Table 1. Acronyms

CC	Cloud computing
CMS	Content management system
CIMP	Computer integrated manufacturing pyramid
HMS	Heterogeneous multiprotocol scenario
HTML	Hypertext markup language
IIoT	Industrial internet of things
IMS	Information management system
IoT	Internet of things
IT	Information technology
LAN	Local area network
LMS	Learning management system
M2M	Machine to machine
MQTT	Message queuing telemetry transport
nbAcc	NBPIIoT's software service element
nbInteg	NBPIIoT's integration element
nbGW	NBPIIoT's gateway element
nbManag	NBPIIoT's management element
NBPIIoT	NEBSYST platform for industrial IoT
nbUI	NBPIIoT's interface element
nbVF	NBPIIoT's frontier element
OT	Operation technology
PLC	Programable logic controller
PSI	Private software interface
REST	Representational state transfer
RFID	Passive radio frequency identification
TCP	Transmission control protocol
URL	Uniform resource locator
VPN	Virtual private network

1. Introduction.

We are currently living the era of the internet of things (IoT), [1], which has been fostered by the electronic and communications revolution happened in recent decades. The already great number of devices connected is continuously increasing, while their size and energy consumption keep decreasing. These IoT devices offer network interfaces that allow the interaction between a user/manager and the device through the network. These interfaces are usually developed by the manufacturers and so, they constitute a private software

interface (PSI). Within the IoT, a great variety of devices, as for example appliances and other electric equipment, are publicly accessed. The essence of the IoT's structure is presented in Figure 1, where appliances are accessible through a smartphone and their local area network (LAN). This basic architecture has been used in older IoT works such as [2]. To get this accessibility, the user must first register in a cloud, which is usually run by the manufacturer of the appliance, meaning that the management of the data is completely unknown for the end user in most cases. This lack of privacy does not dissuade people from using those devices (in many cases, because the only alternative is not to use such device at all), but also, nowadays, people manage a large part of their professional, personal and leisure information through the Internet, [3], within a cloud (cloud computing CC), [4].

Thus, the accessibility provided by the IoT to connected devices poses an interesting scenario. However, its lack of security and privacy rules out its use in the business and the industrial environments, [5]. For this reason, in the last decade, the technical literature presents a great number of works that analyse and try to solve this problem, [6]-[7].

Apart from smart homes and the industrial world, we consider and additional important use case: research and higher education. In this scenario, industrial plants are also used in scientistic and technological areas. However, research and educational plants are managed at laboratory scale and are usually referred to as pilot plants, [8]-[10]. Essentially, a pilot plant is the same as an industrial plant, only in a smaller scale, [9]. Most of the pilot plants currently used in research and teaching are used in a traditional hands-on manner. However, their remote access presents several advantages that have been underlined by the recent pandemic.

This paper proposes a complete communications management system, named NEBSYST platform for industrial IoT (NBPIIoT), that makes possible the easy implementation of

remote access to the data and devices belonging to a company, institution, or person. The remote access implemented by this system is secure, controlled, organized and collaborative. It is secure because the data are encrypted to be transmitted and the access is carried out point-to-point and by means of user profiles. It is controlled because filters with different operating criteria can be applied to NBPIIoT's access, such as the time zone. It is ordered because access can be sequenced, and it is collaborative because concurrent access can also be established, if required. To emphasize the security, note that the accesses implemented by NBPIIoT are point to point, unlike those provided by the VPN (virtual private network) method, which connects networks. So, using a VPN, the user has access to all the computers and devices connected to the network, while using NBPIIoT the user only has access to one computer/device per connection.

NBPIIoT can be used to easily implement cloud services for configurating and accessing to all type of sensors, actuators, and controllers. The access to the LANs in which the data is stored and the devices are connected, is configured as a cloud accessible from the internet. This LAN, turned into a cloud, is completely controlled by the owner, which solves the problem of the lack of privacy for the owned IoT devices. Among other features, NBPIIoT allows defining user profiles to control the selective access to the different devices and data. In addition, NBPIIoT allows connecting to different LANs with distributed devices and data storage systems. Moreover, the LANs can be mobile. Finally, the cloud can be configured within a private server or within an IaaS (Infrastructure-as-a-Service) provider, replacing a cloud that is unknown and/or uncontrollable by the user. All these characteristics make NBPIIoT a secure and private system useful not only in smart homes but also in industrial and research/training scenarios.

To cover the large casuistry of cases that can occur in all scenarios (homes, industry, research, and teaching), an IoT platform should be able to support both PSIs and open systems, as NBPIIoT does.

In this paper, the authors propose not only a theoretical framework, but also an implemented and operative IoT platform, that is modular and applicable to all the discussed scenarios.

2. The IoT in the industry.

This section is dedicated to reviewing the IoT in industry contexts where security and privacy are key issues with more strict requirements than other use scenarios like smart homes or education. By presenting this particular context, we set a high standard NBPIIoT must meet. If it does (which is discussed in Sections 3 and 5), we can extrapolate its suitability to other, less restrictive, cases like smart homes, research, and education.

As discussed in the introduction, IoT, as it is currently working in smart homes~~,~~ is not suitable for industries to make their devices accessible from the internet. However, one of the main innovative objectives in which many companies are currently involved is to improve their accessibility. I.e. many companies are enabling the remote access to the information technology (IT) layer, which is the upper layer of the traditional communications model currently used in industrial scenarios. This model is denominated computer integrated manufacturing pyramid (CIMP), it is represented in Figure 2 and similar representations can be found in other modern IoT works, such as [11]. It is traditionally related to the commercial management, whilst the lowest levels of the pyramid correspond to the layer of operational technology (OT) and are directly related to the physical devices involved in manufacturing processes. Thus, IT is currently

immersed in the task of its own connectivity, while OT faces the security and privacy problems discussed above to achieve that same objective.

In this framework, the integration of the IT and OT layers in the cloud can generate numerous advantages to the companies and to the society in general. Thus, IT/OT convergence enables direct control of the complete monitoring system in an industry, through the automation and the integration of communications systems and industrial networks. To achieve this convergence, there are several commercial platforms. However, in many cases, they do not support all the applications existing in a company because, as noted above, the manufacturer of each device provides its own PSI, [12]-[14].

The overall situation becomes even more complex because open solutions are becoming increasingly popular and should ideally be supported by IoT platforms too, [15]-[17]. The popularity of low-cost platforms such as Arduino [18], Phidget [19] or Raspberry Pi [20], among others, is increasing greatly, as they present very similar functionalities to those of the PSI's provided by the IoT devices manufacturers, [21]-[22].

Either with commercial devices or with devices designed and configured with open hardware, the introduction of the IoT into the industrial world is a trend known as industrial internet of things (IIoT). The structure presented in Figure 1 for smart homes IoT must be modified to fit the IIoT. First, in the industrial world, the appliances are replaced by complex machinery equipped with sensors and actuators, included in the device layer in Figure 3, which is similar to the one presented in [23]. Another difference between Figures 1 and 3 is the existence of controllers. Most of the machinery need controllers, and the set of all these controllers constitutes the fog layer in Figure 3. Consequently, a great variety of protocols can be used: those typically used in the industry, such as Modbus, [24], low-cost ones used in IoT, such as MQTT (message queuing telemetry transport) or REST (representational state transfer), or those used in

low-level communications, such as TCP (transmission control protocol) Sockets. In addition, the PSI from commercial devices must be considered and supported.

Thus, in Figure 3, open-hardware and free-software platforms are connected to a LAN, as well as controllers that use PSI, as for example industrial PLCs (programmable logic controller). The protocol each platform uses is different. Moreover, although in Figure 3 one only LAN is represented, an institution may use several, and they all must be integrated to achieve the global connectivity.

Finally, the last modification in Figure 3 with respect to Figure 1 is that controllers used in the industries are usually not accessible from the internet, but only from the LAN they are connected to. In addition, client connections are usually carried out by means of computers (or, in some cases, tablets). instead of smartphones.

3. The NBPIIoT platform.

3.1. Introduction to NBPIIoT

The main objective of NBPIIoT is to provide a communication system that enables and manages the connection of a user interfaces to the devices connected to a LAN. Its architecture is based on a 4-stage IoT structure [23] called device-to-gateway-to-cloud, (see Figure 4), and interested readers can find more details about it in [24]. The rest of this section describes and analyses how this structure is suitable and appliable to IoT and IIoT scenarios, and what role do the different elements and components of NBPIIoT (mainly, nbVF and nbGW) play in this.

3.2.Application of NBPIIoT to IoT scenarios

In the IoT architecture described in Section 1, the access to the different elements and data accessible from the cloud, is unsorted and non-interrelated. Each device or equipment may be accessed from the internet by anyone. However, to introduce privacy

and security, the devices should be accessible only through a cloud and just by a selected set of users (internal or external to the institution). They may also set the permissions associated to each user by means of user profiles. In addition, the access should be point-to-point (instead of an access that enables connections to all the devices connected to the LAN, like a VPN does), as well as the permissions associated to each user. This new scenario provides a secure and private access to the information and the devices, that can be remotely used and configured. These are the functionalities corresponding to NBPIIoT, whose architecture is shown in Figure 4. Just like in the architecture represented in Figure 3, in this case, a heterogeneous multiprotocol scenario is considered, and the improvements introduced in Figure 4 versus Figures 1 and 3 (and thus, the works based on such architectures, like [2] and [22], respectively) are the following:

1. A new layer has been added (the cloud layer) that supports the users to access to the fog layer through a cloud. Data centres and the NBPIIoT's element named nbVF are in this layer. Although the cloud layer has been widely used in technical previous work, nbVF is one of the novelties introduced by NBPIIoT.
2. The cloud is accessible from the internet through computers, smartphones, etc., as in Figure 1, and using any of commercial browser, despite any possible limitations imposed by them to the free connectivity.
3. There is a new element in the fog layer: nbGW. This element is other novelty introduced by NBPIIoT.

nbVF and nbGW are modules that specifically belong to the architecture proposed and used by NBPIIoT. On the one hand, nbGW acts as a gateway between fog and cloud layers and enables the machine-to-machine (M2M) communications between all the controllers connected to the fog layer (see Figure 4). In this way, the information between

the fog and the cloud layers can be decreased. On the other hand, nbGW sorts the information generated in the fog layer before sending it to the cloud layer, increasing the system performance and decreases the traffic through the cloud layer, [27]-[28]. The information transfer between fog and cloud layers constitutes the machine-to-people (M2P) communication mode, lines green and black in Figure 4. NBPIIoT provides a variant applicable to the M2P: the remote access to the devices through the cloud layer must be established through nbVF. Thus, users can access all those configurable resources, whose data can be stored and reviewed with minimal computational costs. This scenario presents IoT advantages with the possibility of controlling the access by means of nbVF.

The role of nbGW, located in the fog layer, is to publish the access to the controllers in the cloud in a sorted, controlled, and transparent way, making it transparent to the communication protocol that is used (whether it is proprietary or open). In the case of using PSI (proprietary platform), the variety of protocols is very wide, and the communication channels are implemented by socket tunnels. In the case of open platforms, the chosen protocol is web-based to achieve interoperability and usability; and the access channels between the user computer and the fog layer are identified by the corresponding URL (Uniform Resource Locator).

Therefore, nbVF incorporates the necessary protocol to establish the communication between nbGW and the cloud. Thus, nbGW makes public in the cloud layer (using nbVF) the access to the fog layer from the internet, using a middleware layer, which makes the communication process between the user computer and the controller allocated in the fog layer transparent, [29]-[30].

A user interface, running in a PC (or smartphone, etc.) is necessary by the user to interact with the devices, because it includes the elements necessary to display the sensor readings

and to send reference values to the actuators, among others. If the interface is developed in open platforms and/or runs in a web browser, it is denominated nbUI and carried out within NBPIIoT. Otherwise, the interface is provided by the device manufacturer, and it is denominated PSI. nbUI is directly connected to the fog layer through the cloud layer (using nbVF and nbGW) and a web-based protocol. To access the cloud from the user's browser through a PSI, NBPIIoT proposes the installation of a software service, denominated nbAcc, on the user's computer. This service is the link between the user's computer, its browser, the PSI and the cloud. I.e., nbAcc receives browser commands through a WebSocket connection and opens the necessary communication channels between the user's computer and the cloud, and also runs the PSI.

Regarding the rest of connections, two tunnels are created by nbGW to enable communications between nbVF and the corresponding controller in the fog layer. The first tunnel allows the access based on open platforms through the URL that refers to the corresponding controller. The second tunnel is the socket tunnel necessary to establish the access to the devices from the PSI. In both cases, the information is encrypted.

Thus, NBPIIoT establishes the most suitable topology for each device/equipment requirements and makes the intricacies of the communications process transparent to users and system managers in companies/institutions, while supporting choosing which devices should be remotely accessible and defining different user profiles with different permissions to access them. Moreover, an NBPIIoT manager can also sort and filter the data related to the operating/production devices, hardware data and maintenance software, among others. All this information can be safely accessed to retrieve information or to manage the physical devices or systems. NBPIIoT also allows setting up a network in which data from multiple industries/institutions are collected and

analysed to support the decision-making process. Therefore, the IT and OT integration is achieved, as well as the complete connectivity of the company/institution.

4. The practical implementation of NBPIIoT.

NBPIIoT is suitable for any installation size, from a single house to an industrial plant, including office buildings and research or educational labs. The platform is presented in Figure 5, in which the controllers are connected to a LAN where nbGW is also located. There must be a nbGW device connected to each LAN in the Institution. All nbGW devices deployed in a company/institution can work with the same single nbVF module. Moreover, several companies/institutions can share an nbVF, if they want.

In addition to the modules described above (nbGW, nbVF and nbUI), whose roles have already been described, Figure 5 introduces a new module called nbInteg. nbInteg integrates the cloud services and nbUIs applications in a wide variety of web content management systems (CMS), learning management systems (LMS) or other general-purpose information management system (IMS). This element is necessary to achieve the complete convergence in those companies/institutions with a corporate IMS. nbInteg also allows the addition of applications as a booking system to order the remote access to each device. In the URL https://moodle.nebsyst.com/ the remote access to physical experiments from several universities has been provided by NBPIIoT for several years.

As explained in Section 3, nbUIs manage the configuration of convergent sensors, actuators, and controllers to be used with HTML5 (hypertext markup language) web applications.

NBPIIoT also provides an intuitive web application (nbManag, see Figure 6) to configure accesses. It allows, among many other options, assigning connections and access levels

to different user profiles for accessing the controllers. This application makes the NBPIIoT administration accessible to users with no technical skills.

NBPIIoT presents the possibility of creating point-to-point single connections and point-to-point multiple simultaneous connections (for collaborative access). In the latter case, NBPIIoT allows selecting the user which has control over the system, while the rest would have the role of spectators. In the same line, NBPIIoT can configure a system to allow just one single connection simultaneously, in which case, the order of the accesses between the different users is managed by means of a booking system that may be integrated within and IMS, as explained before.

Therefore, the physical implementation of NBPIIoT, which operation can be tested in the URL https:/moodle.nebsyst.com, indicated above, until obtaining a commercial product with its own configuration software can be considered as a novelty presented in this work.

5. NBPIIoT main applications.

One of the main advantages of the architecture used by NBPIIoT is its versatility. A set of possible applications are detailed bellow. The applications have been chosen to involve all the sectors in which the 4.0 philosophy has been introduced so far.

A. Smart homes.

NBPIIoT makes any home LAN accessible from anywhere with security and privacy. This way, the devices, systems, microprocessors, and microcontrollers at that home can be used and configured through the internet. Thus, the home becomes a smart home, providing the possibility of monitoring and managing appliances and systems, such as lighting, climate, or entertainment, remotely. The user interfaces can be those provided by the manufacturers or designed ad-hoc. The different connections and the different

users' permissions can be managed by the homeowner in an easy way, by means of nbManag.

The main novelty with respect to the existing solutions is, besides its improved security and privacy, that it enables the access to the computers connected to the LAN, too. This is the base of a particular case of smart home which deserves being mentioned explicitly: remote offices. Indeed, offices could implement remote work by simply connecting nbGW to their respective LANs. This way, all computers with nbAcc would be remotely accessible with all the guaranties of security and privacy.

B. Remote training and remote research.

Experimental work in education and research organizations presents a use case scenario that can be enhanced by supporting the remote access to the lab resources. In fact, limitations like lack of financial resources to attend face-to-face classes or traditional hands-on lab work sessions and living in remote locations, can be overcome with remote access to classes, as well as handicapped people's difficulties. Traditional methodologies are becoming obsolete and are being replaced by blended learning methodologies that can be easily implemented with the NBPIIoT framework. The main novelty with respect to the existing solutions is that NBPIIoT also allows different institutions to easily share their experiment catalogues, keeping their accessibility to students 7 days a week, 24 hours a day. This way, lab work can even be carried out in times of pandemic.

C. Industrial world.

NBPIIoT provides the main design principles in Industry 4.0 with the necessary security and privacy. In fact, NBPIIoT allows the integration of IT and OT layers and the implementation of data analytics in conjunction with a real-time decision support system. NBPIIoT supports building highly flexible production systems, with real-time

interactions between people, products, and devices during the production process. The adaptability provided by NBPIIoT enables the shift from mass production to mass customization. Each product, at the end of the supply chain, can have unique characteristics defined by the end customer. The optimization of M2M and M2P connections drives significant improvements in terms of waste and cost reduction, generates robust processes and reduced downtime related to maintenance operations. The main novelty with respect to the existing solutions is the real-time end-to-end transparency provided by NBPIIoT, which enables early verification of engineering decisions, more flexible responses to disruptions, and overall optimization at the production level.

6. Discussion and comparative.

Nowadays, there are many, and heterogeneous, IoT devices in use for different purposes, and this number keeps increasing every year. In addition, there are numerous companies that address the implementation of the Industry 4.0 philosophy in factories. Finally, some of the main manufacturers of educational experimental systems provide remote access to their equipment. NBPIIoT improves all these systems as follows:

- IoT devices may benefit from NBPIIoT thanks to the increase in security and privacy.
- For smart factories, NBPIIoT improves the current Industrial IoT systems because it supports the integration of equipment connected to different LANs and provided by different manufactures with their own proprietary interfaces, as well as those based on open hardware platforms.
- Regarding the educational use case, most manufacturers do not support an unattended remote access to their experimental platforms. NBPIIoT covers this

shortcoming, turns on and off the energy automatically, and provides a solution to integrate the lab application user interface into an LMS, where a booking system can also be included to manage multiple accesses.

Finally, it can be noted that NBPIIoT is more than a VPN because:

- It provides the option of limiting access to only one single application on a shared computer.
- It provides private workspaces for each user.
- It integrates webcams.
- Communications are established in point-to-point connections, thus, making the overall system more secure.
- It provides a cloud IoT platform to manage users, computers, cameras, and other physical equipment.

7. Conclusions.

The revolution caused by the adoption of the IoT is one of the keys of the future automation in the industrial sector. Industry 4.0 has come to stay, and old communication systems must change to new ones. However, the variety of protocols and control applications found in current contexts is enormous. There is room for many different systems to take care of carrying this migration, although all of them should meet some minimum requirements. In particular, they should:

- Be applicable to networks of heterogeneous multiprotocol devices.
- Respect the interfaces designed by the manufacturers of different physical devices.

- Be easily installable and configurable.

NBPIIoT proposes an architecture that meets all the requirements above, and implements a friendly application to support secure, controlled, organized and collaborative access with different user profiles. In this way, the system can be managed by people without technical skills. In addition, the remote access implemented by NBPIIoT improves the VPN because they are point-to-point. Finally, its versatility makes it applicable to a wide variety of scenarios, from a small home to a complex industrial plant.

In this paper, a communications solution that is suitable for different contexts is described and its implementation into a working platform (NBPIIoT) is presented. In particular, NBPIIoT has been providing remote access to physical experiments in several universities for several years now.

Acknowledgment

This paper is framed in the project “Integral control system to optimize the microgrids energy demand” funded by the Spanish Ministry of Science and Innovation, call for Scientific and Technical Research and Innovation 2020-2023.

References:

[1] S. N. Swamy and S. R. Kota, “An Empirical Study on System Level Aspects of Internet of Things (IoT)”, IEEE Access, 8 (2020).

[2] T. Yashiro, S. Kobayashi, N. Koshizuka, and K. Sakamura, “An Internet of Things (IoT) Architecture for Embedded Appliances”, IEEE Region 10 Humanitarian Technology Conference, (2013) 314-319.

[3] H. L. Jing Ting, X. Kang, T. Li, H. Wang and C.K. Chu, “On the Trust and Trust Modeling for the Future Fully-Connected Digital World: A Comprehensive Study”, IEEE Access, 9 (2021).

[4] F. Tao, Y. Cheng, L. D. Xu, L. Zhang, and B. H. Li, ``CCIoT-CMfg: Cloud computing and Internet of Things-based cloud manufacturing service system," IEEE Trans Ind. Informat., 10.2 (2014) 1435-1442.

[5] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum and N. Ghani, “Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations”, IEEE Communications Surveys & Tutorials, 21.3 (2019).

[6] F. Meneghello, M. Calore, D. Zucchetto, M. Polese and A. Zanella, “IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices”, IEEE Internet of Things Journal, 6.5 (2019).

[7] M. Frustaci, P. Pace, G. Aloi and G. Fortino, “Evaluating Critical Security Issues of the IoT World: Present and Future Challenges”, IEEE Internet of Things Journal, 5.4 (2018).

[8] A. K. Sukede and J. Arora, “Auto tuning of PID controller,” in Proc. Int. Conf. Ind. Instrum. Control (2015) 1459–1462.

[9] R. Sanchez-Herrera, A. Mejías, M.A. Márquez, J.M. Andújar, A fully integrated open solution for the remote operation of pilot plants, IEEE transactions on Industrial Informatics 15.7 (2019) 3943 – 3951.

[10] A. D’Angelo, M. Tedesco, A. Cipollina, A. Galia, G. Micale, and O. Scialdone, “Reverse electrodialysis performed at pilot plant scale: Evaluation of redox processes and

simultaneous generation of electric energy and treatment of wastewater," Water Res., 125.C (2017) 123–131.

[11] A. Ali Mirani, G. Velasco-Hernandez, A. Awasthi, and J. Walsh "Key Challenges and Emerging Technologies in Industrial IoT Architectures: A Review", Sensors, 22, (2022) 1-31.

[12] L. De La Torre, M. Guinaldo, R. Heradio, and S. Dormido, ``The ball and beam system: A case study of virtual and remote Lab enhancement with Moodle," IEEE Trans. Ind. Informat., 11.4 (2015) 934-945.

[13] M. A. Prada, J. J. Fuertes, S. Alonso, S. García, and M. Domínguez, ``Challenges and solutions in remote laboratories. Application to a remote laboratory of an electro-pneumatic classification cell," Comput. Educ., 85 (2015) 180-190.

[14] U. Hernandez-Jayo and J. Garcia-Zubia, ``Remote measurement and instrumentation laboratory for training in real analog electronic experiments," Measurement, 82 (2016) 123-134.

[15] J. Kundrat, M. Vasko, R. Krejci, V. Kubernat, T. Pecka, O. Havlis, M. Slapak, J. Jedlinsky and J. Vojtech, "Opening up ROADMs: streaming telemetry", IEEE/OSA Journal of Optical Communications and Networking, 13.10 (2021).

[16] L. Fang, Y. Wu, C. Wu and Y. Yu, "A Nonintrusive Elderly Home Monitoring System", IEEE Internet of Things Journal, 8.4 (2021).

[17] F. A. Durmaz, A. Brusan and C. Ozturk, "Unified Open Hardware Platform for Digital X-Ray Devices; its Conceptual Model and First Implementation", IEEE Journal of Translational Engineering in Health and Medicine, 8 (2020).

[18] ArduinoHome. Accessed: Feb. 4, 2021. [Online]. Available: https://www.arduino.cc/

[19] Phidgets Inc. Products for USB Sensing and Control. Accessed: Apr. 17, 2021. [Online]. Available: https://www.phidgets.com/

[20] Raspberry Pi Foundation. Raspberry Pi-Teach, Learn, and Make with Raspberry Pi. Accessed: Feb. 4, 2021. [Online]. Available: https://www.raspberrypi.org

[21] T. Ewing, P. T. Ha, J. T. Babauta, N. T. Tang, D. Heo, and H. Beyenal, ``Scale-up of sediment microbial fuel cells," J. Power Sources, 272 (2014) 311-319.

[22] H. Gad and H. E. Gad, ``Development of a new temperature data acquisition system for solar energy applications," Renew. Energy, 74 (2015) 337-343.

[23] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, “The industrial internet of things (IIoT): An analysis framework”, Computers in Industry, 101 (2018), 1-12.

[24] T. Qiu et. al., “Edge Computing in Industrial Internet of Things: Architecture, Advances and Challenges”, IEEE Communications Surveys & Tutorials, 22, (2020) 2462-2488.

[25] The Modbus Organization. Accessed: Apr. 3, 2021. [Online]. Available: http://www.modbus.org/

[26] M. Márquez, R. Sánchez-Herrera, A. Majías, F. Esquembre and J.M. Adújar, “Controlled and Secure Access to Promote the Industrial Internet of Things”, IEEE Access, 6 (2018) 48289 – 48299.

[27] C. K. Dehury and P. K. Sahoo, ``Design and implementation of a novel service management framework for IoT devices in cloud," J. Syst. Softw., 119 (2016) 149-161.

[28] S. Abdelwahab, B. Hamdaoui, M. Guizani, and T. Znati, ``Cloud of things for sensing-as-a-service: Architecture, algorithms, and use case," IEEE Internet Things J., 3.6 (2016) 1099-1112.

[29] D. F. H. Sadok, L. L. Gomes, M. Eisenhauer, and J. Kelner, ``A middleware for industry," Comput. Ind., 71 (2015) 58-76.

[30] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, ``Middleware for Internet of Things: A survey," IEEE Internet Things J., 3.1 (2016) 70-95.

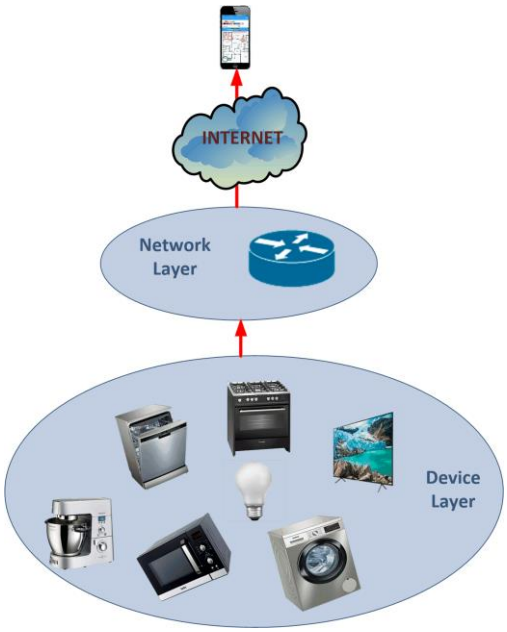

Figure 1. The structure usually used in a smart home IoT.

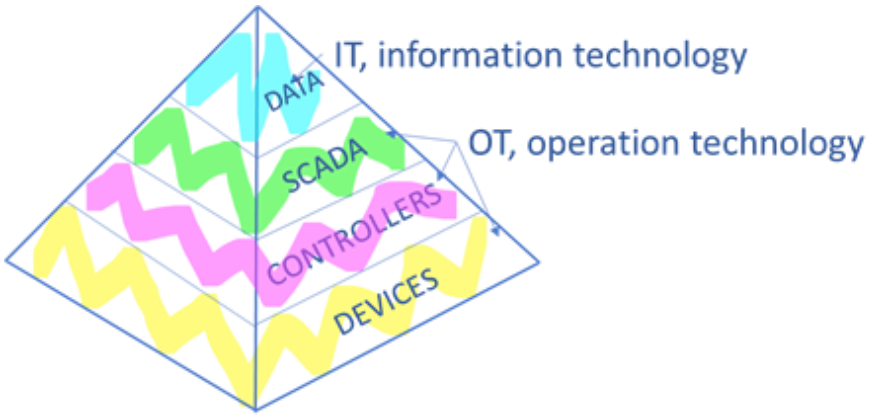

Figure 2. CIMP pyramid.

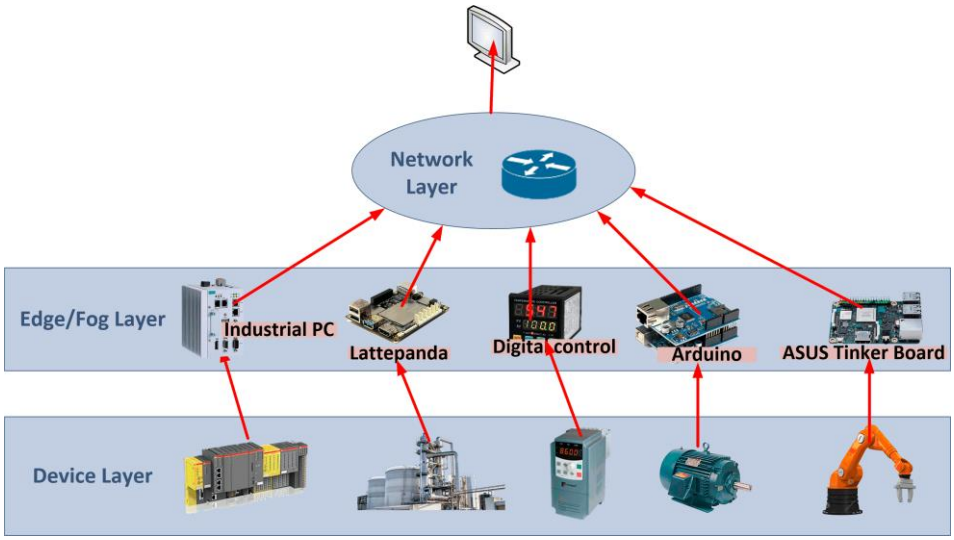

Figure 3. The structure necessary in industrial IoT.

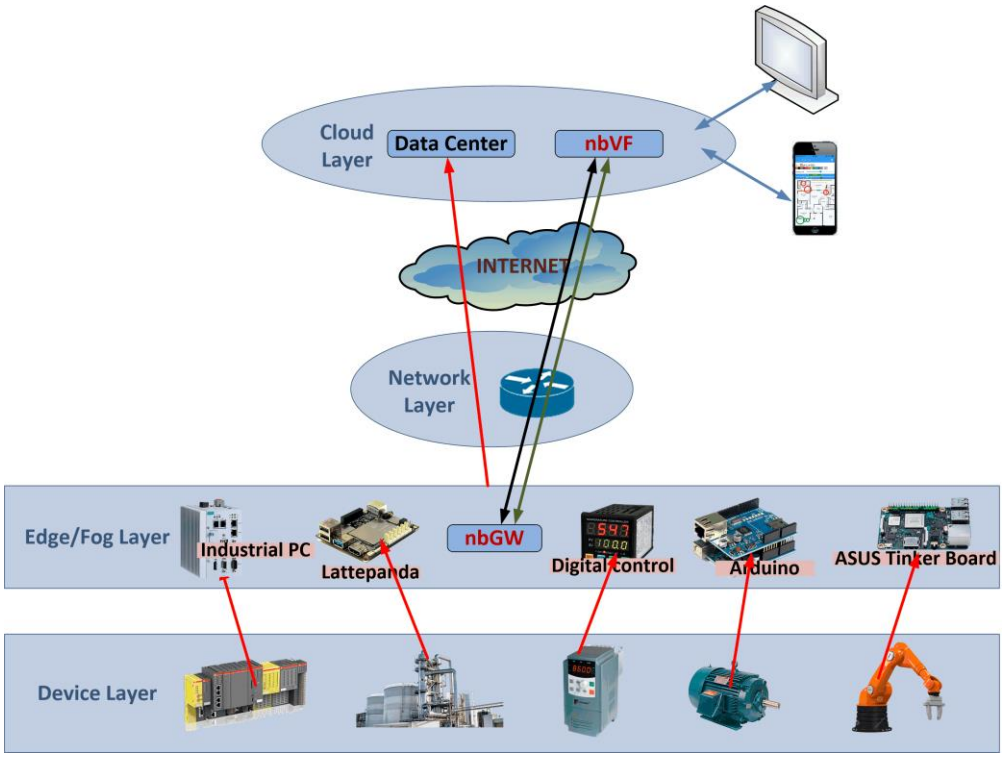

Figure 4. NEBSYST Communications Architecture.

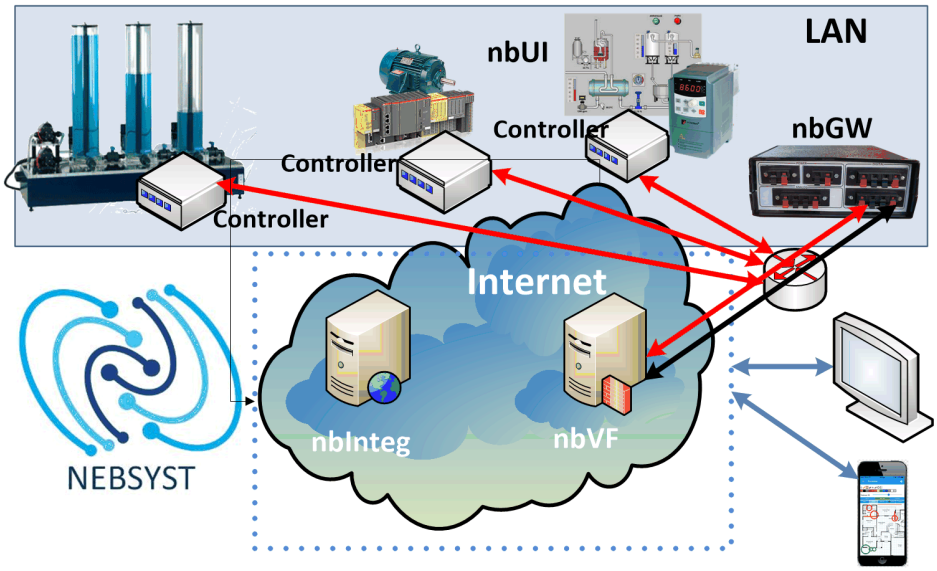

Figure 5. NBPIIoT's architecture.

Figure 6. Interface of web application to configure NBPIIoT (nbManag).