilities that attackers can exploit to gain unauthorized access to the network.

Another essential practice is to enforce strong password policies across the network. Encouraging users to create complex passwords that include a combination of letters, numbers, and special characters. Additionally, consider implementing multi-factor authentication (MFA) for an added layer of security.

Network segmentation is also a recommended practice. By dividing the network into segments or subnets. This limit the impact of potential breaches. This segregation of sensitive data and resources helps contain any unauthorized access or malicious activities, minimizing the potential damage to the entire network.

Educating employees about network security is crucial. Teach them about safe browsing practices, the importance of network security, and how to recognize and report potential threats such as phishing attacks. Conduct regular training sessions and provide ongoing awareness programs to ensure that security practices remain a top priority.

Implementing proper access controls and privilege management is another important practice. This ensures that users have appropriate permissions based on their roles and responsibilities. Regularly reviewing and updating user access privileges helps minimize the risk of unauthorized access.

Network monitoring and incident response are vital practices for maintaining network security. Deploy robust network monitoring tools to continuously monitor network traffic and detect any abnormal activities. Establish an incident response plan that outlines the steps to be taken in the event of a security incident, ensuring a prompt and effective response.

Lastly, performing regular backups of critical data and storing them securely is essential. This practice helps protect data in the event of a security breach or system failure.

By implementing these best practices, the network security posture is significantly enhancing and the potential risks of cyber threats is reduced.

2.5 Software implementation for remote Maintenance

In remote maintenance software are the HMI interface, Remote maintenance software are a type of software that enable professionals to monitor and maintain client process and network security and stability remotely. With remote maintenance software, administrators can automate an increasing number of processes involving process control, network maintenance and security, ensuring networks are safer and tech support more effective and accurate.

2.5.1 Remote desktop controller:

One such software is TeamViewer [27]. It offers extensive options to customize the remote maintenance policies you have in place for your network. With TeamViewer’s remote maintenance software, it is possible to schedule software updates and checks on the status of various elements of the computer network, such as CPU usage, antivirus software, and whether the system remains online and uninterrupted. This means that issues can be resolved instantly and costly downtime can be avoided. TeamViewer offers the option to automate responses and resolve certain issues automatically, without an IT technician needing to step in. Of course, issues that require an IT technician may still arise, but with a remote maintenance solution, IT professionals gain direct access to the affected computers in the network and troubleshoot the relevant technical problems.

Additional remote maintenance software choices are G2 [28] and Secomea [29]. RMM tools commonly offer functionalities that enable IT experts to monitor problems, supervise systems, assign tasks, and streamline maintenance operations. By utilizing RMM software, organizations can obtain valuable information regarding the efficiency, well-being, and condition of their diverse IT resources. Granting access to a remote desktop enables the execution of maintenance tasks on the control remote desktop.

Figure 16 Remote access via TeamViewers

2.5.2 Augmented Reality and Remote Maintenance in Industry

Augmented Reality involves the visualization of digital models and other related data in real time, overlayed on the physical context of the industrial process. Studies on augmented reality (AR) in maintenance have demonstrated encouraging outcomes in enhancing human performance during technical maintenance tasks, optimizing the management of maintenance operations, and facilitating decision-making for maintenance managers. The Hardware characteristic consists of the devices utilized in the AR system. It has been divided in 6 categories:

1. Head Mounted Display (HMD)

2. Hand Held Display (HHD)

3. Desktop PC

4. Projector

5. Haptic

6. Sensors

Figure 17 is the pie chart of the use on AR in maintenance actions. The 'training' slice stands out as the smallest in the pie chart. This can be justified by the focus on avoiding or minimizing training when discussing AR. Instead, the emphasis is on proposing a solution that directly impacts maintenance operations [30]. By utilizing AR, maintainers gain the immediate capability to complete tasks on the job. Among the various maintenance tasks considered, assembly and disassembly appear to be the most common, starting from the top right slice of the pie chart. As early as 1997, Azuma [31] highlighted that superimposing 3-D animated drawings could simplify assembly processes compared to traditional user manuals. More recently, Westerfield et al. [31] regarded AR as the ideal tool for situations involving object manipulation, such as manual assembly.

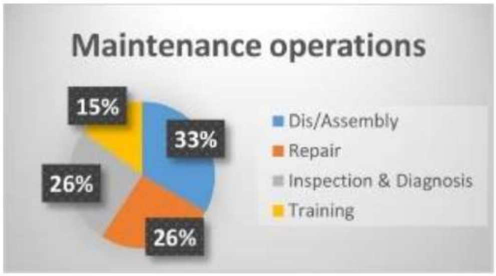


Figure 17 AR used in maintenance tasks

Smart glasses, integrated with augmented reality, were developed by our team [30] to provide maintenance personnel with precise, hands-free access to comprehensive information related to the equipment before them. This information includes technical documentation, intervention histories, as well as preventative and repair procedures, all while maintaining an unobstructed field of vision.

To complement this, an Android application was designed to establish a connection with the smart glasses. This app facilitates historical updates, data input, and the display of PDF files for in-depth equipment information, including detailed photos and diagrams.

Furthermore, the application incorporates Google Sheets, serving as a database for the lenses. This feature allows service managers to oversee the tasks performed by employees, ensuring efficient monitoring of operations.

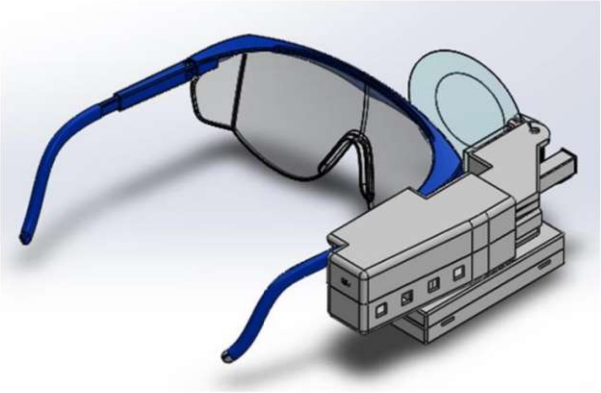


Figure 18 developed Smart Glasses in [30]

2.5.3 Specific developed applications

Despite the aforementioned tools available for remote maintenance, a significant challenge lies in the absence of a practical framework for identifying appropriate remote maintenance strategies within intelligent manufacturing systems [32]. Each manufacturing plant presents unique demands and potential for remote maintenance. To develop a comprehensive framework and offer guidance for future application, it becomes crucial to understand the specific prerequisites that should be fulfilled, encompassing the nature of the maintenance task, the plant's characteristics, as well as the performance expectations of maintenance experts and machine operators. Historically, remote maintenance has predominantly been examined from a technical perspective, focusing on its technical feasibility.

As of today, a lot of researches and practice have been proposed to develop remote monitoring and maintenance system (RMMS), also known as Intelligent Service System.

In [33] The implementation of a remote monitoring and maintenance system for machine tool manufacturers is presented. The communication method employed by the system involves the utilization of mobile phone units to establish a connection between the customer and the machine tool manufacturer (figure 19). This approach facilitates the seamless installation of the system at the customers' premises. It is worth noting that the system has been successfully implemented in over 10,000 machine tools, thereby substantiating its efficacy in enhancing service efficiency during practical application.

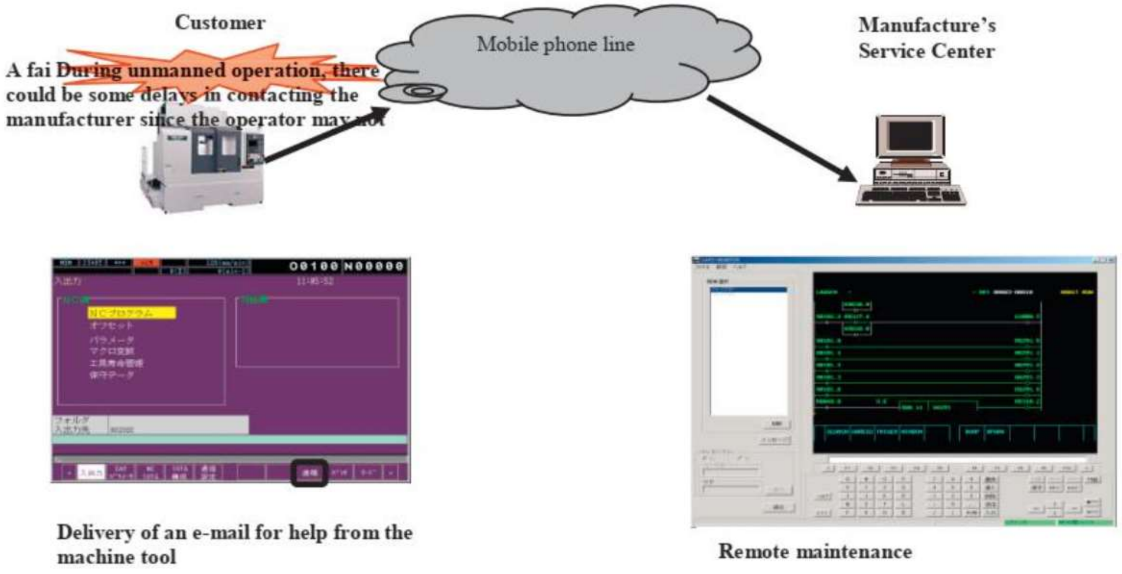


Figure 19 Remote maintenance in[33]

CHAPTER 3: Example of Known application for remote maintenance

1. Introduction

Even though this course is designed for students enrolled in the conventional Master's program in "Maintenance of Automation and Industrial Instrumentation" in collaboration with SIEMENS Algeria, the solution offered by SIEMENS will be discussed in this chapter, along with another application tailored specifically to Siemens PLCs.

2. SINEMA Remote Connect

Sinema Remote Connect is a management platform for remote networks that provides easy and secure remote access for teleservice and remote maintenance. It allows access remote plants or machines conveniently and securely, even if they are integrated into other networks. Sinema Remote Connect can be used to establish secured remote access to distributed plants or machines [34]. SINEMA Remote Connect ensures secure VPN tunnel connections between the maintenance service (telemaintenance environment) and the client network in which the components of the relevant installation are deployed. The maintenance service and the SIEMENS SCALANCE router at the client site establish an independent connection with the SINEMA Connect Server management platform. The identities of both participants are verified using a certificate before granting access to the machine.

2.1 Requirement for application of SINEMA Remote Connect

A Sinema RC system is comprised of a single server (either a dedicated server PC or potentially a virtual machine) and at least one device (known as a ‘Client’) on the distributed network.

As shown in figure 20, required equipment are:

A remote maintenance master station PC with SINEMA RC client license: a computer system that serves as the central or controlling station for remote maintenance activities. It is equipped with a software license "SINEMA RC client" to enable it to connect and communicate with remote devices or systems for the purpose of maintenance and control. This configuration allows the master station to manage and oversee maintenance operations on remote equipment.

SINEMA RC Server (VPN server): is a software application, and it does not have a physical form in the traditional sense. It is typically installed on a physical server or computer within an industrial or automation system. The server or computer running the SINEMA RC Server software provides the necessary computing resources and network connectivity to enable remote maintenance and control of industrial equipment and processes.

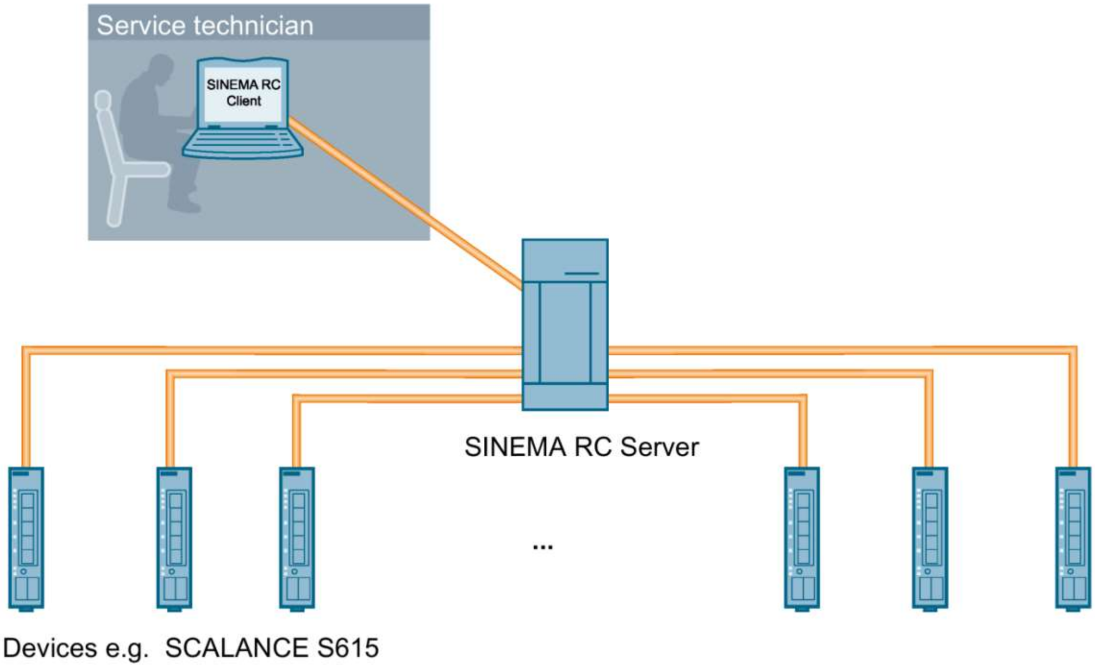


Figure 20 General Architecture of Sinema Remote connect in [35]

SCALANCE router that establish a VPN tunnel to the SINEMA RC Server and connect to the plan: is a network device designed to enable secure and efficient remote access and communication in industrial and automation environments. These routers can be configured and managed through a web-based interface or management software provided by the manufacturer. They are typically installed in industrial cabinets, control panels, or other suitable locations near the equipment or systems to be remotely monitored and controlled. Regular firmware updates and technical support are often provided to ensure the routers operate effectively and securely.

2.2 Setup and IP address configuration

Let explain it within example (figure 21):

The SCALANCE SC-600 security appliance establishes a connection between its internal network and an automation cell, which comprises various nodes including a SIMATIC station, a panel, drives, and PCs. To facilitate communication between the service technician and the automation cell, SINEMA RC Server is employed. The remote access is safeguarded through the implementation of two VPN tunnels.

- VPN tunnel 1: Client access from the PC to SINEMA RC Server is established with the "SINEMA RC Client" software.

- VPN tunnel 2: Client access from the automation cell to SINEMA RC Server runs via the SCALANCE SC-600 security appliance.

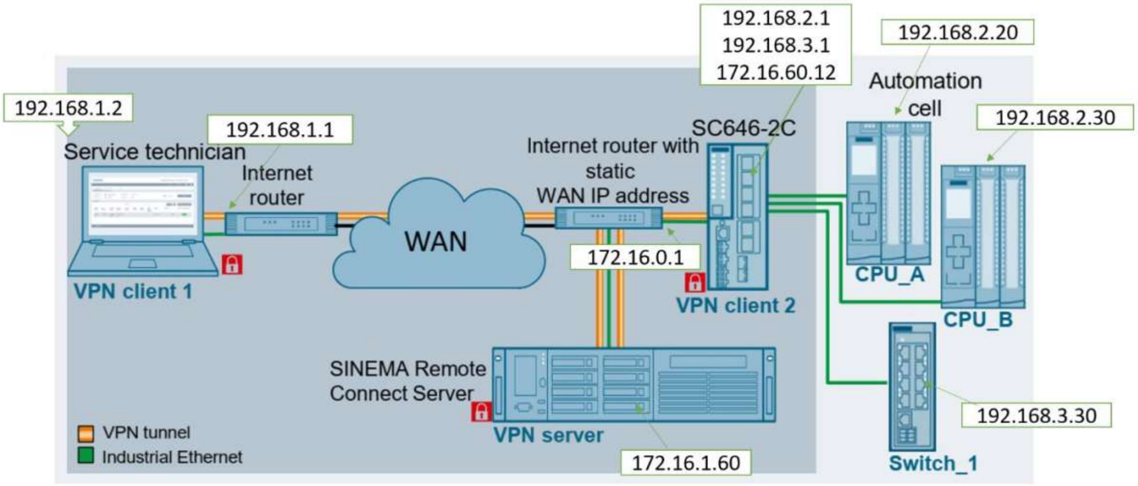


Figure 21 IP address configuration

SINEMA RC Server effectively directs traffic between distinct VPN tunnels based on the established communication relationships and security configurations. The accessibility to the VPN server, which is the SINEMA RC Server, is determined by a fixed WAN IP address. It is worth noting that the service technician enjoys adaptable access, and the external IP address of the router holds no significance in this context.

Steps for that configuration are simplified as follow [34]:

TIA Portal

1. Install TIA Portal on the client PC.

2. Set up a TIA Portal project with your CPUs.

3. Configure the interfaces of the CPUs load the modules "CPU_A" and "CPU_B".

Switch

Configure the IP address of "Switch_1"

SINEMA RC Client

1. Install the "SINEMA RC Client" software on the client PC. The installation is almost entirely automatic. The SETUP routine automatically detects whether other program components need to be installed in addition to SINEMA RC Client itself. The installation routine executes the necessary actions as required
2. Set the network settings on the PC

SINEMA RC Server

Proceed as follows to prepare SINEMA RC Server:

1. Install the SINEMA RC Server on a PC. During installation, the WAN interface will be setup: IP address, Netmask and Gateway

2. If SINEMA RC Server is installed, sign in with the default "admin" user

Router and VPN

If VPN connections have been configured on the router and activated, follow step.

LAN port configuration with the appropriate address (figure 21)

The SINEMA RC Server router is configured with a static IP address. The client PC, known as VPN client 1, is able to access the SINEMA RC Server, acting as the VPN server, through a fixed and publicly accessible IP address. This IP address is obtained from the service provider and stored in the DSL router.

To ensure seamless communication between the client PC and SINEMA RC Server, port forwarding is enabled on the SINEMA RC Server router. This allows tunnel packets to freely traverse between the two devices. Specifically, port forwarding is enabled for "OpenVPN" and "HTTPS" protocols using both TCP and UDP. As a result, the packets are directed towards the SINEMA RC Server.

By following these steps, the remote maintenance network is successfully established.

APPLICATION: Students are asked to experiment SINEMA RC server or client installation on Tiaportal [15]

2.3 External published application

Very few work are describing the use of SINEMA Remote Connect, but [36] did it well. The System and Infrastructure of Knowledge for Real Experimentation by means of Cells of Industrial Automation (SIKRECIA) is developed to provide new capabilities for research, development, simulation and testing of the functioning of these systems, and the ability to predict the behavior of a specific system in industrial production. Using SIKRECIA, a specific vulnerability in a PLC was analyzed by testing it with the programming for a traffic light control system. The results show how closely IT and OT (operation technology) systems are interconnected, emphasizing the need to simulate these environments before deployment. SIKRECIA is an open system that can adapt to various industrial equipment, making it suitable for different process industry setups. Remote connect Sinema was tested in cell consists of a PLC S7 1200, 1214 AC / DC Relay (Figure 22).

The cell comprises a PLC S7 1200, 1214 AC/DC Relay, which incorporates a built-in trigger plateforme capable of directly influencing the PLC circuitry, thereby providing manual access to its digital inputs. To enhance security, an SCALANCE S615 industrial firewall has been integrated into the system.

This firewall module features five Ethernet ports that offer protection for various network topologies through the implementation of firewall or virtual private network (VPN) technologies such as IPsec and OpenVPN. This enables the flexible implementation of security concepts. Users have the ability to configure up to four variable security zones with individual firewall rules. The device can be easily integrated and parameterized using the Sinema Remote Connect (SRC) management platform, thanks to its auto configuration interface. Additionally, this device allows the creation of multiple VLANs, which facilitates bidirectional access between the PLC and HMI, PLC and Programming System with TIA Portal, and PLC and SCADA, based on the permissions granted to the respective virtual machines. Using this open system, Authors could determine vulnerabilities of the Industrial plan and it was token in account by the firms.

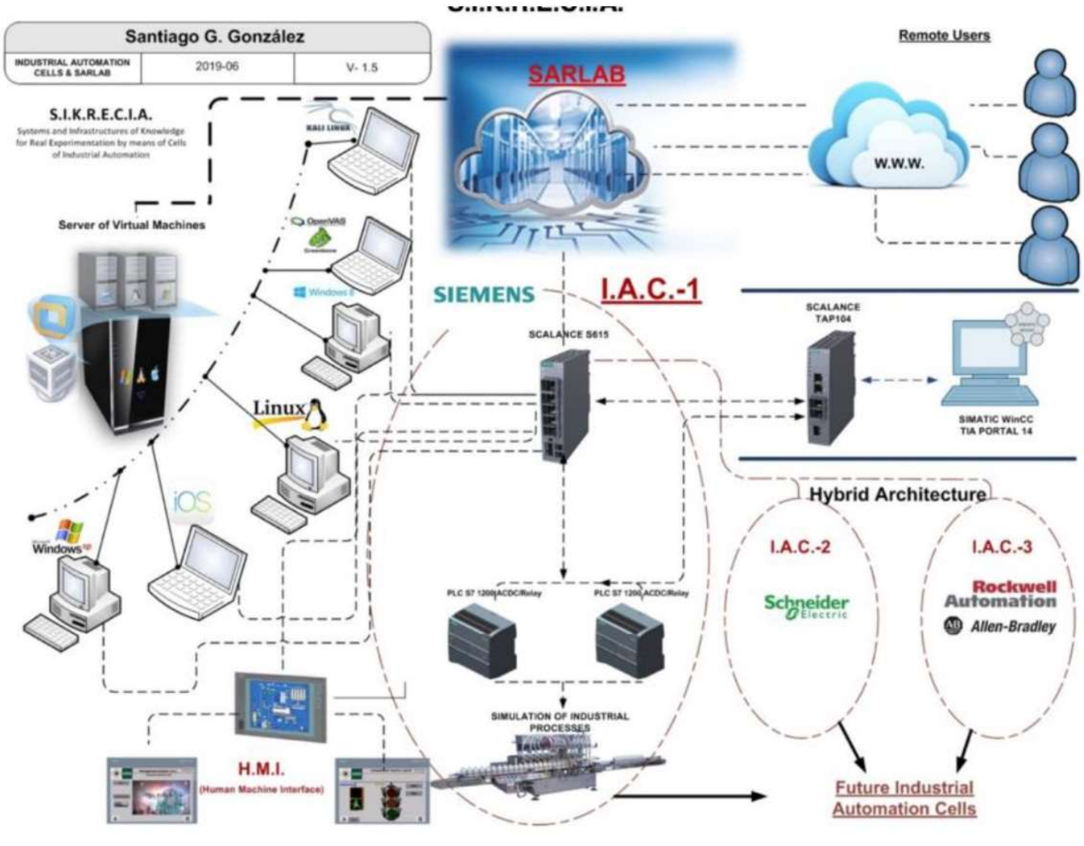


Figure 22 Network scheme and testbed created for Testing Industrial Systems

3. ETIC telecommunication solution

The aim was to take control of a Siemens S7-1200 programmable logic controller (PLC) using the TIA Portal programming environment through the Internet (utilizing an existing Internet connection or a 3G connection) to perform operations such as dynamic visualization, program loading, diagnostics, and debugging... [37]

3.1 Required equipment

To implement this solution, these are the required equipment:

Server RAS : RAS-E-1400 or RAS-3G according the case :

- A « pack M2Me_Connect » including a software M2Me_Secure Version 1.43, a License X509 given by ETIC TELECOM and unlimited access to service M2Me_Connect

- A PLC S7-1211

- TIA Portal V12 or above

Those equipment are connected according to the following architecture:

For RAS-e (wired connection) (figure 23) RAS-3G (GSM connection) (figure 24)

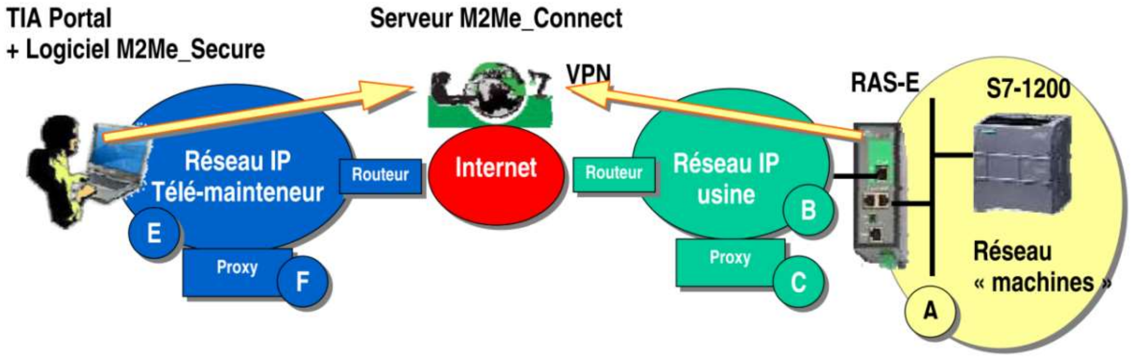


Figure 23 RAS-E connection network

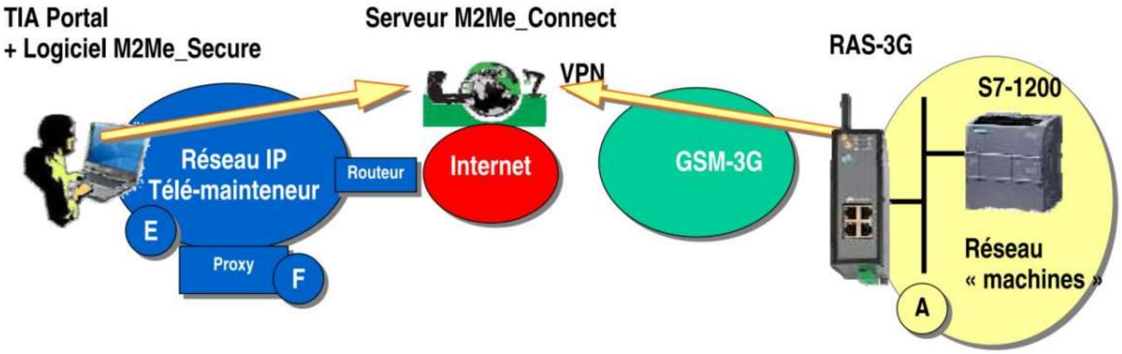


Figure 24 RAS-3G connection network

3.2 RAS-E Setting

IP Address Assignment Rule

The IP address of the 'machines' network A (PLC, other machine devices, and LAN address of the RAS server) must be different from:

The IP address of Factory Network B

The IP address of the Telemaintainer Network E.

For example, with Netmasks set to 255.255.255.0:

@IP address of the Telemaintainer network = 192.168.1.X

@IP address of the Factory network = 192.168.3.X

@IP address of the machine network = 192.168.9.X (for example)

Important Note: The system functions properly even if the IP addresses of the Factory network and the Telemaintainer network happen to be the same.

IP Addresses on the Machine Network (LAN Interface)

The IP address of the LAN interface of the RAS server belongs to the machine network (PLC, etc.).

For example:

@IP of the LAN interface of the RAS server = 192.168.9.1

@IP for remote users = 192.168.9.2 to 192.168.9.4

For example, to reserve three addresses for remote users.

@IP of the PLC = 192.168.9.30

3.2.1 IP Addresses on the Factory Network (WAN Interface)

It can be assigned either by the Factory network's DHCP server or set as a fixed address.

3.2.2 VPN

The RAS-E establishes an outgoing OpenVPN type VPN connection exclusively to the M2Me service carefully managed by ETIC TELECOM.

To avoid scanning authorized ports (a configuration option on the RAS), it is advisable to consult with the network administrator regarding their preference for using TCP or UDP and specifying a port number.

3.2.3 Internet Access Restriction via Proxy

If there is a proxy server on the Factory network that restricts internet access, please consult with the network administrator to obtain information on its type, IP address, as well as login and password.

3.2.4 Connection

Connect the Factory network to the RJ45 interface located within the green rectangle (WAN).

Connect the PLC or automation network to one of the RJ45 connectors located in the lower part (LAN).

3.3 RAS-3G setting

The IP address of the 'machines' network A (PLC, other machine devices, and the LAN address of the RAS server) must be different from the IP address of the Telemaintainer network E.

For example:

Using a Netmask of 255.255.255.0:

Telemaintainer network IP = 192.168.1.X

Machine network IP = 192.168.9.X (for example).

3.3.1 IP Addresses on the Machine Network (LAN Interface)

The IP address of the LAN interface of the RAS server belongs to the machine network (PLC, etc.).

For example:

IP of the LAN interface of the RAS server = 192.168.9.1

IP addresses for remote users = 192.168.9.2 to 192.168.9.4

For instance, to allocate three addresses for remote users.

IP of the PLC = 192.168.9.30

3.3.2 Antenna

The antenna used can be either a magnetic base antenna to be placed on a metal plate or a wall-penetrating antenna to be affixed to a horizontal metal plate using a nut. If the cabinet is metallic, the antenna must be positioned outside the cabinet and, as much as possible, away from the wall.

3.3.3 SIM Card

The subscription must provide internet connectivity and authorize secure VPN communication. A standard subscription like those used for smartphones or USB dongles is suitable. The price paid is generally proportional to the volume of data exchanged. If the PLC is located abroad, it is advisable to obtain a SIM card in the country where the PLC is installed; this way, the cost will be the national rate, and it avoids the high cost of roaming.

3.3.4 Antenna IP Address

When using the M2Me_Connect service, the IP address provided by the mobile network operator to the RAS server's antenna during each connection can be of any type: private or public, dynamic or static. It is recommended to use a private and dynamic IP address (similar to smartphones).

3.3.5 Connection of the RAS-3G

Connect the PLC or the automation network to one of the RJ45 connectors located in the lower part (LAN)

3.4 Configuration

3.4.1 PLC Configuration

Assign an IP address to the PLC.

Reminder:

The IP network of the PLCs (machine network) must be different from the Factory IP network, and

The PLC network must also be different from the Telemaintainer network.

3.4.2 RAS Server Configuration

Below are some installation instructions for the RAS server; for more details, please refer to the manual mentioned earlier.

- Access the HTML configuration server of the RAS server (192.168.0.128).

- Assign an IP address to the Ethernet interface (LAN) of the RAS server, which belongs to the same network as the PLC.

- Reserve a few IP addresses on this network for remote users.

- Configure the connection of the RAS server to the 3G network (RAS-3G) or the Factory network (RAS-E).

- Select the M2Me option.

3.4.3 Declare the Site in M2Me

Below are some indications; for more details, please refer to the manual mentioned earlier.

- Open the M2me_Secure software.

- Select the 'Menu' icon.

- Click on 'New site.'

- Assign a name to the remote site.

- In the 'Connection' tab, check both boxes and enter the Product Key of the RAS server.

3.4.4 Verify the Connection to the PLC

- Select the 'M2Me' gateway.

- Click on the 'Browse the network' button. The PLC label will appear in the tree structure.

- Click 'File' and then 'Save the project.'

- Disconnect the PC from M2Me if necessary."

3.5 Remote Usage on TIA Portal

3.5.1 Connecting the PC to the Remote Network

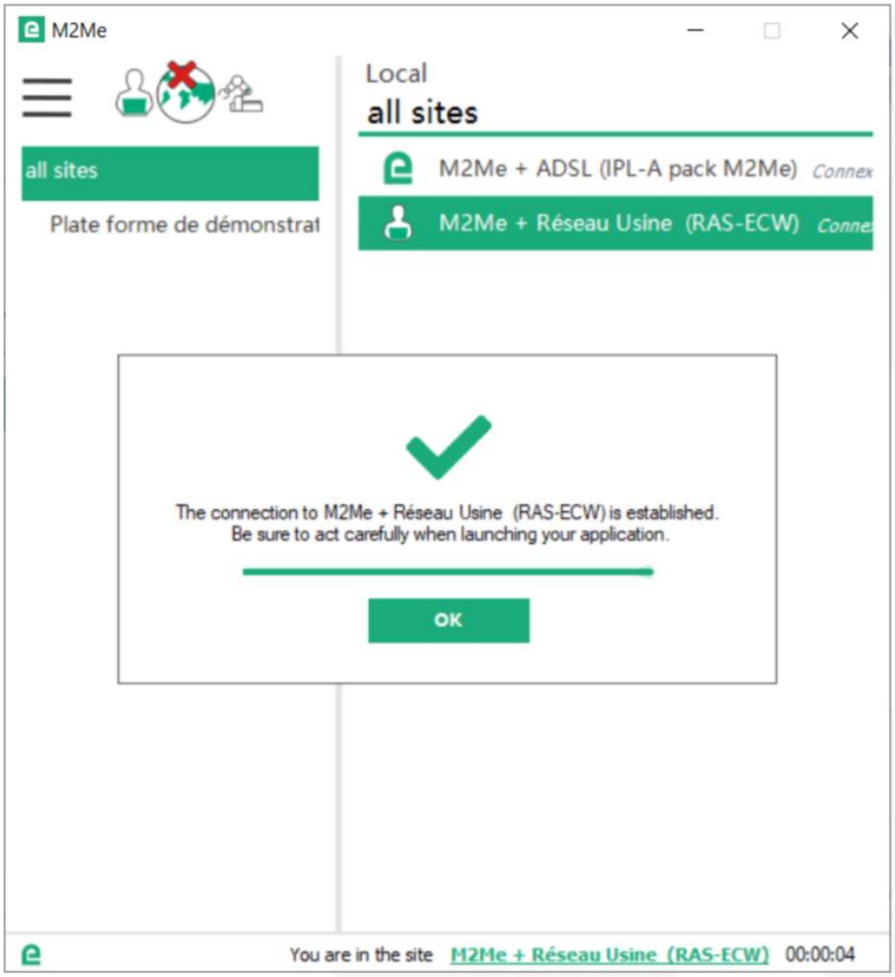
- Open the M2Me_Secure software.

- Connect the PC to the M2Me_Connect service.

- Select the machine from the directory.

- Click the 'Connect to the machine via the Internet' button to establish end-to-end encrypted connection with the machine.

- When the icon appears, the PC is connected to the remote automation network


M2Me
Local
all sites
all sites
Plate forme de démonstrat
M2Me + ADSL (IPL-A pack M2Me) Connex
M2Me + Réseau Usine (RAS-ECW) Conne
OK

The connection to M2Me + Réseau Usine (RAS-ECW) is established.
Be sure to act carefully when launching your application.

You are in the site M2Me + Réseau Usine (RAS-ECW) 00:00:04

Figure 25 Client connection to site

3.5.2 Connecting TIA Portal to the PLC

- Open TIA Portal.
- Select the project from the list and click 'Open.' The project tree is displayed.
- Select 'Open project view.'
- Choose the PLC.
- Click the 'Online connection' icon.
- In the 'Mode' list, select PN/IE.
- In the 'Interface PG/PC' list, choose 'TAPWIN32 ADAPTER V9#2.'

Subnetwork connection: select the parameter based on your configuration.

For an S7-1200, choose '1 X1.'

TIA PORTAL will display the PLCs or other equipment found on the remote network.

- Click the 'Connect' button.

TIA PORTAL indicates that the connection is established. Work as usual

3.5.3 Disconnect

As usual: Disconnect TIA Portal from the PLC: Click the 'Interrupt online connection' icon.

Disconnect the PC from the remote network: Click the 'Disconnect' icon in M2Me.

Close M2Me if necessary

These two applications provide a practical demonstration of the implementation of remote maintenance on an industrial site using Siemens devices.

CHAPTER 4: Remote Maintenance application in MAII lab at IMSI

1. Introduction

In the MAII lab at IMSI (Institut of Maintenance and Industrial Safety) a project was realized, titled "G120 drives in remote maintenance". This project involves implementing remote maintenance for a basic industrial system. This system consists of a G120 variable speed drive, a S7-1200 PLC, a man/machine interface, and an asynchronous motor from Siemens. To facilitate the design of our project, we have divided the work into three parts.

The first part focuses on commissioning and parameterizing the variable speed drive to control the motor's speed variation. Additionally, we have established the local network for our installation.

In the second part, we have developed the program for motor control and created views for the man/machine interface (HMI) and SCADA (Supervisory Control and Data Acquisition) system.

The third part involves configuring the communication between the two routers and the VPN (Virtual Private Network). This configuration is necessary to establish a secure connection and ensure access to the installation.

2. Network architecture of this remote maintenance application

The purpose of this architecture is to access the installation remotely (via the internet) to perform the following operations: diagnostics, program loading, control/command, using a VPN network (Ooredoo VPN).

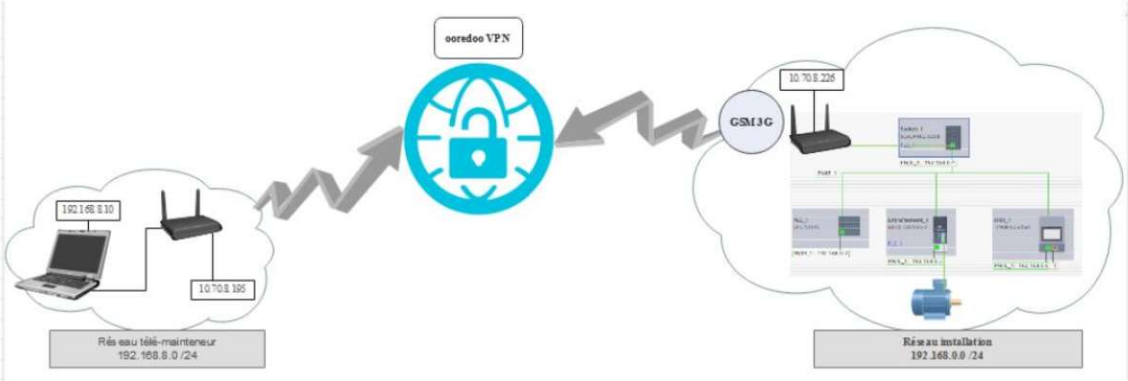


Figure 26 The network architecture of this remote maintenance application

2.1 Necessary equipment

— The site installation comprises

• An S7-1200 a programmable controller system, compact controller a perfect solution for controlling small applications [12].

• A TP900 comfort human/machine interface (HMI) specifically a touch panel interface designed for industrial automation applications. HMIs like the TP900 Comfort are used to provide a user-friendly interface for operators and engineers to interact with and control industrial machines and processes. The TP900 Comfort HMI typically features a color touchscreen that allows users to monitor and control various aspects of the industrial system, such as viewing process data, adjusting settings, and responding to alarms. It's a part of Siemens' Simatic HMI product family and is commonly used in automation and control systems across various industries [38].

• A G120 variable speed drive. Variable Frequency Drive (VFD) from Siemens, specifically the SINAMICS G120 series. These drives are used for controlling the speed of electric motors in various industrial applications [39]. The G120 series VFDs are known for their versatility and flexibility, making them suitable for a wide range of motor control tasks, including pumps, fans, conveyors, and other machinery. They allow precise control of motor speed and are designed to improve energy efficiency and process control in industrial settings.

• A Switch Scalance x208 is a network switch designed for industrial applications. It's part of the Scalance X series of switches, which are known for their robustness and reliability in industrial environments [40]. The Scalance X208 switch provides Ethernet connectivity for various devices in an industrial network. It typically features multiple Ethernet ports, which can be used for connecting devices such as programmable logic controllers (PLCs), human-machine interfaces (HMIs), sensors, and other equipment used in industrial automation and control systems.

These switches are designed to operate in harsh industrial conditions, including high temperatures, humidity, and resistance to vibration and shock. They play a crucial role in creating and maintaining stable and efficient communication networks within industrial settings, helping to ensure the smooth operation of critical processes and machinery.

•Engine Siemens IEC Motor [41].

— Two Hongdian modems. a line of industrial-grade modems produced by the Hongdian Corporation, a Chinese company specializing in the design and manufacturing of communication equipment and IoT (Internet of Things) devices [42]. Hongdian modems are designed for reliable and secure data communication in industrial and remote environments. These modems are known for their ruggedness, durability, and the ability to operate in challenging conditions, making them suitable for applications such as remote monitoring, telemetry, and industrial automation.

Key features of Hongdian modems often include support for various wireless communication technologies such as 2G, 3G, 4G, and sometimes even low-power, wide-area (LPWA) networks like LoRa or NB-IoT. They are used to establish reliable and continuous data connections for collecting and transmitting data from remote sensors and devices back to a central server or control center. This makes them valuable components in various IoT and M2M (machine-to-machine) applications, including agriculture, energy, environmental monitoring, and more.

— Two ooredoo chips.

— Access to ooredoo vpn.

— PC.

— The TIA PORTAL software.

— A cable to connect the PC to the modem.

— A cable to connect the installation to the modem.

The system installation is connected to the switch which is connected to the LAN port of the modem via an ETHERNET cable.

2.2 Setting up the connection

It is a question of assigning IP addresses to the different devices: Assigning an IP address to the PLC (192.168.0.2), as well as the other equipment (Figure 27):

— Variable speed drive (192.168.0.5).

— HMI (192.168.0.6).

— Switch (192.168.0.4).

The addresses must be within the same network range of the facility (192.168.0.0) and must also be different from the maintainer's network. The IP address of the telephony network Maintainer = 192.168.8.0.

The configuration of the connection modems goes through the following steps:

2.2.1 Configuring Modem 1 Connected to the Installation

1. Go to the modem's HTML page to set it up.

2. Assign the modem's LAN interface an IP address within the same range of the Installation network: IP modem 1 = 192.168.0.1

3. Configure the modem connection to the ooredoo chip network, an IP address will be assigned to the modem WAN interface: IP ooredoo chip = 10.70.8.226.

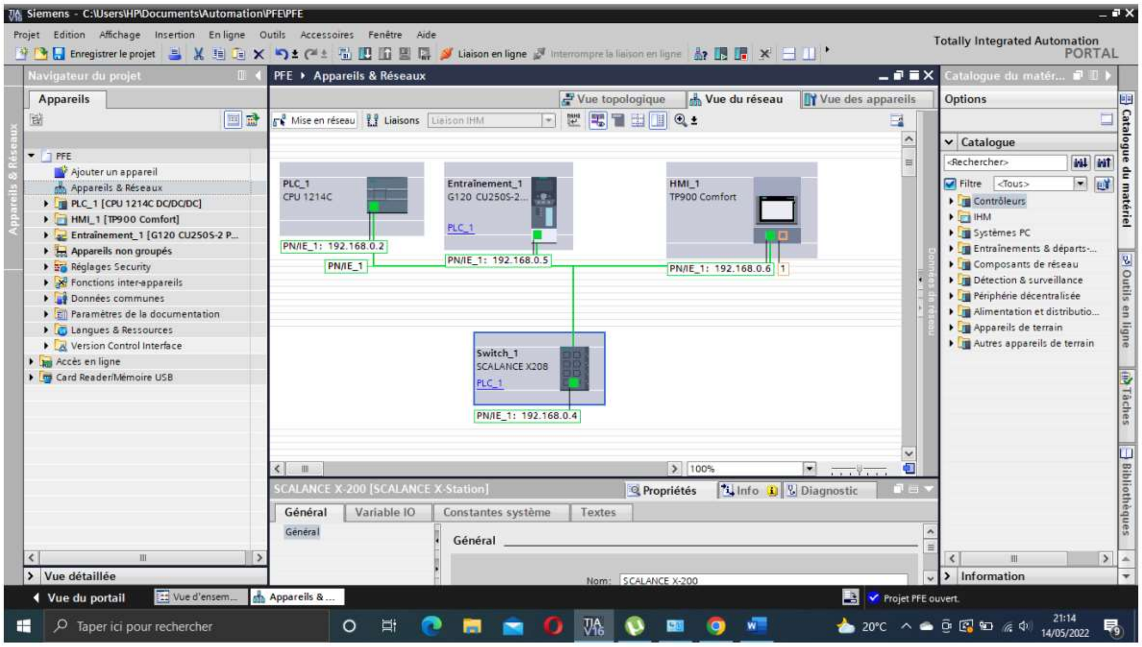
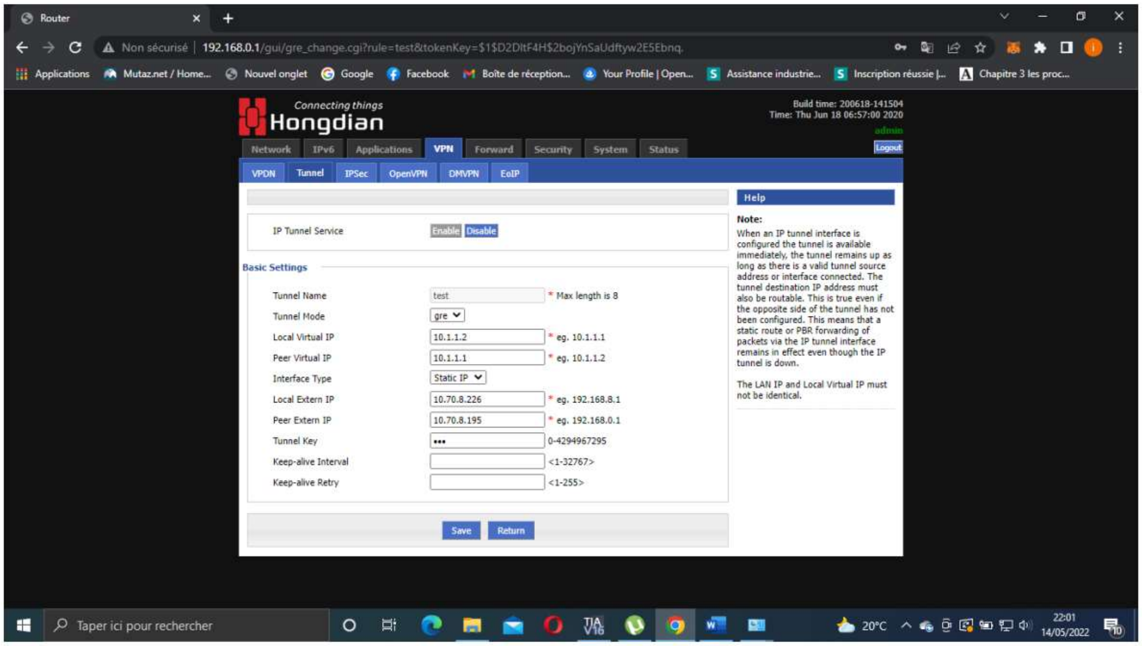


Figure 27 Setting the IP addresses of the installation elements

The Operator assigns the IP address of the chip (static address).

4. Disable the DHCP function of the modem then Configure VPN by following the steps in the figure below (figure 28):



Router
192.168.0.1/gui/gre_change.cgi?rule=test&tokenKey=$1$D2DltF4H$2bojYnSaUdftyw2E5Ebnq.
Connecting things
Hongdian
Build time: 200618-141504
Time: Thu Jun 18 06:57:00 2020
Network
IPv6
Applications
VPN
Forward
Security
System
Status
Logout
VPDN
Tunnel
IPSec
OpenVPN
DMVPN
EoIP
Help
Save
Return

IP Tunnel Service: Enable / Disable

Basic Settings

Tunnel Name: test * Max length is 8
Tunnel Mode: gre
Local Virtual IP: 10.1.1.2 * eg. 10.1.1.1
Peer Virtual IP: 10.1.1.1 * eg. 10.1.1.2
Interface Type: Static IP
Local Extern IP: 10.70.8.226 * eg. 192.168.8.1
Peer Extern IP: 10.70.8.195 * eg. 192.168.0.1
Tunnel Key: ••• 0-4294967295
Keep-alive Interval: <1-32767>
Keep-alive Retry: <1-255>

Note:
When an IP tunnel interface is configured the tunnel is available immediately, the tunnel remains up as long as there is a valid tunnel source address or interface connected. The tunnel destination IP address must also be routable. This is true even if the opposite side of the tunnel has not been configured. This means that a static route or PBR forwarding of packets via the IP tunnel interface remains in effect even though the IP tunnel is down.

The LAN IP and Local Virtual IP must not be identical.

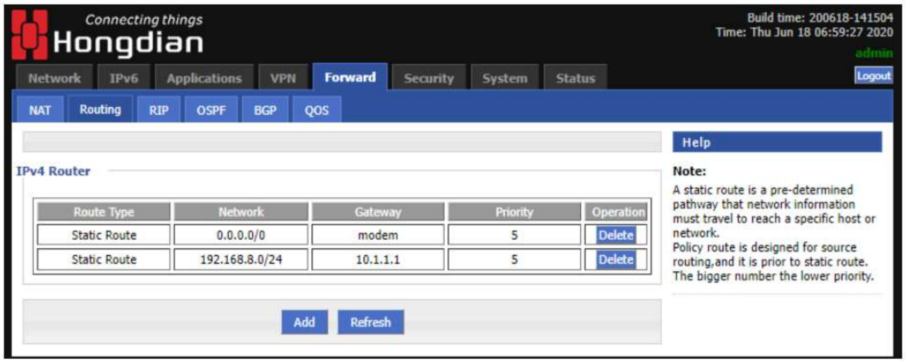
Figure 28 VPN creation

5. Enable the NAT option and then add two MASQs: By default, the router translates addresses Source IPs moving from the private to the public segment. However, the router disables the IP address that is hidden on the specified interface.

— MASQ br0 : LAN output.

— MASQ modem: bus output.

6. Create a routing table so that the telemaintainer's network can be communicated (Figure 29):



Build time: 200618-141504
Time: Thu Jun 18 06:59:27 2020

IPv4 Router

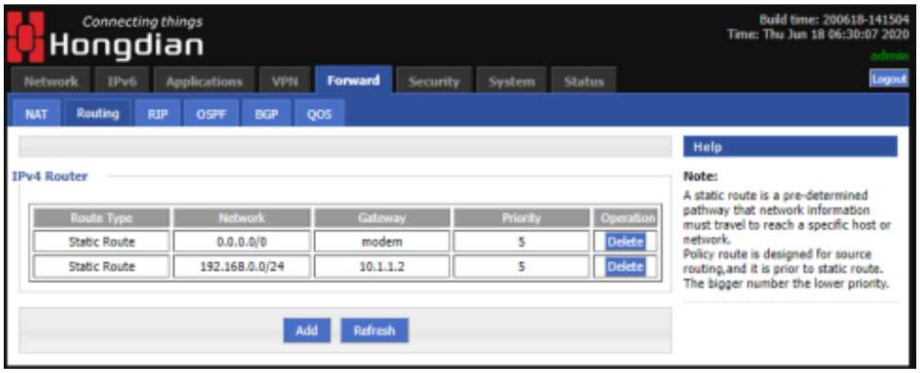
Route Type	Network	Gateway	Priority	Operation
Static Route	0.0.0.0/0	modem	5	Delete
Static Route	192.168.8.0/24	10.1.1.1	5	Delete

Note:
A static route is a pre-determined pathway that network information must travel to reach a specific host or network.
Policy route is designed for source routing,and it is prior to static route.
The bigger number the lower priority.

Figure 29 Creating the Routing Table Modem 1

2.2.2 Configuring Modem 2 Connected to the PC

First, go to the modem's HTML page to configure it. Assign the modem's LAN interface an IP address that is within the same range of the PC network: IP modem 1 = 192.168.8.1. Then, Configure the modem connection to the ooredoo chip network, an IP address will be assigned to the modem WAN interface: IP ooredoo chip = 10.70.8.226. The Operator assigns the IP address of the chip (static address), then continue the same steps as modem 1 with routing table as in figure 30.



Build time: 200618-141504
Time: Thu Jun 18 06:30:07 2020

IPv4 Router

Route Type	Network	Gateway	Priority	Operation
Static Route	0.0.0.0/0	modem	5	Delete
Static Route	192.168.0.0/24	10.1.1.2	5	Delete

Note:
A static route is a pre-determined pathway that network information must travel to reach a specific host or network.
Policy route is designed for source routing,and it is prior to static route.
The bigger number the lower priority.

Figure 30 Creating the Routing Table Modem 2

These tow modems can connect safely on VPN network.

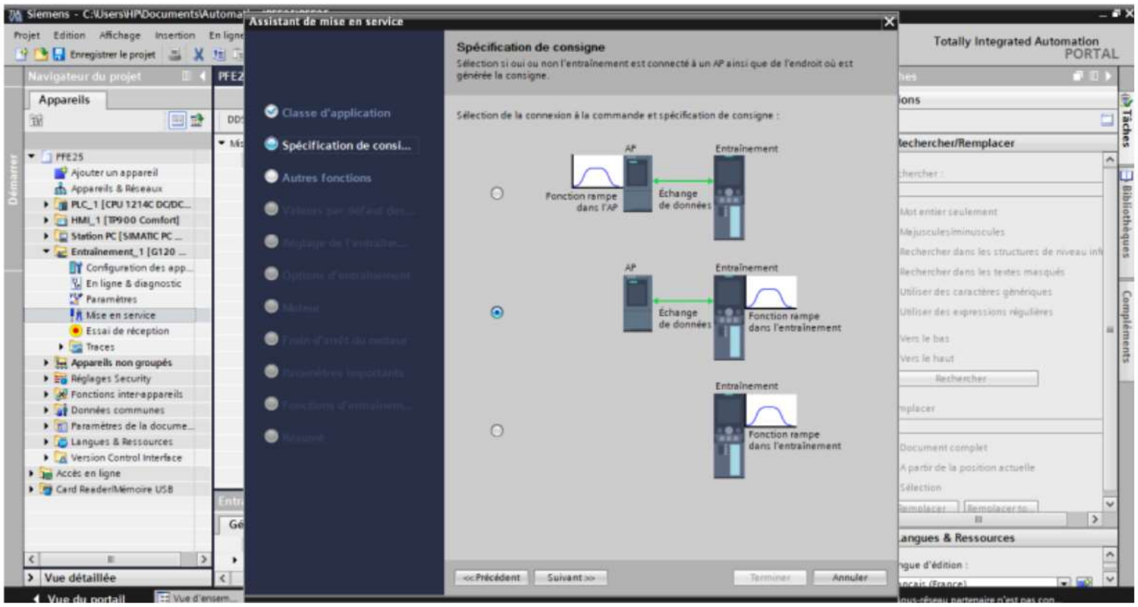
3. Site plan implementation and experiments

3.1 On Tiaportal

The site plan implementation is carried out in TIAPORTAL, enabling the configuration of each piece of equipment within the plan and the design of their respective processes.

It starts by creating a project, adding equipment: S7-1200 Version 1214C DC/DC/DC with the address 192.168.0.2 . Adding the VFD G120 CU250-PN. Afterward, we need to add the power part of the variable frequency drive, and assign it an address of 192.168.0.5, just as we did for the PLC. We also need to add the TP900 comfort human-machine interface (HMI) screen of version 16.0.0.0. Next, we must connect it to the PLC and follow the following steps, assigning it an address of 192.168.0.6.

In order to create the SCADA system, the addition of a PC station is necessary. Following its creation, the installation of the WinCC application is required, which enables the creation and visualization of views. Additionally, the Ethernet module must be installed to establish a connection to the LAN network, with an assigned address of 192.168.0.10. Subsequently, after the incorporation of these components and the allocation of IP addresses to each device, it becomes imperative to interconnect them using a switch (SCALANCE X208) and assign it an address of 192.168.0.4. At this stage, it can be stated that a LAN network has been established, encompassing multiple devices interconnected within the address range of 192.168.0.0/24.



Assistant de mise en service

Spécification de consigne

Sélection si oui ou non l'entraînement est connecté à un AP ainsi que de l'endroit où est générée la consigne.

Sélection de la connexion à la commande et spécification de consigne :

Figure 31 Setpoint Specification

The PLC is assigned the IP address of 192.168.0.2, while the Variable Frequency Drive is allocated the IP address of 192.168.0.5. Furthermore, the HMI is assigned the IP address of

192.168.0.6, and the PC Station is assigned the IP address of 192.168.0.10. Lastly, the SWITCH is assigned the IP address of 192.168.0.4.

To proceed, it is necessary to configure the variable frequency drive in accordance with the motor nameplate specifications (like in figure 31). Once the configuration of the variable frequency drive is successfully completed, the motor can be identified.

3.2 The PLC program

In order to regulate the variation in motor speed, the utilization of a function block known as SINASPEED (figure 32), along with a telegram1, is employed. In the present investigation, the motor is regarded as a centrifugal pump, thus the motor speed will be adjusted based on the analog input signal received from the level transmitter (4-20mA). It is assumed that the motor will operate at its mean speed (430 rpm) when the level is at its midpoint (50%). In simpler terms, when a 12mA signal is transmitted by the transmitter, the motor will operate at a speed of 430 rpm.

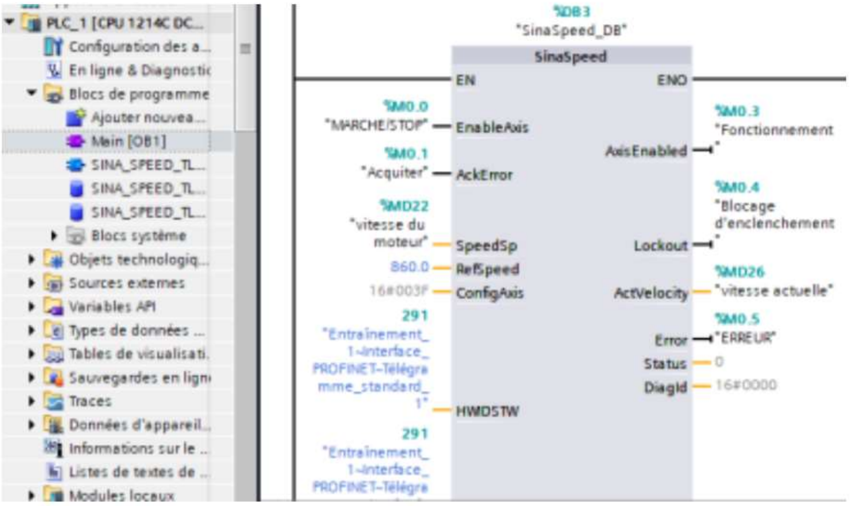


Figure 32 VFD principal function

Subsequently, the SCADA system has been developed for the purpose of real-time supervision and control of the process. The addition of views and their configuration can be easily accomplished using the WinCC Advanced software (figure 33), which encompasses a library for the inclusion of objects, their configuration, and the programming of their animations within the views.

The 'Operation' variable is to be assigned to the pump.

The motor speed variable is to be assigned to the speed display.

The 'Acknowledge' variable is to be assigned to the acknowledge button.

The 'RUN/STOP' variable is to be assigned to the switch.

The 'Signal' variable is to be assigned to the transmitter signal display.

The 'ERROR' variable is to be assigned to the error indicator.

The 'Measurement' variable is to be assigned to the level display.

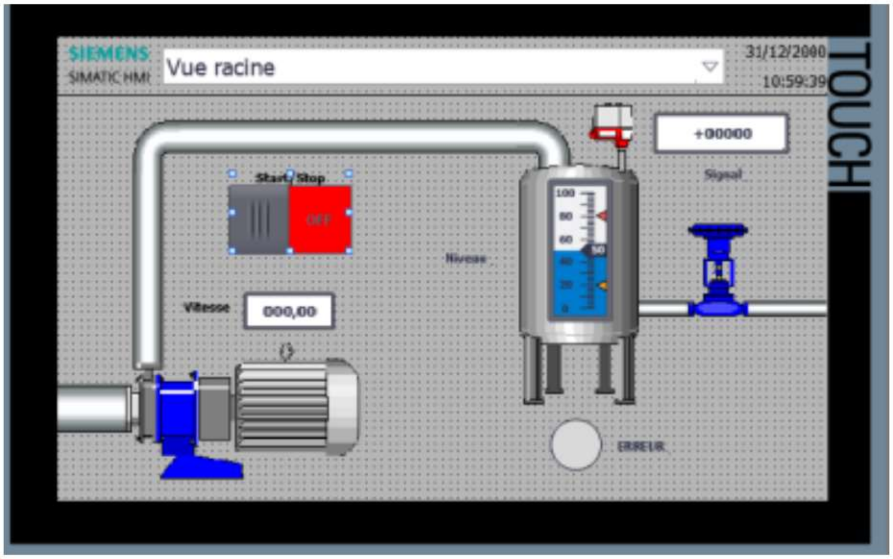


Figure 33 HMI view

In order to facilitate monitoring within the installation, it is imperative to incorporate a human-machine interface (HMI) screen that allows for seamless communication with the system. Similar to the approach taken during the development of the SCADA view, the same procedural steps will be followed to establish the HMI. Furthermore, alongside the process view, an additional diagnostic view will be integrated.

4. Remote access experimentation

The station must be connected to the modem having the address 192.168.0.1, which houses the chip with the address 10.70.8.226. On the other hand, the PC with the network card configured as 192.168.8.10 should be connected to the modem having the address 192.168.8.1, which contains the chip with the address 10.70.8.195. Figure 34 presents an overview of the system.

To assess the connectivity between the two networks, the ping function is utilized on the personal computer. The evaluation commences with the modem having an IP address of 192.168.8.1, which is linked to the PC. Subsequently, we test the chip with an address of 10.70.8.195 that is inserted into this modem, followed by the chip with an address of 10.70.8.226 that is inserted into the station's modem. Finally, we evaluate the connectivity of the modem with an IP address of 192.168.0.1.

Next, the TIAPORTAL software is utilized to establish a remote connection, enabling us to remotely manage the installation through SCADA.

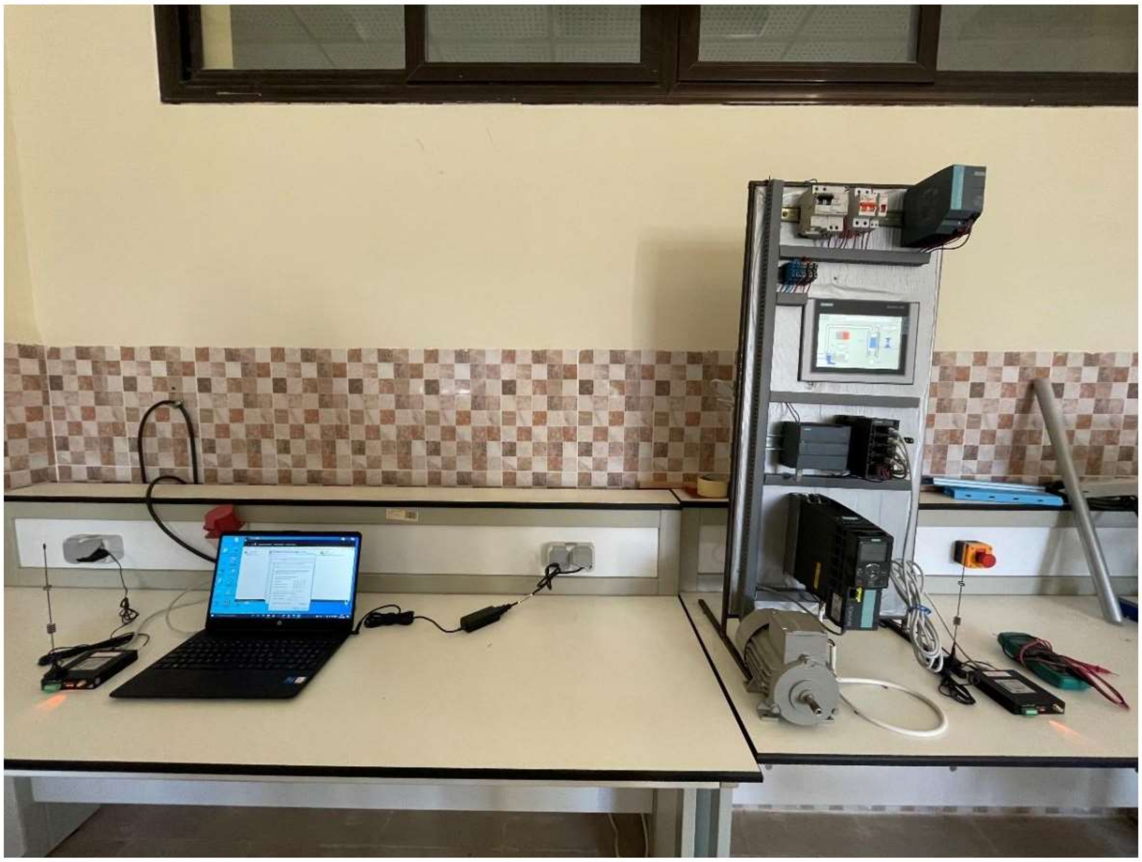


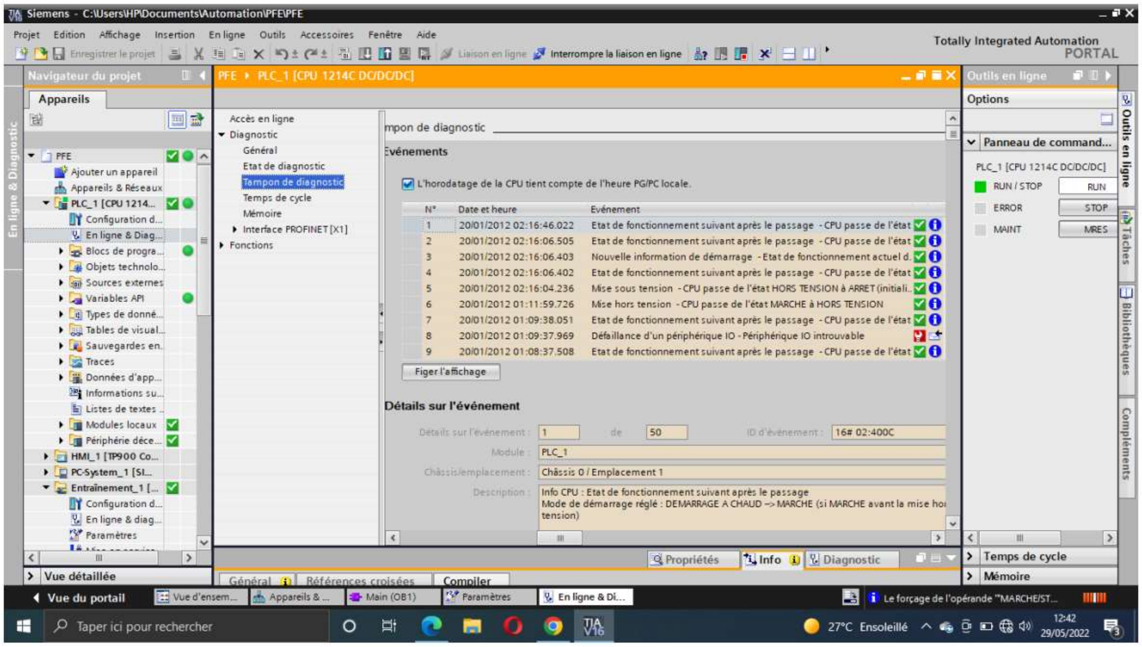
Figure 34 General view of the experimental system

4.1 Diagnosis

We have the capability to perform system diagnostics, enabling us to directly monitor the status of the different components within our setup, which includes the PLC, variable speed drive, HMI, and motor. TIA Portal offers this functionality, granting us access to the parameters of the variable speed drive, allowing us to make adjustments to both the drive settings and PLC status, and providing a comprehensive overview of all system parameters and any associated alarms (figure 35).

4.2 Maintenance

After diagnosing the system remotely, it's also possible to perform maintenance when there's a software issue. Updating and modifying the PLC program is achievable using TIA Portal and the VPN network. The transferred data is encrypted, making it possible to intervene as if one were on-site. The loading process takes only a few seconds (approximately 5 to 10 seconds).



mpon de diagnostic

Evénements

☑ L'horodatage de la CPU tient compte de l'heure PG/PC locale.

N°	Date et heure	Evénement
1	20/01/2012 02:16:46.022	Etat de fonctionnement suivant après le passage - CPU passe de l'état
2	20/01/2012 02:16:06.505	Etat de fonctionnement suivant après le passage - CPU passe de l'état
3	20/01/2012 02:16:06.403	Nouvelle information de démarrage - Etat de fonctionnement actuel d.
4	20/01/2012 02:16:06.402	Etat de fonctionnement suivant après le passage - CPU passe de l'état
5	20/01/2012 02:16:04.236	Mise sous tension - CPU passe de l'état HORS TENSION à ARRET (initiali..
6	20/01/2012 01:11:59.726	Mise hors tension - CPU passe de l'état MARCHE à HORS TENSION
7	20/01/2012 01:09:38.051	Etat de fonctionnement suivant après le passage - CPU passe de l'état
8	20/01/2012 01:09:37.969	Défaillance d'un périphérique IO - Périphérique IO introuvable
9	20/01/2012 01:08:37.508	Etat de fonctionnement suivant après le passage - CPU passe de l'état

Figer l'affichage

Détails sur l'événement

Détails sur l'événement : 1 de 50 ID d'événement : 16# 02:400C

Module : PLC_1

Châssis/emplacement : Châssis 0 / Emplacement 1

Description : Info CPU : Etat de fonctionnement suivant après le passage
Mode de démarrage réglé : DEMARRAGE A CHAUD –> MARCHE (si MARCHE avant la mise hor
tension)

Figure 35 Diagnosis view

<u>APPLICATION: Students are asked to watch a video about this project https://www.youtube.com/watch?v=G4DO9k1AsOk&t=310s</u>

BIBLIOGRAPHY

[1] N. Aissani, I. Mechrour, et A. Filali, « Overview of Maintenance 4.0 and the associated approaches, and a preliminary case study in Algeria », in *2021 International Conference on Networking and Advanced Systems (ICNAS)*, oct. 2021, p. 1-6. doi: 10.1109/ICNAS53565.2021.9628931.

[2] « Federal Standard 1037C », *Wikipedia*. 1 août 2023. Consulté le: 13 août 2023. [En ligne]. Disponible sur: https://en.wikipedia.org/w/index.php?title=Federal_Standard_1037C&oldid=1168140089

[3] E. Wilke, « Minimizing Asset Downtime with CMMS-Assisted Troubleshooting », FTMaintenance CMMS. Consulté le: 27 août 2023. [En ligne]. Disponible sur: https://ftmaintenance.com/cmms/minimizing-asset-downtime-with-cmms-assisted-troubleshooting/

[4] P. Gackowiec, « General overview of maintenance strategies – concepts and approaches », *Multidiscip. Asp. Prod. Eng.*, vol. 2, p. 126-139, sept. 2019, doi: 10.2478/mape-2019-0013.

[5] « [PDF] PREVENTIVE MAINTENANCE STRATEGIES : LITERATURE REVIEW AND DIRECTIONS | Semantic Scholar ». Consulté le: 14 septembre 2023. [En ligne]. Disponible sur: https://www.semanticscholar.org/paper/PREVENTIVE-MAINTENANCE-STRATEGIES-%3A-LITERATURE-AND-Supriatna-Singgih/6b94809b5a6a5042bc9713c64b3e15747382b949

[6] M. G. Deighton, « Chapter 5 - Maintenance Management », in *Facility Integrity Management*, M. G. Deighton, Éd., Boston: Gulf Professional Publishing, 2016, p. 87-139. doi: 10.1016/B978-0-12-801764-7.00005-X.

[7] « What is Predictive Maintenance and How is it Transforming Manufacturing? | PTC ». Consulté le: 15 septembre 2023. [En ligne]. Disponible sur: https://www.ptc.com/en/blogs/iiot/what-is-predictive-maintenance

[8] « What is a condition-based maintenance? | IBM ». Consulté le: 15 septembre 2023. [En ligne]. Disponible sur: https://www.ibm.com/topics/condition-based-maintenance

[9] « FAILURE | English meaning - Cambridge Dictionary ». Consulté le: 15 septembre 2023. [En ligne]. Disponible sur: https://dictionary.cambridge.org/dictionary/english/failure

[10] L. H. Chiang, E. L. Russell, et R. D. Braatz, *Fault Detection and Diagnosis in Industrial Systems*. Springer Science & Business Media, 2000.

[11] Y.-J. Park, S.-K. S. Fan, et C.-Y. Hsu, « A Review on Fault Detection and Process Diagnostics in Industrial Processes », *Processes*, vol. 8, nº 9, Art. nº 9, sept. 2020, doi: 10.3390/pr8091123.

[12] « s71200_system_manual_en-US_en-US.pdf - SIMATIC S7 S7-1200 Programmable controller - ID: 109741593 - Industry Support Siemens ». Consulté le: 22 octobre 2023. [En ligne]. Disponible sur: https://support.industry.siemens.com/cs/document/109741593/simatic-s7-s7-1200-programmable-controller?dti=0&lc=en-AE

[13] N. Aissani, B. Beldjilali, et D. Trentesaux, « Efficient and effective reactive scheduling of manufacturing system using Sarsa-multi-objective agents », in *MOSIM'08: 7th Conference Internationale de Modelisation et Simulation*, 2008, p. 698-707. Consulté le: 23 octobre 2023. [En ligne]. Disponible sur: https://www.researchgate.net/profile/Damien-

Trentesaux/publication/280352692_EFFICIENT_AND_EFFECTIVE_REACTIVE_SCHEDULING_FOR_MANUFACTURING_SYSTEMS_USING_SARSA_MULTI-OBJECTIVE_AGENTS/links/55b33ed008ae092e9650b064/EFFICIENT-AND-EFFECTIVE-REACTIVE-SCHEDULING-FOR-MANUFACTURING-SYSTEMS-USING-SARSA-MULTI-OBJECTIVE-AGENTS.pdf

[14] M. Biehl, E. Prater, et J. Mcintyre, « Remote repair, diagnostics, and maintenance », *Commun ACM*, vol. 47, p. 100-106, nov. 2004, doi: 10.1145/1029496.1029501.

[15] « TeleService V6.1 Logiciel de maintenance SIMATIC S7 et C7 », *et C*.

[16] « A Brief History of the Internet », Internet Society. Consulté le: 4 novembre 2023. [En ligne]. Disponible sur: https://www.internetsociety.org/internet/history-internet/brief-history-internet/

[17] H. Karray, B. Chebel-Morello, et N. Zerhouni, « Towards A Maintenance Semantic Architecture », *World Congr. Eng. Asset Manag. WCEAM09*, sept. 2009, doi: 10.1007/978-0-85729-320-6_12.

[18] « Industrial Ethernet and Fieldbus | Renesas ». Consulté le: 4 novembre 2023. [En ligne]. Disponible sur: https://www.renesas.com/us/en/application/industrial/industrial-communication/industrial-ethernet-fieldbus

[19] « Modular TS Adapter ».

[20] D. Dzung, M. Naedele, T. P. Von Hoff, et M. Crevatin, « Security for Industrial Communication Systems », *Proc. IEEE*, vol. 93, n° 6, p. 1152-1177, juin 2005, doi: 10.1109/JPROC.2005.849714.

[21] « Industrial Network Security, 2nd Edition [PDF] [75elvohn33o0] ». Consulté le: 4 novembre 2023. [En ligne]. Disponible sur: https://vdoc.pub/documents/industrial-network-security-2nd-edition-75elvohn33o0

[22] « What Is a Firewall? », Cisco. Consulté le: 4 novembre 2023. [En ligne]. Disponible sur: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

[23] A. Sari, A. Lekidis, et I. Butun, « Industrial Networks and IIoT: Now and Future Trends », 2020, p. 3-55. doi: 10.1007/978-3-030-42500-5_1.

[24] H. Meyer, « Doors open to simpler VPNs », *Comput. Secur.*, vol. 18, n° 1, p. 78-79, janv. 1999, doi: 10.1016/S0167-4048(99)80022-4.

[25] S. Rahimi et M. Zargham, « Analysis of the security of VPN configurations in industrial control environments », *Int. J. Crit. Infrastruct. Prot.*, vol. 5, n° 1, p. 3-13, mars 2012, doi: 10.1016/j.ijcip.2012.01.001.

[26] « Network Security: Firewalls, Intrusion Detection Systems, and VPNs » WPHotShot ». Consulté le: 5 novembre 2023. [En ligne]. Disponible sur: https://wphotshot.com/network-security-firewalls-intrusion-detection-systems-and-vpns/

[27] « TeamViewer – The Remote Connectivity Software », TeamViewer. Consulté le: 5 novembre 2023. [En ligne]. Disponible sur: https://www.teamviewer.com/en-us/

[28] « Business Software and Services Reviews », G2. Consulté le: 5 novembre 2023. [En ligne]. Disponible sur: https://www.g2.com/

[29] « Secomea - Your Industrial IoT Solution for Remote Maintenance », Secomea. Consulté le: 5 novembre 2023. [En ligne]. Disponible sur: https://www.secomea.com/

[30] B. I. Bouabdellah et N. Aissani, « Smart Glasses and Augmented Reality for Maintenance 4.0 ». Rochester, NY, 19 avril 2022. doi: 10.2139/ssrn.4087651.

[31] R. T. Azuma, « A Survey of Augmented Reality », *Presence Teleoperators Virtual Environ.*, vol. 6, n° 4, p. 355-385, août 1997, doi: 10.1162/pres.1997.6.4.355.

[32] B. Marques, S. Silva, J. Alves, A. Rocha, P. Dias, et B. S. Santos, « Remote collaboration in maintenance contexts using augmented reality: insights from a participatory process », *Int. J. Interact. Des. Manuf. IJIDeM*, vol. 16, nº 1, p. 419-438, mars 2022, doi: 10.1007/s12008-021-00798-6.

[33] M. Mori et M. Fujishima, « Remote Monitoring and Maintenance System for CNC Machine Tools », *Procedia CIRP*, vol. 12, p. 7-12, janv. 2013, doi: 10.1016/j.procir.2013.09.003.

[34] « Dedicated Remote Access with SINEMA Remote Connect », 2022.

[35] « SINEMA Remote Connect V3.1 - Server ».

[36] S. G. González, S. Dormido Canto, et J. Sánchez Moreno, « Obtaining high preventive and resilience capacities in critical infrastructure by industrial automation cells », *Int. J. Crit. Infrastruct. Prot.*, vol. 29, p. 100355, juin 2020, doi: 10.1016/j.ijcip.2020.100355.

[37] « DOC_MPR_M2Me_Starter-kit_D.pdf ». Consulté le: 6 novembre 2023. [En ligne]. Disponible sur: https://www.etictelecom.com/wp-content/uploads/2020/09/DOC_MPR_M2Me_Starter-kit_D.pdf

[38] « 9 Inch 24v Dc SIEMENS HMI TP900 COMFORT, Model Name/Number: 6AV2124-0JC01-0AX0 - PDF Catalogue ». Consulté le: 6 novembre 2023. [En ligne]. Disponible sur: https://pdf.indiamart.com/impdf/20746340273/SELLER-46286824/siemens-hmi-tp900-comfort-panel.pdf

[39] « SINAMICS G120 - Parameter Manual - Siemens - [PDF Document] ». Consulté le: 6 novembre 2023. [En ligne]. Disponible sur: https://vdocument.in/sinamics-g120-parameter-manual-siemens.html

[40] « PH_SCALANCE-X-200_77.pdf ». Consulté le: 6 novembre 2023. [En ligne]. Disponible sur: https://cache.industry.siemens.com/dl/files/789/109482789/att_868125/v1/PH_SCALANCE-X-200_77.pdf

[41] « Siemens IEC Motor Catalog | PDF | Electric Motor | Automation », Scribd. Consulté le: 6 novembre 2023. [En ligne]. Disponible sur: https://www.scribd.com/doc/36472860/Siemens-IEC-Motor-Catalog

[42] Excellence Moves Creativity J., « X1 Industrial Gateway ». Consulté le: 6 novembre 2023. [En ligne]. Disponible sur: http://en-file.hongdian.com//products/x1-industrial-gateway.html