ITEA Office
High Tech Campus 69 - 3
5656 AG Eindhoven
The Netherlands

T + 31 88 003 6136
E info@itea3.org
W www.itea3.org

ITEA 3 is a EUREKA strategic ICT cluster programme

State of the Art

PIANiSM

Predictive and Prescriptive Automation Smart Manufacturing

Edited by: SISTRADE

Date: 10/02/2020

This document is handled by the ITEA Office as public information.

Table of Contents

Revision History

Version	Date	By	Entity	Changelog
1.0	25/06/2019	João Mourinho	Sistrade	Technology SOTA Structure
2.0	03/07/2019	Marta Fernandes	ISEP - GECAD	Scientific SOTA Structure Reformulated Global Structure
3.0	10/07/2019	João Mourinho	Sistrade	Added Descriptions Added Revision History Reformulated SOTA Structure
4.0	09/08/2019	Miriam Moreno Javier Gavilanes	Experis IT	Revision
5.0	14/10/2019	Pedro Valente	Sistrade	Partner contributions
5.1	16/10/2019	Pedro Valente	Sistrade	Partner contributions
5.2	18/10/2019	Pedro Valente	Sistrade	Partner contributions: - update KocDigital contribution - consolidate Bib KocDigital - consolidate Bib NIMBEO
5.3	30/10/2019	Pedro Valente	Sistrade	Partner contributions updates: - 3.4, 5.1, 5.1.5: KocDigital - 4.2, 5.2: Nimbeo - 4.4:ISEP/GECAD
5.4	04/11/2019	Pedro Valente	Sistrade	Partner contributions updates: - 3.4: KocDigital
5.5	06/11/2019	Pedro Valente	Sistrade	Partner contributions updates: - 5.3, 5.4: B3 Systems Inc.
5.6	03/12/2019	Pedro Valente, João Mourinho	Sistrade	Partner contributions updates: - 5.1: KocDigital Solutions Inc.
5.7	18/12/2019	Pedro Valente	Sistrade	Partner contributions updates: - 4.3: ISEP/GECAD
5.8	13/01/2020	Pedro Valente	Sistrade	Partner contributions updates: - 5.3, 5.4: B3 Systems Inc.

Version	Date	By	Entity	Changelog
5.9	17/01/20	Pedro Valente	Sistrade	Partner contributions updates: - 4.2, 5.2: Nimbeo
6.0	07/02/20	Pedro Valente	Sistrade	Partner contributions updates (Nimbeo and Experis) Final revisions

Authors

Company	Author	E-mail Address
KoçSistem	Rümeysa Kübra Çiftçi Mehmet Mustafa Özalp Şebnem Güneş Söyler	rumeysakubra.ciftci@kocdigital.com mehmetmustafa.ozalp@kocdigital.com sebnemgunes.soyler@kocdigital.com
Sistrade	João Mourinho José Silva Pedro Valente	joao.mourinho@sistrade.com jose.silva@sistrade.com pedro.valente@sistrade.com
ISEP - GECAD	Marta Fernandes Alda Canito	mmdaf@isep.ipp.pt alrfc@isep.ipp.pt
Experis IT	Javier Gavilanes Miriam Moreno	javier.gavilanes@experis.es
Nimbeo	Angel Lagares	alagares@nimbeo.com
B3 Systems	Chris Graham Vlad Katkov	chris.graham@runb3.com vlad.katkov@runb3.com
Erste Software	Gokhan Yanmaz Mustafa Kemal Tas	gokhan@ersteyazilim.com mustafa@ersteyazilim.com

Acronyms

PdM	Predictive Maintenance
IOT	Internet of Things
I-IOT	Industrial Internet of Things
API	Application Programming Interface
BI	Business Intelligence
BMS	Building Management System
FR	Failure Rate
ICT	Information and Communications Technologies
OEE	Overall Equipment Efficiency
WP	Work Package
RtF	Run-to-Failure
UFR	Unintended Failure Maintenance
TbM	Time-based maintenance
CMMS	Computerized maintenance management system
ERP	Enterprise Resource Planning
ESA	Electrical Signature Analysis
MIS	Manufacturing Information System
RCA	Root-cause Analysis

1. Summary

The Pianism project aims at putting together predictive and prescriptive maintenance techniques in order to achieve an end-to-end automated manufacturing process and optimize end-to-end value chains. To achieve this objective, the project requires integrating knowledge and technologies from different fields, namely from the industrial maintenance strategies, industrial IOT, and Data Science. These fields present the theoretical and technological framework where PIANISM bases its approach.

Predictive Maintenance (PdM) uses extensive data exploration techniques (ex: machine learning algorithms and simulation) which convolute real-time streaming data with previously trained models. In an industrial environment, this streaming data comes from the equipment. Data is acquired by sensors strategically placed in the equipment or environment. Therefore, the selection of relevant data, the elicitation of the adequate sensors and their placement are necessary conditions to successfully acquire data from the shop floor. Contextual and management information is also provided by the management information systems (ex: ERP, MES, Quality Management) present in the organizations. This information is fundamental to align the equipment maintenance to the company strategy, organizational structure and customer requirements and feedback.

This document analyses the current state of the art of the base technologies of the Pianism project: it starts by reviewing the literature regarding the evolution Maintenance Strategies. It then examines the current technologies in the Industrial IOT (I-IOT) field in what concerns to data acquisition. The document continues by describing the Data Science techniques and technologies relevant for the Pianism project. The state of the art finalizes by presenting the relevant Management Systems, the way they provide the necessary context to the maintenance strategy implementation.

2. Introduction

Since the outset of the Industrial Revolution, maintenance of engineering equipment in the field has been a challenge. While impressive progress has been made in maintaining equipment in the field in an effective manner, maintenance of equipment is still a challenge due to factors such as size, cost, complexity, and competition[1].

Maintenance is defined according to the European standard (EN 13306: 2001) as "*the combination of all technical, administrative and managerial actions during the life cycle of an item intended to retain it in or restore it to a state in which it can perform the required function*".

Global Asset Protection Services[2], defines maintenance as "the most important factor in equipment availability and reliability. Equipment can and should be properly designed for its purpose; carefully built, installed and protected; and skilfully operated. However, the day that equipment is installed, it begins to age. (…) Placing equipment in service provides other stresses that accelerate aging."

The earliest maintenance records date from the 10th century, when the Vikings relied heavily on maintenance to keep their ships in perfect battle condition[1]. According to Dhillon [3], the history of maintenance goes with the technical-industrial development of humanity. Maintenance was of minor importance and was performed by the same operations staff until 1914. But with the advent of World War I and the introduction of serial production, established by Ford, companies felt the need to create teams that could repair machines, in a short time manner. Thus, arose an agency subordinate to the operation, whose basic purpose was to perform maintenance, known today as corrective.

From the 1930s onwards, the maintenance history can be divided into three generations with the following aspects [1], [3], [4]:

- The first generation covers the period before World War II, when the industry was poorly mechanized. During this period maintenance was fundamentally corrective, that is, the repair was made only after the failure event. Due to the economic climate of the time, productivity was not a priority. Therefore, no systematic maintenance was required.
- In the second generation, ranging from World War II to the 1960s, there was a sharp increase in mechanization as well as the complexity of industrial facilities. New maintenance techniques began to be used, such as manual work planning and control systems, and time monitoring. During this period, the concept of preventive maintenance emerged, as the need for greater availability and reliability in the pursuit of productivity was evidenced. The industry was very dependent on the appropriate functioning of the machines. This has achieved a longer equipment life.
- The third generation began in the 1970s. During this period, the growth of automation and mechanization began to indicate that reliability and availability became key points in sectors as diverse as transportation, health services, data processing, telecommunications. and building management.

The notions of prediction or prevention didn't exist, as we know in the present, so maintenance suffered from quite a bad image back then [1]. The industrial world, as well as the implications, were very different from the ones we know today. At that time, the industry was prospering, so the

[1] I. S. Klæsøe, Viking Trade and Settlement in Continental Western Europe, Copenhagen, Denmark: Museum Tusculanum Press, University of Copenhagen, 2010, p. 165.

consequences on production lines weren't the same (e.g. equipment were not integrated to a more general system) [3], [5].

3. Maintenance Strategies

Several industrial managers overlooked the positive influence of proper maintenance management on their company's activity. Yet, it is a major performance factor and a cause for prompt gains within the company: in terms of productivity as well technology, suitable industrial maintenance management has positive consequences on organizations and their products [3].

In recent years, manufacturing industry has been facing a major shift of the manufacturing requirements (e.g. consumer demand for customized products continues to grow), resulting in a much shorter product life cycle, unlike the traditional mass production of standardized products [6]. These changes are impacting companies, rising the need for adaptation, driving all sectors of the manufacturing activity to move correspondingly. Maintenance activities can impact the entire manufacturing/production cost and quality, and consequently, customer satisfaction [6].

3.1. Types of Failure

Maintenance exists because failures happen. Failure of an equipment is an event in which the equipment cannot accomplish its intended purpose or task. There are basically two types of failure: potential failure or functional failure (Table 1 - Examples of industrial failure prune of maintenanceTable 1). The potential failure is a failure at an early stage, which indicates that something is wrong, but the equipment is still performing its function in the production process. We can state that there is a potential fault (leak). That is, if it is not treated it will lead the equipment to functional failure [6], [7].

Table 1 - Examples of industrial failure prune of maintenance

Potential failure	Functional failure
Imagine that in each hydraulic system there is a leak in one of the hoses. Despite the leak, the hydraulic system is still performing its function within the production process (triggering the required pressure, speed and force parameters).	*Assuming the leak grows, and the hydraulic system oil level drops critically making it impracticable to operate. At this point we have a functional failure; the hydraulic system is no longer able to perform its function due to leakage in the hydraulic hose.*

Functional failure is when equipment is no longer able to perform its function in the production process. If the leak had been repaired when it was still in its early stages and was just a potential failure, the functional failure would not have occurred. So, corrective maintenance will always be linked to potential failure or functional failure [6].

3.2. Taxonomy and Classification

Maintenance can be classified as **planned or unplanned**. Planned maintenance refers to any maintenance activity that is designed, documented, and scheduled [4]. The aim of it is to moderate downtime by having all necessary resources on hand, such as labour and parts, and a strategy to use these resources. It is performed while the equipment is still online, preventing it fails.

Although planned and unplanned maintenance are two of the main ways to categorize maintenance types, when defining maintenance procedures in an organization it's helpful to look at three fundamental types [2], in which literature agrees on: reactive, preventive, predictive.

- **Reactive Maintenance** (or Unplanned Maintenance): is fixing things as they break. It's simple and inexpensive (if nothing breaks). This type of maintenance often leads to worse and more regular breakdowns, as well as costly downtimes.
- **Preventive Maintenance** (or Planned Maintenance): combines a series of smaller, scheduled maintenance tasks to overcome the number and severity of breakdowns. It also adds greater predictability in managing your parts and labour.
- **Predictive Maintenance** (PdM): concerns monitoring equipment conditions to predict when it is destined to fail, then performing maintenance to avoid that failure.

To these three main types, two more can be added: condition-based maintenance and proactive maintenance:

- **Condition-based Maintenance** (CbM): concerns monitoring equipment conditions to assess what maintenance needs to be performed.
- **Pro-active Maintenance** (PbM): is focused on by undertaking activities that avoid the underlying conditions that lead to machine faults and degradation.

The taxonomy of the maintenance strategies of these conditions is illustrated at Figure 1.

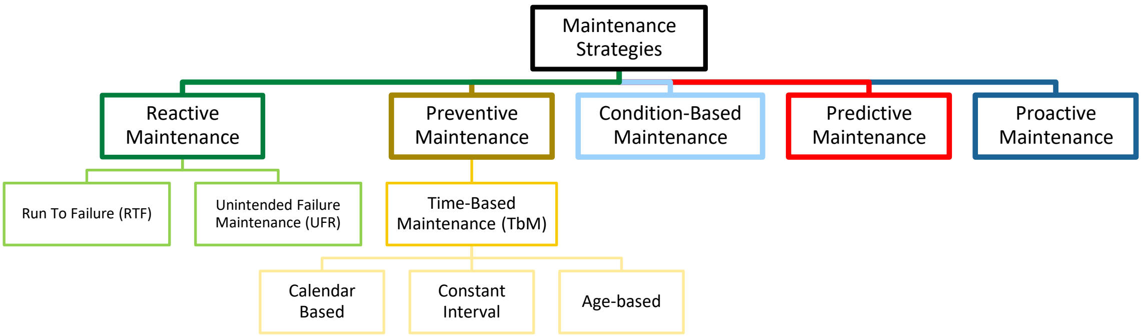


Figure 1 - Maintenance strategies classification. Adapted from assetinsights.net, accessed September 11, 2019

Reactive maintenance can be divided into two subtypes: Run-to-fail (RtF) and Unintended Failure maintenance (UFR). The first one is the simplest one: resources are deliberately allowed to operate until they break-down, at which point, reactive maintenance is performed (also called "Fit and forget"). No action, including preventive one, is performed on the resource up until the failure event. However, a plan can be in place taking into consideration this event, so that the resource can be fixed with the minor production issues. UFR is slightly different in the sense that in this maintenance type, equipment owners do not intentionally and deliberately allow their assets to run-to-failure. Still, the equipment's may fail due to inadequate maintenance budgets, poor planning and ignorance.

Preventive maintenance is a type of planned maintenance that is performed on equipment, to prevent malfunctions and minimize the consequences of equipment breakdowns. It is therefore appropriate for assets whose function is essential, that is, without which the company's operations cannot continue normally, as well as higher value equipment, which can be very expensive to repair or replace. It is a time-based maintenance (TBM) TBM can be calendar based (i.e. in fixed days), performed at constant intervals or depending on the age of the equipment.

Condition-based maintenance (CbM) is a maintenance strategy that monitors the actual condition of an asset to decide what maintenance needs to be done. CBM dictates that maintenance should only be performed when certain indicators show signs of decreasing performance or upcoming failure. Checking a machine for these indicators may include non-invasive measurements, visual inspection, performance data and scheduled tests. Condition data can then be gathered at certain intervals, or continuously (as is done when a machine has internal sensors). Condition-based maintenance can be applied to mission critical and non-mission critical assets. This is not a planned maintenance as it is not performed based upon predefined scheduled intervals. It is instead performed only after a decrease in the condition of the equipment has been observed. Compared with preventive maintenance, this increases the time between maintenance repairs, because maintenance is done on an as-needed basis.

Predictive maintenance (PdM) makes heavy use of the data about current and past equipment condition and performance to infer failure conditions and failures events, allowing the prediction of failure occurrence and allowing intervention in the equipment before the failure actually happens.

3.3. Reactive Maintenance

Reactive maintenance (or breakdown maintenance) refers to repairs that are done when equipment has already broken down, to restore to its normal operating condition. A typical example of reactive maintenance (and the impact of it can cause) is having a car breakdown on the side of the road and having to wait for roadside assistance to repair it. The trigger for this type of maintenance is a failure trigger. One type of reactive maintenance could be unplanned equipment downtime repairs (or failure). This is probably the most common type in a manufacturing environment [3]. An example of this could be lubricant or another contaminant dripping into a shop-floor zone.

Although the equipment is not technically broken down it must be repaired to prevent product loss.

3.3.1. Reactive Maintenance Impact

Despite being the most basic and common type of maintenance, the level of knowledge about such maintenance is still very low. Because this maintenance type is both unplanned and unscheduled, its performance is highly unproductive [1]: It usually needs a high amount of time to understand the problem and also to get the resource fixed. On top of that, waiting for parts, supplies or other staff members to complete the maintenance task adds up to the required time.

Reactive maintenance is naturally bound with the functional failure and is essentially the "*run it till it breaks*" maintenance mode. No actions or efforts are taken to maintain the equipment as the designer originally intended to ensure design life is reached. This type of maintenance can also be very expensive.

Supplemental costs (e.g., embrace time spent idling, the premium costs that may be spent on fast part orders and shipping, and the possible overtime payments that may be required for extra, or specialized personnel) needs to accomplish the task.

In addition, because it is likely that the operation of other parts of the facility will be negatively impacted by the breakdown of the equipment in need of repair, the cost of disrupt production needs to be reflected into the cost of this type of maintenance. If no planning is initiated, then this type of maintenance becomes the default one. This happens as planned and predictive maintenance techniques, described later, need investing in planning beforehand, in order to be successfully used [3].

Run-to-failure is usually demonstrated using a bath-tub graph (Figure 2), composed of three distinct sections: introductory failures, normal degradation, and excessive degradation followed by failure [8]. The cycle shows the initial investment in a system or machine, after which the useful life period begins, in which the systems are subject to internal and external factors that degrade its operation and, on the other hand, corrective actions are taken to the anomaly states. where at a certain point you decide to overhaul or opt to replace it [9]. The conjunction of these failure profiles comprises the observed failure rate.

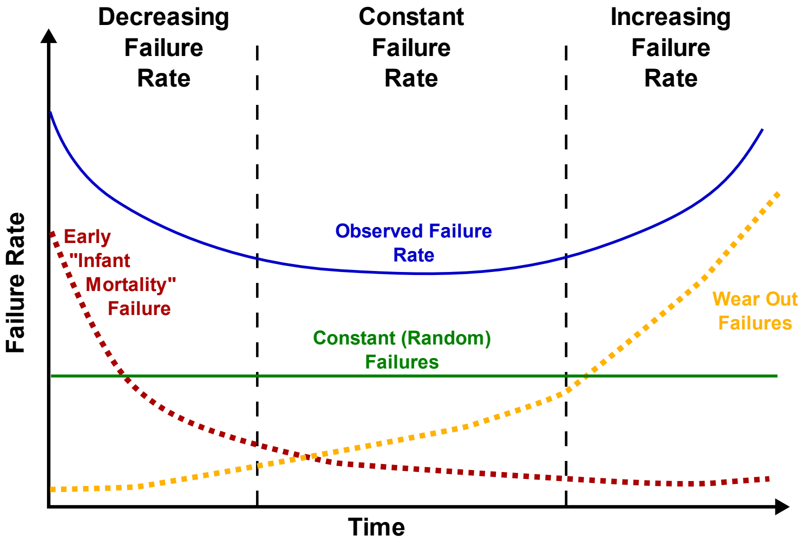


Figure 2 -The 'bathtub curve' hazard function.

source: https://en.wikipedia.org/wiki/Bathtub_curve, accessed on September 12, 2019

The graph depicts the lifecycle of equipment and infrastructure normally considered for a maintenance program such as run to failure; however, this type of diagram describes the relative failure rate of an entire population of products over time, rather than single examples of it.

A conscious decision is made by the owner to neglect the asset, regardless of any signs of Potential Failure ("P") and to wait until the point at which Functional Failure ("F") occurs (section 3.5.3).

Failure is usually preceded by noticeable degradation, culminating in either abrupt failure, or a decision that the equipment should be stopped or replaced as it is in danger of either causing damage or becoming a safety hazard.

Reactive maintenance implies often, that production needs to be stopped so that the equipment can be repaired or replaced. This can be catastrophic for the organizations as most of the times the negative consequences go far beyond the measurable (economics of production halt, bottlenecks and decreased output) such as loss of trust by customers and business partners, inconsistent quality products, low occupation rates of equipment, etc. The impact can, however, be positive if criticality of production.

3.3.2. Advantages of Run-to-Failure maintenance

The with run-to-fail strategy, implies having spare parts and personnel promptly to replace the failed part and hold equipment availability. This approach should not be confused with reactive maintenance, because of the action plan to allow the resource to run-to-failure. This strategy is useful for assets that, on the breakdown, act no safety risks and have the least impact on production [9]. A common example of run-to-failure maintenance is the maintenance plan for and ordinary light bulb. This asset is tolerable to run until it fails. When it occurs, the plan to fix the asset is carried out. A new item is collected from stocks and replaced at a suitable time.

This strategy doesn’t plan of time but reacts when the occurrence happens. For that reason, this strategy is easy to understand and implement. Minimal planning is needed since maintenance does not require to be scheduled in advance, the resources planning is quite low. Maintenance only needs to happen after breakdown has occurred. Also, less staff are required as less work is done day-to-day. Situations that could take advantages of this strategy [10]:

- It is regarded as a short life asset, such as cheap, high-flow pumps, batteries, or high-traffic doors. Some companies consider that equipment such as fire extinguishers can be placed on RTF list, and that is okay, provided that any statutory checks or expiry dates – most safety equipment has some level of replacement criteria.
- Assets with disposable parts which are intended to be swapped out or replaced rather than repaired. This can include floor and wall surfaces.
- Non-critical assets such as service and repair tools that can simply be replaced rather than repaired. This could include hand tools and even small electrical devices like multi-meters, provided that suitably calibrated and usable alternatives are available to use.
- Durable Assets – Assets that are not subject to wear or assets that are unlikely to fail inside normal operating criteria. This may include signage and labelling but would not include racking which may fail catastrophically and dangerously.
- Assets that exhibit Random Failure Patterns which cannot be predicted and there is no other choice other than to run to failure.

This kind of maintenance program is a quite reasonable method of dealing with the sorts of assets stated above but it shouldn't be confused with having any maintenance policy at all. Nevertheless, having a run to failure maintenance policy isn’t perhaps as easy as it may sound, since many parts of your maintenance schedule don’t fail abruptly, and some level of discretion is required.

3.3.3. Disadvantages of Run-to-Failure maintenance

Sometimes referred to as fit and forget maintenance, run-to-failure is perhaps the most cost-effective of the maintenance strategies, and one that is widely adopted by companies that have a have certain types of equipment or meet other criteria.

In time (Figure 3), unexpected downtime during the production can lead to missing a customer, damaged goods, standards drop, late deliveries, consequently, impact the revenue. The company can end up losing money for emergency spare parts shipping and overtime. Other direct effect, relying on reactive maintenance means that labour and spare parts might not be estimated accurately, and the organization won’t be able to repair equipment after the failure happens. This strategy does not involve keeping equipment online in an optimal way and therefore it does not maximize initial investment on the asset. Maintaining the machinery before failures can increase asset life expectancy.

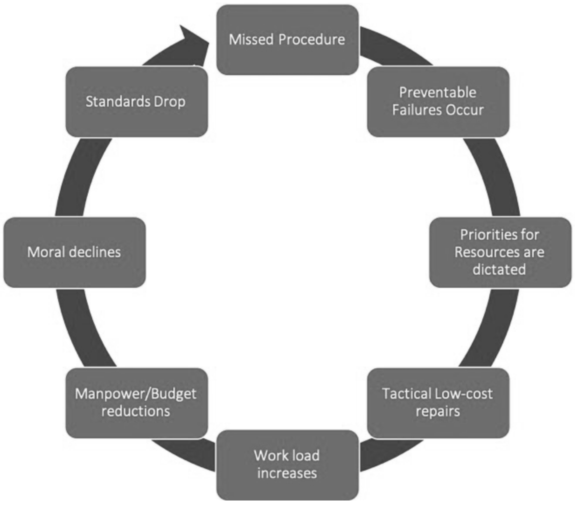

Missed Procedure
Preventable Failures Occur
Priorities for Resources are dictated
Tactical Low-cost repairs
Work load increases
Manpower/Budget reductions
Moral declines
Standards Drop

Figure 3 Reactive Maintenance Impact.

Adapted from instrumentationforum.com, accessed on September 10, 2019.

When a maintenance work order is programmed, staff have time to prepare and review standard procedures to preserve a specific piece of equipment. Every asset has safety requirements to perform the job accordantly. Using reactive maintenance procedures, everything must be on-the-fly, leading staff under stress. Consequently, they tend to rise more risks to keep the machine up and running.

When an asset is not properly maintained, it consumes more resources. Simple maintenance jobs, such as greasing parts or changing filters, can reduce energy consumption by 15% [3]. With time to plan the maintenance activities, it increases time to analyse, evaluate and take actions based on past events and production schedule. With a reactive approach, failures occur unexpectedly, pushing staff to look around correct safety/procedures' manuals and documentation, as well for hardware parts (e.g. spare parts, tools).

3.3.4. When to use Reactive maintenance

From the previous study, isn't clear that reactive maintenance is deprecated for industrial domain, but it should be use within a careful plan and resources analysis. Companies will run a series of maintenance plans, some of which will ensure that expensive and/or critical equipment must kept running, while other parts of it, will consider less critical elements which can be added to a Reactive plan. Continue evaluation of the areas should be taken – as long as six months even, or even monitored by circumstantial evidence from manual observation.

This approach is best suited to companies with the following attributes: a) A high-risk tolerance, b) A sophisticated maintenance program. Also, RTF is most appropriate when combined with a larger maintenance strategy that explores an optimal maintenance mix for the different assets.

While RTF might sound easy to understand, it requires time and high degree of human expertise (good knowledge of the type of equipment used), to run properly. It also depends upon the equipment, and is best to be align with other strategies, so that while the equipment and company infrastructure is comprised, on the safety requirements [6].

3.4. Preventive Maintenance

Many companies do not deliberately allow their assets to run to failure - Unintended Failure Replacement (UFR). While they may find that they are neglecting some of their assets, this is not a conscious decision but rather an unfortunate unintended consequence of other factors such as poor planning, ignorance or inadequate maintenance budgets [11]. There is a slight distinction (but very important) that should be made between Corrective Maintenance (CM)[2] and Reactive Maintenance (RM). In the case of CM, the owners anticipate the consequences of their planned inaction, they are ready for these consequences and they are therefore still in control.

“Machines break. That’s the first and probably oldest rule in manufacturing. It used to be the best way to manage that was hoping someone on the production floor, using a combination of instinct and experience, would see the indications of an asset about to go down and repair it in time. (…) hope is no longer a viable strategy.” [12]

Today, companies to be competitive need to adopt cost-cutting policies and increased product or service quality. Industrial maintenance, more specifically preventive maintenance, has shown over several decades that it is an area of high importance within companies, contributing substantially to better performance.

Preventive work is performed regularly and typically determined by time (e.g. every 6 months), events (e.g. every 600 uses), or meter readings (e.g. every 3.000 kilometres) with limits. Which are often established based on statistics about the average or expected life of the equipment [11].

3.4.1. Preventive maintenance planning

Corporations progressively became aware of the safety aspect. They desired to protect their employees, so they started to take an interest in maintenance to promote it and to give it more meaning. Equipment had evolved, combining more advanced technologies, so there were more accident risks and companies wanted to diminish them. Maintenance became more important within plants: first maintenance procedures were born, in virtue of it, uncertainty risks were drastically reduced, the equipment performance was nearly followed and critical breakdowns on the entire production line were limited as much as possible. Corporations wanted to develop maintenance for human reasons rather than for purely economic ones [13][14].

No one wants downtime. It is detrimental to businesses, both in terms of cost and reliability and customer trust. Focusing on preventive maintenance plans will reduce the number of unexpected breakdowns in critical equipment that can result in downtime [14].

The main advantage of having a preventive maintenance plan is that you can prevent all these situations by replacing used components promptly, preserving and restoring all necessary parts. For this, it is recommended to use maintenance support software where the maintenance manager can: **a)** Improve the technical and operational state of the equipment; **b)** Reduce equipment degradation; **c)** Decrease the risk of equipment damage; **d)** Schedule prevention work; **e)** Perform repairs under conditions beneficial to the operation; **f)** Reduce costs; **g)** Extend equipment life and **h)** Diminish impact on customer/user.

[2] “*Corrective maintenance is a maintenance task performed to identify, isolate, and rectify a fault so that the failed equipment, machine, or system can be restored to an operational condition within the tolerances or limits established for in-service operations*”. Source: Wikipedia, accessed September 11, 2019.

A preventive maintenance plan is ideal when the maintenance manager can avoid any damage to their equipment or can predict and schedule so that the damage has the least possible impact on the customer.

Table 2 preventive maintenance plan design example [15].

Steps	description
1. Information gathering	*The first step is to take a survey of all the working machines, parts replacement history and the amount of activities that have already been done. Measure what are the most common occurrences found on equipment that has long-term defects.*
2. Creation of Maintenance Checklist	*Create a procedure for checking the condition of each equipment after the intervention, whether preventive or corrective. The most common checklists are: Mechanical, Lubrication, Electrical and Safety.*
3. Cost Estimation	*Plan budget and costs are made. It must include all the expenses that will be required for the execution of the project. Maintaining project profitability is very important for the process to be profitable and efficient.*
4. Setting a schedule	*Define how often each review and maintenance should take place and divide it by the number of contributors you will allocate. Increase the number of visits to the equipment with the largest volume and time of use.*
5. Tracking each activity	*Controlling each activity in the field is critical for proper execution. Set a report standard with each checklist, photos, arrival and departure times, and set a minimum quality level.*
6. Structure Productivity KPIs	*Key performance indicators are critical in executing the maintenance plan. It is this data that will show you if the project is on track or if adjustments are needed. (e.g. Avg. Service Time, Repair Interval, Profitability, Scheduling)*

The preventive maintenance plan is a measure that, in addition to bringing more safety and quality to the work of its technicians, works as an important strategic decision to reduce operating costs in a company.

To adopt Preventive Maintenance as your main strategy, companies need to develop a Preventive Maintenance Plan, which is a document created annually by the Maintenance Manager, listing equipment and periods during which maintenance should be maintained during year: monthly, annually, twice a month, or as required [15].

3.4.2. Advantages of preventive maintenance

While aware of the benefits of preventive maintenance, many managers still devote most of their time and resources to corrective maintenance, viewing preventive as an unnecessary additional cost. Preventive maintenance when properly planned can greatly lower overall maintenance costs and even increase the productivity of equipment and facilities.

This approach has many advantages over Corrective Maintenance (CM), which is only performed when equipment malfunctions are reported. Advantages include helping to improve equipment life and equipment reliability, and to prevent unexpected downtime. These factors are important for lowering long term costs.

Table 3 Advantages of Preventive Maintenance

Adapted from blog.infraspeak.com/advantages-preventive-maintenance/, accessed September 11, 2019

Equipment will be more efficient	*Technicians and managers can have more faith that equipment will function smoothly and without complications.*
Savings on your resources	*Any piece of equipment that is showing signs of wear and tear or is approaching the end of its usability, there is a good chance it will be using far more energy than it is worth.*
Longer lasting equipment	*Implementing preventive maintenance can extend the life of functioning equipment by keeping all parts in good working order.*
Full and accurate information on operations	*Provides the manager with access to more holistic information on operations such as on consumption and income. This can help to make well informed decisions, such as when it comes to opening new equipment*
The creation of a Preventive Maintenance Plan (PMP)	*This generates an annual calendar (or biannual/triennial, depending on the preferences of management) which helps to schedule an event for the coming months*
A more motivated and efficient team	*Having better organized progression plans and a more transparent system to reward strong performance will help to motivate your team and encourage yet more improvement*

Through preventive maintenance, technicians and maintenance managers can reduce the degradation of their equipment, extending their life span and avoiding corrective interventions that generate high costs and have negative impacts on their customers.

3.4.3. Disadvantages of preventive maintenance

The main problem with Preventive Maintenance is that, since it is not based on the actual condition of the equipment, it can result in maintenance actions, including replacement of parts, which are unnecessary and cost time and money.

Though time-based and hands-on equipment maintenance is still common in the industrial processes, these techniques have increasingly been bottlenecking and unreliable in recent years[4].

The quality of the machine spare parts, although pass through into a systematic quality process during their manufactured, under identical conditions, can show different times of failure (Figure 1), as they are part of an endemic system. The conclusion to be drawn is that it is impossible to tell how long a component may last in an industrial process [13].

Performing preventative imposes to perform surveillance or monitoring tasks. Otherwise, there is no guaranty to remain preventive (requires no surveillance). This is a blind type of maintenance where interventions are performed disregardful of equipment condition [11]. The same task could be deemed preventive or corrective depending on when the task is done i.e. before or after failure. For a complex asset, the overall failure pattern would most likely be random, in which case time-based repair or renewal would not be an effective strategy.

The "scheduled maintenance" (or preventive maintenance) regime is also widely used on more complex larger machines where failure can affect production. However, Nowlan et. al. [16] has shown that routine maintenance on some types of machine can actually reduce the reliability of the machine rather than improving it, throwing into question the assumption that routine maintenance should be used when reliability is important.

There are many instances in which preventive is the best maintenance strategy to use, and it’s much easier to carry out a PM strategy with the help of maintenance software.

3.4.4. Computerized maintenance management system (CMMS)

While the computerized maintenance management system (CMMS) gave the first appearance in the 1960s, in the format of a punch-card system used to manage work orders, it evolves dramatically over the past 50 or more year to the present. Nowadays, CMMS software is used to centralized record of all assets and equipment that maintenance team is responsible for, as well as planning and track activities, keeping a detailed track of the work performed.

These systems monitor all maintenance work for each technician and are even able to calculate the time each work takes to complete, thus giving a better insight into each technician's performance.

This maintenance management system is extremely useful management software to help with scheduling and managing maintenance work, as well as its assets and costs. As a maintenance manager, you may think you have everything under control, but some signs may indicate that it needs to consider investing in one of these tools to help perform your tasks smoothly [4]. With a CMMS, is possible to make much more informed decisions about various aspects of your work, such as maintenance plans, technician allocation, or equipment investments.

Table 4 CMMS Benefits for planned maintenance.

Adapted from www.fiixsoftware.com/cmms/, accessed September 11, 2019

Measure maintenance performance	*A CMMS makes it easy to do preventive maintenance, which means there are fewer surprise breakdowns and work outages. Allowing you to make better business decisions.*
Less overtime	*Better scheduling means that your team isn’t sitting idle or working overtime, which means work can be distributed evenly.*
Savings on purchases	*Inventory planning features give you the time to shop around for spare parts pricing, instead of having to buy in a hurry.*
Better accountability	*Work order tracking makes it possible to quickly see if a technician did their work on time and get alerted when a task is complete.*
Information capture	*Technicians can record problems and solutions, so this information is captured for others to use.*
Certification and analysis	*A full record of assets and performance helps managers analyse energy usage and plan maintenance spend.*

Most CMMS projects that fail, do so because they are too difficult to use, and it is time-consuming to enter data into the system. The next system iteration is focused on optimized user experience design, and efficient ways to push data from a pool of sources [17]. A good CMMS system will streamline workflows and allow maintenance teams to easily manage records of all assets and equipment, which they are responsible for, and the work done on it.

3.5. Condition-Based Maintenance

Common knowledge in the maintenance engineering world is the concepts of systematic maintenance and conditional maintenance (see Figure 1): Systematic preventive maintenance aims at introducing planned maintenance actions as well as reducing production losses. Maintenance actions are scheduled according to the experience of the technical maintenance team or the recommendations of the equipment manufacturers. In systematic maintenance, the component is replaced with historical, experience-based or more common, high-flow of data in large spreadsheets of individual component life, statistically exploring the breakpoint of a particular component and replacing it before this point (section 3.3.4 and 3.4.2).

Equipment failure is not a single event – it is a process. In this notion, the breakdowns/failures are both a path and a target, which become tightly established in the core of maintenance best practises. In this way, Condition-based maintenance (CBM) can act as a monitor to failure detection. The need to know the state of conservation of the various dynamic equipment led to the development of the so-called Conditioned Maintenance, sometimes also known as Predictive Maintenance [17].

Condition-based maintenance (CBM) carried out by evaluating the condition of the machine, usually performed on an ongoing basis. The components replacement process is based on predictive analysis (e.g. Thermography, Ultrasound and Current Analysis in AC motors, vibration). Under CBM, maintenance only occurs when data indicates a decline in performance or the early warning signs of failure. This differentiates CBM from preventive maintenance, where tasks are performed at regular intervals.

Just as the electrocardiogram provides a doctor with a set of information about the "state of conservation" of the heart, the spectrum of vibration, among other analysis techniques, provides information about the "health" of the equipment. *“Predictive maintenance typically reduces machine downtime by 30 to 50 percent and increases machine life by 20 to 40 percent.”* [12]

The goal of CBM is to detect failure before it happens, so maintenance can occur exactly when needed. Because this maintenance method is supported on collecting and analysing data, it can be used to identify trends in asset performance and track their lifecycle status. This help to support decisions from scheduling, labour to budgeting.

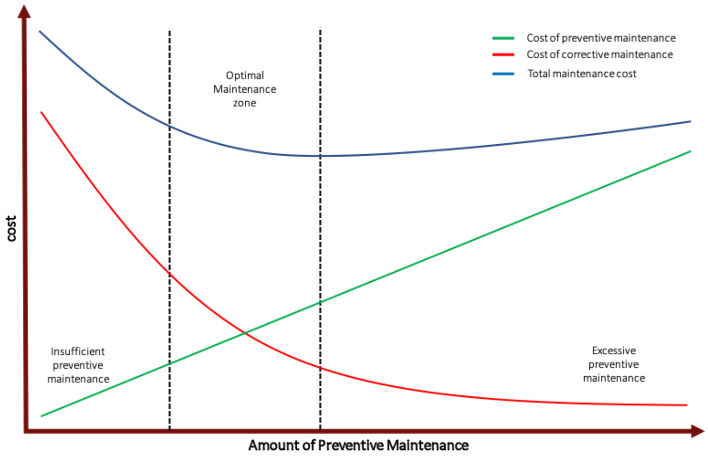


Figure 4 Total Maintenance Cost

Adapted from http://onupkeep.com, accessed September 16, 2019

One example of CBM, is tracking pressure readings on equipment with water system. Pressure levels data let personnel to identify when and where a leak is likely to take place before it happens, instead of at the point of failure.

Not all condition-monitoring techniques require complex algorithms or intricate models, as data-drive condition-monitoring approaches rely on simple queries, which runs periodically or in real-time, against time-series data generated by machines and external sensors. If a damage parameter exceeds a certain threshold, these systems can trigger a deeper analysis or corrective action in reliability engineering workflow, or directly pass to maintenance execution [13], [18], [19].

3.5.1. Benefits of condition-based maintenance

CBM fits on the predictive maintenance (PdM) scope, "*being a philosophy or attitude that, simply stated, uses the actual operating condition of plant equipment and systems to optimize total plant operation. A comprehensive predictive maintenance management program uses the most cost-effective tools (e.g., vibration monitoring, thermography, tribology) to obtain the actual operating condition of critical plant systems and based on this actual data schedules all maintenance activities on an as-needed basis (…)*" [14].

PdM (which has been around for many years now) utilizes data from various sources, such as critical equipment sensors, enterprise resource planning (ERP) systems, computerized maintenance management systems (CMMS), and production data.

Is also called intelligent maintenance, as an intervention is only by manifesting the need. Generally applied to machines vital to production, equipment whose failure compromises safety and critical equipment with expensive and frequent breakdowns. It becomes easier over time because the features of each machine are learned, and the diagnostics get faster to act on the failure. Ideally, alarm limits are set high enough to rule out false alarms but conservative enough not to reach a critical condition. Alarm limits are continuously adjusted as more equipment is known in the maintenance program.

After the repair is fixed, condition-based analyses run again, this time to measure vibration levels, e.g., in the repaired equipment to create a new reading. Thus, quantifying the repair effort and ensuring quality repair results from the equipment. This maintenance program can reduce unscheduled breakdowns of all mechanical equipment in the plant and assure that repaired equipment is inacceptable mechanical condition. The program can also identify machine-train problems before they become serious. Normal mechanical failure modes degrade at a speed directly proportional to their severity. If the problem is detected early, major repairs can usually be prevented [14].

The current state of the art in the field of sensing, telecommunications, micro-electronics and Artificial Intelligence (AI), unlocked a new variety of machine condition-based monitoring, which empower business to gain many of the benefits of transitioning from reactive and preventive maintenance to a CBM management on a wide range of machines, without the high up-front cost of traditional CBM systems [20].

A direct correlation with cost-effective advantage, these new systems use small, low cost and easily attached wireless sensors, being able of measure a range of condition indicators, with low latency time, transmitting to a central database. Users access online data about machine condition ubiquitously (e.g. mobile or web app). Earlier warnings can be triggered to nominated staff if machine health degrades [19].

According to Coleman et al. [15], maintenance operation costs are reduced by more than 50%, and there are several competitive advantages related to the adoption of predictive maintenance, such as:

- Increased reliability,
- improvement quality and productivity,
- maintenance cost reduction,
- increases life of components/equipment and facilities,
- improved process, equipment, facilities and people safety.

With Condition Monitoring, it considers a much wider set of granular data that includes sensor data from the asset, previous inspections, other components of the same type, location and condition of the plant, and historical trends.

3.5.2. Types of condition-based monitoring

Condition-based maintenance is rooted in condition-based monitoring. This involves keeping track of the state of an asset using specific performance indicators. Different tools and techniques allow the maintenance staff to do an assessment. These methods can include low-tech approaches, such as observation by a technician, or more technologically advanced processes, like gathering data through sensors. A variety of technologies can, and should be, used as part of a comprehensive predictive maintenance program [14], [21]–[23]:

- **Visual inspections:** Visual inspection was the primary method used for predictive maintenance. Almost from the beginning of the Industrial Revolution, maintenance technicians performed daily inspections of critical production and manufacturing systems to identify potential failures or maintenance-related problems that could impact reliability, product quality, and production costs.
- **Vibration analysis:** Vibration is the oscillation of a body over a reference point due to a given force. There are some fundamental concepts about vibrations that must be understood clearly. Vibratory movements include the movement of pendulums, strings of musical instruments and even the atoms that make up the solids vibrating around fixed positions in the crystal lattice. Physically, the vibration phenomenon is the result of the energy exchange between two deposits of the same system. When kinetic energy is exchanged into potential energy and vice-versa, we get the natural vibration.
- **Infrared and thermal analysis:** The temperature variable is defined as the measure of the average kinetic energy of atoms or molecules of a substance, given in degrees Celsius, Kelvin or Fahrenheit. Whenever there is a temperature difference within a system there will be a transfer of that energy towards the lower temperatures. The transferred energy is called heat, and the transport process is called heat transmission. There are 3 basic mechanisms of heat transmission[3]: conduction, convection and radiation.
- **Ultrasonic analysis:** Ultrasound testing is one of the main non-destructive testing methods applied in the industry as it allows the analysis of the part in its entirety. The use of ultrasonic technology results in increased production, reduced maintenance costs and energy

[3] *Conduction: is the transfer of energy between adjacent parts of a solid as a result of a temperature difference in it. Convection: is a mass conduction heat transfer process, characteristic of fluids. Radiation: is the transfer of heat through electromagnetic waves*. Source: Machine Design Website - www.machinedesign.com/, consulted on September 16, 2019.

consumption as well as more efficient staff utilization. Companies end up having greater profitability. Ultrasound testing detects internal discontinuities in a particular part by the propagation of sound waves. Ultrasonic instruments have been used for leak detection. Its ability to accurately measure pressure and vacuum leaks in tanks, pipelines, heat exchangers and valves.

- **Acoustic analysis:** Is the measurement of sound waves caused by component contacts inside the equipment. sound is created when a medium vibrates, which occurs when rolling elements inside a bearing are allowed to touch one another or the element raceway. is related to vibration analysis; however, its focus is not to detect causes for rotating equipment failure by measuring and monitoring vibrations at discrete frequencies and recording data for trending purposes.
- **Oil analysis:** The smooth running and long-term performance of plant machinery have proved to be so critical, that some equipment manufacturers offer their customers a preventative maintenance oil analysis program. They will take samples of oil regularly and by a combination of physical and chemical tests, gauge how well a gearbox or hydraulic system is performing. Monitoring its physical properties, contamination levels, and wear debris fingerprint over time to get a better knowledge of the lifetime of the moving parts. Some of the most important tests include: Viscosity, water, Total Acid Number (TAN) and Total Base Number (TBN)[4], Wear Metals, Ferrous Metal Content, Particle counting.
- **Electrical analysis:** electrical machinery produces a specific electrical signature when operate on normal conditions - Electrical Signature Analysis (ESA) [24]. Is the general term for a set of electrical machine condition monitoring techniques through the analysis of electrical signals such as current and voltage. Traditional electrical testing methods must be used in conjunction with vibration analysis to prevent premature failure of electric motors (e.g. *Resistance testing, Megger testing, Impedance testing, HiPot testing*).

Using condition-based maintenance doesn’t mean using it effectively. As it was stated previously, it doesn’t exist the right systems, processes and procedures, this maintenance can cost more time, money and patience. Is necessary to understand everything about how equipment functions, so sensors can be properly calibrated, identify probable problems as soon as possible, and suggest proper solutions. Asset context-awareness should aggregate baselines, from manufacturer recommendations to historical trends. Building baselines for each system, demands expert knowledge, to reduce uncertainty, and do decisions more efficient and effective.

The baseline of an equipment’s stable period is never accurately known and will vary for different types of equipment and the different conditions in which that equipment is used. For an industrial component such as a process sensor, a shaft in a motor, or tubes in a heat exchanger, maintenance and replacement schedules are not easy to establish [25]. Determining the best actions to prolong the lifespan of an asset takes a great deal of knowledge about how specific assets fail. In some cases, problems don’t always reveal a clear cause.

[4] “*Monitor organic acids and bases respectively that are produced from a combination of heat-generated oxidation products and the breakdown of additives in the used oil*”. Source: www.plantengineering.com, consulted on September 16, 2019

3.5.3. Understand and use the potential failure (P-F) curve

The Potential Failure (PF) Curve is an essential analytical tool for a maintenance plan that is based on reliability and follows Reliability Centered Maintenance (RCM) standards [26]. Knowing this curve makes one aware of both the useful life and the points of failure of equipment. understanding the data, it will be even more directional to structure the maintenance plan. Equipment is not built to last forever, but it can last much longer than expected. Only 11% of equipment failures are linked to ageing, meaning that if there is a good reliability-centered maintenance strategy, 89% of equipment can be kept available and reliable for extended periods of time [27].

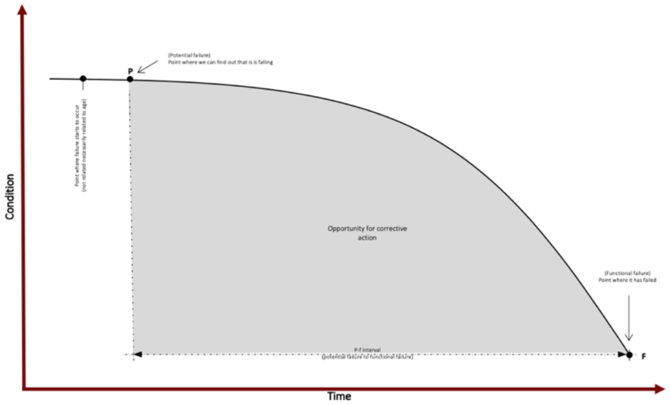


Figure 5 – P-F curve

Adapted from Nowlan's and Heap's original P-F curve [16]

The P-F curve describes the correlation between machine breakdown, cost, and how it can be prevented. It is based on the basis that equipment might be in the early stages of failing still if seems to be working fine. Along the X-axis of the curve is time. Along the Y-axis is the machine's condition. The machine progresses from top working condition to point of failure, and then down from there until actual failure.

Point P (Potential): It is the same as saying that there is a failure mode, or a "symptom". Examples of failure symptoms include rising vibration levels, rising temperature levels, a certain leak, etc., is any change in the way the equipment works before the failure. Thus, it can be said that this is the moment when the failure is born in the asset. It is still a failure at an early stage, it does not completely compromise the operation of the equipment but decreases its performance with every passing minute.

Point F (Functional): The equipment has failed/it cannot perform its work within the process, i.e. it is the inability of a system to meet a specified design performance standard.

A complete loss of function is a functional failure. However, a functional failure also includes the inability to function at the performance level that has been specified as satisfactory. Defining functional failures for any component or system requires a clear understanding of their functions [26]. It is extremely important to determine all functions that are meaningful in each operational context since it is only in these terms that their functional failure can be defined.

The most important part of the P-F curve is the P-F interval. The P-F interval is the time between an asset's potential failure and its functional predicted failure. For successful CBM, it must ensure that inspection intervals are smaller than the P-F interval so it can catch a failure after it's detectable, but before it happens. Calibrating your maintenance intervals is also crucial to optimize condition-based maintenance.

Once the time interval between potential failure and functional failure is known, the maintenance plan will be planned and executed so that it can further extend the life of this analysed equipment. Understanding the P-F curve and the P-F interval is key to building an efficient CBM strategy. The P-F curve and interval allow you to determine how often you should complete a CBM task. The frequency of maintenance is reduced, as are the costs and time commitments associated with maintenance [28].

The PF Curve is essential for determining preventive and predictive action intervals so that they can be performed at the exact times: as close as possible to potential failure and as far as possible from functional failure.

While CBM relies heavily on technology and automated systems (e.g. sensors and software), there will always be a human element involved. To improve efficiency and effectiveness from CBM strategy, it is relevant that all maintenance personnel are properly trained for CBM benefits and how to use the systems. This action will reduce user errors and increase reliability throughout the process.

Training should take in consideration the condition monitoring complexity and different types, and how it affects each asset inside the company. Also, should be clear how every maintenance personnel gather sensor data correctly (i.e. identify it reliability status/calibration quality process), and how resulting maintenance tasks should be treated. In this stage of CBM implementation, is advisable to add and asset management policy[5], as it will help all staff members, not only maintenance [25]. Part of the strategy is to implicate everyone on the benefits of maintenance techniques, how them will impact the organization, and consequently, to ensure the strategy works to its full potential.

3.5.4. Challenges for predictive maintenance systems

Condition-based Maintenance (i.e. predictive maintenance approach) enables more efficient, longer-term planning for maintenance operations and makes it easier to define operational maintenance goals and to allocate maintenance resources.

Examining data from hundreds or thousands of sensors, gathered over months or even years, is well beyond the capabilities of human operators. Furthermore, the mathematical models, which describe an equipment's evolution (and predict potential faults) based on such a wealth of data, are generally prohibitively complex to be used by humans. For data scientists, predictive maintenance has several promising outcomes, including reducing machine downtime and avoiding unnecessary maintenance costs while adding revenue streams for equipment vendors with aftermarket services. However, engineers and scientists face challenges around process and data when applying predictive maintenance technologies into their business operations [29]:

- Being unaware of how to do predictive maintenance
- Lacking data to create proper predictive maintenance systems
- Lacking failure data to achieve accuracy
- Understand failures but not being able to predict them

[5] An asset refers to anything that is used in the regular operation of an organization. It can be a physical object (e.g. buildings, equipment, raw materials), as well as intangible, such as staff or money. In this approach, asset management scope is higher than the maintenance assets objects, but all in the organization, such as computers, staff and infrastructures

The growing digitalization of companies marks the beginning of a new era for industrial maintenance: the emergence of predictive maintenance. A new generation of smart sensors appeals to an increasing number of manufacturers who wish to improve their maintenance methods. Companies should press well beyond one digital tool and think about how digital and advanced analytical techniques can transform their entire maintenance and reliability system. This means looking end to end for opportunities to make better use of data and apply user-centric design principles to digitize processes. The sustainable impact will require a blend of new digital tools, changes in asset strategy, and improved reliability practices [13], [29].

3.6. Predictive Maintenance

Predictive maintenance is a proactive maintenance strategy that tries to predict when a piece of equipment might fail so that maintenance work can be performed just before that happens. Thus, equipment downtime is minimized, and the component lifetime is maximized. The aim of predictive maintenance (PdM) is first to predict when equipment failure might occur, and secondly, to prevent the occurrence of the failure by performing maintenance. Monitoring for future failure allows maintenance to be planned before the failure occurs. Ideally, predictive maintenance allows the maintenance frequency to be as low as possible to prevent unplanned reactive maintenance, without incurring costs associated with doing too much preventive maintenance.

Any predictive maintenance program should be characterized by a combination of three phases: [30]

- **Surveillance** - monitoring machinery condition to detect incipient problems
- **Diagnosis** - isolating the cause of the problem
- **Remedy** - performing corrective action.

Analysis of data is where the knowledge and experience of maintenance personnel becomes the most important in a PdM program. It normally requires extensive training not only in the analysis techniques, but also in the use of the hardware and software employed. There are five important analysis techniques in PdM:

- **Data comparison:** Recognition of changes in data as compared to earlier data or baseline data on similar equipment.
- **Limit or range tests:** Specific testing to discover operating parameters that do not follow continuous trends or repeatable patterns.
- **Pattern recognition:** Identification of deviations from established patterns.
- **Correlation analysis:** Comparison of data from multiple sources, related technologies, or different analysts.
- **Statistical process analysis:** Use of statistical techniques to identify deviations from the norm.[30]

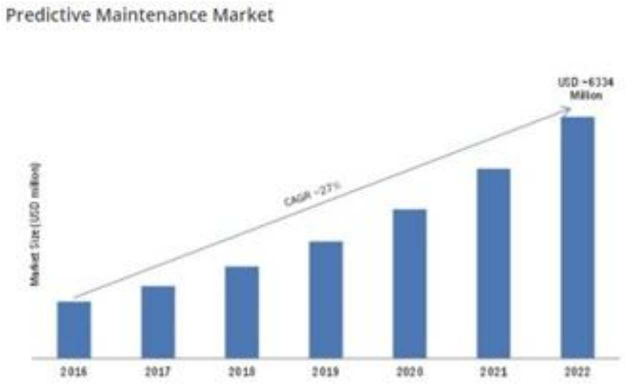


Figure 6 – Predictive Maintenance Market

(Source: Predictive Maintenance Market Research Report- Forecast to 2022)

For predictive maintenance to be carried out on an industrial asset, the following base components are required:

- **Sensors** – data-collecting sensors installed in the physical product or machine
- **Data communication** – the communication system that allows data to securely flow between the monitored asset and the central data store
- **Central data store** – the central data hub in which asset data (from OT systems), and business data (from IT systems) are stored, processed and analysed; either on premise or on-cloud
- **Predictive analytics** – predictive analytics algorithms applied to the aggregated data to recognize patterns and generate insights in the form of dashboards and alerts
- **Root cause analysis** – data analysis tools used by maintenance and process engineers to investigate the insights and determine the corrective action to be performed [31].

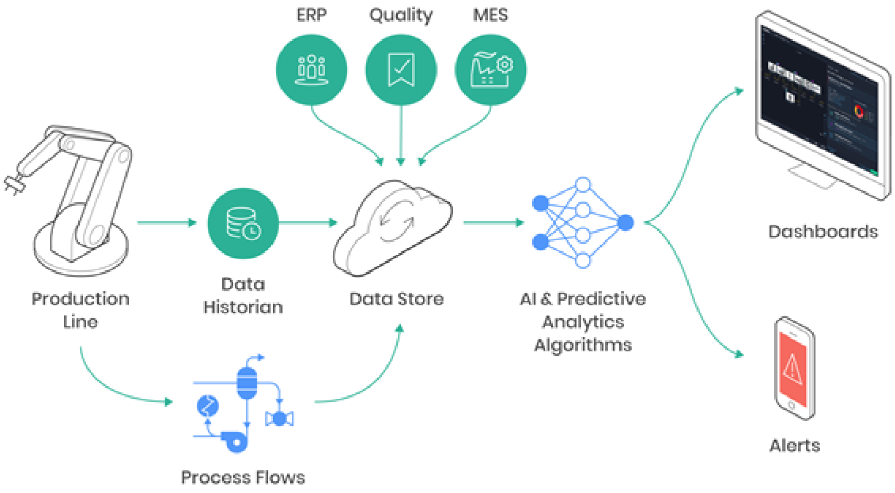


Figure 7 – PdM architecture

(Image Source: https://www.seebo.com/predictive-maintenance/)

3.6.1. Data Sources for Predictive Maintenance

In order to get the performance of assets in real-time, PdM relies on condition-monitoring equipment. The formula for PdM can be stated as follows: condition-based diagnostics, predictive formulas and internet of things.

Condition-monitoring Equipment

With condition-monitoring equipment, each asset is monitored in predictive maintenance. Specifically, the machines are fitted with sensors that capture data about the equipment to enable evaluation of the asset's efficiency and track wear in real-time. This step is essential because although physical inspections of equipment have traditionally been the major way through which maintenance personnel observe assets, there has been a critical shortcoming in that procedure – the most wear and tear happens "inside" the machines, which means you need to take them apart to do a proper inspection. However, by using condition-monitoring sensors and predictive maintenance, you can have an accurate representation of what is happening inside the asset without any kind of productivity disruptions.

These sensors measure different kinds of parameters depending on the type of machine. Most commonly, they measure vibration, noise, temperature, pressure, and oil levels, but you can go beyond that and even measure things like electrical currents and corrosion. [32]

Figure 8 –Condition Monitoring Equipment sensors

(Image Source: https://limblecmms.com/blog/predictive-maintenance/)

The Internet of Things

It is one thing to gather data, but quite another to be able to analyse and use the data for its intended purpose. By using the IoT technology, the different sensors mentioned earlier can collect and share data. PdM relies heavily on these sensors to connect the assets to a central system that stores the information coming in. These central hubs run using WLAN or LAN-based connectivity or cloud technology. From there, the assets can communicate, work together, analyse data, and recommend remedial action or act directly based on how the system is set up. This exchange of information is at the core of predictive maintenance and allows maintenance techs to make sense of what is happening in the machines and identify any assets that (will) need attention. [32]

Predictive Formulas

This is where predictive maintenance goes beyond condition-based maintenance. The data collected previously is analysed using predictive algorithms that identify trends with the aim of detecting when an asset will require repair, servicing, or replacement.

These algorithms follow a set of predetermined rules that compare the asset's current behaviour against its expected behaviour. Deviations are an indication of gradual deterioration that will lead to asset failure. Service technicians can then intervene as required to avoid breakdowns. [32]

3.6.2. Predictive Maintenance Techniques

PdM is a group of emerging scientific technologies that can be employed to detect potential failures that may not be evident through a preventative maintenance program. If the failure characteristics of the equipment are known, PdM can detect the failure well in advance and appropriate actions can be taken in a planned manner. The use of condition-based maintenance has dramatically reduced non-value-added maintenance by eliminating the need to unnecessarily shutdown equipment for maintenance checks. [33]

In this section, six techniques will be focused which are stated below: Alignment, Oil analysis, Wear particle analysis, Infrared thermography, Vibration monitoring, Motor analysis.

Alignment

Misalignment of shafted equipment will not only cause equipment malfunctions or breakdowns, it may be an indicator of other problems. Checking and adjusting alignments used to be a very slow procedure. But the advent of laser alignment systems has reduced labour time by more than half and increased accuracy significantly.

Laser alignment systems for shafts have been available for many years. Laser devices for aligning sheaves and pulleys have recently come to market. [30]

Ultrasonic testing: Instruments designed for ultrasonic testing sense ultrasound waves produced by operating machinery as well as the turbulent flow of leakage. They provide fast, accurate diagnosis of such problems as valves in blowby mode, faulty steam traps, and vacuum and pressure leaks. Ultrasonic observations may be taken in either airborne or contact mode.

Airborne ultrasonic is extremely useful in the location and diagnosis of mechanical problems, but the technology is not capable of isolating specific sources of ultrasound within a machine. Testing instruments are usually battery operated for portability. Their electronic circuitry converts a narrow band of ultrasound (between 20 and 100 kHz) into the audible range so that a user can recognize the qualitative sounds of operating equipment through headphones. Intensity of signal strength is also displayed on the instrument.

As scanners, ultrasonic instruments are most often used to detect gas pressure or vacuum leaks. Because they are sensitive only to ultrasound, they are not limited to a specific gas, as are most other leak detectors.

In contact mode, a metal rod acts as a waveguide. When it touches a surface, it is stimulated by ultrasound on the opposite side of the surface. This technique is commonly used for locating turbulent flow or flow restrictions in piping.

Ultrasonic detectors are somewhat limited in their use. For example, they may help identify the presence of suspicious vibrations within a machine, but they are not enough for isolating the sources or causes of those vibrations.

On the plus side, ultrasonic monitoring is easy (requiring minimal training), and the instruments are inexpensive. [30]

Oil analysis

Full benefit of oil analysis can be achieved only by taking frequent samples and trending the data for each machine in the program. The length of the sampling intervals varies with different types of equipment and operating conditions. Based on the results of the analyses, lubricants can be changed or upgraded to meet the specific operating requirements. It is nearly always best to work with a reputable laboratory for sample analysis and data interpretation.

It cannot be overemphasized that sampling technique is critical to meaningful oil analysis. Sampling locations must be carefully selected to provide a representative sample and sampling conditions should be uniform so that accurate comparisons can be made.

A thorough oil analysis typically includes 11 tests:

- Viscosity is one of the most important properties of a lubricating oil. The analysis consists of comparing a sample of oil from a machine to a sample of unused oil to determine if thinning or thickening of the oil has occurred during use.
- Contamination of oil by water or coolant can cause major problems. Because many of the additives in lubricants contain the same elements used in coolant additives, samples for analysis must be compared to samples of new oil.
- Fuel dilution of engine oil weakens the oil's film strength, sealing ability, and detergency. Dilution may indicate such problems as improper operation, fuel system leaks, ignition problems, improper timing, or other deficiencies.
- Solids content is a general test indicating total solids in the oil as a percentage of the sample volume or weight. Any unexpected rise in solids is cause for concern, because the presence of solids can significantly increase wear on lubricated parts.
- Fuel soot content is an important indicator for oil in diesel engines. Although fuel soot is always present in diesel engine oil to some extent, increases above normal levels may indicate fuel-burning problems.
- Oxidation of lubricating oil can result in lacquer deposits, metal corrosion, or thickening of the oil.
- Nitration results from fuel combustion in engines. The products formed are highly acidic, and they may leave deposits in combustion areas and accelerate oil oxidation.
- Total acid number (TAN) is a measure of the amount of acid or acid-like materials in oil.
- Total base number (TBN) indicates an oil's ability to neutralize acidity. Low TBN is often an indicator that the wrong oil is being used for the application, intervals between oil changes are too long, oil has been overheated, or a high-sulphur fuel is being used.
- Particle count as part of a standard oil analysis is quite different from the wear particle analysis offered as a separate, specialized service (see following section). High particle counts indicate that machinery may be wearing abnormally or that failures could be caused by blocked orifices. Particle count tests are especially important in hydraulic systems.
- Spectrographic analysis reveals the presence of such elements as wear metals, contaminants, and additives in oil. [30]

Wear particle analysis

While oil analysis provides information about the lubricant itself, wear particle analysis provides direct information about wearing conditions inside the machinery. This information is derived from the study of particle shapes, composition, sizes, and quantities. Wear particle analysis is conducted in **two stages**:

- The first involves monitoring collected particles to determine normal conditions and trends.
- The second is the diagnosis of abnormal conditions as indicated by changes in the particle types, sizes, and quantities.

Rubbing wear results from the normal sliding wear in a machine and should remain stable as a surface wear normally. But a dramatic increase in wear particles indicates impending trouble. Cutting wear particles are generated with one surface penetrates another, much as a cutting tool removes material. Cutting wear particles are abnormal and are always worthy of attention. These particles are produced when a misaligned or fractured hard surface produces an edge that cuts into a softer surface, or when abrasive contaminants become embedded in a surface and cut an opposing surface. Increasing quantities of longer particles signal a potentially imminent component failure.

Rolling fatigue is associated primarily with rolling contact bearings and may produce **three distinct particle types**:

- fatigue spall particles,
- spherical particles, and
- laminar particles.

Rolling spall particles are the most critical, because they indicate damage to a rolling element has already occurred.

Combined rolling and sliding wear results from the moving contact of surfaces in gear systems. The chunkier particles result from tensile stresses on the gear surface, causing the fatigue cracks to spread deeper into the gear tooth before pitting. Scuffing of gears occurs when excessive heat from a high load or speed breaks down the lubricant film. Once started, scuffing usually affects each gear tooth.

Severe sliding wear also results from excessive loads or heat in a gear system. Large particles break away from the wear surfaces. If conditions are not corrected, catastrophic wear is the likely result. [30]

Infrared thermography

Infrared thermography uses special instruments to detect, identify, and measure the heat energy objects radiate in proportion to their temperature and emissivity. Midwave-range instruments detect infrared in the 2-to-5 micron range; longwave-range instruments detect the 8-to-14 micron range.

Infrared inspections can be qualitative or quantitative. Qualitative inspection concerns relative differences, hot and cold spots, and deviations from normal or expected temperatures. Quantitative inspection concerns accurate measurement of the temperature of the target.

As one of the most versatile predictive maintenance technologies available, infrared thermography is used to study everything from individual components of machinery to plant systems, roofs, and even entire buildings.

Infrared instruments include an optical system to collect radiant energy from the object and focus it, a detector to convert the focused energy pattern to an electrical signal, and an electronic system to amplify the detector output signal and process it into a form that can be displayed. Most instruments include the ability to produce an image that can be displayed and recorded. These thermographs, as the images are called, can be interpreted directly by the eye or analysed by computer to produce additional detailed information. High-end systems can isolate readings for separate points, calculate average readings for a defined area, produce temperature traces along a line, and make isothermal images showing thermal contours.

It is essential that infrared studies be conducted by technicians who are thoroughly trained in the operation of the equipment and interpretation of the imagery. Variables than can destroy the accuracy and repeatability of thermal data, for example, must be compensated for each time data is acquired. In addition, interpretation of infrared data requires extensive training and experience. [30]

Vibration monitoring

Vibration monitoring might be considered the "grandfather" of predictive maintenance, and it provides the foundation for most plants' PdM programs. Monitoring the vibration from plant machinery can provide direct correlation between the mechanical condition and recorded vibration data of each machine in the plant. Used properly, it can identify specific degrading machine components or the failure mode of plant machinery before serious damage occurs.

Vibration monitoring and trending works on the premise that every machine has a naturally correct vibration signature. This signature can be measured when the machine is in good working order, and subsequent measurements can be compared with what is considered the norm. As the machine wears or ages, the vibration spectra change. Analysing the changes identifies components that require further watching, repair, or replacement.

Most vibration based PdM programs rely on one or more of the following techniques:

- **Broadband trending** provides a broadband or overall value that represents the total vibration of the machine at the specific measurement point where the data was acquired. It does not provide information on the individual frequency components or machine dynamics that created the measured value. Collected data is compared either to a baseline reading taken when the machine was new (or sometimes data from a new duplicate machine) or to vibration severity charts to determine the relative condition of the machine.

- **Narrowband trending** monitors the total energy for a specific bandwidth of vibration frequencies and is thus more specific. Narrowband analysis utilizes frequencies that represent specific machine components or failure modes.

- **Signature analysis** provides visual representation of each frequency component generated by a machine. With appropriate training and experience, plant personnel can use vibration signatures to determine the specific maintenance required on the machine being studied. [30]

Motor analysis

Until recently, predictive maintenance technologies for motors were limited to vibration testing, high-voltage surge testing for winding faults, meg-Ohm and high-potential tests for insulation resistance to ground, and voltage and current tests for testing phase balance. Many of these tests still have their place in plant maintenance, but several of them are impractical, dangerous, or harmful when tests are conducted with motors in place.

New technologies allow for portable, safe, and trendable tests that can be used for more accurate commissioning and troubleshooting. Each of these technologies has its strengths and weaknesses. But as part of a PdM program, they can accurately detect potential faults and avoid costly downtime.

Static motor circuit analysis (MCA) provides a low-voltage, safe method of testing motor winding and rotor defects. The best instruments for this analysis use impedance-based tests coupled with insulation-to-ground testing. Impedance-based instruments are simple to use, and the results are easy to evaluate. Inductive-based instruments are for trending. Tests detect faults in motors, transformers, cabling, and connections. Motors must be de-energized.

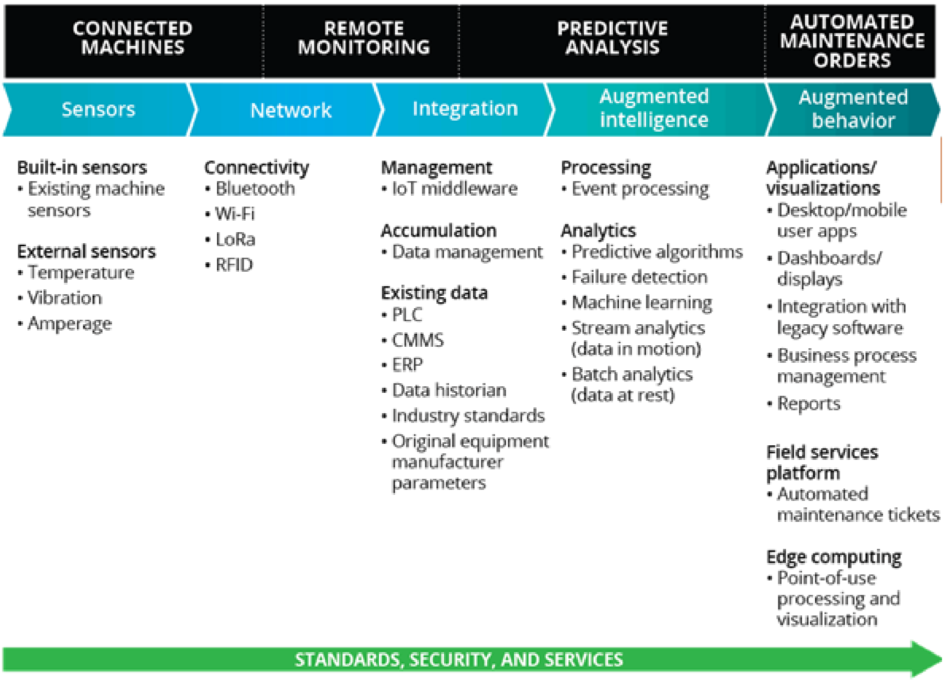
Motor current signature analysis (MCSA) is performed by taking current data and analysing it using Fourier transform analysis. Primary purpose of the test is rotor bar fault detection, but it is also useful for detecting rotor faults and power quality problems as well as other motor and load defects in later stages of failure. Motors must be energized and loaded during tests.

Surge comparison testing uses high-voltage pulses to detect winding faults. Only experienced operators should conduct these tests because of the potentially harmful effects of high voltage impressed on used windings and cables. There are also challenges with testing assembled motors due to rotor effects on the motor circuit. Motor being tested must be de-energized with controls disconnected.

High potential testing uses high-voltage AC or DC to detect faults to ground. Only the insulation condition between stator windings and ground can be evaluated and there is a potential for damage to the insulation system if the test is improperly applied or controlled. Motors must be de-energized with controls disconnected during tests. [30]

3.6.3. Predictive Maintenance Technologies

Understanding how PdM works requires an examination of the specific connected technologies that enable it: sensors and communication protocols, analytics and data-handling tools, and data visualization and collaborative tools.



Source: Deloitte analysis.

Deloitte University Press | dupress.deloitte.com

Figure 9 – Technologies that drive PdM

Sensors and networks

Perhaps the most important pieces of the PdM puzzle are the sensors that create the data and the communications needed to get those data to where they can be stored and analysed. These sensors translate physical actions from machines into digital signals that communicate variables such as temperature, vibration, or conductivity. Data can also be streamed from other sources, such as a machine's programmable logic controller (PLC), MES, CMMS, or even an ERP system. GE's Condition Forecaster system, for example, uses this aggregation approach to maximize the performance and reliability of their plant motors by combining data from over 250 sensors per motor with over 40,000 historical maintenance records.

Whether the types of protocols that enable this sort of transparency are custom designed for a specific application or for general use such as Wi-Fi and Bluetooth, today's low cost and affordability of bandwidth and storage mean that massive amounts of data can be transmitted. This allows manufacturers to have a full picture of not only assets in a single plant but also an entire production network—leveraging the end-to-end transparency of the DSN.[34]

Data integration and augmented intelligence

Once digital information has been centralized, it typically must be parsed, stored, and analysed using advanced analytics and predictive algorithms. Simply gathering data on machinery from sensors is not enough. Predicting the failure of individual parts likely requires high-level solutions for unstructured data, augmented intelligence (AI), or machine learning. These technologies are needed to sift through the mountains of data to find the "signal" of a part about to fail in the "noise" of daily operation. Put simply, while PdM depends on the accuracy of failure thresholds determined in a pilot program or review cycle, machine learning technologies improve these thresholds iteratively over time by analysing the outcomes of each prediction and adjusting the thresholds accordingly. As a result, choosing the right analytics or algorithms is a critical step in creating a PdM capability. But the results can be significant: One manufacturer recently reduced downtime on a robotic manufacturing line by 50 percent and increased performance by 25 percent by leveraging a machine learning platform for its predictive algorithms.

As these tools move further into the mainstream, they may no longer require a degree in statistics or computer science to use, putting them within reach of many organizations that may not have had the expertise or resources to leverage them in the past. Operations analysts, who are more in touch with manufacturing processes, can easily create dashboards using modern application program interfaces (APIs) created specifically for the everyday user.

Another trend is the movement of data to the edge. Like the lean technique of storing tooling at the point of use, data computation is done at the "edge," meaning it is processed at the machine where it is generated. Insights can thus be pushed directly to machine operators as well as maintenance technicians. As data continue to proliferate, edge computing reduces the overall burden on a computer network by distributing some of the processing work to a network's outer nodes to alleviate core network traffic and improve application performance. [34]

Augmented behaviour

Once data have been analysed, they can be presented to humans and machines in a manner that enables them to act, either manually (in the case of humans) or autonomously (in the case of machines). At this stage, augmented behaviour becomes relevant. Technologies such as wearables and augmented reality can allow maintainers to see large amounts of data, such as a maintenance manual or expert advice, while immersed in a task. These technologies use overlaid systematic instructions to help operators immediately solve problems as they arise (even in noisy environments), and help disseminate knowledge via immersive, on-demand training. They also allow teams in other locations to remotely monitor and supervise operations.

For example, a leading technology manufacturer deployed a suite of industry-leading wearable technology to troubleshoot issues remotely and disseminate specialized knowledge in real time. The solution supported the manufacturing incident resolution processes, which often witnessed severe delays during critical component assembly. The company saw a 50 percent reduction in repair cycle time for defects and estimated savings of $500,000 in a single product line through reduced downtime.

Finally, after the signals have been processed, analysed, and visualized, digital insights are translated into physical action. In some cases, the digital conclusions drawn may instruct robots or machines to alter their functions. In other cases, maintenance alerts will spur a technician into action. Consider a situation where the predictive algorithms trigger a maintenance work order in the company's CMMS system, check the ERP system for spares on hand, and automatically create a purchase request for any additional parts required, all automated and prior to unplanned downtime. Then the maintenance manager only must approve the items in the workflow and dispatch the appropriate technician. [34]

3.6.4. Dimensions and Technical Infrastructure for Predictive Maintenance

Alarm detail levels such as asset, line, area and factory should be integrated to digital twin layout. Besides, time dimensions including shift, day and week are important in manufacturing use cases. In addition, users should configure how predictions will be converted to work orders with platform rule engine integration. For instance, if the alarm probability were above 70%, the system would start a work order. However, different thresholds apply for critical equipment.

Transparency and accountability are two main issues regarding the use of predictive maintenance in manufacturing units. Currently, most advanced analytic solutions are black box. When a system gives an alarm, the reason might not be known, or the engineers may have doubts about the calculation process. Critical capabilities for successful maintenance include:

- Having transparent and measurable success rate: False positives would create unnecessary maintenance work orders thus additional cost to customer.
- Easy to implement with Manufacturing Information System (MIS): End-users should view the product as a tool that can be used by them in order to get buy-in from enterprise digital transformation teams

Model Reinforcement capabilities: For higher success-rates additional consultancy from domain experts and data scientist may be required.

3.6.5. Implementation Stages of Predictive Maintenance

The implementation approach is based on gradually building up the PdM model for selected assets. Seven steps of implementation can be stated as follows:

1. Asset value ranking & feasibility study: Identify assets for which it is worthwhile and feasible to apply PdM in order to increase asset reliability. Only high-critical and possibly medium-critical assets will justify the required investments, and only assets for which the required data can be obtained are suitable candidates. This selection of assets will help to build an initial positive business case that should be part of the feasibility study.

2. Asset selection for PdM: Keep it manageable and do not try to cover your entire fleet or factory in one go. Select assets that can be tackled in pilot-projects draw the necessary lessons from the pilots and apply these to the rollout of PdM per asset type.

3. Reliability modelling: Use root cause analysis (RCA) and failure mode effects analysis (FMEA) per asset type to point you in the right direction. What data do you need to monitor root causes and failure modes? What sensory data and what external data sets do you need for this? How are the various root causes and failure modes interrelated?

4. PdM algorithm design: This is really the art of data analytics. Choosing an algorithm is the single most important factor in determining the quality of your predictions. It may be relatively straightforward to design the best algorithm if you have already built a suitable model for asset reliability in the previous step. It may also require several data scientists to construct a self-learning algorithm capable of finding meaningful insights in pools of data.

5. Real-time performance monitoring: This is where your PdM model goes live. The algorithm processes data from various sources - sensors embedded in the asset, the asset's maintenance and failure history, or third-party providers of environmental data - to monitor and visualize the performance of your assets in real-time.

6. Failure prediction (early warning): The algorithm will start to predict future failures. Acting on these predictions - by shutting down a machine or taking a perfectly operational train out of circulation - may initially require a big leap of faith, especially if management and maintenance staff have little experience with, or affinity for, data analytics. If this is the case, PdM 4.0 could run parallel to existing maintenance procedures without maintenance actions being taken based on its predictions. This may help to further build confidence in the predictions.

7. Preventive task prescription: At the top level of PdM, the algorithm not only predicts when a failure is likely to occur, but it also draws from a library of standard maintenance tasks to prescribe the best action to avoid such a failure. It may even execute such tasks, for example, by automatically issuing the corresponding work order.[35]

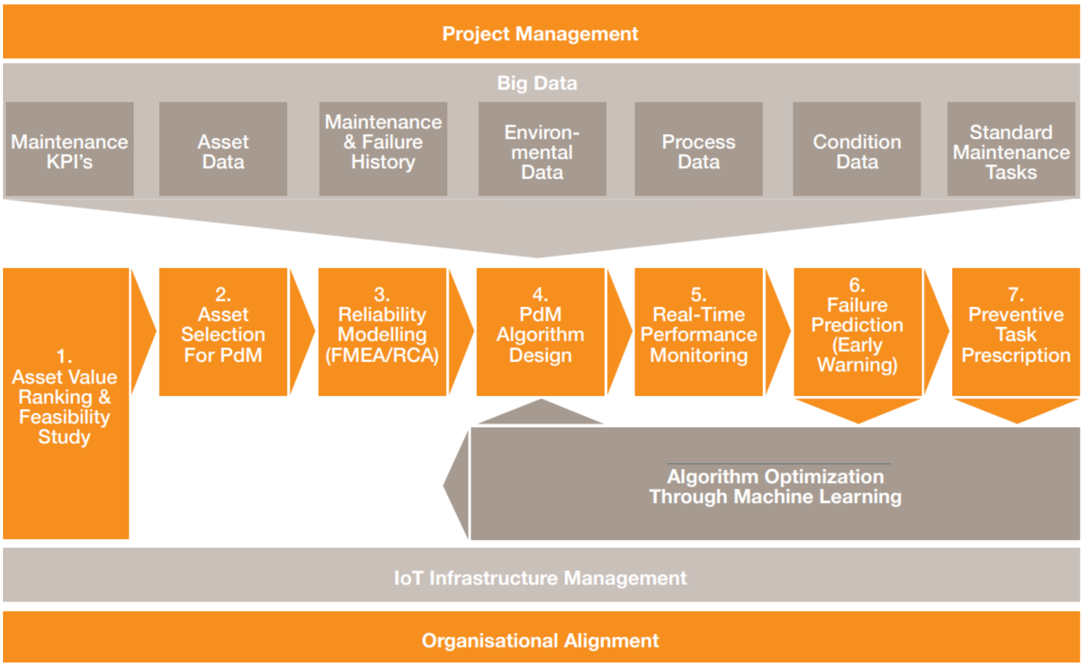

Project Management
Big Data
Maintenance KPI's
Asset Data
Maintenance & Failure History
Environ-mental Data
Process Data
Condition Data
Standard Maintenance Tasks
1. Asset Value Ranking & Feasibility Study
2. Asset Selection For PdM
3. Reliability Modelling (FMEA/RCA)
4. PdM Algorithm Design
5. Real-Time Performance Monitoring
6. Failure Prediction (Early Warning)
7. Preventive Task Prescription
Algorithm Optimization Through Machine Learning
IoT Infrastructure Management
Organisational Alignment

Figure 10 – Implementation stages of PdM

(Image Source: https://www.mainnovation.com/wp-content/uploads/tmp/58e418c645624c08e147d5f9c476d1370f2cc191.pdf)

This seven-step implementation process is grouped under the 'putting the predictive model in place' title which is located in the middle at figure above. It is the technical core of PdM implementation. After that, the 'putting technology infrastructure in place' phase comes. In this phase, there are three building blocks: big data infrastructure, internet of things infrastructure, and algorithm optimization. Finally, 'putting the organisational support structure in place' phase comes which is the softer side of PdM implementation. This phase is consisting of building data analytics capabilities and building a digital culture.

Overall, this implementation approach includes the technological and organisational aspects that companies must address to the most of PdM.

PdM is very popular lately and when it comes to developing PdM processes, companies get ambitious about it. Companies should take organisational dimensions seriously and make sure the project management and change management skills are the skills that they need for a successful PdM implementation process. Also, for a successful PdM implementation process, significant efforts and resources will be needed.

3.6.6. Commercial Applications of Predictive Maintenance

Predictive maintenance can be applicable to all industries where machines produce significant amounts of data and require maintenance or fine tuning of their parameters.

A significant share of vendors is actually industry agnostic and serve most industries as their work relies on data interpretation and can be abstracted from the specifics of machinery in the factory floor.

An overview of industries where predictive maintenance applications is already gaining traction:

- **Automotive:** Automotive companies operate some of the largest robot parks in the world. With the aim to reduce inventory costs, automotive companies developed Just-In-Time manufacturing methodology since the 1960s and 1970s. As a result, they have tightly integrated supply chains. Though tight supply chain integration allows reduced inventory, any reduction in manufacturing efficiency results in significant disruption to the supply chain. It is no surprise that automotive companies stand to gain significantly from a technology that reduces downtime.
- **Airlines:** Airlines are no stranger to closely monitoring sensor data from planes. Today's analytical capabilities allow them to analyse more data increasing safety of passengers.
- **High tech manufacturing:** Operating complex equipment at optimal parameters is the key challenge to improve efficiency for high tech manufacturers like semiconductor manufacturers. Predictive maintenance systems allow them to operate at a level closer to optimal parameters.
- **Transportation:** Though airlines lead the pack in terms of complexity of their equipment, other means of transportation like trains also involve complex machinery that can benefit from predictive maintenance.
- **Oil & gas:** Despite the rise in green energy, oil & gas is still one of the largest industries. Both extraction and refining involve expensive equipment that can cause health and environmental hazards in case of failure. For example, Deepwater Horizon oil spill in 2010, which led to 11 dead and ~ 5 M barrels of oil, spilled, has been one of the worst disasters in the last decade. Stakes are high to prevent such disasters with better analytics and maintenance.
- **Ports:** Exposed to harsh conditions, port equipment's' conditions deteriorate quickly. For example, cranes are critical components, but they are prone to failure. Crane downtime means more waiting time for ships and less throughput for ports. Reducing downtime improves service quality and reduces waste for ports.[36]

Both discrete industries like consumer packaged goods (CPG), automotive, electronics, textiles, aerospace and process industries like food and beverage, chemicals, oil&gas, pharma can be transformed with predictive maintenance. [36]

3.6.7. Predictive Maintenance Algorithms

There are multiple modelling strategies for predictive maintenance, and we will describe four of them in relation to the question they aim to answer and which kind of data they require:

- Regression models to predict remaining useful lifetime (RUL)
- Classification models to predict failure within a given time window
- Flagging anomalous behaviour
- Survival models for the prediction of failure probability over time

STRATEGY 1: Regression models to predict remaining useful lifetime (RUL)

Output: How many days/cycles are left before the system fails?

Data characteristics: Static and historical data are available, and every event is labelled. Several events of each type of failure are present in the dataset.

Basic assumptions/Requirements:

- Based on static characteristics of the system and on how it behaves now, the remaining useful time can be predicted which implies that both static and historical data are required and that the degradation process is smooth.
- Just one type of "path to failure" is being modelled: if many types of failure are possible and the system's behaviour preceding each one of them differs, one dedicated model should be made for each of them.
- Labelled data is available, and measurements were taken at different moments during the system's lifetime.[37]

STRATEGY 2: Classification models to predict failure within a given time window

Creating a model that can predict lifetimes very accurate can be very challenging. In practice however, one usually does not need to predict the lifetime very accurate far in the future. Often the maintenance team only needs to know if the machine will fail 'soon'. This results in the next strategy:

Question: Will a machine fail in the next N days/cycles?

Data Characteristics: Same as for strategy 1

Basic assumptions/Requirements:

- The assumptions of a classification model are very similar to those of regression models. They mostly differ on:
- Since we are defining a failure in a time window instead of an exact time, the requirement of smoothness of the degradation process is relaxed.
- Classification models can deal with multiple types of failure, as long as they are framed as a multi-class problem, e.g.: class = 0 corresponding to no failure in the next n days, class = 1 for failure type 1 in the next n days, class = 2 for failure type 2 in the next n days and so forth.
- Labelled data is available and there are "enough" cases of each type of failure to train and evaluate the model.

In general, what regression and classification models are doing is modelling the relationship between features and the degradation path of the system. That means that if the model is applied to a system that will exhibit a different type of failure not present in the training data, the model will fail to predict it. [37]

STRATEGY 3: Flagging anomalous behaviour

Both previous strategies require many examples of both normal behaviour (of which we often have a lot of) and examples of failures. However, how many planes will you let crash to collect data? If you have mission critical systems, in which acute repairs are difficult, there are often only limited, or no examples of failures at all. In this case, a different strategy is necessary:

Question: Is the behaviour shown normal?

Data Characteristics: Static and historical data are available, but either labels are unknown or too few failure events were observed or there are too many types of failure.

Basic assumptions/Requirements: It is possible to define what normal behaviour is and the difference between current and “normal” behaviour is related to degradation leading to failure.

The generality of an anomaly detection model is both its biggest advantage and pitfall: the model should be able to flag every type of failure, despite of not having any previous knowledge about them. Anomalous behaviour, however, does not necessarily lead to failure. In addition, if it does, the model does not give information about the time span it should occur.

The evaluation of an anomaly detection model is also challenging due to the lack of labelled data. If at least some labelled data of failure events is available, it can and should be used for evaluating the algorithm. When no labelled data is available, the model is usually made available and domain experts provide feedback on the quality of its anomaly flagging ability. [37]

STRATEGY 4: Survival models for the prediction of failure probability over time

The previous three approaches focus on prediction, giving you enough information to apply maintenance before failure. If you however are interested in the degradation process itself and the resulting failure probability, this last strategy suits you best.

Question: Given a set of characteristics, how does the risk of failure change in time?

Data Characteristics: Static data available, information on the reported failure time of each machine or recorded date of when a given machine became unobservable for failure.

A survival model estimates the probability of failure for a given type of machine given static features and is useful to analyse the impact of certain features on lifetime. It provides, therefore, estimates for a group of machines of similar characteristics. Therefore, for a specific machine under investigation it does not consider its specific status.[37]

3.6.8. Predictive Maintenance Solutions (Competitor Analysis)

1. SAP Predictive Maintenance and Service[6]

Combine sensor data with business information in your ERP, customer relationship management (CRM), enterprise asset management (EAM), and augmented reality systems using SAP Predictive Maintenance and Service, part of the SAP Intelligent Asset Management solution portfolio.

- Cloud and on-premise deployment
- Insight from sensor data

[6] Webpage: https://www.sap.com/turkey/products/predictive-maintenance.html

- Prediction of equipment malfunctions
- Optimized resource management

Key Capabilities

- Management and decision support: Enable a closed-loop maintenance and service process by optimizing asset maintenance with anomaly detection, spectral analysis, and machine learning algorithms.
- Enablement of IoT and IIoT connectivity: Monitor connected devices and support IoT data transfer services to optimize data management with scalable and cost-effective storage for time-series data.
- Visualization of predictive analytics: Expose valuable insights through real-time data analytics – according to business needs – with a unified and intuitive user experience.

Integration with a range of SAP solutions: Integrate your predictive maintenance and services capabilities with SAP enterprise solutions – such as SAP S/4HANA – and third-party maintenance execution systems.

2. Honeywell Forge APM – Asset Performance Management[7]

Honeywell Forge APM is a real-time machinery analytics solution that continuously monitors asset and process performance, detects impending health issues, and predicts time to failure. It helps industrial facilities reveal opportunities for performance improvement and expedites analysis toward root cause of inefficiencies or impending issues. Honeywell Forge APM helps reduce cost of operations and maintenance and allows personnel to manage more assets concurrently.

- Calculation and Visualization applications help engineers combine process knowledge and plant data to analyse plant efficiency and identify trends.
- Advanced Planning and Scheduling tools help planners and schedulers come up with optimal and feasible plans for a unit, plant or group of plants.
- Blending and Movement Automation helps plan, control and track manufacturing performance for offsites, control optimum in-line blending and control material movements.
- Asset Performance Management tools provide an objective view of machinery performance metrics and calculations.

Production Management tools track determine and report production, material use and inventory.

3. Oracle IoT Asset Monitoring Cloud[8]

Sensor data streaming to Oracle IoT Asset Monitoring Cloud Service is continually analysed in real time. Using customizable prediction analytics, your assets will tell you when they need maintenance, often long before they fail.

- Perform preventive maintenance on critical assets.
- Improve asset availability.
- Reduce operating costs.

[7] Webpage:https://www.honeywellprocess.com/library/marketing/notes/PIN-Forge-APM-R1-2may19.pdf
[8] Webpage: https://cloud.oracle.com/opc/saas/iotam/ebooks/oracle-iot-asset-monitoring-cloud-ebook.pdf

4. Limble Modular IoT Predictive Maintenance[9]

With Limble you don't have to spend $50,000+ or months' worth of time to figure out if a Predictive Maintenance strategy right for you. Limble's Modular IOT approach allows you to quickly, easily and cheaply test if a Predictive Maintenance strategy will work in your facility.

- Plug and play sensor setup.
- Instant alerts when sensor levels reach unacceptable thresholds.
- Automatically triggered corrective tasks to your maintenance team when certain thresholds are met.
- Mundane data entry tasks eliminated.
- Get real time actionable data that trends over time allowing you to make precise analysis such as root cause analysis.
- A test program implemented and proven for under $1000.

3.7. Proactive maintenance

Proactive maintenance is any form of maintenance that is done before any significant breakdowns or failures occur. As opposed to reactive maintenance, it focuses on anticipating and managing machine failures before they take place. To achieve that, a proactive maintenance strategy requires to identify the root causes of a failure that can be removed, to determine potential failure locations and to avoid breakdowns caused by deteriorating equipment conditions. In short, proactive maintenance aims at correcting the root source of the error, rather than the error itself:

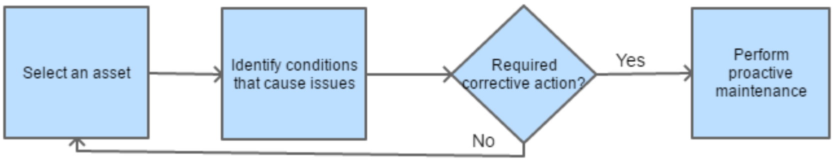
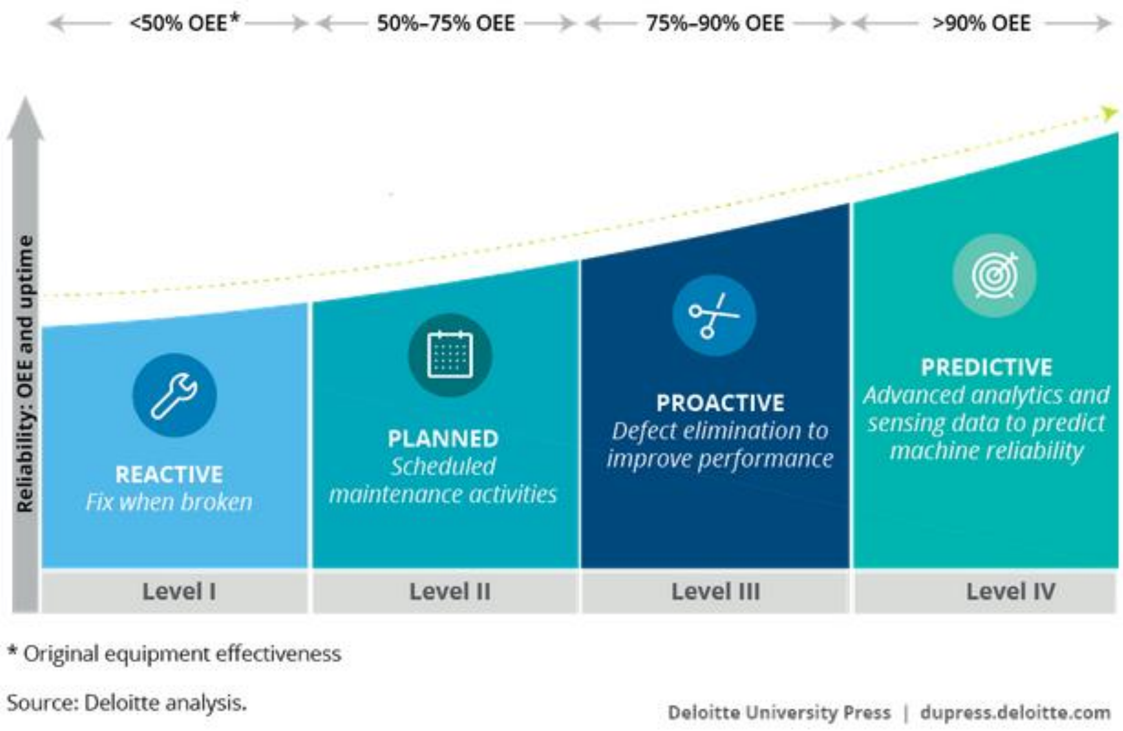

Select an asset
Identify conditions that cause issues
Required corrective action?
Yes
No
Perform proactive maintenance

Figure 11 Proactive Maintenance

Whereas reactive maintenance focuses on repairing equipment only after it has failed, and planned maintenance on substituting pieces of equipment at regular intervals, proactive maintenance aims at identifying the potential problems that would eventually lead to equipment breakdowns. Those potential problems can be improper machinery lubrication, contamination, misalignments or environmental conditions.

Proactive maintenance is the penultimate step in the maintenance strategy continuum, only behind predictive maintenance, which has only become possible recently thanks to the use of smart technologies that allow to unite physical and digital assets [1]:

[9] Webpage: https://limblecmms.com/predictive-maintenance-software.php



* Original equipment effectiveness

Source: Deloitte analysis.

Deloitte University Press | dupress.deloitte.com

Figure 12. Maintenance strategy continuum

3.7.1. Advantages and challenges

Having a successful proactive maintenance policy in place typically helps reducing the amount of times organizations have to perform maintenance tasks. Besides, having a clear idea of the most likely failure points implies fewer unnecessary repairs, lower wear and tear in the most sensible components, less need for keeping an inventory of spare parts and longer lifespan of equipment, ultimately reducing costs for the company. In turn, a proactive maintenance strategy comes with certain challenges, such as the need for organizational changes or increased training for employees [1]:

Table 5. Benefits and challenges of proactive maintenance

Benefits:	**Challenges**:
• Longer lifespan of equipment	• Ongoing maintenance and monitoring
• Decreased downtime, both planned and unplanned	• Need for organizational changes
• More cost effective than other maintenance strategies	• Increased training required
• Lower spare parts inventory	

3.7.2. Implementation of proactive maintenance strategy

The approaches followed for predictive and preventive maintenance can also help building a proactive maintenance strategy: collecting baseline data, tracking trends and analyzing the data produced after a certain fault is detected can, on its own, help companies perform maintenance only when necessary. At the same time, a proactive strategy increases the efficiency of predictive and preventive maintenance by aiding in the avoidance of the root causes of machine failure, addressing problems before they cause failure, and extending machine life.

However, the biggest challenge to implement a proactive maintenance program lies in deciding what amount of resources will be directed to maintenance. Ideally, data from all healthy and faulty equipment should be analyzed to determine when a certain component will fail. Since the majority of organizations do not have unlimited resources, the challenge consists in deciding which failures pose the biggest risk to the company.

To that end, it is helpful to assess the criticality of each asset the organization has. Instead of using only “critical” and “non-critical” as classification options, four different categories should be used, attending to the impact that asset has on the company’s ability to generate revenue [2]:

- **Star athletes**: these are the assets that directly determine the ability of an organization to win and by how much. In addition to uptime and downtime, performance and company’s revenue are directly related, so any performance improvement translates into additional revenue. Thus, these assets should be constantly monitored, regardless of their age.
- **Critical assets**: critical assets must be up and running for a company to obtain benefits from them. For this type, uptime is the key performance indicator, so it is critical to be able to anticipate pending failures.
- **Semi-critical assets**: these assets do not necessarily stop production when they are down, but they do strain the system, increasing labor costs and slowing down production.
- **Non-critical assets**: they do not affect the revenue of the company, no matter how big, expensive or complex they are. They do need to be fixed eventually though.

4. Scientific State of the Art

4.1. Fault Prediction and Root Cause Analysis

Fault detection and isolation (FDI) is a pertinent and challenging problem in many areas of engineering [38]–[42]. Fault detection involves determining if something is wrong with the system and fault diagnosis concerns itself with identifying the source and nature of the fault [43]. FDI is closely related to fault detection and diagnosis (FDD), in the sense that both fields aim to detect discrepancies between observed data and the predictions made by the models built for fault detection [44].

The term *fault* refers to malfunctions in one or several components of a technical system (power stations, airplanes, automobiles, etc). They may affect core parts of a system, such as motors and pumps, or peripheral devices, like sensors and actuators, that connect the main system to control, monitoring or other computerized systems. *Failures* are extremes cases of faults, when a malfunction is severe [44], [45].

The simplest form of FDI consists in implementing an alarm system, whereby measurements of different of individual parameters are compared to pre-set limits [45]. More sophisticated FDI methods are based on hardware redundancy or analytical redundancy. Hardware redundancy consists in measuring the same parameters using more than one sensor and then comparing the different signals by means of signal processing methods, such as Fourier analysis, spectrum analysis or wavelet analysis, among others. Analytical redundancy methods are based on mathematical models of the system and can be divided in quantitative, or model-based, methods and qualitative, or artificial intelligence-based, methods. Since these methods don't require any hardware, they are easier and less expensive to implement. However, analytical redundancy methods must deal with issues like noise, model uncertainties and other disturbances [44], [45].

4.1.1. Fault Detection/Prediction

Alarm Systems

Alarm systems work by comparing measured values with their theoretical thresholds. These systems can be implemented using upper and lower limits or only upper limits and may have one or two alarm levels. Albeit simple to implement, alarm systems have limited fault specificity as well as sensitivity. A fault in a single component can cause several parameters to exceed their thresholds and a specific alarm might be related to several faults. Additionally, in a real-world scenario the "true" limit of a given output parameter depends on the system's input and might differ significantly from its theoretical value. For an alarm system to be reliable, the alarm thresholds need to be set conservatively high [45].

Alarm systems are simple when compared to hardware and analytical redundancy methods, but that is precisely why they are still widely used in industrial applications, in spite of their limitations [45].

Analytical Redundancy – Model-based Methods

There are basically three types of faults: actuator faults, sensor faults and component faults. As the name implies, sensor and actuator faults refer to faults in the sensors and actuators of the system and are usually modelled as additive faults, while component faults represent changes in the system's parameters and are modelled as multiplicative faults [44], [46].

The first step in model-based FDI consists in generating a set of residuals. The residual of an observed value is the difference between the observed value and the estimated value of the quantity of interest. The generation of residuals is, therefore, based on a mathematical model of the system, which may reflect the basic physics of the system or may be based on past experience or observations [44], [46].

In the absence of faults, the residuals should be zero or have mean equal to zero. Deviation from zero should thus represent the occurrence of a fault. However, due to errors and uncertainties in parameters, mathematical models often don't represent the system accurately. Additionally, the system is affected by noise and other perturbations. This causes the residuals to be non-zero, even when no fault has occurred, in which case they aren't useful in practical applications [44], [45]. As a result, several methods to generate robust residuals that are insensitive to noise and uncertainties, while being maximally sensitive to faults, have been developed. These include the full-state observer-based methods [47], the parameter estimation methods [48] and the parity relations method [49], among others.

To reduce the effects of noise, the following action may be taken [45]:

- *Residual filtering* consists in using moving averages of the residuals or applying low-pass filters to the residuals. It's also possible to incorporate low-pass behaviour into the residual generators.
- *Statistical testing of the residuals*: the testing thresholds are determined either by making assumptions about the source of the noise, or by using measurements taken under no-fault conditions.

Disturbances to the system can be dealt with by designing the residuals to be insensitive to them. However, this is dependent on knowing the disturbance-to-output transfer function and is also subject to a trade-off with fault isolation enhancements. As such, if there is a large number of disturbances or if their transfer function is unknown only an approximate solution will be possible[45], [46].

Reducing the sensitivity of the residuals to model errors is the most important challenge to model-based FDI. As in the case of disturbances, it can normally only be achieved by approximate solutions, but reducing the sensitivity of the residuals to modelling errors also tends to reduce their sensitivity to faults[45], [46].

After the residuals have been generated, the next step in FDI consists in determining if a fault has occurred (fault detection) and what type of fault it is (fault isolation). Fault detection can be performed by testing for significant changes in the residuals. The simplest way of achieving this is by comparing a residual vector to a constant threshold [44]. There are, however, other methods that combine the history and trend of the residuals with statistical test techniques to produce more robust results, such as the *sequential probability ratio test* (SPRT) [50], the *CUSUM* algorithm [51] or the *generalized likelihood ratio test*.

Analytical Redundancy – Artificial Intelligence-based Methods

The fault detection methods described in the previous section are based on control and statistical theories. However, artificial intelligence (AI) methods, like machine learning and data mining models, can also be employed to detect and, particularly, predict faults. In fact, efforts have been made to combine the knowledge and methods from both fields and develop innovative solutions to the problem of fault detection and isolation [44], [52], [53].

Machine Learning approaches commonly used for fault detection and prediction include *artificial neural networks* [40], [54], *support vector machines* [39], [55] and *decision trees* [41]. These and other machine learning models used for fault prediction will be described in detail in sections 4.1.2 and 4.1.3.

4.1.2. Root Cause Analysis

Root-cause analysis (RCA), also known as fault diagnosis, is a method of solving problems that tries to identify the failure mechanisms or the fundamental causes of faults or problems. This is also referred to as *fault isolation*, especially when emphasizing the distinction from fault detection.

Since a fault can propagate between elements of the system, it's important to determine its root cause and propagation pathways, understanding the system's topology and the causality between variables [56]. To identify a fault, the residuals generated by the model-based methods described above need to not only be sensitive to faults, but also be able to distinguish between types of faults. One way to facilitate the isolation of faults is by performing enhancement manipulations on the residuals. The most commonly used techniques are [44], [45]:

- *Structured residuals sets:* in the event of a fault, only a specific subset of residuals become non-zero;
- *Directional residuals*: the response to each particular fault is confined to a fault-specific direction in the space of residuals. Isolating a fault becomes a matter of determining the direction of the residual vector;
- *Diagonal residuals*: each residual is sensitive only to a particular fault.

Graphical models may also be used to model the causality in the system. For example, *signed directed graphs* (SDG) represent the system's parameters as graph nodes and the causal relations as directed arcs [56], [57]. Other causal graphs, such as *bond graphs* and *temporal causal graphs* can also be used [58]–[60]. Moreover, the knowledge used to build a SDG can also be represented by a *rule-based model* [61]. *Ontologies* are another way of representing the system, by which the relationships between resources are defined by the taxonomy of classes and subclasses, and the directed logic relationship is described by their properties. [56]. Additionally, root cause analysis can also be performed by analysing historical process data with methods such as *cross-correlation analysis* [X], *Granger causality* or *Bayesian nets*, among others [56], [62]–[64].

4.2. Data Science

As stated before, Big Data's general definition is a collection of protocols, techniques, and infrastructures for storing, processing, and managing large amounts of data [65]. However, there is no commonly accepted definition for such a term. Nonetheless, this data for itself has no value. Consequently, when we mentioned the example of the Rolls Royce manufacturing, the extraction, and storage of data performed by nanobots was in the Big Data field. However, the actual knowledge from that data would be in the domain of data science.

Data science will play a very important role in predictive maintenance in machine centres owing to their complexity and high machining precision.

There is still a need for interpreting them and drive to conclusions out of them. The set of models, scientific methods, and use technologies to extract the value for the data is data science. Data science employs technologies like machine learning to obtain knowledge from data, as well as techniques like data mining [66]. There are thousands of algorithms involved in data science, describing all of them may be an intricate task, and not very useful for the reader.

Nevertheless, it is possible to assume that all the algorithms and technics have a set of principles of data science in common. Following and understanding the before-mentioned principles will heighten the prospects of success.

4.2.1. Evaluation criteria

One of these postulates, and perhaps the most important of them, is the evaluation criteria. Big Data algorithms have performed pre-filtering, which has eliminated redundant and corrupted data. However, it is now time for correlating variables and establishing the value of the data. There are many suitable manners to perform such a task. For this reason, it is crucial to decide the most performing algorithm. There are four general criteria to determine which algorithm is more suitable for the data mining process [67]:

1. Performance: In terms of time, it is very significant to select algorithms that induce to conclusions satisfying time requirements. For this reason, too slow algorithms must be discarded. In addition to the value of the data, it is important to be able to use it at a suitable time.
2. Data utility: The utility of the data after having done all the transformations, it can be equivalent to the information loss caused by all the data processing. The more relevant parameters that we can use, the better the algorithm is.
3. The level of uncertainty: We can define it as the amount of hidden information you can still predict by the information given, we are interested in reducing the level of uncertainty as much as we can.

Resistance to data mining techniques: We must not forget that the owners of some datasets protect them from data mining. Ciber terrorist and sometimes, even the competence often extract knowledge from datasets with malicious outcomes.

4.2.2. Data Science in predictive maintenance

We can briefly describe predictive maintenance is log-based maintenance. The key is using some Artificial Intelligence algorithms like machine learning, and the input is processed data provided by Data Science algorithms. Predictive maintenance must fulfil a set of requirements to be truly useful for users and stakeholders.

One of the most important features is the timing of an alarm. It is quite useful to have an idea of when failures should be occurring. In that approach, it is feasible to detect irregular situations. Furthermore, the alarm timing has dual functionality, as it works to evaluate the state of equipment [66].

There are three intervals in the alarm timing, which indicate three states of the equipment [3]:

1. Predictive Interval: It is the time interlude, that should pass right before a fault occurs. A fault alarm in this period will have the reparation ready. That is something advantageous because the devices will consume a shorter period unavailable for staying under reparation.
2. Infected Interval: It is the time passed right after the fault occurs. As stated before, the equipment remains unavailable until the reparation is complete, so the model should consider making this period as brief as possible. Data obtained during this interval should not be reflected in the model, because during part of this interval, the machinery will not be working correctly.
3. Responsive Duration: It is the time that passes between the performance of reparation and the time until the confirmation that the machine is able for suitable performance.

The model must be robust and precise. Data science will take information both from the environment, and the engineers, and it will set the intervals accurately.

Another important feature of a good predictive maintenance model is the interpretability [4]. Interpretability is the quality of being reviewed by experts. For this purpose, it is crucial to have an understandable model. There should not be too many variables so as not to use extra variables that are not necessary to describe the system´s behaviour. However, there should be enough to make the model explicative enough.

It is crucial to have a clear idea of the importance of every variable in the model. In that fashion, the model will be clean, explicative, and scalable. There is a direct implication of Big Data and Data Science techniques in such a task, from extracting the information from structured and unstructured sources to interpret the mining of the processed information using Data Science algorithms.

4.2.3. Examples of the use of Data Science in predictive maintenance

The use of information as an asset is becoming a cornerstone in modern enterprises, we have seen in the last section how Rolls Royce has utilized Big data and data science for their predictive maintenance. It may not be a surprise that data science is a technique that most of the modernized manufacturers employ to keep their equipment in the most suitable conditions possible and not to lose performance or waste energy.

In this section, we are going to focus not only on the methods for extracting the information but also on the value obtained from it.

For instance, Hyundai Motors, one of the most cutting-edge car manufacturers implemented an *AI Car Diagnosis Systems* which prevents knocks and car faults [68].

These systems use data mining techniques together with Artificial Intelligence for preventing the impact of noise in the deterioration of car manufacturing. Furthermore, the system has been recently installed in their reparation center in Korea this year for enhancing the performance of reparations and to find faults in recently produced vehicles. As a result, Hyundai will be able to improve production and reducing the costs of it, which will result in a considerable profit.

As said before, Bosch [69], which is one of the most prestigious manufacturers in Europe, is also a representative case of a corporation, that uses Data science for its predictive maintenance.

Bosch has deeply integrated into Industry 4.0. As a result, their factory floors are highly IoTized, yet they can maintain an excellent rate of production, and seldom their equipment has faults. It is all due to their support system. This system has a very simplistic green/red light system to deliver the wired and wireless elements on their manufacturing chain. Such a system has a double function, on the one hand, it enables and fastens the connection between IoT devices. On the other hand, it delivers the status of the elements in the supply chain to the staff to give some decision support.

For maintenance, BOSCH utilizes *Nexeed* Production Performance Manager, which is a tool that collects data from structured and unstructured sources, and after using a set of algorithms it provides some graphic information for decision support.

The third vital requisite to have robust models in predictive maintenance is Handling the imbalance, failures in a determined environment must not be something frequent [70]. On the contrary, there will be orders of ten thousand cases of observed failures in some of the environments. From very rare instances, the model should find very general and accurate behavioural patterns, which are difficult to find and reproduce. For this reason, not only it is needed to have efficient data methods, but also it is required to have some learning algorithms. There are, of course, other important features that are important to consider defining behavioural patterns, such as cost reduction, defining the fault tolerance and the business model.

4.2.4. Data Pre-Processing

A hard problem on data science is to obtain data from a huge variety of sources when the integration is not properly performed redundancies and inconsistencies. Matching all the sources can be hard to perform. Data pre-processing takes a long time and it is often faster to do the pre-processing in external files [66].

Redundancy is a problem that should be avoided, it makes the datasets grow unnecessarily and hampers scalability in big data techniques [7]. Redundant attributes are the major field for optimization in datasets. An attribute is considered redundant when it can be derived from other attribute or from a combination of sets of attributes. The most common techniques to find inconsistencies are correlation analysis such as chi squared. In case of numerical attributes, a high correlation in value usually means that they are redundant or a combination of several numerical values.

After the redundancy checking it is important to check if data is correct or not. Data must be correct and consistent and fulfil the standards of representation. More concretely in case of predictive maintenance data is stored in the warehouse in order to do the previously mentioned step for data pre-processing. In regular factory floor operations datasets are huge and redundant and they take advantage of the processes of cleaning, redundancy elimination, integration and feature extraction [8]. All such process occurs in the warehouse.

4.2.5. Machine Learning

As stated, before data needs to be formatted in a manner that is feasible for being used as an input for machine learning algorithms. In most of predictive maintenance examples data is presented in a way in which rows represent examples to predict or learn from, and columns represent variables, including both Predictive Variables and Goals [9]. In the following paragraphs the key concepts in machine Learning and predictive maintenance will be described.

A goal variable is the feature of the system which must be predicted, for instance, a goal variable would be the life cycle of an asset. Depending on how Goal variables are computed, it will determine the size of the training datasets. In other words, the more efficient are goal variables, the less computing time they will need.

Next task consists of defining which of the variables taken are suitable examples for training, for instance, if the goal variable is life cycle of an asset, it is necessary to define which previous information needs to be considered for take as training examples. Later, a statistical analysis must be carried out, all collinear variables will be eliminated. In this point we have, the goal variable and a suitable number of training examples which will serve as an input for running the algorithms.

Predictive algorithms are extremely useful in the domain of predictive maintenance [9]. Firstly, they are the main asset to predict the failure time and therefore calculate when a piece of Equipment’s should be replaced. Secondly, machine learning is the manner to be constantly adapted to the new changes in the factory floor, which allows the stakeholders view the results in the changes performed. Finally, predictive analysis machine learning algorithms serves for identifying which variables are important in the performance, deterioration and life cycle of the assets, which is a real powerful for decision support.

4.2.6. Big Data Analytics

Big data has a descriptive task in predictive maintenance, in order to draw to conclusions using existent data, it is necessary to identify patterns in values. As a result, the true impact of some variables and the hidden relationships among certain variables that may look not evident at first glance. The kinds of analysis offered by Big Data are the following: [71]

- Classification analysis: it consists of building a model for prediction based on predefined sets of classes, the instances for this classes will be classified using IF-THEN-ELSE clauses. Decision trees are a good example of such kind of technology.
- Clustering analysis: Clustering analysis is the process of separate data into groups of different objects, it is very useful to find certain characteristics that can separate the data into different categories, concretely in predictive maintenance, this kind of analysis is made to find the possible causes of faults.
- Association analysis: Association models is commonly used for identifying when certain events may occur. These algorithms are commonly accompanied with certain level of confidence which serves for identifying how reliable results are.
- Regression analysis: Regression analysis serves to find the relationship between a dependent variable with several independent variables. The output will be a predictive analysis and the weight of all the independent variables in the function.

As it has been shown in this section, Big Data Analytics can provide fully explicative models in predictive maintenance. Despite that fact, the analysis and management of such huge amounts of data is quite time-consuming and not-fully optimized. Even though Big Data optimization is a cutting-edge field for study, there is still a considerable compute time used in activities with no value.

4.3. Simulation and Industry 4.0

Probabilistic models have long been used to simulate real-world scenarios [72]. Computer models are frequently used for simulation purposes in manufacturing systems, allowing for a study of their products and equipment characteristics and lifecycles. The quality of these simulations depends on how closely these models can mimic reality and, therefore, better models are born of the proper identification and characterization of the different behaviours and variables that can affect the system and how these affect each other.

4.3.1. Simulation Models

Simulation aims to imitate – or model – how a given system operates, and if and how its behaviour evolves over time. Using simulation is it possible to assess whether the underlying assumptions concerning a system were true – by comparing the outputs of the simulation with real events – and to predict eventual real effects of changes to the system, such as alternative scenarios, among other things [73].

Static simulations do not take in consideration the time factor, if the system always behaves in a similar fashion. Dynamic simulations, on the other hand, evolve over time, and therefore how and what changes can happen must be accounted for. If changes are continuous, it is considered a continuous simulation; if between two states changes to the system are to be disregarded, it is called a discrete simulation – i.e., a simulation is a transition between states. These transitions may be the consequence of events – in the case of event-driven simulation – or the progress of time – i.e. time-stepped simulation [73].

When it comes to how randomness is considered in the simulation, it can happen in either a deterministic or stochastic fashion. In a deterministic simulation, running the simulation with the same parameters is guaranteed to generate the same result; contrarily, in the stochastic approach, a randomness factor is added, meaning that different results can arise.

While simulation can be done in any programming language and adapted to the particular needs of specific scenarios, there are a number of generic simulation tools to help design and run simulations for industry scenarios, such as *Anylogic* [74], *Arena* [75], *FlexSim* [76], *ProcesModel* [77] and *Witness* [78].

As far as predictive maintenance is concerned, the wear down of equipment is one of the main issues to address. In simulation, the degradation of physical objects – such as machines and their components – can be modelled in different ways. More traditionally, physics-based models were used to compute possible alterations in components over time [79][80]. These are often based on the initial conditions on the system and expected wear rates, and do not take in consideration major unexpected events that could shift the equipment's status and, therefore, the wear down processes.

Applying real data to the simulation makes it possible to assess if its predictions/results are accurate and, therefore, useful [81]. The growing sensorization of equipment brought by the advent of Industry 4.0 and the Internet of Things allows for collecting and fusing more real data about the equipment and generate a more realistic picture of its condition [82]. If this data can be processed and used to generate models, more reliable forecasts can be obtained – straightening the gap between the digital simulation and its real counterpart. However, this also means that the data grows continuously over time and that regular probabilistic approaches may not be suitable; in order to tackle this situation, more intelligent approaches have been proposed, such as the use of machine learning and data mining algorithms. These allow the simulation to evolve over time as more real data is known, and thus assessing possible wear trends and even recognizing when the behaviour of the physical assets is off the norm [81].

4.3.2. Simulation and Cyber-Physical Systems

Cyber-physical systems are an important part of the Industry 4.0 and, i.e., how machines and software communicate and take advantage of each other is of particular importance. Software can be used to substitute physical interaction with machines, as often happens in digital dashboards that can be used to switch machines on and off, or alter the tasks being performed. In order to take full advantage of the capabilities provided by Cyber-Physical Systems and the Internet of Things, proper data models of those are required [83].

Simulation models find application in Cyber-physical systems in different ways, including but not limited to: (1) Augmented and Virtual Reality, (2) Computer Aided Design, Manufacturing and Process Planning, (3) Enterprise Resource Planning, (4) Digital Mock Up, (5) Lifecycle Assessment, (6) Product Data Management, (7) Ergonomics Simulation, (8) Manufacturing Executing Systems, (9) Supervisory Control and Data Acquisition and (10) Supply Chain Simulation.

4.3.3. Predictive simulation applications

Predictive simulation can be used to assess the consequences of changes in the environment, such as the addition/removal of machines, unexpected machine failure and changes to policy or production processes. Different possible uses are outlined in [83], and include but are not limited to:

- Monitorization of anomalies (e.g. fatigue) in the physical counterpart by comparing with the simulated version;

- Monitorization of material deformation;
- Life-cycle simulation: what are the expected changes on the equipment during its lifecycle and how the real components deviate from them [79];
- Assessment of possible design flaws before they are implemented in the physical system (prognostic assessment at design stage);
- Study of long-term behaviour: predict future performance and compare it to actual performance;
- System optimization both during design phase and of its future activities;
- Training operators on a virtual environment, preventing potential damage to the machines and diminishing human error;
- Maintenance activities can be evaluated before they are put into action by assessing their effectiveness and consequences to the Digital Twin;
- Optimization of duty cycles and activity coordination between systems.

4.3.4. Digital Twin

Using real data and simulation processes to improve decision making processes gave rise to the concept of "Digital Twin". The first definition of Digital Twin is provided by NASA, stating: "an integrated multi-physics, multi-scale, probabilistic simulation of a vehicle or system that uses the best available physical models, sensor updates, fleet history, etc., to mirror the life of its flying twin. It is ultra-realistic and may consider one or more important and interdependent vehicle systems". As research on the topic progressed beyond the field of aeronautics and into that of Cyber-physical systems – and the sensorization of equipment became more ubiquitous – the definition was updated in order to make the role of feeding real-data in real-time into the model more evident.

According to [83], a Digital Twin consists of "a virtual representation of a production system that is able to run on different simulation disciplines that is characterized by the synchronization between the virtual and real system, thanks to sensed data and connected smart devices, mathematical models and real time data elaboration". As the synchronization between virtual and physical system grows, the potential of Digital Twins for the study of the life cycle, prognostic and diagnostic also becomes more established.

The level of integration of real data and the model can be used to establish different subcategories of Digital Twins, as proposed by [84]:

- Digital Model: consists of a digital representation of the physical entity which has no direct contact with its physical counterpart (e.g. mathematical models). Real data from the physical system can be used, but it is supplied to the digital model manually (i.e. not automatically collected). As such, changes in the physical asset have no impact in the digital model.
- Digital Shadow: digital representation of the physical entity where real data from the physical version is automatically transferred. As such, any events or changes that affect the physical version will also affect its Digital Shadow.
- Digital Twin: the data can flow automatically between digital and physical versions of the system. Events affecting the physical asset will equally affect its digital version, and changes to the digital version will be propagated to the physical.

As such, the potential of the Digital Twin as a tool to help studying the behaviour and life cycles of physical systems has become more prevalent as the synchronization between virtual and physical systems grows.

4.4. R&D projects

The current section will feature a number of recent and ongoing Research and Development (R&D) projects focusing on themes similar to those of Pianism. All of the following projects have, at least, dedicated some time and effort to predictive approaches to maintenance, in an effort to facilitate the implementation and application of these approaches in the industry.

4.4.1. InValue: Industrial Enterprise Asset Value Enablers

The main goal of InValue is to make use of emerging Industry 4.0 technologies to promote the change from traditional maintenance practices to more proactive ones in the automotive sector. The InValue platform relies on existing standards combined with novel and integrated solutions for the content and knowledge management of heterogeneous information derived from various sources. Every process the data must go through is addressed by the platform, including information acquisition and aggregation, representation, analysis and exchange between smart devices, automation systems, and information systems.

Consortium:

- Portugal: *Sistrade Software Consulting; ISEP/IPP-GECAD; Evoleo; ISQ; Facort*
- Belgium: *SIRRIS; Barco N.V.*
- Spain: *DATAPIXEL; Engine Power Components G.E., S.L.; Asociación de empresas tecnológicas Innovalia; Unimetrik*
- Turkey: *Acd Bilgi Islem ltd.sti.; Ericsson Arastirma Gelistirme ve Bilisim Hizmetle; Hisbim Bilgi ve Iletisim Teknolojileri; Turkgen*

Duration: June 2016 – December 2018

Webpage: http://www.invalue.com.pt/

4.4.2. SMART-PDM: A Smart Predictive Maintenance Approach based on Cyber Physical Systems

Under the advancement of Industry 4.0, manufacturing is undergoing massive and fast changes. Data acquisition is a fundamental step for diagnosis and prognosis tasks - SMART-PDM's objective is to acquire this data in a financially feasible fashion, lowering costs with maintenance, waste and parts, while also improving product quality and equipment health. Any technological insights validated by the demonstrations will improve existing technologies, add to existing know-how and be applied to future solutions by the various consortium members.

Consortium:

- Finland: *Caverion Suomi Oy, Teollisuuden Ratkaisut; Junkkari Oy; Nome Oy; Ramentor Oy; VTT Technical Research Centre of Finland Ltd.; Wapice Ltd.*
- Portugal: *ISEP CISTER/INESC-TEC; SONAE; Virtual Power Solutions, S.A.*
- Romania: *BEIA Consult International; Societatea de Inginerie Sisteme SIS SA*

- Spain: *CTI SOFT, S.L.; Danobat; Fundacion Tecnalia Research & Innovation; Ideko; IK4-LORTEK; Mondragon Assembly S. Coop; Savvy Data Systems S.L.; ZAYER, S.A.*
- Turkey: *ANADOLU ISUZU OTOMOTİV SAN. TİC. A.Ş.; BitNet Bilişim Hizmetleri Ltd Şti; Enforma Information and Communication Technologies A.S.; KOCAER ROLLING MILL; Netas Telekomunikasyon A.S.; Zorlu Enerji*

Duration: Dec 2018-2020

Webpage: http://www.beiaro.eu/smart-pdm/

4.4.3. DayTiMe: Digital Lifecycle Twins for predictive maintenance

Recently, Digital Twins are advanced a solution for the Predictive Maintenance issue in Smart Manufacturing. While proposals for it are commonly found in literature, very few functional examples of Digital Twin can be found in the industry. DayTiMe aims to fill this gap by integrating findings and solutions from 14 industrial use cases and using a generic value chain model.

Consortium:

- Belgium: *CMI; SIRRIS; Yazzoom*
- Netherlands: *Datenna BV; Eindhoven University of Technology; Philips Electronics Nederland B.V.; Philips Consumer Lifestyle; Philips Medical Systems Nederland B.V.; PS-Tech BV; Target Holding; University of Groningen*
- Turkey: *Havelsan; Mangodo Dijital Pazarlama ve Reklam Çözümleri Tic. Ltd. Şti.; Simeks Tıbbi Sistemler A.S.; Tazi Bilişim Teknolojileri A.Ş.; Triatech Tıbbi Sistemler Tic. ve San. A.S.; Turkcell Teknoloji; V.A.S. Telekom*
- United Kingdom: Centre for Factories of the Future Ltd

Duration: January 2019 – December 2021

Website: https://www.eurekanetwork.org/project/id/17030

4.4.4. CyberFactory: Addressing opportunities and threats for the Factory of the Future (FoF)

The goal of CyberFactory is to facilitate the design, development, integration and demonstration of enabling capabilities to enhance and optimize the resilience of the Factories of the Future. Pilots from Transportation, Automotive, Electronics and Machine manufacturing industries will be addressed, and applied to different use cases such as statistical process control, real time asset tracking, distributed manufacturing and collaborative robotics. Preventive and reactive approaches to security and safety concerns will also be proposed, such as blended cyber-physical threats, manufacturing data theft or adversarial machine learning.

Consortium:

- Canada: *Bluewrist Inc.*
- Findland: *Bittium Wireless Ltd.; High Metal Oy; Houston Analytics Oy; Netox Oy; Rugged Tooling; VTT Technical Research Centre of Finland Ltd.*
- France: *Airbus; Airbus CyberSecurity SAS France; IRT SystemX; LAAS-CNRS; Uwinloc;*
- Germany: *Airbus Cybersecurity GmbH; Aviawerks; BIGS; Bombardier; Fraunhofer AISEC Institute; HTW Berlin University of Applied Sciences; InSystems Automation GmbH; OFFIS*

- Portugal: *IDEPA INDÚSTRIA DE PASSAMANARIAS, LDA; ISEP; SISTRADE Software Consulting, S.A.*
- Spain: *Airbus Defence & Space; ENEO TECNOLOGÍA, S.L; Innovalia Association; Nextel; PAL Robotics; Trimek;*
- Turkey: *GOHM Electronics and Computing Systems Ltd; Lostar Information Security; Vestel*
- United Kingdom: *Accelerite*

Duration: December 2018 – June 2022

Website: https://itea3.org/project/cyberfactory-1.html

4.4.5. Maintenance 4.0: Intelligent and Predictive Maintenance in Manufacturing Systems

The project aims to develop integrated and intelligent solutions for industrial maintenance, aligned with Industry 4.0 principles, considering the following aspects are considered: i) advanced and online analysis of collected data for the earlier detection of failures, and ii) intelligent decision support systems to support technicians during the maintenance interventions. Maintenance 4.0 project constitutes a real-world implementation of intelligent and predictive maintenance through the development of advanced data analytics applications, which will enable the reduction of the unplanned down times by predicting possible failures.

Funded by: Norte 2020

Consortium: *Instituto Politécnico de Bragança, Instituto Politécnico de Viana do Castelo, Instituto Politécnico do Cávado e Ave, Catraport*

Duration: October 2017 - September 2019

Website: http://maintenance40.ipb.pt

4.4.6. PreCoM: Predictive Cognitive Maintenance Decision Support System

Cheaper and more powerful sensors, together with big data analytics, offer an unprecedented opportunity to track machine-tool performance and health condition. However, manufacturers only spend 15% of their total maintenance costs on predictive (vs reactive or preventative) maintenance.

Funded by: H2020-EU.2.1.5.1.

Consortium: *e-maintenance sweden ab,paragon anonymh etaireia meleton erevnas kai emporiou proigmenhs texnologias, savvy data systems sl, vertech group bosch rexroth ag, soraluce s. Coop., sakana, sociedad cooperativa, overbeck gmbh, spinea sro, goma camps sociedad anonima, lantier sl, ideko s coop, commissariat a l energie atomique et aux energies alternatives, consorcio instituto tecnoloxico matematica industrial itmati, technische universitaet muenchen, technische universitaet chemnitz,*

Duration: 1 November 2017 - 31 October 2020

Website: https://cordis.europa.eu/programme/rcn/701830/en

4.4.7. SERENA VerSatilE: plug-and-play platform enabling remote pREdictive mainteNAnce

The growing complexity of modern engineering systems and manufacturing processes is an obstacle to concept and implement Intelligent Manufacturing Systems (IMS) and keep these systems operating at high levels of reliability. Additionally, the number of sensors and the amount.

Duration: 1 October 2017 to 30 September 2020

Funded: H2020-EU.2.1.5.1.

Consortium: *finn-power oy, vdl weweler bv, whirlpool emea spa, kone industrial oy, engineering - ingegneria informatica spa, oculavis gmbh, synarea consultants srl, emc information systems international, panepistimio patron, fraunhofer gesellschaft zur foerderung der angewandten forschung e.v., teknologian tutkimuskeskus vtt oy, trimek sa, politecnico di torino*

Website: https://cordis.europa.eu/project/rcn/211752/factsheet/en

4.4.8. PROPHESY: Platform for rapid deployment of self-configuring and optimized predictive maintenance services

The advent of Industry 4.0 provides opportunities for adopting predictive maintenance (PdM), which represents the ultimate maintenance vision for manufacturers and machine vendors. Nevertheless, there are still barriers to successful deployment including the issues of data fragmentation, limited data interoperability, poor deployment of advanced analytics and lack of effective integration with other systems at the enterprise and field levels. PROPHESY will deliver and validate (in two complex demonstrators) in real plants a PdM services platform, which will alleviate these issues based on the following innovations:

- A CPS platform optimized for PdM activities (PROPHESY-CPS), which will enable maintenance driven real-time control, large scale distributed data collection and processing, as well as improved production processes driven by maintenance predictions and FMECA activities.
- Novel Machine Learning and Statistical Data processing techniques for PdM (PROPHESY-ML), which will be able to identify invisible patterns associated with machine degradation and assets depreciation, while at the same time using them to optimize FMECA activities.
- Visualization, knowledge sharing and augmented reality (AR) services (PROPHESY-AR), which will enable remotely supported maintenance that can optimize maintenance time and costs, while increasing the safety of maintenance tasks.
- A PdM service optimization engine (PROPHESY-SOE), which will enable composition of optimal PdM solutions based on the capabilities provided by PROPHESY-CPS, PROPHESY-ML and PROPHESY-AR. Service optimization aspects will consider the whole range of factors that impact PdM effectiveness (e.g., OEE, EOL, MTBF and more).

PROPHESY will establish and expand an ecosystem of PdM stakeholders around the PROPHESY-SOE, which will serve as a basis for the wider update of the project's results, as it will offer to the CPS manufacturing community access to innovative, turn-key solutions for PdM operations.

Duration: 1 October 2017 to 30 September 2020

Funded: H2020-EU.2.1.5.1.

Consortium: *philips consumer lifestyle bv, marposs monitoring solutions gmbh, jaguar land rover limited, industrial consulting automation research engineering, oculavis gmbh, unparallel innovation lda, fraunhofer gesellschaft zur foerderung der angewandten forschung e.v., nova id fct - associacao para a inovacao e desenvolvimento da fct, mondragon goi eskola politeknikoa jose maria arizmendiarrieta s coop, research and education laboratory in information technologies, technische universiteit eindhoven, sensap microsystems anonimi etairia ilektronikon systimaton kai efarmogon logismikou*

Website: https://cordis.europa.eu/project/rcn/211300/factsheet/en

5. Industrial State of the Art

5.1. Industrial IOT

As it is known [85], IoT is the network of connected objects that can build an aware, autonomous and actionable system. Just like the Internet of Things in general, the Industrial IoT consists of internet-connected machinery and the advance analytics platforms that process the real time data they produce. Sensor embedded devices or machines collect and transmit the data via the internet connectivity and then the software manages the data. Those IIoT devices range from sensors to complex industrial robots [85].

IIoT technologies are used in many industries and applications, including manufacturing (Industry 4.0), logistics, oil and gas, transportation, energy, mining, aviation, agriculture, healthcare, financial services, retail & advertising and other sectors that are similar to these industries [85]. It also includes consumer-facing applications such as wearable devices, smart home technology and self-driving cars.

On a larger scale, the IIoT is a key element of modern cloud computing with intelligent and self-optimizing industrial equipment or facilities. Therefore, IIoT can create game-changing operational efficiencies and new business models. Thanks to this technology, industries initially focus on the optimization of operational efficiency, real time remote monitoring and data driven automation. With this perspective, IIoT technologies create opportunities in automation, optimization, intelligent manufacturing, smart factory systems, remote asset management and maintenance capabilities [85]. Then, this led to creation of new revenue models and new ways of servicing customers as a result of industrial digital transformation.

Briefly, it has many benefits, but if we need to group the most important ones, they can be listed as follows: [85]

- **Operational Efficiency & Productivity:** One of the biggest benefits of the IIoT is the improvement in operational efficiency and productivity. Many companies are using it to automate business and manufacturing processes, remotely monitor assets and control operations or optimize supply chains. It let industrial systems continuously improve their operations and find new ways for cost-efficient autonomy.
- **New Business Models:** The IIoT is disrupting traditional business models and creating massive opportunities for companies to create new services based on real time sensor data information like machine learning and AI applications or robotic process automation.
- **Cost Efficiency:** Enabled with IIoT, separate parts of a production line communicate with each other in near real time and makes the entire manufacturing process much easier to remotely monitor and control. It allows tracking sensor data, detecting the earliest signs of malfunction, managing asset lifecycle and creating smart rules for autonomous device behaviour, and many more. Therefore, IIoT is reducing TCO (Total Cost of Ownership), including maintenance cost by reducing downtime and maximizing asset utilization.
- **Workforce Productivity & Safety:** Thanks to wearable and other IoT-enabled devices, workforce productivity and job satisfaction are increasing. The technology is helping

employees improve decision making, automate routine tasks, fast-track communication, and more.

- **Enhanced Customer Experiences:** From integrating customer care with actual product performance and usage, to delivering highly personalized products and services, the IoT offers many ways to create customer experiences across digital and physical worlds. Based on the analysis of collected sensor data and history record, decision-making process is largely improving by more precise root cause analysis, because the collected real-time and historic data is a rich source of actionable information. That results in a better customer service, satisfaction and loyalty.

As a result, the Industrial Internet of Things has strategic priority and critical importance for manufacturing companies as it allows them to give more value to their customers as well as improve cost-efficiency of their internal operations. Finally, IIoT promotes more flexible, open architectures that support greater customization and digital upgrades across lots of devices.

5.1.1. IOT Reference Model

Members of the Internet of Things World Forum (IoTWF)[10] consist of technology firms, industry visionaries, executives and educators and they are committed to accelerate the awareness and adoption of Internet of Things technologies. One of the resources of this community is whitepaper about IoT reference model from Cisco [86]. This paper aims to provide clear definitions and descriptions that can be applied accurately to elements and layers of the IoT platforms.

Before explanation of the reference model, it is more suitable to start with the IoT architecture components. Details about them can be found in the following titles but basically, IoT architecture is comprised of sensor nodes, gateways, internet with cloud (server) and visualization with control endpoints.

Based on this architecture, the proposed IoT reference model from IoT World Forum contains seven levels and defines how IoT system can be complete. Figure 13 shows these levels and data flow directions. Most of the IoT systems have bidirectional data flow. In terms of control pattern, information flows from the top to the bottom; however, in terms of monitoring pattern, data flow direction is reverse.

[10] https://www.iotwf.com

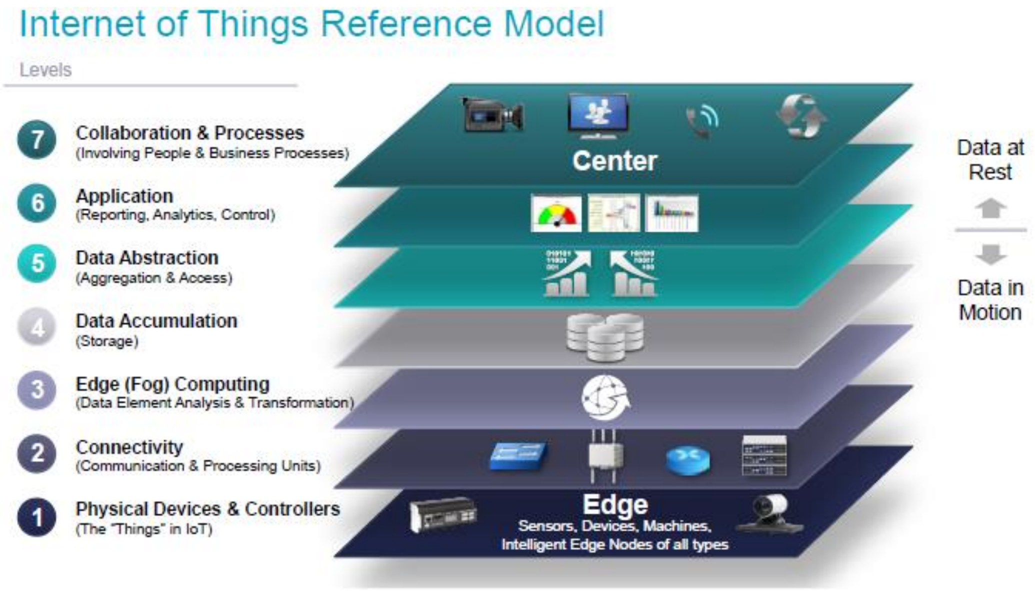

Internet of Things Reference Model
Levels
7 Collaboration & Processes
(Involving People & Business Processes)
6 Application
(Reporting, Analytics, Control)
5 Data Abstraction
(Aggregation & Access)
4 Data Accumulation
(Storage)
3 Edge (Fog) Computing
(Data Element Analysis & Transformation)
2 Connectivity
(Communication & Processing Units)
1 Physical Devices & Controllers
(The "Things" in IoT)
Center
Edge
Sensors, Devices, Machines,
Intelligent Edge Nodes of all types
Data at Rest
Data in Motion

Figure 13 – IoT Word Forum Reference Model
(Image Source: http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf)

Levels can be called like: 1 to 3 "edge-side layer", 4 to 6 "server/cloud-side layer", 7 "user-side layer": [86]

1. **Physical Devices and Controllers:** This starting level is also called the "edge level" and contains the actual "things" in the Internet of Things, such as sensors, devices, gateways and virtual objects. They are capable of generating data, being queried or controlled over the net, sending and receiving information.

2. **Connectivity:** Second level consists of the communication and processing units. It performs routing, switching and translation of protocols by facilitating communications between Level 1 devices and Level 2 connectivity equipment or across networks. Therefore, reliable and timely information transmission is the most critical function of Level 2. Security and self-learning network analytics are also provided at this level.

3. **Edge (Fog) Computing:** This level receives the network data packets and outputs information that is understandable and suitable for storage and higher-level processing at Level 4. It means that Level 3 focuses on high-volume data element analysis and transformation, data filtering, clean up, aggregation, packet content inspection and event generation.

4. **Data Accumulation:** The data that is sent over the internet via gateways by the sensor nodes are acquired and stored in a database on the cloud. It means that this level converts data-in-motion to data-at rest by converting data from network packets to database relational tables. Therefore, applications can access the historic data when necessary, beside real time usage thanks to transformation of event-based computing to query-based computing.

5. **Data Abstraction:** This level combines data from multiple sources and creates schemas and views of data that applications want. The main aim is to get the required and significant data out of all the data collected. In order to do this, it reconciles the differences in data shape, format, semantics, access protocol and security. Then, it simplifies, filters, selects, projects and reformats data to serve client applications.

6. **Application:** Level 6 controls the applications and performs business intelligence reporting and analytics. Software at this level interacts with data "in motion" and data "at rest" in order

to interpret the information by using several applications. For example, monitoring assets' data, controlling devices, mobile applications, business intelligence reports, analytic applications etc.

7. **Collaboration and Processes:** Final level of the IoT Reference Model involves the people and business processes. Main objective is to empower people to do their work better not the application itself because applications provide people to right data at the right time in order to do the right thing. Not only the device should be smart enough to perform certain tasks, but they should also have some intuitive interactions with the human. The involvement of people and business processes is an essential part of developing IoT application.

Lastly, for each level and the movement of data between levels, security is one of the most critical topics. It must involve the entire model: secure each device, secure network access, secure communications (protocols & encryption), secure storage, authentication & authorization, identity management etc.

To sum up, this reference model provides industries to baseline for understanding its requirements and its potential by describing how tasks at each level should be handled to maintain simplicity, allow high scalability and ensure supportability.

5.1.2. Implementation

IIoT is a trending concept for industries and it provides a huge opportunity to operate systems more safely and productively while improving efficiency and reducing costs. Still, lots of companies face problems with the adoption of IIoT without knowing where to start and which automated processes will contribute to the highest increase in effectiveness [87]. Therefore, along with the rapid growth of IIoT, companies need to know potential challenges and the way of IIoT implementation.

Main challenges that have to be kept in mind during implementation of IIoT may be list as follows:[87][85]

- **Security:** Security challenges for IIoT technologies are the biggest concern that affect both individuals and organizations in terms of financial and operational damage. It is important to save critical data from cyber-attacks. All your data in cloud or in-house storage via network connectivity requires new security tools that means increased cost and heavy maintenance. Thus, businesses are usually resisting the idea of IIoT.

- **Connectivity & Visibility:** The critical IIoT-implementation challenges are rooted in the lack of connectivity. There is a constant need for uninterrupted connectivity if an enterprise is planning to go IIoT. It is vital to monitor assets in real time as well as ensure those assets are performing at an optimal level to improve production. Increased visibility and better insights on the health of the asset is also critical in order to detect anomalies and fix issues before they occur. However, even if using Internet connectivity, its availability of 100% is nearly impossible. There may be trouble in synchronizing and connection may be lost as a result of internet outages, power blackouts, technical errors and maintenance. This issue result in the removal of connected devices from the network, which affects the entire production process and costs millions in damages.

- **Integration of IT & OT:** Another challenge faced by the IIoT implementation is the integration of the information technology (IT) and operational technology (OT). IoT devices are commonly developed as independent solutions, and in best-case scenarios, they are injected into the manufacturing process to become a part of the system. In this case, integration between IT and OT lacks effective connectivity and synchronization. Therefore, it is important to integrate them securely without data loss and vulnerability.

- **Investment Costs:** Finally, investment cost that involves new hardware, modifying existing ones, hiring specialized personnel, building infrastructure etc. is also important challenge for implementation of the IIoT.

It is important to know not only what to implement it, but also how to implement it. Therefore, implementation steps can be followed in order to design a successful enterprise IIoT strategy: [88] [87]

- **Define Business Goals & Expected Outcomes:** Aligning strategy, operations, and technology with new business models requires attention from the start. Therefore, strategic concerns should be addressed before the start of IoT implementation. It means that the success of an IoT solution is dependent on the clarity of problem statement. It is critical to define key performance indicators that can be measured and improved. Therefore, the stakeholders of an organization should identify the expected outcome and business goal along with the key success metrics. Is it a reduction in cost, person-hours or waste? They should precisely know how the solution would influence the productivity, efficiency, and customer satisfaction in the short term and long term.

- **Start Small:** Create a plan and road map that determine which percentage of company or which one of the business cases will be piloted. Company's target should not be the transformation of all business processes in short term. First, pilot study should be conducted for a specific business segment and then a dissemination study should be planned.

- **Decide on the Correct Hardware:** What needs to be used depends on what company want to achieve. It must identify the hardware, equipment, and machinery based on the business goals and expected outcome, for example, appropriate sensors, gateways, edge computers, actuators, adapters, bridges, and other hardware. In general, the sensors need to be low energy devices in order to maintain operable for a long period without having to replace energy sources.

- **Gather Useful Data:** The sensors attached to the devices generate multiple data points that translate to massive datasets. That means generating gigabytes of data every hour, every minute, or even every second. Therefore, it is important to choose carefully the right data points that contribute to the metrics. Some of those data points need to be analyzed in real-time while the others are stored for long-term analysis. For example, in a connected car scenario, vital statistics of an engine are monitored in near real-time while the fuel consumption data is archived for calculating aggregated values at the end of the quarter.

- **Apply Cold & Hot Path Analyze:** Cold path analytics should be defined for long term decision-making process, on the other hand, hot path analytics should be done for near real time processing. Thanks to hot path analytics, immediate action can be triggered by rules, in case of anomaly detection. Therefore, vital statistics can be monitored by real time processing before is too late. On the other hand, cold path analytics is also important because it is possible to know the status of your asses, production, resources and systems over time, including the present data. Data should be analyzed and re-analyzed at any time in order to see the effects of changes.

- **Make it Visual:** For the operation managers and business decision makers, designing an intuitive user experience is important. Operation managers are the supervisors who manage the device layer of IIoT. They are responsible to control of the functions of devices, sensors or actuators. Analysts and other decision makers are also responsible for data driven. They need to access to dashboards that shows critical parameters of collected data.

- **Think About Security:** In order to protect business, it should be implemented security, governance and policy across each layer. Security is critical for IoT projects so datasets must be carefully encrypted. Policies also should define the roles allowed to control the devices and access the business intelligence dashboards.
- **Build a Strong IoT Teamwork:** Successful IoT implementation requires time and teamwork. It should be defined how functional groups can work together and how to enable smart collaborations across the teams. This includes sharing data in operations, maintenance, system reliability, supply chain management and other potential synergies. Therefore, it should be gathered a team from various departments to think IoT thoroughly.

It is clearly seen that implementation steps are important to design a successful enterprise IIoT strategy to the business. In this part, all steps and processes should be thought attentively. Otherwise, it may not be possible to increase effectiveness of the business and to reduce costs without having a strong IIoT strategy.[88] [87]

5.1.3. Sensors

It is obviously clear that to implement IoT it is a must to have some data. So, where does this data come from? Answer is clear that data is produced from the sensors. It will be better to have retrofittable IoT sensors. Retrofitting means updating or adding equipment, sensors, or services to existing hardware so, it helps to make use of new technologies[89][90]

By retrofitting IoT sensors, the company can have the opportunity of implementing a well-functioning IoT solution. Moreover, retrofitting is the best cost-effective way to make your system connective, because IoT retrofit sensors only cost a few hundred euros. Today, nearly every value chain is improved with retrofitted IoT sensors.[89][90]

According to IEEE, sensors can be defined as an electronic device that produces electrical, optical or digital data derived from a physical condition or event. Data produced from sensors is transformed into information that is useful for business decision makers. The selection of sensors is done according to factors, including purpose (temperature, vibration etc.), accuracy, range, power consumption, security, interoperability etc. Some types of the key sensors used for building smart IIoT applications can be listed as follows:[91][92]

- **Temperature Sensor:** Temperature sensors measure the amount of heat energy in a source, allowing them to detect temperature changes and convert these changes into an electrical signal. Machinery used in manufacturing often requires environmental and device temperatures to be at specific levels. Similarly, within agriculture, soil temperature is a key factor for crop growth.
- **Pressure Sensor:** Pressure sensors senses the force per unit area, and it converts into electrical signal. When the pressure changes, the sensor detects these changes, and communicates them to connected systems. Common use cases include manufacturing of water systems to detect fluctuations or drops in pressure.
- **Proximity Sensor:** Proximity sensors are used for non-contact detection of objects near the sensor. These types of sensors emit electromagnetic fields or beams of radiation and look for changes in the field. In retail, a proximity sensor can detect the motion between a customer and a product in which he or she is interested. Proximity sensors are also used in

the parking lots of malls, stadiums and airports to indicate parking availability. They can also be used on the assembly lines of chemical, food and many other types of industries.

- **Optical Sensor:** Optical sensors convert light rays into electrical signals. It measures a physical quantity of light and transforms into a readable form. There are many applications and use cases for optical sensors. In the auto industry, vehicles use optical sensors to recognize signs, obstacles, and other things that a driver would notice when driving or parking. While optical sensors are playing a big role in the development of driverless cars, it is very common in smart phones. For example, ambient light sensors can extend battery life. They are also used in the biomedical field including breath analysis and heart rate monitors. In addition, it is used in mining, chemical factories, refineries and alarm systems that can detect the presence of objects.
- **Accelerometer & Gyroscope Sensor:** Accelerometers detect the rate of change of the object’s velocity with respect to time based on vibration. Gyroscope sensors measure the angular rate or velocity by determining angular position. They are used for acquiring acceleration and rotational information in drones, mobile phones, automobiles, airplanes, and mobile IoT devices in order to detect the orientation of the objects. Additional use cases include motion sensing for video games, and camera-shake detection systems.
- **Gas & Smoke Sensor:** These types of sensors detect changes in air quality, including the presence of toxic, combustible, flammable, odourless and colourless gasses. They are very helpful in safety systems. Industries using gas sensors include mining, oil and gas, chemical research and manufacturing.
- **Infrared Sensor:** An infrared sensor senses certain characteristic of its surroundings by emitting infrared radiation. It can measure the heat emitted by objects and measures the distance. It has been implemented in various applications including healthcare as they simplify the monitoring of blood flow and blood pressure. IR sensors are also used for thermal imagers and night vision.
- **Humidity Sensor:** These types of sensors measure the amount of water vapour in the atmosphere of air or other gases. Humidity sensors are commonly found in heating and air conditioning (HVAC) systems in both residential and industrial domains including hospitals, meteorology stations to predict weather and manufacturing processes for perfect working conditions.
- **Level Sensor:** They are used to detect the level of substances including liquids, powders and granular materials. Many industries including oil manufacturing, water treatment, food manufacturing factories and waste management systems use level sensors.

Before implementing an IIoT solution, you must identify which metrics are key to assessing its effectiveness. What key metrics are the most important to you? Once these metrics have been established, you will need to determine whether or not this data is natively available through sensors or if retrofitting is needed to augment the currently available data [93][94].

Most industrial processes operate at very high speeds and thus generate extremely large amounts of data when retrofitted/instrumented through an IIoT solution. Therefore, it can definitely be the right solution for the business to retrofit the sensors [93][94].

5.1.4. I-IOT devices

An edge device is any piece of hardware that controls data flow at the boundary between two networks. Edge devices essentially serve as network entry (or exit) points. Some common functions of them are the transmission, routing, processing, monitoring, filtering, translation and storage of data passing between networks. Need for more intelligence, computing power and advanced services at the network edge for Internet of things (IoT) gives important role for edge devices. [95]

Most common types of IoT devices at edge level includes sensors, actuators and IoT gateways. The data that is generated by sensors and actuators play an important role in the internet of things. Actuators is a mechanism for turning energy into motion and may be categorized by the energy source to generate motion. For example, in order to generate motion:

- Hydraulic actuators use liquid;
- Pneumatic actuators use compressed air;
- Electric actuators use an external power source, such as a battery;
- Thermal actuators use a heat source.

An IoT gateway is a physical device or software program that serves as the connection point between the cloud and controllers, sensors and intelligent devices like a bridge. All data moving to the cloud, or vice versa, goes through the gateway. Some sensors generate thousands of data points per second. A gateway can pre-process that data locally at the edge before sending it on to the cloud. When data is aggregated, summarized and analysed at the edge, it minimizes the volume of data that needs to be forwarded on to the cloud. It creates a big impact on response times and network transmission costs. [96]

5.1.5. Network and Data Transmission

Huge number of objects are enabled to collect, process and send data to other objects, applications or servers. In the IoT ecosystem, they can transfer information in the online mode only when objects are safely connected to a communication network. Therefore, IoT network protocols have been developed and new ones are still evolving in order to make this connection possible. Fundamentally, connection and network types form a basis for data transmission in IoT systems.

- **Types of IoT Connections**: An IoT system has a three-level architecture: assets, gateways and data systems. The data moves between these levels via four types of transmission channels.[97]

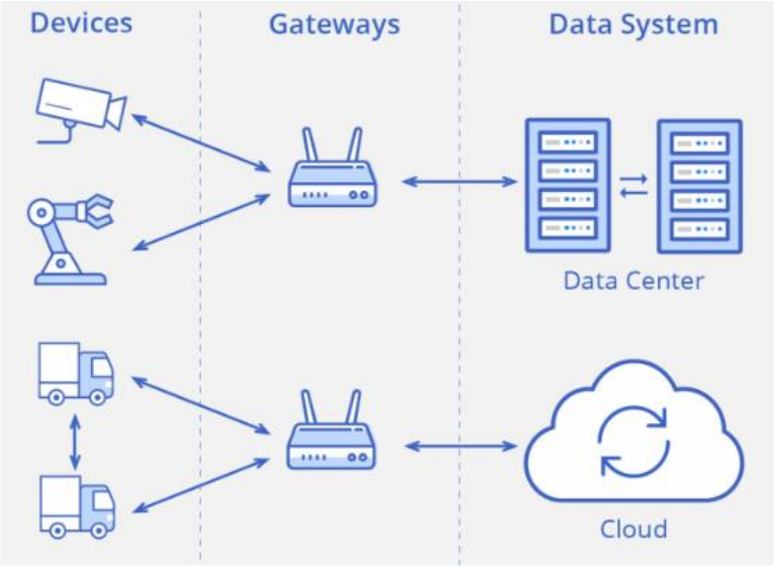


Figure 14 – IoT System Architecture
(Image Source: https://www.sam-solutions.com/blog/internet-of-things-iot-protocols-and-connectivity-options-an-overview/)

- **Device to Device (D2D):** It is direct contact between two smart objects without intermediaries. They can share information instantaneously between each other's. For example, industrial robots and sensors are connected to one another directly in order to coordinate their actions and perform the assembly of components.
- **Device to Gateway:** It is telecommunication between sensors and gateway nodes. Gateways are more powerful computing devices than sensors. They have two main functions:
  - Consolidate data from sensors and route it to the relevant data system
  - Analyse data and, if some problems are found, return it back to the device

  These IoT gateway protocols depends on the gateway computing capabilities, network capacity, reliability, frequency of data generation and its quality.
- **Gateway to Data Systems:** It is data transmission from a gateway to the appropriate data system. To determine what protocol to use, data traffic should be analysed.
- **Between Data Systems:** It is information transfer within data centers or clouds. Protocols for this type of connection should be easy to deploy and integrate with existing apps.

- **Types of IoT Networks:** IoT networks are divided into categories based on the distance range they provide. [97][98]
  - **Nano Network:** Set of small devices (sized a few micrometers at most) that perform very simple tasks such as sensing, computing, storing, and actuation. Such systems are biometrical, military and other nanotechnologies.
  - **NFC (Near Field Communication):** Low-speed network to connect electronic devices at a distance within 4 cm from each other. Such applications are contactless payment systems, identity documents and key cards.

- **BAN (Body Area Network):** Network to connect wearable computing devices like fixed on the body, near the body in different positions, or embedded inside the body (implants).
- **PAN (Personal Area Network):** Net to link up devices within a radius of roughly one or a couple of rooms.
- **LAN (Local Area Network):** Network covering the area of one building.
- **CAN (Corporate Area Network):** Network that unites smaller local area networks within a limited geographical area (enterprise, university).
- **MAN (Metropolitan Area Network):** Big network for a certain metropolitan area powered by the microwave transmission technology.
- **WAN (Wide Area Network):** Network that exists over a large-scale geographical area and unites different smaller networks, including LANs and MANs.

Beside range of communication they offer, networks can also be categorized according to their connectivity configurations known as topologies. There may be various combinations of connections between nodes: line, ring, star, mesh, fully connected, tree, bus.

Mesh networks have the most beneficial if compared to other types of networks, because they don’t have a hierarchy, and the hub and each node is connected to as many other nodes as possible. Information can be routed more directly and efficiently so this reduces maintenance costs and prevents communication problems. This makes mesh networks an excellent and popular solution for the connected objects.

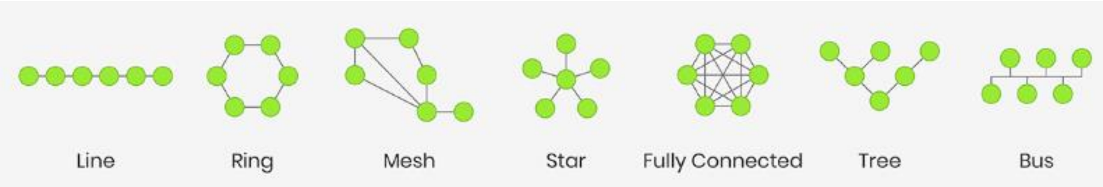


Figure 15 -Network Types based on Topologies
(Image Source: https://www.seebo.com/iot-connectivity/)

In addition to these connection and network types, there is also some invisible language that allows communication between two or more physical objects. Most popular IoT protocols, standards and communication technologies can be listed as follows: [97][98]

- **MQTT (Message Queue Telemetry Transport):** It is a lightweight protocol for sending simple data flows from sensors to applications and middleware. It includes three components: subscriber, publisher and broker. The publisher collects data and sends it to subscribers. The broker tests publishers and subscribers, checking their authorization and ensuring security. MQTT suits small, cheap, low-memory and low-power devices.
- **DDS (Data Distribution Service)**: It is an IoT standard for real-time, scalable and high-performance machine-to-machine communication. The DDS standard has two main layers. Data-Centric Publish-Subscribe (DCPS), which delivers the information to subscribers and Data-Local Reconstruction Layer (DLRL), which provides an interface to DCPS functionalities.
- **AMQP (Advanced Message Queuing Protocol):** It is an application layer protocol for message-oriented middleware environments. The processing chain of the protocol includes three components. Exchange (gets messages and puts them in the queues), Message

queue (stores messages until they can be safely processed by the client app), Binding (states the relationship between the first and the second components)

- **Bluetooth:** It is a short-range communications technology integrated into most smartphones and mobile devices, which is a major advantage for personal products, particularly wearables. This technology is a real foundation for the IoT, as it is scalable and flexible to all market innovations. Moreover, it is designed to reduce power consumption.
- **ZigBee:** It is a low power, low data-rate wireless network used mostly in industrial settings. It is created the universal language for the Internet of Things, so it makes it possible for smart objects to work securely on any network and seamlessly understand each other.
- **Wi-Fi:** It is the technology for radio wireless networking of devices. It offers fast data transfer and is able to process large amounts of data. This is the most popular type of connectivity in LAN environments.
- **Cellular:** It is the basis of mobile phone networks, but it is also suitable for the IoT apps that need functioning over longer distances. They can take advantage of cellular communication capabilities such as GSM, 3G, 4G (and 5G soon). The technology is able to transfer high quantities of data, but the power consumption and the expenses are high too. Therefore, it can be a perfect solution for projects.
- **LoRaWAN (Long Range Wide Area Network):** It is a protocol for wide area networks. It is designed to support huge networks (e.g. smart cities) with millions of low-power devices. It can provide low-cost mobile and secure bidirectional communication in various industries.

Choosing the appropriate type of connectivity is an inevitable part of IoT projects because it has an impact on the design of IoT devices. For example, network range, data rate, and power consumption are all directly related. If you increase the network range or rate and volume of data that is transmitted, IoT devices will require additional power to transmit the data under those conditions. At this point, requirements for IoT networks may be listed as follows:

- The capacity to connect a large number of heterogeneous elements;
- High reliability;
- Real-time data transmission with minimum delays;
- The ability to protect all data flows;
- The ability to configure applications;
- Monitoring and traffic management at the device level;
- Cost-effectiveness for a large number of connected objects.

Therefore, it is important to consider the IoT networking challenges to find the technologies that will be the best fit for IoT application.

5.1.6. Trust and Security

IoT security includes both physical device security and network security by protecting IoT devices as well as the networks they're connected to. IoT device security must protect systems, networks, and data from IoT security attacks, which target four types of vulnerabilities:[85]

- Communication attacks, which put the data transmitted between IoT devices and servers at risk

- Lifecycle attacks, which put the integrity of the IoT device as it changes hands from user to maintenance
- Attacks on the device software
- Physical attacks, which target the chip in the device directly

IoT security allows developers to protect their devices from all types of vulnerabilities while deploying the security level. Cryptography technologies are used to combat communication attacks. Security services are offered for protecting against lifecycle attacks. Isolation measures can be implemented to beat off software attacks. In addition, finally, IoT security should include tamper mitigation and side-channel attack mitigation technologies for fighting physical attacks of the chip.

In order to implement a sufficient solution to measure the security of the IoT, first there is need to agree on the objectives to be achieved and then re-adapt existing security certification frameworks in order to meet these objectives: [85]

- Allow a quick and agile product manufacturing lifecycle;
- Reduce costs and time of evaluations;
- Motivate and educate the developer;
- Include training;
- Recognize accredited self-assessment (for basic security assurance level);
- Provide simple methods / metrics for developers;
- Recognize existing evaluation methodologies and security standards;
- Consider the operating environment / process / context / complete domain;
- Allow the customer and the supplier to compare the different products in an objective way;
- Mutual recognition.

Keeping these goals and concepts in mind reduces the costs of security assessment and consulting services, eliminates the lack of cybersecurity experts, raises business and consumer security awareness and ultimately creates a level of trust between the stakeholders.

5.2. Big Data Infrastructure

The term Big Data often refers to the management of enormous amounts of data. Such term has become popular during the 20 latest years [1]. Big Data technology is under constant growth, and it is calculated to double at least every two years [3]. Although the term Big Data is abstract, people often refer to it as enormous amounts of unstructured data, harder to store and analyse [99]. We can define Big Data as datasets with a volume of data that cannot be processed by traditional IT systems in an acceptable time.

Such data needs to be suitably structured to be useful to provide further knowledge and to be helpful to match data from unstructured fonts. For this reason, Big Data is working with some cutting-edge technologies, such as cloud computing or the Internet of Things, among others.

5.2.1. Challenges

Big Data technology still has several limitations to face. These limitations hamper the potential of such technology as well as the management, acquisition, processing, and storage of data. The research community has proposed several solutions to some of these problems. For instance, cloud computing is the most popular method for providing an infrastructure for Big Data systems. These problems have been beneficial for certain technologies that have developed rapidly to help the deployment of Big Data systems [100] .

However, to deploy and implement a suitable Big Data model is not at all trivial. Some of the setbacks [101] of using Big Data are listed below:

- Data representation: Big Data systems often incorporate datasets with different data types. Such heterogeneity may be a problem for storing this data and make it accessible in a suitable time.
- Redundancy in data representation: Big Data systems are known for producing redundant datasets. Consequently, Big Data systems are slower and more complex than they could be, which hinders its scalability. Nonetheless, by compressing this data without losing its value systems can make transcendent improvements in terms of efficiency.
- Data Life Cycle: Some of the systems supported by Big Data technologies such as IoT systems provide some Data which becomes useless after a certain amount of time. The previously mentioned data causes the system to grow and can reach a size that the infrastructure will not be able to sustain. For this reason, one of the most critical issues in Big Data is to choose which data is no longer useful to keep a suitable scope for the system.
- Analytical Mechanism:[101] Structured database schemas have not been designed in terms of scalability. Big Data systems are a mix of structured and non-structured sources of data. A suitable architecture should be defined to support Big Data systems reaching performance requirements.
- Security in analysed data: Big Data systems are so large that data often cannot be analysed by people. Big Data analysts will frequently need to rely on tools designed to execute such duties.
- Energy management: Big Data systems are increasing in size, which leads them to consume more and more electric energy. This is not proper for the environment and some power management protocols must be implemented.
- Scalability: As said before in this state-of-the-art, data is experimenting an extremely fast growth and systems need to be prepared for it in their architecture as well as in their way to manage resource consumption.

Although the number of challenges is noticeable, they can all be overcome with a good design and implementation of the Big Data architecture.

5.2.2. Big Data generation and acquisition

Data generation and data acquisition are the two very first of the Big Data life cycle. Both steps are therefore very relevant and need to be treated consistently.

The first step in any Big Data process is to collect the data [4]. This data comes from any variety of sources that can be structured and non-structured. These datasets come from clicks, streams, videos, queries as well as other sources of data that highly surpass the current IT capacity.

Big Data systems will have to face the massive data produced by enterprises to higher certain levels of profitability, the heterogeneity of IoT sources, unstructured data collected from the Internet among other sources [5]:

The second step in the Big Data process is Data Acquisition. Sometimes Data comes from some sources which give an unsuitable size to datasets, filled with useless data. The Internet of Things is an example of such kind of redundant data provided by sensors. However, some techniques to select the useful data and compressing datasets are essential for an adequate way to process the data and, therefore, make the system work properly.

Three data acquisition procedures are generally used to sustain Big Data applications. The following techniques make it easier for data processing.

- Log files: these are some text files automatically generated by the system. For instance, Web Servers use such information to collect searches, clicks, and visits [102]. Databases use log files as well to perform it more efficient for certain complex queries.
- Sensors: Sensors are commonly employed to handle data from environmental sources and represent them into something understandable for the system. Usually, the way to classify this information is into categories like heat, sound, and weight, among others.
- Techniques to collect network data: The network holds an extensive source of data that needs to be processed by Big Data systems. For this purpose, it is common to employ several tools to process and handle that before-mentioned data. Web Crawlers [103] are the most used of those tools. They are programs that look into the URLs containing a particular word, index, or any information specified which can categorize web pages into specific parameters.

The vast majority of data storage will occur in the data center. Data transmission should be done appropriately so as not to waste hardware resources. Consequently, there are two main ways of transmitting the data: the internal ones, named Intra-DCN, which will take place in the Data Center Network (DCN) and the external ones, named Inter-DCN, which are transmissions from the source to the data center[6].

- External data transmissions generally depend on the network's physical infrastructure. In most of the world, they use optic fiber technologies. Optical fiber usually uses wavelength division multiplexing (WDM) network architecture, which makes smart management of optical fiber systems. As a result, data transmission has arrived at speeds of 100 Gb/s. Furthermore, prospects figure that it will be feasible to reach speeds of Tb/s.
- Internal data transmissions depend on the data center infrastructure and its communication protocol, which usually consists of server racks connected in a tree structure with two or three layers.

5.2.3. Data Storage

Big Data storage is a cornerstone of the use of such technology [7]. However, data filtering is a necessary step before storing the data so as not to store inaccurate or corrupted data. Such measures include implementing a general visualization interface. Afterward, it is of paramount importance to eliminate all redundancies and data of poor quality. Before-mentioned operations require the creation of plans for determining the format of high-grade quality data, defining the form of possible errors and document it. Therefore, the error correction mechanism must modify or eliminate such corrupted data.

After data has developed the filtering steps outlined before, it is time to store it. The primary matter on it is to find a manner to save an enormous amount of data reliably and also suitable for hardware infrastructures. Numerous schemes have been built only to fulfil the need to reach a fitting data storage infrastructure.

There are three qualities that Big data systems must fulfil to build a distributed storage system to host massive amounts of data. They are the following:

- **Consistency**: The most common manner for storing data consist of dividing data into pieces, which is common to allocate different servers. The more servers, the more possibilities of failure of one of them. For this reason, as we are talking of warehouses with an order of thousands of servers, probabilities are proportionately quite high. By no means should be permitted to store copies of the same data with different information. Consequently, action needs to fail if executing this action, risk the integrity of the systems. In other words, the atomicity regarding actions demands to be protected.
- **Availability:** We consider a system available if the vast majority of requests receive a response. Currently, cloud servers can guarantee a disponibility rate of more than 99,99%.
- **Partition Tolerance:** As distributed systems store data in different data centers, they must be tolerant of network failures. This means not only to detect network failures but also to recover the state of the system and, afterward recover from such failure.

However, Eric Brewe proved in the year 2000 [104] that only two of the three requirements can be fulfilled at a time in the CAP theorem. Even though this limitation still exists many years later of the discovery of such theorem, systems may be designed avoiding partitioning to minimize the two-out-of-three inconsistency.

5.2.4. Big Data applied to predictive maintenance

Preventive maintenance is a technique that can ensure the functioning of a system through activities of regular revision, while the system is working. Their main goals are the following:

- Lengthen the productive life of the system.
- Reduce the likelihood of failure in the system components
- Reduce productivity due to equipment faults.

Proper predictive maintenance should detect errors even before they occur. For this purpose, it is necessary to carry out several tests and cleaning activities.[105]

To reach the previously mentioned aims, it will be necessary to build a Big Data system to support it.

The whole Big Data system will focus on the storage, collection, and managing of the monitored data, and it will send the results to other applications. For instance, Big Data in industrial environments is automatically stored, analysed, and triggered by such kind of Big Data ecosystems.

In such a kind of ecosystem, it is necessary to collect data from structured and unstructured sources [101]. Then such data is going to be stored in a platform where it can be analysed. For this reason, it is important to connect the system to different applications, of different volumes and rates, and with different data models. Furthermore, the information from all the previously mentioned sources requires a real-time visualization of the changes in their values.

The most competitive enterprises such as Bosch of Rolls Royce do use this kind of predictive maintenance in their production systems.

In the case of Rolls Royce, their production of engines has experimented with numerous changes due to their approach in Industry 4.0 [106]. The vast production of engines for aircraft systems has driven to the use of Big Data toward error detection and the increase of production.

Rolls Royce uses Big Data in its monitorization of manufacturing processes with an extensive plan for error detection. More concretely, Rolls Royce has hundreds of nanobots placed in locations which are inaccessible for humans. These nanobots collect data that their engineers monitor in real-time, avoiding the equipment failure or programming errors. Such information is essential for later decision support.

As we have seen in the Rolls Royce example, it is possible to make a significant cost reduction in manufacturing processes by utilizing the constant feedback provided by Big Data systems with a predictive maintenance approach. Big Data ecosystems can explain the relationship between the loss of performance and the environment.

The factory floor's situation usually takes place in environments where certain conditions such as humidity, temperature, and noise. These kinds of conditions can gradually deteriorate the equipment and reduce staff productivity.

Big Data systems can do a matching between the human-machine intercommunication and the environment, through the use of large datasets for examining the conditions. By the proper formatting and manipulation of this data, it is possible to find the patterns of equipment deterioration and waste of energy [8].

As stated before, losses of productivity caused by equipment degradation can lead to the loss of considerable amounts of money. However, after obtaining the degradation patterns generated by the environment and thousands of inputs from the applications connected to the Big Data ecosystem, it is possible to figure out the performance of the same equipment in different case scenarios, considering the staff and the environment. By analysing all the situations, it is possible to figure out the best combination, which will, therefore, optimize the production or the cost reduction.

Another important source of optimization is power saving, equipment in an idle state can considerable amounts of money. There are many ways to reduce energy costs. However, Big Data has provided many inputs that will find the most appropriate policies for cost reduction [9].

5.2.5. Architecture

The new challenges of big data analysis demand that researches investigate an develop new and high-performance computing architectures [10]. The rising of **Cloud Computing** and Cloud Storage in industry provides a solution to support dynamic scalability in several predictive maintenance applications. Here below, some of the most used architectures for big data processing are shown in detail.

The Lambda Architecture [11] uses three layers to decompose the problem as can be seen in Figure 16. The batch and speed layers store and process all the incoming data using the Apache Kafka technology. The batch layer makes use of the Hadoop Distributed File System (HDFS) to store the master dataset and the MapReduce in order to perform the batch views. The speed layer analyses data in real-time compensating the high latency of updates in the serving layer. The serving layer indexes the batch views so that views can be efficiently queried with less latency thanks to the use of the speed layer. This layer makes use of technologies such as Oracle, HBase, Storm and Cassandra.

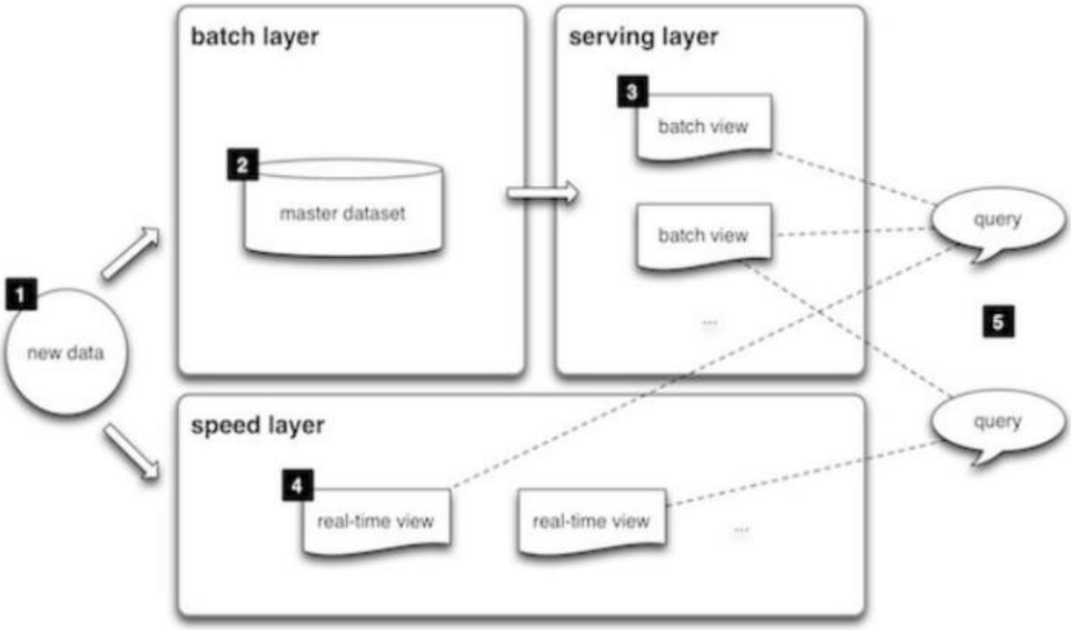


Figure 16 - Lambda architecture
(Image source: [12])

Another big data referenced architecture is the one proposed by Microsoft [13] which includes four main functional features. The collected data can be used for a variety of purposes, so it is important to choose a reliable data source. The second step is to transform and process the collected data to extract useful information. Then, the data infrastructure is defined as the software, servers and networks where the collected data is stored and, therefore, transformed. Finally, the last component of the big data architecture defined by Microsoft is the data usage having in consideration that data can be provided in different formats and under different security managements.

NBDRA [14] is a big data reference architecture proposed by NIST (National Institute of Standards and Technology) developed to ensure the secure and the effective usage of big data. This architecture is composed of five layers which are the following:

- System orchestrator: defines and composes the data application activities into an operational vertical system.
- Data provider: collects the incoming data and feeds it into the big data system for data preparation, collection, analysis, visualization and access.
- Data consumer: is continuously receiving the output from the big data system in order to accomplish data searching, querying, exploring and analysing. It can be the end user or another system receiving the output.
- Big data application provider: executes the data life cycle considering the privacy and security requirements. It collects data from various sources and perform data cleaning, analysis, visualization and security and privacy management.
- Big data framework provider: provides various services for the big data system to accomplish some data transformations. It gives the complete computing framework such as hardware, storage and network. It comprises three sub-components: infrastructure frameworks, data platform frameworks and processing frameworks.

Figure 17 shows the complete NBDRA architecture.

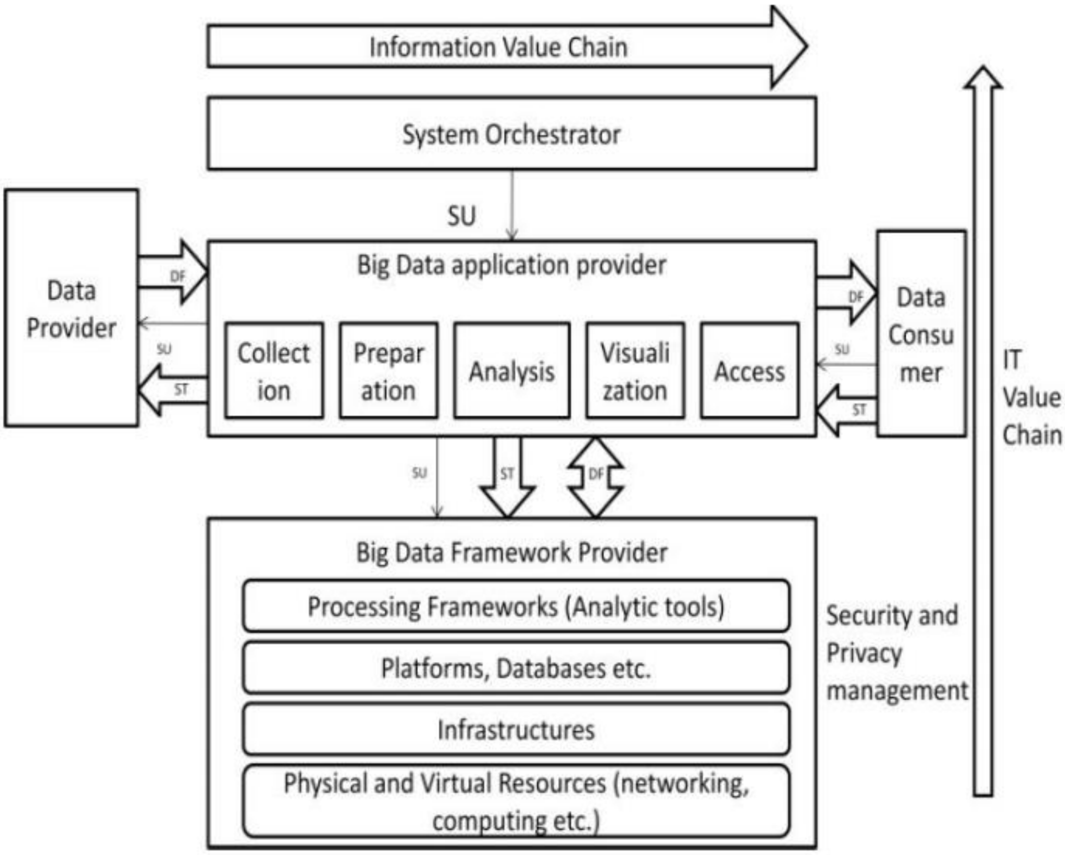
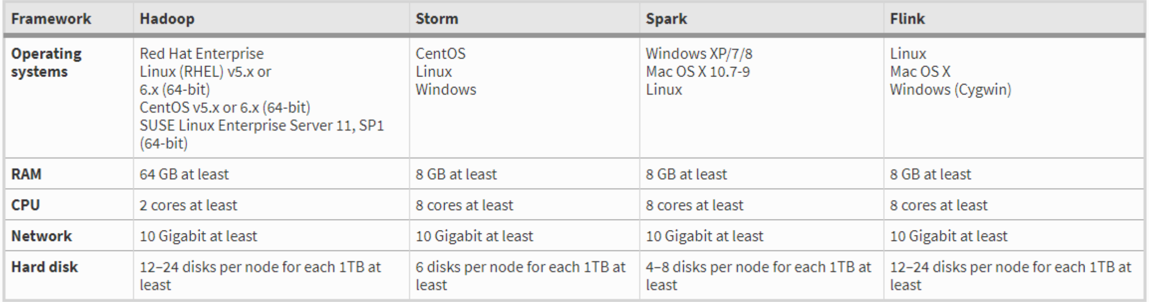

Information Value Chain
System Orchestrator
SU
Data Provider
DF
SU
ST
Big Data application provider
Collection
Preparation
Analysis
Visualization
Access
DF
SU
ST
Data Consumer
IT Value Chain
SU
ST
DF
Big Data Framework Provider
Processing Frameworks (Analytic tools)
Platforms, Databases etc.
Infrastructures
Physical and Virtual Resources (networking, computing etc.)
Security and Privacy management

Figure 17 - NBDRA architecture
(Image source: [12])

As these, there are multiple other architectures that have been defined by the National Institute of Standards and Technology (NIST) as are collected in [13].

5.2.6. Hardware

Big data collects and analyses enormous quantities of data. This means that it is crucial to arrange high volumes of data storage as well as high velocity data processing. Some of the essential hardware requirements for large-data processing are the engines and framework used for the data computing [15]. Figure 18 shows the hardware requirements for the main big data frameworks: Hadoop, Storm, Spark and Flink.



Framework	Hadoop	Storm	Spark	Flink
Operating systems	Red Hat Enterprise Linux (RHEL) v5.x or 6.x (64-bit) CentOS v5.x or 6.x (64-bit) SUSE Linux Enterprise Server 11, SP1 (64-bit)	CentOS Linux Windows	Windows XP/7/8 Mac OS X 10.7-9 Linux	Linux Mac OS X Windows (Cygwin)
RAM	64 GB at least	8 GB at least	8 GB at least	8 GB at least
CPU	2 cores at least	8 cores at least	8 cores at least	8 cores at least
Network	10 Gigabit at least	10 Gigabit at least	10 Gigabit at least	10 Gigabit at least
Hard disk	12–24 disks per node for each 1TB at least	6 disks per node for each 1TB at least	4–8 disks per node for each 1TB at least	12–24 disks per node for each 1TB at least

Figure 18 - Hardware requirements for big data frameworks
(Image source: [15])

Hardware architectures have developed huge changes and advances since the 1960s and with the emergence of the need to process large amounts of data. From this time, hardware has moved from faster sequential machines, to vector processors and from massive parallel systems to multicore systems with accelerators. However, despite the advantages provided by these hardware innovations, there are still some issues that are far from being solved, such as the problem of I/O tasks. Also, each of the used frameworks requires different programming models and hardware requirements what outcome in an increase in cost and effort.

One of the main hardware choices in cloud systems are Graphic Processing Units (GPUs) which provides high rendering capabilities and resolutions lending to the appearance of Ge Force 8800 graphic card designed by NVIDIA in 2006 granting advantages for computing applications.

In what concerns to the network, the collection and analysis of large data sets require enormous amounts of processing power. For this reason, distributed computing is performed in order process more amounts of data at the same time in different machines. The management and storage of large amounts of data requires networks architectures that differ from traditional client-server applications. For accomplish this task it is important to understand how data flow behaves. Traditional north-south traffic from clients to servers and serves to clients with no communication between clients is quite easy to model while big data applications require east-west communications between the different nodes which is much more difficult to understand. An example of a network topology that allows east-west communications is Spine Fabric. Data Center Bridging (DCB) is available on 10G and 40G networks and it helps to manages data flow enabling data segregation based on priorities or classes of the processed data. Another important hardware issue related with the last one commented is that it must have the ability to handle traffic burst effectively in order to not miss any data [16].

There is also a need of security and protection in big data in order to detect and prevent advanced threats and malwares. Data security does not only involve de encryption of the data but also its privacy policies. The main challenges on security in cloud computing are summarised into de following:

- Network: it deals with network security protocols by using distributed nodes, data and internode communications.
- Authentication: it deals with encryption/decryption techniques, authentication methods, logging.
- Data: it deals with data integrity and availability. It is important to protect the distributed data.
- General: it deals with some traditional security tools and technologies.

In [17] some security approaches that deal with the commented challenges are shown. Some of these are:

- File and network encryption: all data and network communications should be encrypted to prevent hacking attacks.
- Logging: all the map reduce jobs should be logged before modifying the data as well as the responsible user`s information.
- Nodes authentication: authentication techniques such Kerberos can be used to validate authorized nodes form malicious ones when joining a cluster.

- Honeypot nodes: honeypots are used to trap the hackers that are trying to access the data and take the necessary actions to eliminate them.

As a conclusion it is important to stress the importance of maintaining data security and privacy.

5.2.7. Big Data Frameworks

Big Data frameworks are the working environment in Big Data analytics. The objective of a Big Data Framework is to represent all the relevant aspects of Big Data user, framework and environment. [107]

In the rest of the section the most relevant big data frameworks will be analysed, the three following Big Data Frameworks are going to be analysed [18].

Apache Hadoop: Apache Hadoop is an open software library which includes a framework. Hadoop can be configured for single computer or thousands of them. Hadoop can be divided into two core components; Hadoop Distributed Files are used to allocate the data, MapReduce that is mainly used to process the data. HDFS is mainly allocated in the File System, the Hadoop File System mainly offers quick access to the data and a determined number of replicas to get data quickly to the user. Map Reduce is the component which process the data and offers it in form of key-value pairs. As the reader may infer from this paragraph Hadoop offers a low-level programming paradigm.

In factory floors Master-slave architecture is relevant because it is a quite frequent configuration among IoT devices. HBase's architecture is based on two different server types:

- Masters (HBase Master)
- Slaves (HBase Region)

Each of them needs a different configuration and specifications. For example, the master server doesn't need as much space as a slave server, so a master server doesn't have to have a lot of memory.

Project storm: Hadoop and related technologies can store data to awesome levels. However, they are not real time systems. Predictive maintenance is based in taking data from an environment which is under constant change. Storm count on a real time processing data based on topologies. Storm clusters are quite similar to Hadoop ones. There are two types of nodes on a Storm cluster: the master node and the worker one. “Nimbus” is a daemon ran by the master node which is the responsible for the code distribution around the cluster, assigning tasks and monitoring for failures. Then the “Supervisors” are daemons ran by the worker nodes and are the responsible for accomplishing the tasks assigned by Nimbus and to start and stop the processes. The Zookeeper cluster coordinates the communications between Nimbus and the Supervisors in the distributed environment as is shown in Figure 19.

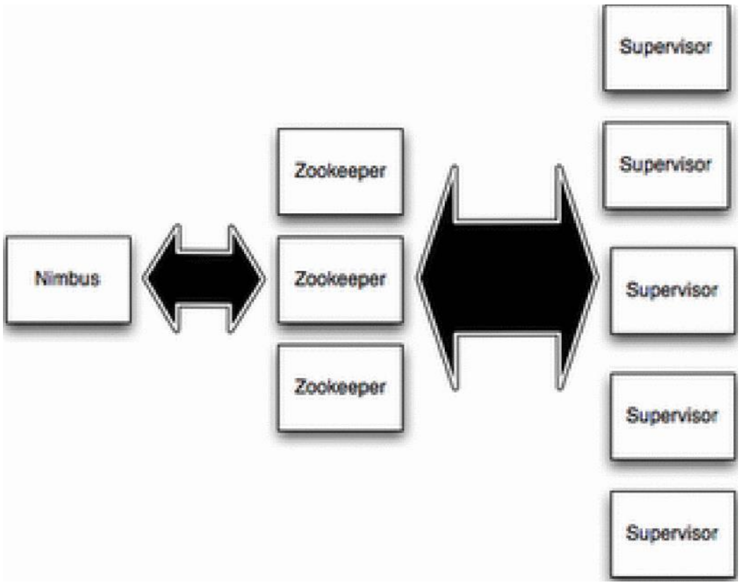


Figure 19 - Project Storm framework
(Image source: [18])

Apache Drill: Apache Drill is a distributed system built for performing huge datasets of the order of petabytes. Apache Drill has been designed for any kind of user or business logic with many modes such as terminal or user mode. It is also a suitable option due to the huge amount of query language that it supports. The main goal of this framework is to reply to ad-hoc queries maintaining a low latency mode while providing a flexible query execution framework.

The showed frameworks are the main ones required to process large-scale data. More information about these frameworks is collected in [18].

5.3. Standards and Regulations

The need to capitalize on Big Data and Industrial Internet of Things (IIoT) has resulted in the need to unlock and maximally utilize whatever value results from the data gathered. Nevertheless, value is variable, and the same can be said concerning machine and production data. The priorities of a machine builder's Big Data may significantly differ from that of an end-user manufacturer. Determining the type of data necessary for every possible application takes the first step by figuring out the challenges faced by IIoT technology in key business and production areas, which must be addressed. A plan is then created to generate further insights that will ensure consistent improvement efforts in the company's operation.

In light of rapid technological advancement, the demand for technological integration and standardization has also significantly increased. Standards play a crucial role in ensuring the reduction of technical barriers, at the same time providing technical harmonization to promote the idea of a common technical understanding and efficiently analyse digital systems.

5.3.1. Standards

Published standards on IoT and big data, which are also applicable to technologies that cannot be overlooked, such as automation systems, software, and system management, and artificial intelligence, are seen in this section. According to Unal [93], some of these standards include:

1. Industrial - process measurement, control and automation (TC 65)

- IEC TS 62832 Industrial - process measurement, control, and automation - Digital factory framework
- IEC PAS 63088 Smart manufacturing - Reference architecture model industry 4.0 (RAMI4.0) (Publicly Available Specification)
- IEC 62424 Representation of process control engineering - Requests in P&I diagrams and data exchange between P&ID tools and PCE-CAE tools
- IEC TR 62794 Industrial-process measurement, control, and automation - Reference model for the representation of production facilities

2. Industrial networks (TC 65/SC 65C)

- IEC 61784 Industrial communication networks -Profiles
- IEC 61158 Industrial communication networks -Fieldbus specifications

3. Cloud Computing and Distributed Platforms (ISO/IEC JTC 1/SC 38)

- ISO/IEC 17788 Information technology – Cloud computing - Overview and vocabulary
- ISO/IEC 17789 Information technology – Cloud computing - Reference architecture
- ISO/IEC 18384 Information technology – Reference Architecture for Service Oriented Architecture (SOA RA)

4. Safety of machinery - Electrotechnical aspects (TC44)

- IEC 62061 Safety of machinery - Functional safety of safety-related electrical, electronic, and programmable electronic control systems.

5.3.2. Regulations

In the light of recent high-profile data mishaps in the technology industry, the government and politicians now have the technology industry in their purview. As stated by Wood [94], some relevant regulations in the industry include:

1. Antitrust Laws

Any time a company conspires with its competitors, third-party vendors, or other relevant parties, it may run afoul of antitrust laws. These are the issues antitrust laws strive to address, such as the following:

- **Conspiring to fix market prices:** Discussing prices with competitors—even if it affects a small marketplace.
- **Price discrimination:** Securing favourable product prices from buyers when other companies can't.
- **Conspiring to boycott:** Conversations with other businesses regarding the potential boycott of another competitor or supplier.

- **Conspiring to allocate markets or customers:** Agreements between competitors to divide up customers, territories, or markets are illegal. This provision applies even when the competitors do not dominate the particular market or industry.
- **Monopolization:** Preserving a monopoly position through the acquisition of competitors, the exclusion of competitors to the given market, or the control of market prices.

If your company runs afoul of any of these regulations, the federal trade commission might contact you.

2. Privacy

The Internet of Things (IoT) has suffered from being unregulated. The privacy of the data created and consumed by connected devices is now under the regulation spotlight. Protecting this data is vital for companies and consumers to avoid being accessed for malicious intent. There are a number of regulations world-wide with the focus on personal data but not a much that has been formalized around business data and use of business data.

3. Auditing

Defining the scope of your audit is key and looking for the risks can help outline a protocol for your audit. Risks can include:

- Software updates and patches. The time for a patch to be released may be longer than the typical cycle for non-IoT devices.
- Hardware lifespan. IoT devices have their own life cycle, often with built-in obsolescence. Components such as nonreplaceable batteries in IoT devices require life cycle planning and asset management processes specific to IoT.
- User IDs and passwords to control access either do not exist or are hard coded.
- IoT devices can be hacked quickly but take days or weeks to rectify. The wider consequences remain unknown because it is difficult to know what has been seen, modified or stolen.
- Cybercriminals can plant back doors for future automated attacks in or from IoT devices; typical attacks include botnet distributed denial-of service (DDoS) attacks.
- Hackers can use IoT devices as an entry point to an enterprise’s networks.

Now that the risks have been outlined you can then assess the steps to evaluate these risks:

- General baseline controls—Minimum controls that need to be applied to all aspects of the technology
- Data-related controls—Such as controls that apply to the data forming a key part of IoT
- Analysis and learning-related controls—Applied to ensure that the analysis is ethical and enables trusted use of the data and that outcomes of analysis can be applied to business decision-making
- Business and process alignment—Related aspects which ensure that the IoT implementation is aligned to business needs and that business benefits are delivered as required.

5.4. Industrial Management Solutions

The concept of industrial management follows a process that engages in strategic planning, setting objectives, resource management, as well as the deployment of human and financial assets required to achieve specified objectives, and analysing the results. Management is also a result of facts storing, recording, and storing information for future use, available to others in the organization. An effective industrial management solution would ensure planning, organization, staffing, coordination, and control of the industry.

Some of the solutions for industrial management include:

- Ensuring maximum output with minimal production cost
- Individual activities in the industry must be coordinated to achieve the organization's shared purpose
- Production and delivery of goods and services on the agreed-upon date
- Proper accounting, reporting and overseeing of all operations in the industry
- Wastage and loss prevention
- Production of quality alone
- Innovation
- Attention to customers' needs, and
- Maximum utilization of the industry.

Software Management Solution

Most organizations largely depend on the enterprise resource planning system (ERP). A lot of money is invested in software, implementation, and training costs in relation to their ERP systems to collect, track, and report on vital business data. Some of the rules that will efficiently manage and improve the ERP system operating with the least potential issues are seen below:

1. **Documentation and Verification of a formidable disaster recovery plan:** in the event of a hard disk failure or server crash, one must wonder what will happen. A well-documented disaster recovery plan is vital to any ERP implementation. When a disaster recovery plan is efficiently implemented, several types of disasters will be accounted for, be it man-made or natural, which may pose a threat to the ERP system. It is impossible to eradicate disasters, but their impacts, such as loss of data and downtime, can be significantly minimized.

A disaster recovery plan is designed to identify preventative and corrective measures required should the unfortunate event of a disaster arise. It must address backup, how to store them, preferably offsite, and how often to create them. It should as well address how to recover from a disaster with a formerly verified and tested recovery solution.

2. **Documentation of Maintenance Plan:** critical areas of the ERP system should be identified with a clear definition of plans of expansion or roadmap. Constant revaluation of requirements and what area of the ERP system may be improved. Key players for the ERP must be identified in the plan. Questions ranging from "who the vendor is" to "who is in charge of the system internally?" must be answered clearly.

Keep the software Update: the prospect of software continuously developing additional features is inevitable. It is, therefore, paramount to know what software version you are using and the latest updates. Service packs or version upgrades provided by vendors are directed towards addressing bugs that have been identified, as well as adding new functions, improve navigation, and likewise change the appearance of the software. For the system to be up-to-date, these updates are necessary. A consistently updated system gives one the liberty of utilizing new available features that may significantly improve one's system. Hardware be evaluated by asking, what has changed about this software? How can the new features be capitalized on to improve system efficiency? and upgraded periodically to ensure its adequacy for the ERP software.

Practical training of the staff: after implementation, without the presence of training, the ERP system will not run smoothly. Training, therefore, keeps the ERP system running effectively, with negligible or a rather microscopic level of user issues. Starting up training is a significant step, but it is of no good if it is not provided over a selected period. Sequential training ensures and monitors staff utilization of the system efficiently and users aware of the new processes, and if or not, users are able to maximize the system's new features efficiently. Furthermore, consistent training allows users to identify improvements in functionality and processes within the organization. The development of a maintenance plan takes the necessary steps to backup and ensure the safety of valuable information, ensuring software updates and providing continuous training to the staff, the features of an ERP system can be maximally utilized.

Bibliography

[1] B. S. Dhillon, *Engineering Maintenance: A Modern Approach*. CRC Press, 2002.

[2] G. 1. 3. 0. 1. M. P. Elements, “Global Asset Protection Services,” 2015.

[3] B. S. Dhillon, *Maintainability, maintenance, and reliability for engineers*. CRC Press, 2006.

[4] A. Garg and S. Deshmukh, “Maintenance management: literature review and directions,” *J. Qual. Maint. Eng.*, vol. 12, no. 3, pp. 205–238, 2006.

[5] T. H. Davenport and J. E. Short, *The new industrial engineering: information technology and business proess redesign*. Cambridge, Massachusetts: Center of Information Systems Research, MIT, 1990.

[6] G. A. Pantazopoulos, “A Process-Based Approach in Failure Analysis,” *J. Fail. Anal. Prev.*, vol. 14, no. 5, pp. 551–553, 2014.

[7] D. P. Dennies, *How to Organize and Run a Failure Investigation*. Ohio: ASM International, 2005.

[8] M. A. Moss, *Designing for Minimal Maintenance Expense: The Practical Application of Reliability and Maintainability*. CRC Press, 1985.

[9] Fiix Inc., “What is RTF? | Run to Failure Maintenance Examples | Fiix.” .

[10] UpKeep, “What is Run to Failure Maintenance?” [Online]. Available: https://www.onupkeep.com/blog/what-is-run-to-failure-maintenance/. [Accessed: 11-Sep-2019].

[11] R. E. Barlow and L. C. Hunter, “Optimum preventive maintenance policies,” in *Operations Research*, INFORMS, 1960, pp. 90–100.

[12] V. Dilda, L. Mori, and C. Schmitz, “Manufacturing: Analytics unleashes productivity and profitability,” *McKinsey Insights*, 2017.

[13] S. Bradbury, B. Carpizo, M. Gentzel, D. Horah, and J. Thibert, “Digitally enabled reliability: Beyond predictive maintenance,” 2018.

[14] R. K. Mobley, *An introduction to predictive maintenance, 2nd Edition*. Woburn, MA: Butterworth Heinemann, Elsevier Science, 2002.

[15] C. Coleman, S. Damofaran, and E. Deuel, “Predictive maintenance and the smart factory,” *Deloitte*, p. 8, 2017.

[16] F. S. Nowlan and H. F. Heap, “Reliability Centered Maintenance,” San Francisco, California, 1978.

[17] A. Rastegari and M. Mobin, “Maintenance decision making, supported by computerized maintenance management system,” in *2016 Annual Reliability and Maintainability Symposium (RAMS)*, 2016.

[18] A. Rastegari, *Condition Based Maintenance in the Manufacturing Industry: From Strategy to Implementation*. Västerås, Sweden: Mälardalen University Press Dissertations, 2017.

[19] T. Dong, R. T. Haftka, and N. H. Kim, “Advantages of Condition-Based Maintenance over Scheduled Maintenance using Structural Health Monitoring System,” in *System Reliability*, London, UK: IntechOpen, 2019.

[20] A. Rastegari and M. Bengtsson, “Cost Effectiveness of Condition Based Maintenance in Manufacturing,” in *Reliability and Maintainability Symposium, RAMS 2015*, 2015.

[21] S. Haussener, P. Coray, W. Lipinski, P. Wyss, and A. Steinfeld, “Tomography-Based Heat and Mass Transfer Characterization of Reticulate Porous Ceramics for High-Temperature Processing,” *J. Heat Transfer*, vol. 132, no. 023305–1, 2009.

[22] J. Coady, D. J. F. Toal, T. Newe, and G. Dooly, “Remote acoustic analysis for tool condition monitoring,” in *Flexible Automation and Intelligent Manufacturing (FAIM2019)*, 2019.

[23] E. L. Bonaldi, L. E. de L. Oliveira, and J. G. B. Silva, “Predictive Maintenance by Electrical Signature Analysis to Induction Motors,” in *Induction Motors - Modelling and Control*, London, UK: IntechOpen Limited, 2012.

[24] C. P. Salomon, C. Ferreira, and W. C. Sant’Ana, “A Study of Fault Diagnosis Based on Electrical Signature Analysis for Synchronous Generators Predictive Maintenance in Bulk Electric Systems,” *Energies 2019, MDPI*, vol. 12, no. 1506, p. 16, 2019.

[25] S. I. A. Sani, M. S. Misnan, and M. A. H. . et. al. Mohammed, “Improvement maintenance work through adopting a maintenance culture: focused the determinant factor which influence maintenance culture,” in *3rd international conference on business and economic research*, 2012.

[26] J. Moubray, *Reliability-centered Maintenance, 2nd edition*. New York, New York, USA: Industrial Press Inc., 2001.

[27] M. Usrey and R. G. Wilmeth, “Reliability-Centered Maintenance: A Case Study,” *Eng. Manag. J.*, vol. 12, pp. 25–31, 2000.

[28] A. Parida, U. Kumar, D. Galar, and C. Stenstrom, “Performance measurement and management for maintenance: a literature review,” *J. Qual. Maint. Eng.*, vol. 21, no. 1, pp. 2–33, 2015.

[29] J. Mourinho, F. Leiras, R. Correia, and A. Et, “A Vertical Predictive Maintenance Approach for Manufacturing 4.0,” in *Proceedings of Maintenance Performance Measurement and Management (MPMM) Conference*, 2018.

[30] R. L. . Dunn, “Predictive Maintenance Technologies,” *PLANT ENGINEERING MAGAZINE*, 2002. [Online]. Available: https://www.plantengineering.com/articles/predictive-maintenance-technologies/. [Accessed: 14-Oct-2019].

[31] Seebo, “INDUSTRY 4.0 PREDICTIVE MAINTENANCE - The Complete Guide.” .

[32] B. Christiansen, “A Complete Guide To Predictive Maintenance,” *Limble CMMS*, 2019. [Online]. Available: https://limblecmms.com/blog/predictive-maintenance/. [Accessed: 28-Oct-2019].

[33] D. Liggan, Liggan; Lyons, “Applying Predictive Maintenance Techniques to Utility Systems,” *Pharm. Eng. Off. Mag. ISPE*, vol. 31, no. 6, 2011.

[34] M. Coleman, Chris; Chandramouli, “Making maintenance smarter: Predictive maintenance and the digital supply network,” *Deloitte’s Digital Supply Networks capabilities*, 2017. [Online]. Available: https://www2.deloitte.com/us/en/insights/focus/industry-4-0/using-predictive-technologies-for-asset-maintenance.html. [Accessed: 14-Oct-2019].

[35] M. Mulders, Michel; Haarman, “Beyond the hype: PdM 4.0 delivers results,” *Predictive Maintenance 4.0*, p. 36, Sep-2018.

[36] AI Multiple, “Predictive Maintenance: In-depth Guide,” 2019. [Online]. Available: https://blog.aimultiple.com/predictive-maintenance/. [Accessed: 14-Oct-2019].

[37] BigData Republic, “Machine learning for predictive maintenance: where to start?,” 2017. [Online]. Available: https://medium.com/bigdatarepublic/machine-learning-for-predictive-maintenance-where-to-start-5f3b7586acfb. [Accessed: 14-Oct-2019].

[38] T. P. Banerjee and S. Das, “Multi-sensor data fusion using support vector machine for motor fault detection,” *Inf. Sci. (Ny).*, vol. 217, pp. 96–107, 2012.

[39] H. Li *et al.*, “Improving rail network velocity: A machine learning approach to predictive maintenance,” *Transp. Res. Part C Emerg. Technol.*, vol. 45, pp. 17–26, 2014.

[40] Z. Zhang, Y. Wang, and K. Wang, “Fault diagnosis and prognosis using wavelet packet decomposition, Fourier transform and artificial neural network,” *J. Intell. Manuf.*, vol. 24, no. 6, pp. 1213–1227, Dec. 2013.

[41] S. G. He, Z. He, and G. A. Wang, “Online monitoring and fault identification of mean shifts in bivariate processes using decision tree learning techniques,” *J. Intell. Manuf.*, vol. 24, no. 1, pp. 25–34, Feb. 2013.

[42] K. Y. Chen, L. S. Chen, M. C. Chen, and C. L. Lee, “Using SVM based method for equipment fault detection in a thermal power plant,” *Comput. Ind.*, vol. 62, no. 1, pp. 42–50, 2011.

[43] A. S. Willsky, “A survey of design methods for failure detection in dynamic systems,” *Automatica*, vol. 12, no. 6, pp. 601–611, 1976.

[44] I. Hwang, S. Kim, Y. Kim, and C. E. Seah, “A survey of fault detection, isolation, and reconfiguration methods,” *IEEE Trans. Control Syst. Technol.*, vol. 18, no. 3, pp. 636–653, 2010.

[45] J. J. Gertler, *Fault detection and diagnosis in engineering systems*. Routledge, 2017.

[46] V. Venkatasubramanian, R. Rengaswamy, K. Yin, and S. N. Kavuri, “A review of process fault detection and diagnosis part I: Quantitative model-based methods,” *Comput. Chem. Eng.*, vol. 27, no. 3, pp. 293–311, 2003.

[47] R. N. N. Clark, D. C. C. Fosth, and V. M. M. Walton, “Detecting Instrument Malfunctions in Control Systems,” *IEEE Trans. Aerosp. Electron. Syst.*, vol. AES-11, no. 4, pp. 465–473, 1975.

[48] R. Isermann, “Process fault detection based on modeling and estimation methods-A survey,” *Automatica*, vol. 20, no. 4, pp. 387–404, 1984.

[49] J. Gertler, “Fault detection and isolation using parity relations,” in *Control Engineering Practice*, 1997, vol. 5, no. 5, pp. 653–661.

[50] A. Wald, “Sequential tests of statistical hypotheses,” *Ann. Math. Stat.*, vol. 16, no. 2, pp. 117–186, 1945.

[51] E. S. Page, “Continuous Inspection Schemes,” *Biometrika*, vol. 41, no. 1/2, p. 100, 1954.

[52] S. Gentil, J. Montmain, and C. Combastel, “Combining FDI and AI approaches within causal-model-based diagnosis,” *EEE Trans. Syst. Man, Cybern. Part B Cybern.*, vol. 34, no. 5, pp. 2207–2221, 2004.

[53] D. Martínez-Rego, D. Fernández-Francos, O. Fontenla-Romero, and A. Alonso-Betanzos, “Stream change detection via passive-aggressive classification and Bernoulli CUSUM,” *Inf. Sci. (Ny).*, vol. 305, pp. 130–145, 2015.

[54] Z. Tian, “An artificial neural network method for remaining useful life prediction of equipment subject to condition monitoring,” *J. Intell. Manuf.*, vol. 23, no. 2, pp. 227–237, 2012.

[55] G. A. Susto, A. Schirru, S. Pampuri, S. McLoone, and A. Beghi, “Machine learning for predictive maintenance: A multiple classifier approach,” *IEEE Trans. Ind. Informatics*, vol. 11, no. 3, pp. 812–820, 2015.

[56] F. Yang and D. Xiao, “Progress in root cause and fault propagation analysis of large-scale industrial processes,” *J. Control Sci. Eng.*, 2012.

[57] M. Iri, K. Aoki, E. Oshima, and H. Matsuyama, “A Graphical Approach To The Problem Of Locating The Origin Of The System Failure,” *J. Oper. Res. Soc. Japan*, vol. 23, no. 4, pp. 295–312, 1980.

[58] H. M. Paynter, *Analysis and design of engineering systems*. MIT Press, 1961.

[59] H. and T. Cheng *et al.*, “Application of the enhanced dynamic causal digraph method on a three-layer board machine,” *IEEE Trans. Control Syst. Technol.*, vol. 19, no. 3, pp. 644–655, 2010.

[60] L. Leyval, S. Gentil, and S. Feray-Beamont, “Model-based causal reasoning for process supervision,” *Automatica*, vol. 30, no. 8, pp. 1295–1306, 1994.

[61] M. A. Kramer and B. L. Palowitch, “A rule-based approach to fault diagnosis using the signed directed graph,” *AIChE J.*, vol. 33, no. 7, pp. 1067–1078, Jul. 1987.

[62] F. Yang and D. Xiao, “Model and fault inference with the framework of probabilistic SDG,” in *9th International Conference on Control, Automation, Robotics and Vision, 2006, ICARCV ’06*, 2006.

[63] S. L. Bressler and A. K. Seth, “Wiener-Granger Causality: A well established methodology,” *Neuroimage*, vol. 58, no. 2, pp. 323–329, 2011.

[64] M. Bauer and N. F. Thornhill, “No A practical method for identifying the propagation path of plant-wide disturbances,” *J. Process Control*, vol. 18, no. 7–8, pp. 707–719, 2008.

[65] V. Dhar, “Data science and prediction,” *Commun. ACM*, vol. 12, pp. 64–73, 2013.

[66] Global Asset Protection Services, “GAPS Guidelines,” *Glob. Asset Prot. Serv.*, pp. 1–6, 2015.

[67] J. . M. K. Han, “Data mining: Concepts and techniques,” *Morgan Kaufmann Publ.*, 2001.

[68] Ulsan Press, “Hyundai motor diagnoses vehicle faults with noise and vibration,” 2018.

[69] R. B. Gmbh, “Predictive maintenance with the Nexeed production performance manager,” Bubenreuth.

[70] C. J. Fan, R.E.; Chang, K.W.; Hsieh, C.J.; Wang, X.R.;Lin, “Liblinear: A library for large linear classification,” *J. Mach. Learn. Res.*, pp. 1871–1874, 2008.

[71] B. Cline, B.; Niculescu, R. S.; Huffman, D.; Deckel, “Predictive maintenance applications for machine learning,” *Annu. Reliab. Maintainab. Symp.*, 2017.

[72] J. Seco and F. Verhaegen, *Monte Carlo techniques in radiation therapy*. CRC/Taylor & Francis, 2013.

[73] J. A. Sokolowski and C. M. Banks, *Principles of modeling and simulation : a multidisciplinary approach*. John Wiley, 2009.

[74] AnyLogic, “AnyLogic: Simulation Modeling Software Tools & Solutions for Business,” *https://www.anylogic.com/*, 2018. [Online]. Available: https://www.anylogic.com/.

[75] “Arena Simulation.” .

[76] “3D Simulation Modeling and Analysis Software | FlexSim.” .

[77] “Simulation Software for Process Improvement • ProcessModel.” .

[78] “WITNESS Simulation Modeling Software | Lanner.” .

[79] M. Garetti, P. Rosa, and S. Terzi, “Life Cycle Simulation for the design of Product-Service Systems,” *Comput. Ind.*, vol. 63, no. 4, pp. 361–369, 2012.

[80] G. N. Schroeder, C. Steinmetz, C. E. Pereira, and D. B. Espindola, “Digital Twin Data Modeling with AutomationML and a Communication Methodology for Data Exchange,” *IFAC-PapersOnLine*, vol. 49, no. 30, pp. 12–17, 2016.

[81] H. Liao, J. Lee, J. Ni, and D. Djurdjanovic, “Intelligent Prognostics Tools and E-maintenance,” *Fac. Publ. Other Work. -- Ind. Inf. Eng.*, Aug. 2006.

[82] Q. Qi and F. Tao, “Digital Twin and Big Data Towards Smart Manufacturing and Industry 4.0: 360 Degree Comparison,” *IEEE Access*, vol. 6, pp. 3585–3593, Jan. 2018.

[83] E. Negri, L. Fumagalli, and M. Macchi, “A Review of the Roles of Digital Twin in CPS-based Production Systems,” *Procedia Manuf.*, vol. 11, pp. 939–948, 2017.

[84] W. Kritzinger, M. Karner, G. Traar, J. Henjes, and W. Sihn, “Digital Twin in manufacturing: A categorical literature review and classification,” *IFAC-PapersOnLine*, vol. 51, no. 11, pp. 1016–1022, Jan. 2018.

[85] I-Scoop, “The Industrial Internet of Things (IIoT): the business guide to Industrial IoT.” [Online]. Available: https://www.i-scoop.eu/internet-of-things-guide/industrial-internet-things-iiot-saving-costs-innovation/#Industrial_Internet_of_Things_in_evolution_from_operational_efficiency_to_innovation.

[86] J. Green (CTO Data Virtualization), “The Internet of Things Reference Model Whitepaper,” *IOT World Forum*, 2014.

[87] J. van Kuilenburg, “The Ultimate Guide To Implementing IoT,” 2019. [Online]. Available: https://www.cloudcredential.org/blog/the-ultimate-guide-to-implementing-iot/. [Accessed: 14-Oct-2019].

[88] J. MSV, “10 Steps To Implementing A Successful Enterprise IoT Strategy,” 2016. [Online]. Available: https://www.forbes.com/sites/janakirammsv/2016/08/22/10-steps-to-implementing-a-successful-enterprise-iot-strategy/#1001e8288b9e.

[89] G. Hardik, “How to retrofit your legacy equipment for IoT enablement,” 2018. [Online]. Available: https://www.softwebsolutions.com/resources/adopting-iot-with-legacy-equipment.html.

[90] D. I. Solutions, “Retrofitting Legacy Assets for IoT Enablement,” 2017. [Online]. Available: https://www.dellemc.com/en-af/collaterals/unauth/offering-overview-documents/retrofitting-legacy-assets-iot-enablement.pdf. [Accessed: 24-Nov-2019].

[91] B. Blog, “Top 10 IoT Sensor Types.” .

[92] R. Sharma, “Top 15 Sensor Types Being Used Most By IoT Application Development Companies.” .

[93] U. P., “Reference Architectures and Standards for the Internet of Things and Big Data in Smart Manufacturing,” *7th Int. Conf. Futur. Internet Things Cloud*, 2019.

[94] M. Wood, “7 Important Government Regulations on Business You Must Know.,” 2019. [Online]. Available: https://www.fundera.com/blog/government-regulations-on-business. [Accessed: 05-Nov-2019].

[95] M. Manulis, “Sensors and Gateways and Edge Devices, Oh My,” 2019. [Online]. Available: https://medium.com/alvarium/sensors-and-gateways-and-edge-devices-oh-my-635f3aeb5fb5. [Accessed: 14-Oct-2019].

[96] A. Banafa, “IoT: Implementation and Challenges,” 2016. .

[97] N. Sakovich, “Internet of Things (IoT) Protocols and Connectivity Options: An Overview,” 2018. .

[98] A. Gerber, “Connecting all the things in the Internet of Things,” 2018. .

[99] M. Beyer, “Gartner says solving ‘big data’ challenge involves more than just managingvolumes of data,” 2011. .

[100] V. C. Chen, M.; Mao, S.; Zhang, Y.; Leung, *Big data: related technologies, challenges and future prospects*. 2014.

[101] H. Labrinidis, Alexandros; Jagadish and J. H. Agrawal, P Bernstein, E Bertino, S Davidson, U Dayal, M Franklin, J Gehrke, L Haas,A Halevy, “Challenges and opportunities with big data,” in *VLDB Endowment*, 2012, pp. 2032–2033.

[102] M. Doostparast, M., Kolahan, F., & Doostparast, “A reliability-based approach to optimize preventive maintenance scheduling for coherent systems,” *Reliab. Eng. Syst. Saf.*, vol. 126, pp. 98–106, 2014.

[103] M. Alexandros, Nanopoulos; Yannis, Manolopoulos; Maciej, Zakrzewicz;Tadeusz, “web access-logs for pattern queries,” in *4th international workshop*.

[104] E. A. brewer, “Towards robust distributed systems,” *InPODC*, p. 7, 2000.

[105] Rolls Royce, “How Rolls-Royce maintains jet engines with the IoT,” *RTInsights*, 2016.

[106] H. WangA, “A survey of maintenance policies of deteriorating systems,” *Eur J Oper Res*, pp. 469–489, 2002.

[107] J. A. Tekiner, F.;Keane, “Big data framework,” *IEEE Int. Conf. Syst. Man, Cybern.*, pp. 1494–1499, 2013.