IoT in Conjunction with Cloud Services for Industrial Applications Optimization

M. Papoutsidakis
Dept. of Automation Engineering
PUAS, Athens, Greece

D. Piromalis
Dept. of Automation Engineering
PUAS, Athens, Greece

E. Symeonaki
Dept. of Automation Engineering
PUAS, Athens, Greece

D. Tseles
Dept. of Automation Engineering
PUAS, Athens, Greece

ABSTRACT
It was recently observed that many companies that use industrial automation, wish to improve the performance of their production due to the competitive market, implement advances methods in the production procedures. These methods, called Industrial Internet of Things, aiming at distributing and managing an information not only from the production field in advanced levels of productive procedures like the one of cloud computing but also among the systems that administer the particular method. In the present paper advanced sensors, the structure of IIoT technology used for the wireless transmission of data from the sensors to the central server, the HMI will be presented along with a detailed description of Cloud services that co- operate with the above. The objective of the research, given that it deals with modern applications in industrial functions and services, will try to answer questions arisen such as if the combination of all previously mentioned optimizes the efficiency and operation of the production and also if it is easily comprehensible from its final users. From all the above mentioned, conclusions will be recorded about the application of such methods in the production procedures, their advantages and disadvantages will be debated and simultaneously refinements will be proposed so as to maximize further the benefits from the IIoT and Cloud co- operation. Possible outcomes of this technology application are expected to be the efficiency which in turn will increase the performance of the production connectivity with an easy transmission of information at real time and eventually the reliability of the method which will produce considerable economic benefits for the companies willing to implement it.

Keywords
Industrial Internet of Things, Cloud computing, Cloud services, Wireless Smart sensors, protocols of wireless communication, HMI, server.

1. INTRODUCTION
The development of technology and generally of electronic devices and electronic services opened up entirely new fields concerning modern industrial applications during the last decade. The procedure of collecting data within the limits of the premises by using smart wireless sensor in combination with HMI installed in clever devices and their transmission via internet in Cloud services boosted automation and scientific observation [1-4]. Moreover, the potential of the above things and clever devices offered initiative motive in order to investigate the perspective of registration and processing data at a distance exploiting the simultaneous development of wireless communication and Cloud services. Merging the above technologies and their application to the productive procedure led to innovation in the field of automation, which is called Industrial Internet of Things. Cloud computing that operates with that technology has greatly helped providing the potential of dynamic expansion at a very low cost exactly because the market of developing and creating new software and servers is not involved [5-7]. Contrary, to the numerous servers and backups located in different geographical positions in and out the industrial environment, Cloud computing that uses IIoT can be used everywhere reducing the cost of all extra expanses and the only drawback- question that needs to be answered is how safe these services can be regarded taking into account the existence of multiple threats in the internet.

This paper will present the potential of IIoT technology along with its advantages and disadvantages, the possibilities offered by wireless industrial sensors and the protocols in communication, the qualities of HMI, the benefits of smart devices compared to the traditional ways of collecting data, an analysis of offered Cloud services when simultaneously applied, the implementation of security methods in wireless industrial networks and Cloud computing and finally, there will be a reference in a simulated environment where the co-operation of all the above technologies will be illustrated.

2. INDUSTRIAL INTERNET OF THINGS (IIoT)
The term Industrial Internet of Things IOT (IIoT) refers to the advances technology which has lately been implemented in the field of Industry and is generally far more advanced that the well- known IoT. Using IIoT technology today by smart factories limits greatly the dependence on systems that collect data only from specific processes as the freedom offered enables accessibility at real time through any electronic means. The ability of a user to gain access through a smart phone, tablet or laptop to any kind of information since appropriate compatible software installed increases effectiveness, control and monitoring so as to reduce drastically the amount of time needed to manipulate and resolve emergency situations.

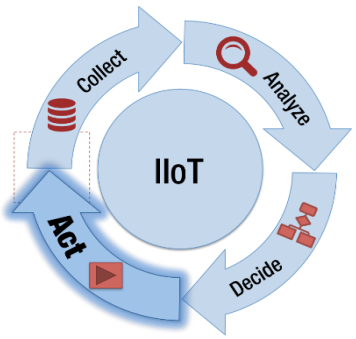

Fig 1: Diagram of IIoT technology

IIoT significantly helps improving performance, security, reliability and finally energy consumption issues and offer advantages which can be analyzed as follows:

- Collecting data from things which are wireless and run on batteries, reducing drastically the cost of actions consering decision taking compared to the past.
- Investigating data in course of action using large operating systems to analyse and transform them into an active and manageable information.
- Transmitting and presenting the active information to the specialist who can be within or out of the premises of the factory at real time.
- Improving the performance of the production under proper management.
- Reducing remedial actions during maintenance.
- Avoiding urgent interruptions in production due to unexpected damage or prolonging them for the machinery systems maintenance.
- Scheduling the maintenance works accordingly ensuring the availability of engineers.

IIoT technology has still to face a lot of challenges. Most of them concerning security, compatibility and cost. As for security, given there are plenty of methods and communication protocols that have a wireless connection with the fields sensors, it's a necessity to have them protected by developing software which offer security against any malicious actions that may adulterate their content and functions [8-11].

Innovations such as in-memory computing and massively distributed processing frameworks (like Hadoop) are important IoT catalysts for organizations that don't want to compromise speed when analyzing millions of data points. As these technologies have progressed in tandem with reduced sensor and wireless network connectivity costs, IoT analytics initiatives have approached a threshold point making investments more accessible to a broader population of organizations. The IoT data that organizations collect comes from machine sensors and logs that are not part of the traditional corporate data analysis lexicon. As such IoT data feeds tend to have a number of unique characteristics that must be accounted for. Given the persistent nature of IoT data feeds, successful streaming analytics is at the core of fundamentally unlocking value from connected devices. Table 1 details the most salient characteristics of IoT data.

Table 1. Characteristics of IoT data

Characteristics of IoT Data	
Streaming	• Machine log data and human-generated data such as messages and news alerts • Emphasis on identifying deltas within data streams • High velocity of data requires new techniques for data capture, processing, and throughput • Importance is in rapid appropriate response
High-Volume	• Requires archiving, data management, and analytics at scale • Key is to productionalize large data environments • High performance analytics must bring reporting to near-real-time results to make data useful
Semi-Structured	• Not modeled to fit well into relational databases • Requires additional parsing, ensuring data quality, and context to fit into a structured environment • Language and keyword frequency analytics are needed to fully analyze
Non-Standard	• Images, videos, voice, binaries • Require image recognition or audio analysis to support • Requires transformation and parsing

The persistent streaming of IoT data feeds presents a fundamental nuance between IoT analytics and more general Big Data analytics. Given the frequency and redundancy of the reported data, the vast majority of IoT data streams are not useful in a broader context. Instead, it is far more economical to focus on identifying deviations in data points rather than their value in absolute terms. Determining baseline levels of behavior allows data analysts to build alerts and take action when irregularities in optimal patterns occur. There are both direct and opportunity costs associated with analyzing data. Given the immense scale of data and all of the possible avenues of analysis, it is imperative to identify what patterns and deviations are vital to transmit, store, and further analyze. This prioritization allows organizations to best allocate their financial and computational resources to only the highest-value opportunities by compressing data storage and analysis time.

Operational data must be used iteratively to create a feedback loop where errors and faults are reduced as the organization finds more predictive and prescriptive indicators. The analytical investigations themselves will identify what new sensors are needed to capture additional data points for addressing business priorities. In this way, companies can create a continuously improving new normal and drive enhancements across all workflows associated with an Internet of Things project.

2.1 Industrial Wireless Sensor Network (IWSNs) and Security

Wireless sensor solutions are now being used in countless situations where it is necessary to monitor remote, difficult, and costly to reach locations, or moving applications. When choosing the best wireless approach, there are many technology tradeoffs and vendors to consider [12-13]. See Tables 1 below, which offer means to compare network selection criteria according to application needs.

Table 2. Criteria of IWSN selection

Criteria	Weight	IWSN A	IWSN B	IWSN C
Battery Life	25%	3	7	5
Security	35%	3	9	9
Network Design Flexibility	13%	1	9	5
Scalability	2%	3	9	7
Support for Future Application	10%	1	9	3
Stranded Investment Risk	7%	1	7	5
Ease of Use	7%	9	5	5
Total	**100%**	**2.8**	**8.1**	**6.3**

1 = Lowest, 9 = Highest

A search of technical publications and websites will turn up a variety of technical comparisons of industrial wireless sensor networks (IWSNs), which provide detailed analysis valuable to large end users or engineering firms with dedicated resources to evaluate technical nuances [14]. But many potential end users lack such resources, have a less formal selection process, and are perhaps not sure of the key differentiators when evaluating various options. Engineers making a selection typically use mixes of similar factors. They assign weights based on the use case, but the factors typically include:

- Availability of the communication link
- Security
- Scalability
- Connectivity to desired devices
- Hazardous location rating
- Power options to meet desired publication period
- Ease of use
- Integration with control systems
- Stranded investment risk
- Other practical factors specific to a given site.

Mesh networks offer many benefits including the ability to self-form, self-heal, and manage routing of communication packets. They also offer multiple takeout points (gateways) for redundancy and scalability. Their self-administering capabilities depend on complex algorithms used to determine the network design or topology. For example, they must constantly evaluate communication paths assigned to each hop between wireless sensors, along with the signal quality of each hop, avoiding hops resulting in more retries due to higher packet-error rates. For IWSNs with adequate mesh density (meaning enough nodes to provide multiple communication paths), the topology of a given network is typically stable.

On the other hand, a mesh network relying solely on its ability to self-organize may not meet determinism requirements for monitoring or control applications unable to tolerate longer latencies or deviations in latency (jitter). Some wireless mesh networks allow users to set the maximum allowable number of hops from a sensor to a takeout point (mesh depth), but flexibility in designing a specific network following a desired structure is often beneficial.

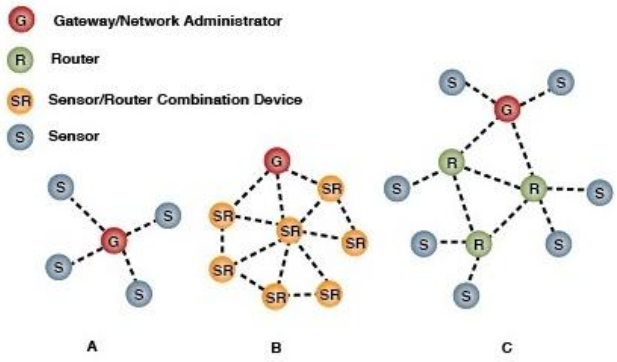

Fig 2: IWSN Topology Diagram

The subject of wireless security is a combination of intrigue, hard work, trial and error, and finally success. The perfection of wireless security has allowed the technology to evolve within two years from a novelty that was untrusted and used only as a last resort to a technology that is becoming an essential part of the fabric of data communication, and everyday life. It is predicted that soon most people will have a mobile smartphone as their primary computer. Wireless has become the communications medium of choice for many people. However, without effective data security, wireless technology could not grow and people would still be reliant on wired systems along with the cost and inconvenience associated with them. The first attempt at securing the network was called wired equivalent privacy (WEP). The intent of WEP was to provide an equivalent measure of data confidentiality to wireless networks as was available in wired networks. WEP was based on the Rivest Algorithm, otherwise known as rivest cipher 4 (RC4), for encryption. WEP used a 24-bit randomly generated "initialization vector" (IV) and a 40- or 104-bit static key (for 64-bit and 128-bit WEP, respectively) to encrypt plain text. The key must match on both the client device and access point. Combining the key, along with its integrity check value (ICV), with the keystream, encrypts a plain text message. Concatenating the secret key with the 24-bit initialization vector (IV) and applying the encryption algorithm, RC4, produce the keystream. Concatenation is a logic function creating a symbol or sequence by placing one value after another, in this case the key with the IV and the message with the ICV. At each round of encryption, the IV would be incremented, producing a unique IV and keystream for each message. WEP suffered from inherent flaws related to key construction and IV reuse. The IV was transmitted plain text, and it was possible to determine the secret key using various techniques exploiting IV reuse and collisions. The ICV was based on CRC-32, which was not designed to be secure; this provided another means of exploitation. Using commonly available tools, WEP can be cracked in fewer than 10 minutes; WEP is no longer used and should be avoided, even in small office/home office (SOHO) environments. Temporal key integrity protocol (TKIP) was designed to remedy the IV reuse issue. TKIP provides data security while using existing equipment that could be upgraded through firmware upgrades. TKIP was developed jointly by the IEEE 802.11i task group and the Wi-Fi Alliance to replace WEP.

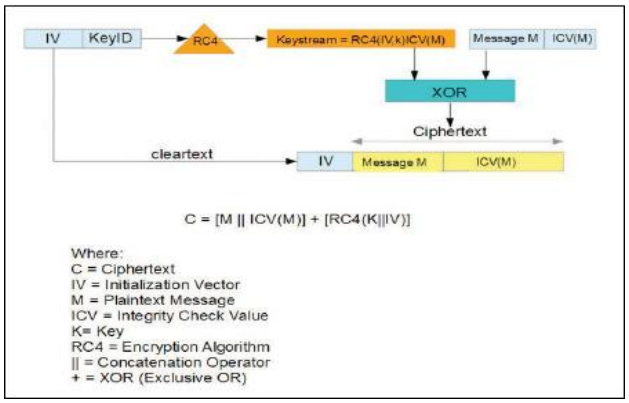

Fig 3: Block Diagram of WEP encryption

Data collection is the first step to make decisions via mobile human-machine interface (HMI) devices such as smartphones, tablets, and laptops. With the right data collected, mobile HMI solutions help bridge the gap between control systems and mobile devices needing access to their information. While these solutions may be installed as just a window into the manufacturing process, data collection functionality also can provide visualization and analysis tools, both of which are critical for mobile HMI applications. There is a whole process that needs to be understood that starts with data collection and ends with better decision making through use of mobile HMI devices. HMI data stored in many different locations is available for remote access by mobile devices. HMIs can store data locally in text files, spreadsheet formats, or a variety of databases and historians. An HMI can be connected to a corporate database or local historian, or even a historian service hosted in the cloud, for data storage and access. Mobile devices can then be connected to these data storage locations. This data can be viewed and used by engineering, operations, scheduling, and management personnel. Additional connections allow field engineers and plant floor personnel to access the data via mobile devices, thin clients, or PCs. Data collected from field devices and viewed on mobile devices has many different uses as listed in the table below. Some of these can be implemented just by viewing field device data, such as maintenance and troubleshooting. Other uses require intermediate analysis and/or combination with other data by specialized applications to yield full value as shown in the table below:

2.2 Statistics of Use

According to the last survey of the Control Engineer Magazine regard to familiarity about IIoT technology the Fifty-nine percent of respondents identified as being "very" or "somewhat" familiar with the IIoT framework, compared to 29% being not very familiar and 12% not at all familiar.

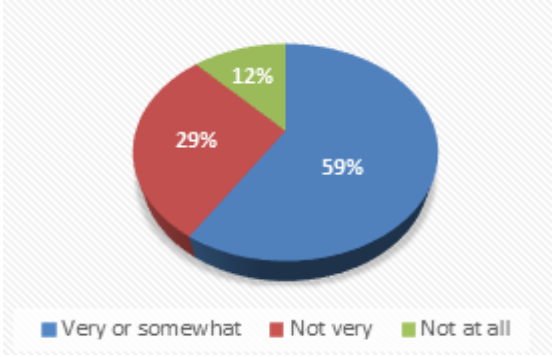

Fig 4: Familiarity of Engineers with IIoT

The survey continues with the installation of security software programs with the 18% of the responders to have completed the implementation compared with the 35% to be in progress and 29% beginning to employ.

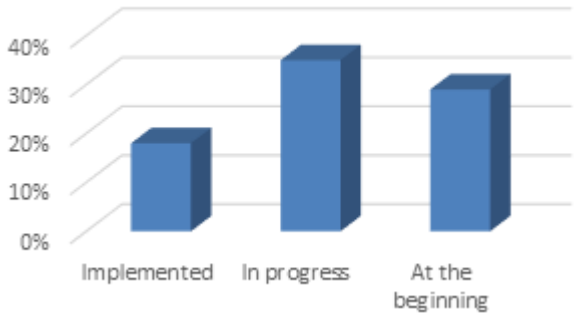

Fig 5: Installation of Security Programs

Finally, concerning the most famous IIoT attributes from the responders that answered the Real time capabilities cover the 83% of all, the interoperability (80%) and the modularity (78%).

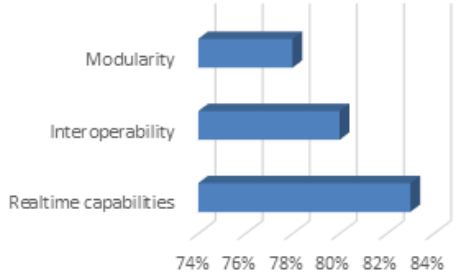

Fig 6: IIoT Attributes

3. CLOUD COMPUTING

The original idea of Cloud Computing dates back to 1950's when large scale central computers became available at universities and businesses accessible through personal terminals. Acquiring a central computer was costly, so it was necessary to find ways to ensure maximum profits from such an investment, allowing multiple users sharing access and CPU time from multiple terminals, eliminating inert time which became known as timesharing in the network industry. As computers were growing in popularity, scientists and technologists wanted to research on ways so as to offer maximum IT capacity to more users through timesharing. This could be done with the use of algorithms in order for the infrastructure and applications to provide efficient use, giving priority to CPU access and finally better service to the final users. Cloud Computing can be separated to three different services which are the follows: Software as a service, Platform as a service, Infrastructure as a service.

- IaaS: Infrastructure as a Service

Cloud infrastructure services known as Infrastructure as a Service (IaaS) are self-service models for accessing, monitoring and managing remote datacenter infrastructures such as compute (virtualized or bare metal), storage, networking and networking services(e.g firewalls).

- PaaS: Platform as a Service

Cloud platform services, or Platform as a Service (PaaS), are used for applications and other development, while providing Cloud components to software. What developers gain with PaaS is a framework they can build upon to develop or customize applications PaaS makes the development testing and deployment of applications quick, simple and cost effective. With this technology enterprise operations or a third- party provider can manage OSes, virtualization, servers, storage, networking and the PaaS software itself.

- SaaS: Software as a Service

Cloud application services, or Software as a Service, uses the web to deliver applications that are managed by a third – party vendor and whose interface is accessed on the clients' side. Most SaaS applications can be run directly from a Web browser without any downloads or installations required.

Cloud Computing can also be separated to three main different models which are private, public and hybrid.

- Private Cloud

A private cloud is a particular model of cloud computing that involves a distinct and secure cloud based environment in which only the specified client can operate. As with other cloud models, private clouds will provide computing power as a service within a virtualized environment using an underlying pool of physical computing resource. However, under the private cloud model, the cloud (the pool of resource) is only accessible by a single organization providing that organization with greater control and privacy.

- Public Cloud

The most recognizable model of cloud computing to many consumers is the public cloud model, under which cloud services are provided in a virtualized environment, constructed using pooled shared physical resources, and accessible over a public network such as the internet. To some extent they can be defined in contrast to private clouds which ring-fence the pool of underlying computing resources, creating a distinct cloud platform to which only a single organization has access. Public clouds, however, provide services to multiple clients using the same shared infrastructure.

- Hybrid Cloud

A hybrid cloud is an integrated cloud service utilizing both private and public clouds to perform distinct functions within the same organization. All cloud computing services should offer certain efficiencies to differing degrees but public cloud services are likely to be more cost efficient and scalable than private clouds. Therefore, an organization can maximize their efficiencies by employing public cloud services for all non-sensitive operations, only relying on a private cloud where they require it and ensuring that all of their platforms are seamlessly integrated.

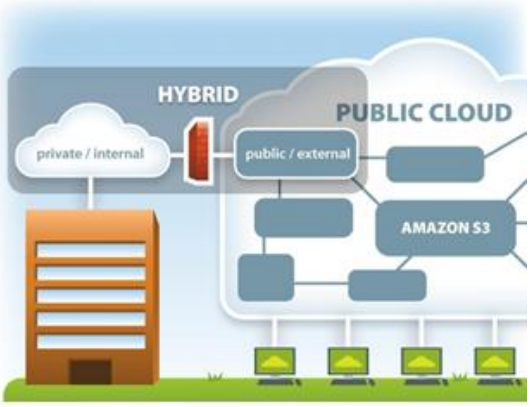

Fig 7: Hybrid Cloud

The combination of Cloud services with IIoT technology offers the opportunity of having access to the production procedure and handling data, always conforming to strict safety protocols. Cloud computing services offer dynamic expanding at a low cost because the market of developing new software and servers is not implicated. In addition, there are plenty other advantages:

- Any applications can be added, whenever needed.
- Buying material and licensed software becomes unnecessary.
- There is infinite storage room which can be bought gradually.
- Improved reliability is offered due to multiple connections to the internet and availability of more backup servers.
- New structure services can be built and function within minutes.
- Data and background information can be provided to any type of device, including a smartphone, at real time, as long as it has internet access.
- Frequent updating Cloud computing services.

The only disadvantage is how secure these services can be regarded, since there are plenty of threats in the Internet. Information and data of the production procedures and processes in the environment of the factory will be available in private and public Cloud computing round the clock. Therefore, firewall protection from any external threats must be installed both within the network of the LAN company and out of it, given the fact Internet is used.

Finally people involved in operating the services provided must be trustworthy in order to reduce as much as possible the risk of leaking information to outsiders pertaining the company's data.

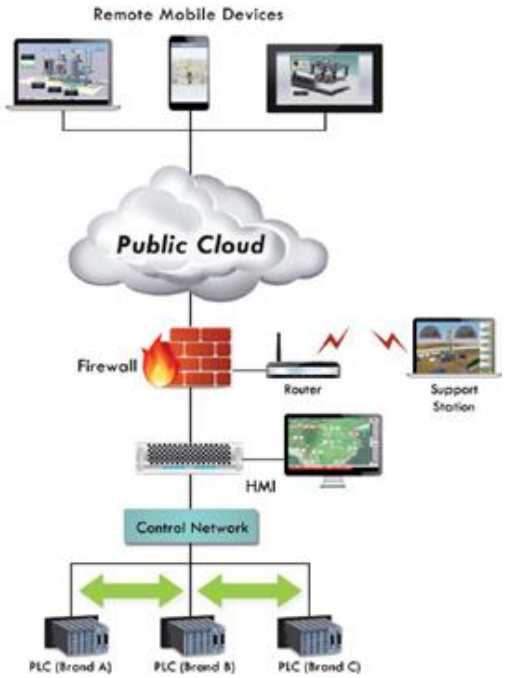

Fig 8: Co-operation IIoT with Cloud Computing Technology

The advantages concerning data security offered by Cloud computing can be summarized like, the displacement of public data in an external Cloud service reduces the exposure of sensitive internal data, the homogeneity of Cloud makes security checks simpler and the fact that Cloud enables automatic management of security.

The challenges regarding data security in Cloud computing systems are:

- Providers' credibility according to the security standards.
- Weakness on the part of the client to respond to established facts of security checks.
- Receiving support for investigations.
- Tacit responsibility of the administrator.
- Loss of control
- Exclusive applications cannot be examined.
- Appealing to hackers (something so commercial and revolutionary is normal to attract them)

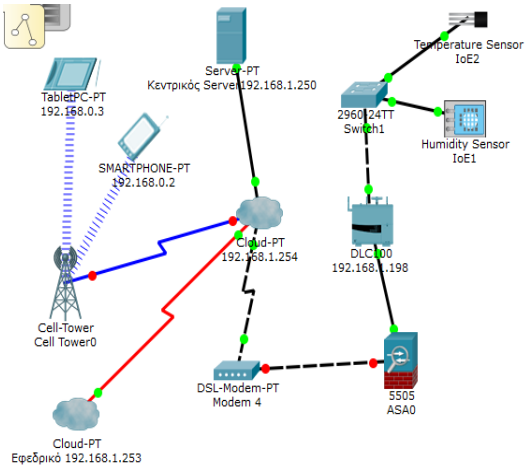

Fig 9: Hybrid Cloud

4. CONCLUSIONS AND FUTURE IMPROVEMENTS

This paper focused on analyzing IIoT technology and Cloud services pinpointed the benefits of their combination in the industrial production. Major benefits include the instant updating at real time by using clever devices, efficiency, reliability, interoperability, prompt prediction to avoid damage, profit by raising revenue and finally security from external threats. All the above, according to recent statistics, makes more and more companies active in the industrial production willing to install these technologies in their premises. However, there are companies which avoid their application mainly because of concern about secure data from Internet threats and also the lack of smart devices, relying on the human factor for the operational procedures. Nevertheless, investment on such systems is expected to be on the rise in the next few years by about 32-55%, with engineers working an average of 10 projects per year.

As the volume of data continuously increases due to the risen productivity with the application of all the above mentioned, a question arises over their management by the systems analysis. This issue relates to the time and cost, as engineers need to put a lot of effort into reaching conclusions pertaining production procedures, thus reducing their productivity. A proposed solution to this is the application of IT technology which will help engineers to arrive at safe solutions and decision- making at a much faster pace. This new application will partially clash with IIoT technology which will be in need of radical reform since many systems comprising it will be replaced with new and more advanced ones, compatible with applications that are going to be developed. The future of smart factories expected to have a rapid and breaking development in the near future.

5. ACKNOWLEDGMENTS

All authors would like to express their gratitude to the Post-Graduate Program of Studies "Automation of Productions and Services" of PUAS, for the financial support to undertake this research project

6. REFERENCES

[1] Richard Clark, August 2016, "Mobile HMI improves plant operations", available: (http://bt.editionsbyfry.com/publication/?i=328299#{"issue_id":328299,"page":0}, last access 17/4/2017).

[2] Michael Zhang, October 2016, "Managing processes with the IIoT available:http://bt.e-ditionsbyfry.com/publication/?i=346513#{"issue_id":346513,"page":0}, last access 17/4/2017).

[3] Dana Pasquali, April 2015, "Validation among insecurities", Control Engineer Magazine.

[4] Daniel E. Capano, April 2015, "Wireless security basics, standards", Control Engineer Magazine.

[5] Amanda Pelliccione, January 2016, "Digital Report IIoT 2016", Control Engineer Magazine.

[6] K. Sohraby, D. Minoli, T. Znati, "Wireless sensor networks: Technology,Protocols, and Applications", Wiley-Interscience, 2007.

[7] Kevin Zamzow, 26 October 2015, "Practical considerations for selecting an industrial wireless sensor network", available: (http://www.controleng.com/industry-news/single-article/practical-considerations-for-selecting-an-industrial-wireless-sensor-network/4981723af570e1ec3ab00dbaf7b552da.html, last access 17/4/2017).

[8] Lynnette Reese, RF Wireless Technology, available:(http://gr.mouser.com/applications/rf-sensor-networks/, last access 17/4/2017).

[9] EngineersGarage, "Sensors: Different Types of Sensors",availiable: (https://www.engineersgarage.com/articles/sensors, last access 17/4/2017).

[10] SAS, "IoT", available: (https://www.sas.com/el_gr/insights/big-data/internet-of-things.html#m=the-internet-of-things-infographic, last access 19/4/2017).

[11] Shshil B., Leena J., Sandeep J. (2010), "Cloud Computing", International Journal of Engineerig and Information Technology.

[12] Gustavo A. A. Santana, April 2016, "Official Cert Guide", CCNA Cloud CLDFND 210-451.

[13] Zebra Technologies, "Electronic Product Code (EPC) RFID technology", available:(https://www.zebra.com/us/en/resource-library/getting-started/rfid-printing-encoding/epc-rfid-technology.html#epc, last access 7/5/2017).

[14] Vael M., Μάϊος 2010, "Cloud Computing, An insight in the Governance & Security aspects", ISACA Belgium.