Journal of
Sensor and Actuator Networks

MDPI

Article

Upgrading a Legacy Manufacturing Cell to IoT

João Cunha [1], Nelson Batista [2,3], Carlos Cardeira [1,3] and Rui Melicio [2,3,*]

[1] Instituto Superior Técnico, Universidade de Lisboa, 1049-001 Lisboa, Portugal; joaopedropcunha@gmail.com (J.C.); carlos.cardeira@tecnico.ulisboa.pt (C.C.)
[2] ICT, Universidade de Évora, 7000-645 Évora, Portugal; nelson.batista@gmail.com
[3] IDMEC, Instituto Superior Técnico, Universidade de Lisboa, 1049-001 Lisboa, Portugal
* Correspondence: ruimelicio@gmail.com

Abstract: Many industries, such as aeronautics construction are still equipped with legacy machines and are not keen to change old, however fully functional, equipment to new ones. Hence, an upgrade must be found to cope the legacy and fully functional machines to IoT technologies. This paper is a contribution to embrace those challenges in a new IoT architecture able to support the creation of solutions for Smart Industries. Internet of Things is increasing acceptance and the infrastructure for them is becoming available. This leads to an insurgence on investments and development of new dedicated IoT infrastructures. Industries need to adapt quickly to this constant technological evolution, implementing measures and connecting machines and robots at critical points to the Internet, instrumenting them using the concept of IoT, with the major goal of implementing a flexible, secure, easy to maintain and capable to evolve infrastructure, when legacy equipment is involved. The availability of machines and other critical assets directly affects the effectiveness of manufacturing operations. The architecture design offers security, flexibility, simplicity of implementation and maintenance, and is resilient to failures or attacks and technologically independent. Field tests are reported to evaluate key aspects of the proposed architecture.

Keywords: Internet of Things (IoT); industry 4.0; smart industry; manufacturing cell; IoT service architecture

check for updates

Citation: Cunha, J.; Batista, N.; Cardeira, C.; Melicio, R. Upgrading a Legacy Manufacturing Cell to IoT. *J. Sens. Actuator Netw.* **2021**, *10*, 65. https://doi.org/10.3390/jsan10040065

Academic Editors: Lei Shu, Adnan Al-Anbuky, Stefan Fischer, Joel J. P. C. Rodrigues and Mário Alves

Received: 18 October 2021
Accepted: 12 November 2021
Published: 17 November 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Cellular manufacturing systems have shown considerable good results in batch manufacturing platforms. Some of the advantages of cellular manufacturing are: throughput time reduction, smaller Work in Process, flexibility increase, product quality improvement and control simplification. The high flexibility cell design is recognized by the research community as a complex optimization problem [1]. This flexibility leads to some wired network implementation difficulties. Implementing wireless technologies should ease the wired connections main drawbacks and facilitates the increase of the number of devices, expanding the factory network, being able to increase the layout flexibility. Machine-to-machine (M2M) communications are not new to industries. Message queuing telemetry transport (MQTT) [2], is very known Internet of Things (IoT) M2M connectivity. Factory automation has been based on tight sensor-actuator control loops, where sensors "feed" data into Programmable Logic Controllers through the wired analog and digital I/O ports of the controllers [3–5].

The availability of machines and other critical assets directly affects the effectiveness of manufacturing operations. Critical information systems may provide either real time or estimated information which presents a great potential for saving production costs. The data collected, being accessible online from anywhere, could be used to optimize decision-making throughout the manufacturing line, increasing its efficiency and responsiveness [6].

With the goal of implementing a flexible, secure, easy to maintain and capable to evolve infrastructure, industries need to adapt quickly to this constant technological evolution, implementing measures and connecting machines and robots at critical points to the Internet, instrumenting them using the concept of IoT.

IoT is getting increased public acceptance, leading to higher investments and developments [7–10]. The cloud services infrastructures supported the rise of new dedicated IoT cloud infrastructures, allowing device representations that ease the integration of sensors and actuators connected with each other by software solutions and Artificial Intelligence (AI) bots [11,12].

The higher investment and adoption of IoT support leads to an increase of IoT solutions offered in the market. The diversified offer of IoT technologies and solutions to solve the same problems and suppress the same needs, lead to new challenges [3,9,10,13–16]. This multiplicity of solutions brings an extra effort to assure extra security measures that can overcome existing threats and overseen future risks [17].

Security is one of the main factors for enabling the widespread adoption of IoT technologies in industries and professional environments. Data encryption, integrity and authentication are the major issues in security that should be carefully analyzed [18].

In [19] the authors propose schemes that can be used to encrypt and authenticate any digital data not only images. In [20] the authors show a comparative analysis versus related works that also use chaotic encryption and classic algorithms, such as: AES, DES, 3DES and IDEA. The security analysis confirms that the proposed process to improve the randomness of chaotic maps, is appropriate to implement an encryption scheme that is secure and robust against several known attacks and other statistical tests. Finally, it was experimentally verified that this chaotic encryption scheme can be used in practical applications such as M2M and IoT.

This paper is a contribution for IoT application in Smart Industries, under the Industry 4.0 scope. Results are shown upgrading a legacy wired manufacturing cell composed by seven stages, towards IoT. A multi-layer wireless solution using ZigBee mesh network is proposed for local communication. The exchange data command frame, the network security using multiple encryption algorithms and necessary modules are presented and discussed. The legacy equipment is kept but adapted to the new IoT technologies.

The paper is organized as follows. Section 2 presents an introduction to manufacturing cells, IoT and the contributions of IoT implementation to the Smart Industry. Section 3 presents the actual state of the existing manufacturing cell. Section 4 presents the IoT services proposed architecture. Section 5 presents the field tests conducted to evaluate the key aspects of the proposed architecture. Finally, Section 6 outlines the conclusions and further work.

2. Internet of Things

The British technology pioneer Kevin Ashton, co-founder of the Auto-ID Center at the Massachusetts Institute of Technology (MIT), is known by introducing the term IoT in 1999. IoT is not just a new definition of interconnected things over the Internet [21]. The exponentially increasing implementation phenomenon has been driven by the recent developments and price reduction of smart devices, cloud computing services, sensors and actuators that are able to interconnect to each other over the internet. The reduced price of those IoT essential components, allied to the open source nature of many of them and recent investments, result on the quick expansion of their adoption.

Multiple IoT definitions and designations have been presented by different technological companies, research institutes, independent organizations and governments. Some of those designations are: Internet of Sensors and Actuators; Internet of Everything; Smarter Planet; Industrial Internet among others. On this work the IoT will be referring the interrelationship of physical and digitally connected world supported by embedded technology and software cloud services, aiming to simplify, facilitate and enhance business processes and operators life, offering at the same time a platform to interconnect and manage all the intervenient devices.

Communication infrastructures are a very important part in the IoT structure, allowing the communication and interaction between different machines, sensors and actuators.

The IoT components are becoming less expensive, smaller, with increased functionality and more interconnected. As they became more accessible in the off-the-shelf market, small entrepreneur companies emerged, which in turn brought new insights of the IoT solutions. The embedded technologies may have restricted processing power that is needed to sense, control and interact with the physical world, offered by simple and cheap microcontroller kits. The embedded devices need to be connected with services that bring the IoT alive by wire or wireless communication devices. The embedded devices although having some internal processing capabilities are not able to offer a full IoT experience. To simplify, facilitate and enhance business processes and operators' activity, the embedded devices must be supported by services and software, which live in their majority in the Cloud. The interconnections between the industrial cell, the operator monitoring and the cloud are illustrated in Figure 1.

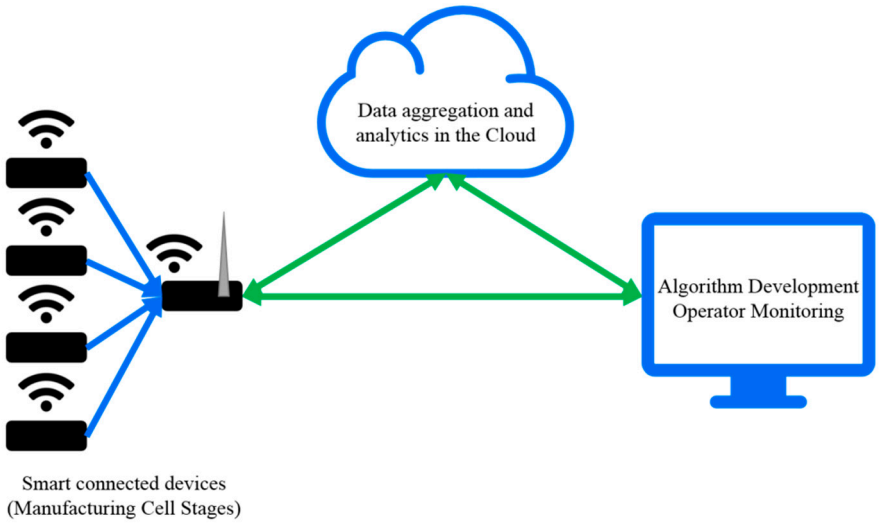

Figure 1. Interconnection between the industrial cell, the operator monitoring and the cloud.

IoT brings new market possibilities for Smart Industries services providers, but at the same time brings several technology and security issues that need to be considered to offer products that are appellant to the clients and market competitive for the present and for the future IoT.

Modern industries can't ignore the integration of IoT, with a growing implementation of control solutions wirelessly using the Internet, converting them into Smart Industries. The most obvious direction is to apply the concepts and all this IoT development to solve and simplify everyday tasks in industries, such as remote monitoring, offline planning, big data analysis or real-time control. It is possible already to find some tools for the selective control of workspace lighting, irrigation systems, measuring stations for the local air quality, among many others.

3. Manufacturing Cell Architecture

The existing manufacturing cell is composed by seven different stages: supervision, lathe machine, milling machine, conveyor, automated guided vehicle, quality control and storage/assembly. All the manufacturing cell stages are illustrated in Figure 2.

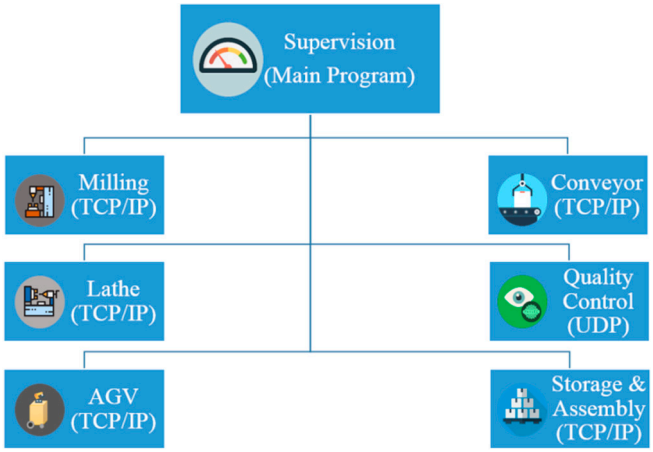

Figure 2. Manufacturing cell stages.

The main objective of this installation is to provide engineering students with a prototype manufacturing cell to build and assemble new products using all the tools.

The actual manufacturing cell plant is illustrated in Figure 3.

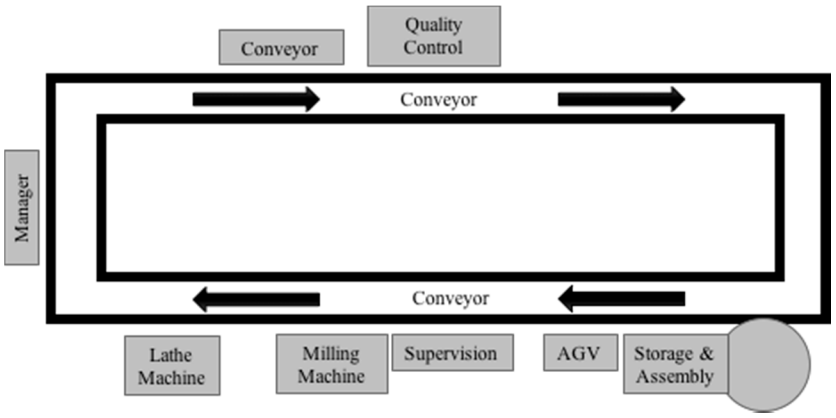

Figure 3. Manufacturing cell plant.

The manufacturing machines (hardware) of all the stages from the cell are illustrated in Figure 4.

The actual state of the manufacturing cell and a future expected one are compared in Table 1.

Table 1. Manufacturing cell actual and future states comparison.

Legacy State	Future State
Centralized control	Partially/Distributed control
Large number sensors and actuators	Much larger number of sensors and actuators
Limited information of the process	Full information of the process
Unidirectional communication	Bi-directional communication
Data accessed only in the central controller	Data accessed in multiple locations using cloud services
Manual fault recovery	Semi-automated fault recovery
Manual data prediction	Real-time data prediction
Fixed original protection systems	Updated and adaptive protection systems
One point monitoring	Multi-point monitoring
Hardly expandable	Easily expandable
Poor flexibility	High flexibility

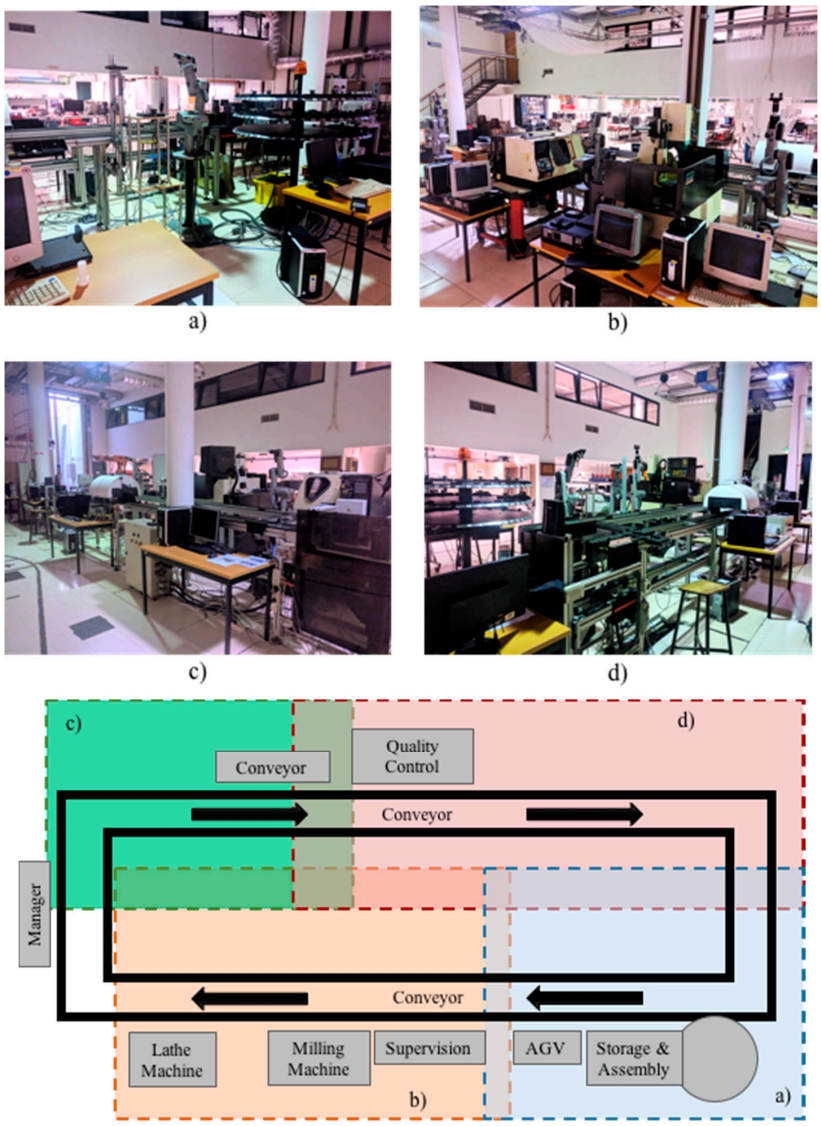

Figure 4. Hardware and the manufacturing machines of all the stages. (a) corresponds to the AGV and the Storage & Assembly stages; (**b**) corresponds to the Lathe and Milling machines as well as the Supervision center; (**c**) corresponds to a Conveyor segment; (**d**) corresponds to the quality control unit.

3.1. Supervision

The supervision has the job to ensure the complete process of manufacture of the product and the communications between all the stages. Using several planning tools such as Gantt diagrams and State Machines, the production is planned. The communications protocols are selected to be adequate to every stage. Using TCP/IP and UDP the cell controllers communicate under the same Local Area Network (LAN). A main program assures the communication between all stages of the manufacturing cell. One dashboard is also created allowing the control and setup of all the machines from one single station. Using software services connected over the internet and supported in the Cloud, the manufacturing machines should show their status as well as the production stage of any product produced in the cell. An example of a manufacturing cell dashboard containing all the cell stages and the connection to the cloud is shown in Figure 5.

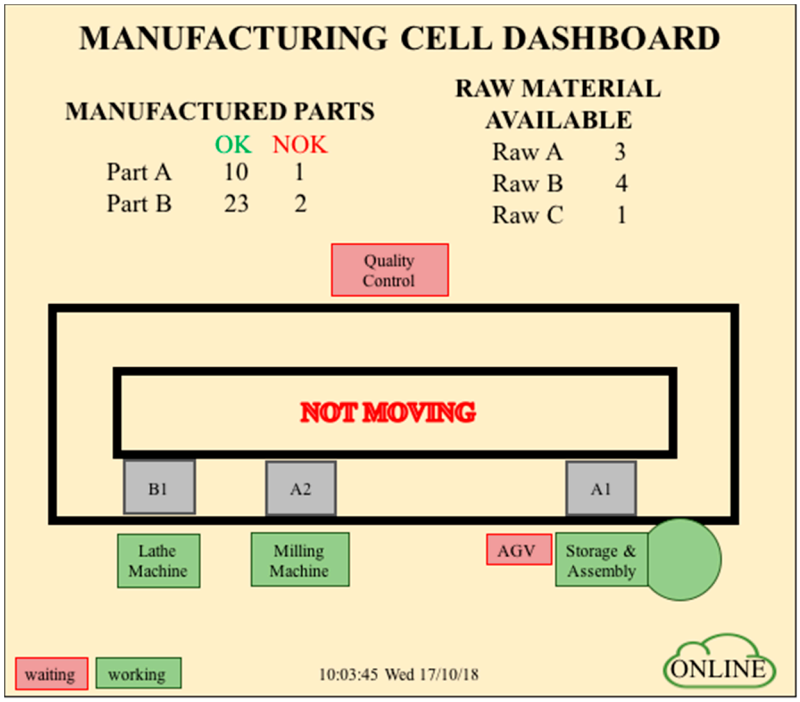

Figure 5. Example of a manufacturing cell dashboard.

3.2. Lathe Machine

The lathe machine in the manufacturing cell is a Legacy Lathe, model Mirac, manufactured by Denford, Brighouse, West Yorkshire, UK. This Computer Numeric Control (CNC) machine understands the common G-Code, to control the different parts such as the spinner, the cutting tool, and the safety door. One robotic arm, model SCORBOT ER VII, manufactured by Eshed Robotec (now RoboGroup Education), Rosh Ha'Ayin, Israel, which grabs and manipulates the parts to be machined. The cell lathe machine and the robotic arm are shown in Figure 6.

Figure 6. Lathe machine and the robotic arm.

3.3. Milling Machine

The milling machine in the manufacturing cell is a Legacy Milling Machine, model Triac Fanuc OM series, manufactured by Denford, Brighouse, West Yorkshire, UK. It uses CNC programming language as interface with the user. There are two ways to operate the machine: the Teach Pendant mode, to introduce the commands manually; and the CNC-Programming mode, to use the CNC program file sent to the machine. As in the lathe machine, one SCORBOT ER VII robotic arm can grab and manipulate the parts to be machined. The manufacturing cell milling machine and the robotic arm are shown in Figure 7.

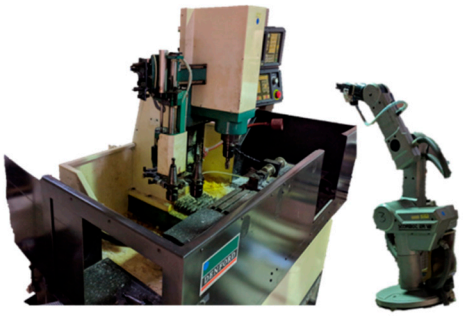

Figure 7. Milling machine and the robotic arm.

3.4. Conveyor

The cell has 3 major conveyor belts in two floors (two belts on the top floor and one in the bottom floor), 28 presence sensors and 6 flow blockers. Several WT2 Bosch platforms allow the products to flow through the workspace and two lifters exchange platforms between floors. All the sensors, motors, blockers and communication with a PC base station are controlled by a centralized automaton BOSCH (Robert Bosch GmbH,) equipped with the modules ZE200 and R200 (Gerlingen, Germany). The ZE200 module assures all the input/output connections with all the sensors and actuators controlled by the automaton. The R200 module registers all the dataflags and memory used by the program and establishes all the communications between the automaton and the cell network using LabVIEW (LabVIEW 2021). The cell ZE200 and R200 automatons modules are shown in Figure 8.

Figure 8. ZE200 and R200 automaton modules.

3.5. Automated Guided Vehicle

The cell has one motorized automated guided vehicle (AGV), which is a prototype built in the laboratory from other researches. It includes a small plastic robotic arm controlled by five servo motors connected to a microcontroller board. An infrared proximity sensor is used in the front of the vehicle to avoid collisions with the different stations of the cell. To control what is the present job and to give warning about the self-operation some RGB LED strips are used. Another separate microcontroller controls the proximity sensor and the LED strips. A webcam is used to follow a line in the cell floor, allowing the robot to move between stations. The network is very flexible being able to increase the number of available AGV's. One computer running MATLAB interconnects everything and establishes the communication with the supervision station. The manufacturing cell AGV is shown in Figure 9 (model Torre, manufactured by IDMEC/Instituto Superior Técnico, Lisboa, Portugal).

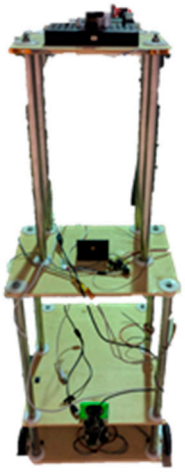

Figure 9. Automated guided vehicle.

3.6. Quality Control

The main goal of this workstation is to check the produced parts for errors and report the results to the Supervision. The velocity in detecting errors in the production line is very important, has it impacts in production costs. This station is composed by a tunnel with white LED lighting, granting the best illumination conditions for a webcam in the top. The webcam captures several images and MATLAB processes all the data in real-time, assuring that the conveyor belt never stops. Some good parts need to be previously analyzed and the descriptors stored, giving values to be compared with the produced parts. The MATLAB communicate via UDP with the LabVIEW and report to the Supervision. The cell quality control setup is shown in Figure 10 (model "Campânula", manufactured by IDMEC/Instituto Superior Técnico, Lisboa, Portugal).

Figure 10. Quality control setup.

3.7. Storage and Assembly

This stage has three main objectives: store the raw material before the production, assemble all the parts of the final product and store the final product.

It is composed by a three-floor tower rotatory storage, one legacy robotic arm SCORBOT ER VII and two assembly pneumatic cylinders.

The cylinders, the storage and the robotic arm are controlled by the SCORBOT. Cylinders are commanded by electro-pneumatic valves. The motor of the storage tower can rotate in one direction and a yellow rotary light warns that the storage tower is moving. The necessary cycles for the production are compiled and programed in HyperTerminal and are called via LabVIEW or Matlab. The manufacturing cell assembly setup with pneumatic cylinders, the robotic arm and the storage tower are shown in Figure 11.

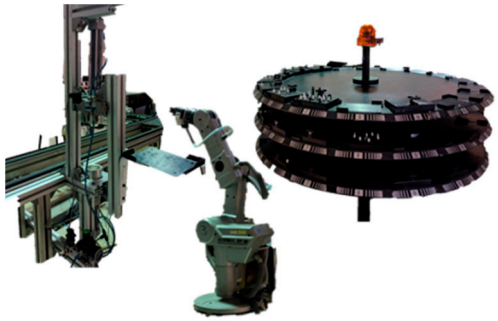

Figure 11. Assembly setup with pneumatic cylinders, the robotic arm, and the storage tower.

4. IoT Services Proposed Architecture

A IoT architecture is proposed for the upgrade of the previously described production cell, enabling the integration of the needed services in a cloud infrastructure, easing the creation of future services and simplifying the existing infrastructure.

The architecture is comprised of 3 main modules: Gateway module, Message module and Business Intelligence Data module and is shown in Figure 12.

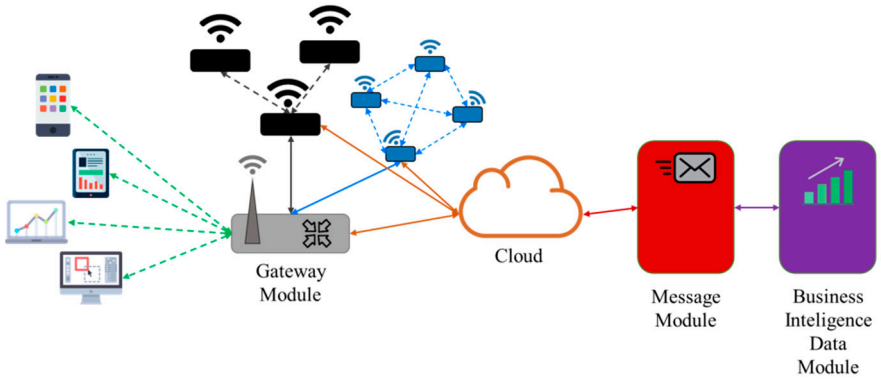

Figure 12. Proposed architecture.

Commands correspond to data exchange among modules, specifying the interaction types. The interaction types can be such as request status, action order, and data transport. The command frame that is shown in Figure 13.

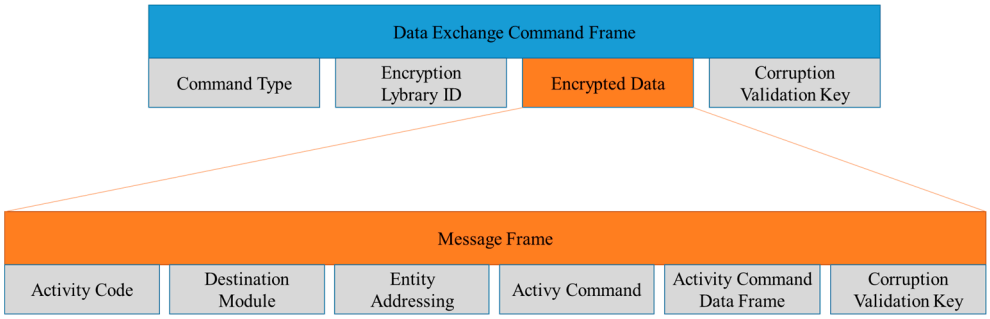

Figure 13. Data exchange command frame.

The encryption library identification defines the library to be used for the encryption and decryption of the message data. As shown in Figure 14, the system can apply different encryption algorithms for each module or within the same module at the same time, boosting network security.

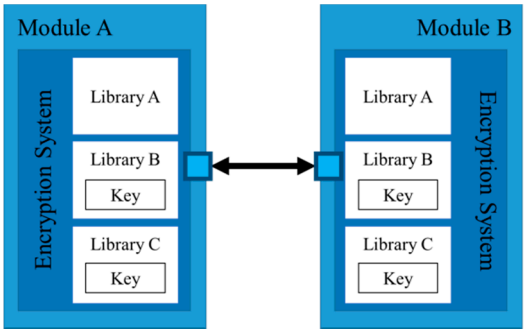

Figure 14. IoT module encryption system example illustration using multiple encryption technologies.

The corruption validation key is used to determine whether the message was changed during transmission. The corruption validation key is calculated using the frame data's other fields, allowing you to check if the message has been modified. A message frame is included in the encrypted message data and is used for the activity itself. The activity code, destination module reference, entity addressing, activity command, activity data frame, and a corruption validation key are all included in the message frame.

4.1. Gateway Module

The Gateway module is liable for the business rationale of the combination of the interrelationship of physical and computerized world. It contains the services expected to present the needs of a specific IoT element activity. It receives and sends orders from and to the various modules. The Gateway module can demand data about the nodes, status of the current activity. A command can be created in this module and sent to an IoT module.

The creation of services eases the client/operator activity and their usability, but the control has to be transparent for the client. The client interacts directly and asynchronously with an embedded device. The Gateway module stays behind communication filtering and firewalls.

The Gateway module is illustrated in Figure 15.

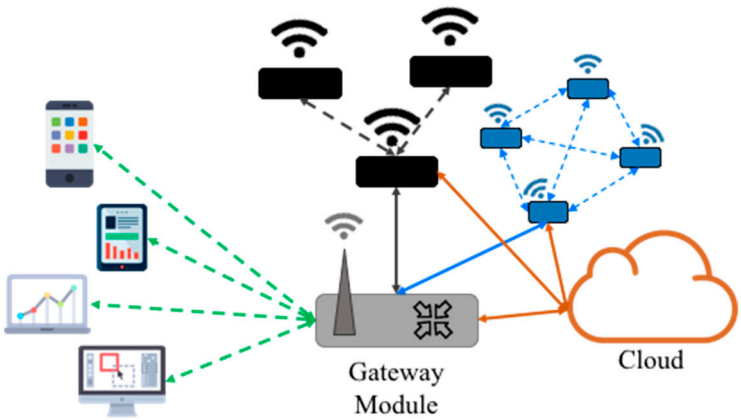

Figure 15. Gateway module.

4.2. Message Module

The Message module deals with the interaction among the embedded devices. The client requests the status update, configuration or software update to the Integration module. Using web services, the Message module offers several types of communications to the clients.

5. System Implementation Tests and Results

Prototypes were developed for testing the implementation of activity data routes, modules, and cloud communication services in the industrial cell. Table 2 shows different wireless technologies [22–24].

Table 2. Different wireless technologies.

Technology	ZigBee (802.15.4)	GSM/GPRS	Z-Wave	WiFi (802.11 b)	Bluetooth (802.15.1)
Application	Monitor/Control	Wide area voice and data	Local area control	mail, streaming, browser	Devices connection
System resources	4 kB–32 kB	16 MB+	2 kB–16 kB	1 MB+	250 kB+
Max *n*. of devices	+65,000	1	232	32	7
Rate (kb/s)	20–250	64–128+	40–100	11,000+	720
Round Response time (s)	<0.030	–	–	<0.003	<10
Max distance (m)	100	Wordwide	30	100	10
Major Strenghts	Reliability, low power and cost	Transmission range	Max *n*. of devices	Throughput	Convenience, Cost

5.1. System Communication Infrastructure

ZigBee [25–35] was the protocol chosen for the implementation using a mesh network topology. There are three different types of ZigBee module functionality: coordinator, router, and end device. The coordinator manages the network. The router relais messages from other nodes. The end device is connected to sensors and actuators and can be asleep to save the device consumption energy. A fully functional wireless network, with interior (LevelID = 0), exterior (LevelID = 2) and hybrid connection (LevelID = 1) networks is shown in Figure 16.

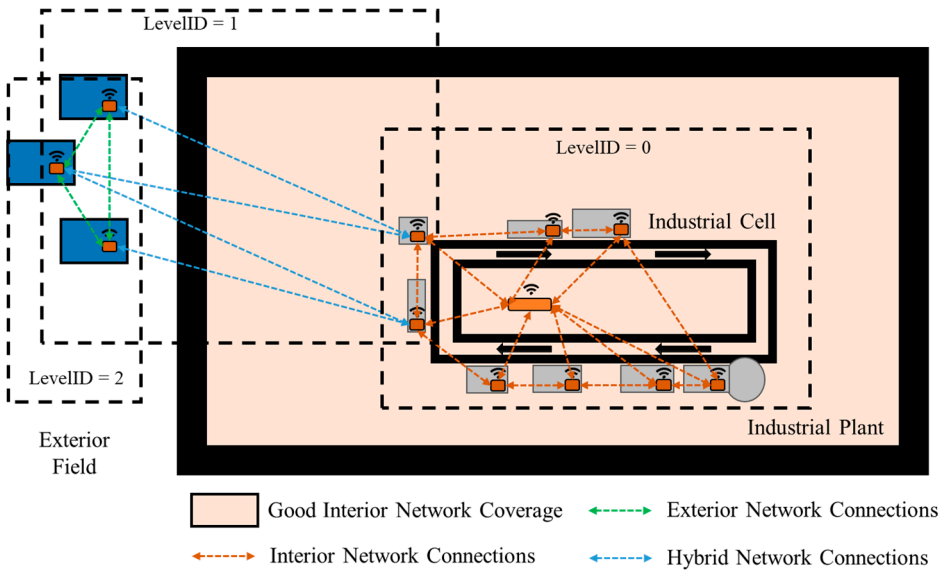

Figure 16. Fully functional industrial wireless network.

5.2. Gateway Module and Cloud Integration Test

A gateway module and cloud integration test has been created to test the communication between the system and the cloud infrastructures. Using a microcontroller with a ESP8266MOD module some information was sent to the cloud using the ThingSpeak

service [36]. The ThingSpeak platform allows to collect the different data from the sensors, instantaneous plot visualization, analyze and processing it using Matlab scripts online.

The microcontroller generates an index number and a timer and sent these two values to the ThingSpeak platform in loop. Exporting the acquired online data and processing it using MATLAB, the time difference between the received messages is shown in Figure 17.

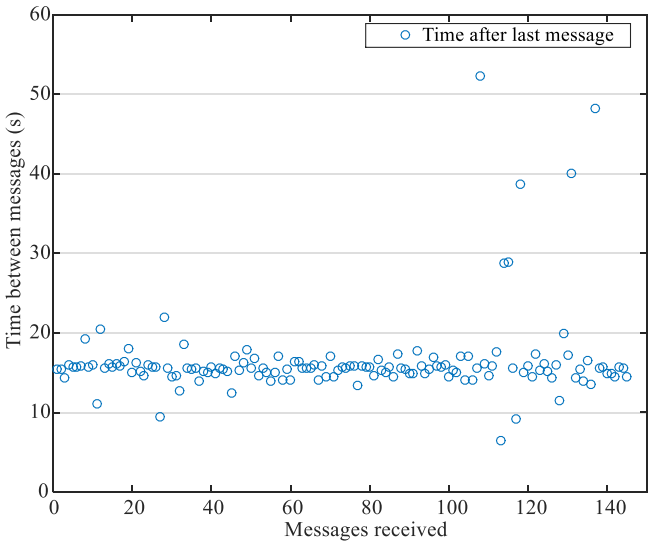

Figure 17. Time difference between the received messages.

From the data collected the mean interval between received messages is 16.43 s. The plot demonstrates a drawback of this free platform being inadequate to real-time data acquisition and control, bellow 15 s of refresh rate.

Due to this bottleneck, some of the messages are expected to not be received as it's confirmed by the discrepancy in the index numbers of the received messages shown in Figure 18.

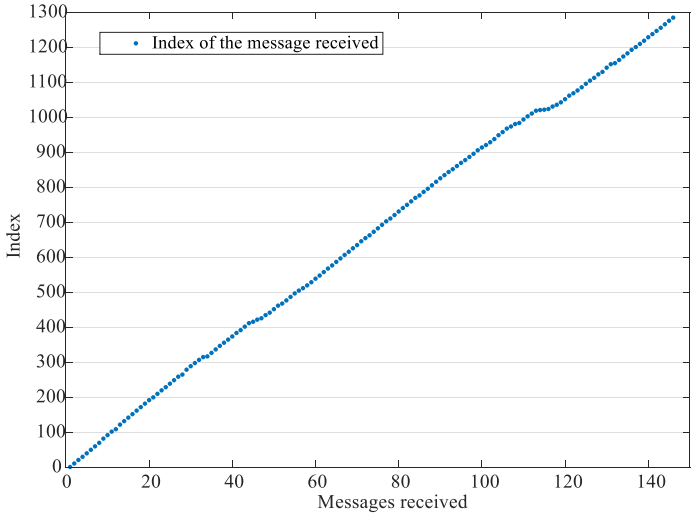

Figure 18. Index numbers of the received messages.

A reception ratio (*RR*) is calculated comparing the number of received messages with the not received messages and it's given by:

$$RR\ (\%) = \frac{received \times 100}{received + not\ received} = \frac{146 \times 100}{146 + 1139} = \frac{14600}{1285} = 11.36\% \quad (1)$$

This shows that near only one message in each 10 is received by the ThingSpeak platform. Important and frequent messages must be avoided to send to cloud using this platform. Some acknowledge measures should be used to assure the correct reception.

5.3. Time Occupation Duty Ratio Analysis

A parameter to be considered when using communications in a multi-level architecture is the Time Occupation Duty Ratio (TODR) that indicates the time period which communication driver can take to transmit data to the FFD coordinator [37]. The final TODR value depends on the quantity of ZigBee levels, q, within the network and it's given by:

$$TODR\ (\%) = \frac{100}{\left(n_{nr\ devices}^{Level\ ID=q}\right)\left(n_{nr\ devices}^{Level\ ID=q-1}\right)\ldots\left(n_{nr\ devices}^{Level\ ID=0}\right)} \quad (2)$$

Using the network example shown in Figure 16 for the *LevelID* = 0, the network coordinator level, based on (2) the TODR value is given by:

$$TODR\ (\%) = \frac{100}{n_{nr\ devices}^{Level\ ID=0}} = \frac{100}{8} = 12.5\% \quad (3)$$

Using the same approach as (3) but for the hybrid level, the *LevelID* = 1 (q = 1) the TODR value is given by:

$$TODR\ (\%) = \frac{100}{\left(n_{nr\ devices}^{Level\ ID=q}\right)\left(n_{nr\ devices}^{Level\ ID=q-1=0}\right)} = \frac{100}{16} = 6.25\% \quad (4)$$

This shows that one FFD in the exterior network has a TODR value 2 times smaller than one FFD in the interior network. Therefore, the communication drivers placement should take this in consideration based on the importance and frequency of data transmission to the main gateway and coordinator.

A manufacturing cell interior connections example diagram with TODR value is shown in Figure 19.

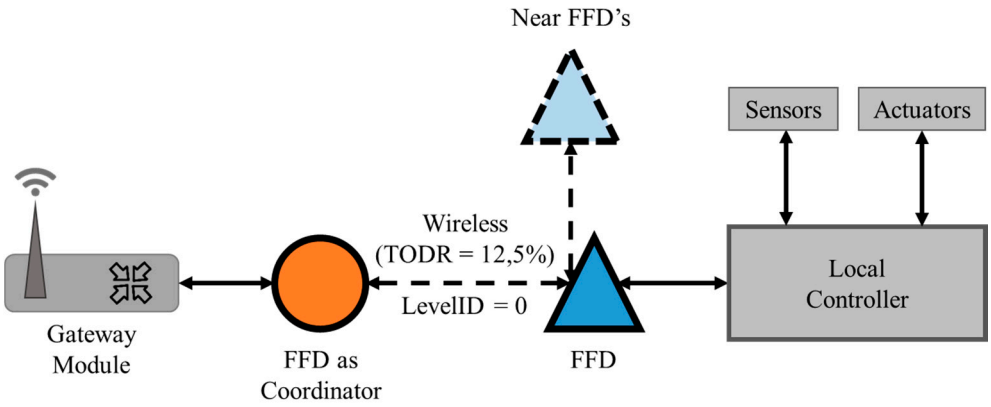

Figure 19. Manufacturing cell interior connections example diagram with TODR value.

A manufacturing cell interior and hybrid connections example diagram with TODR values is shown in Figure 20.

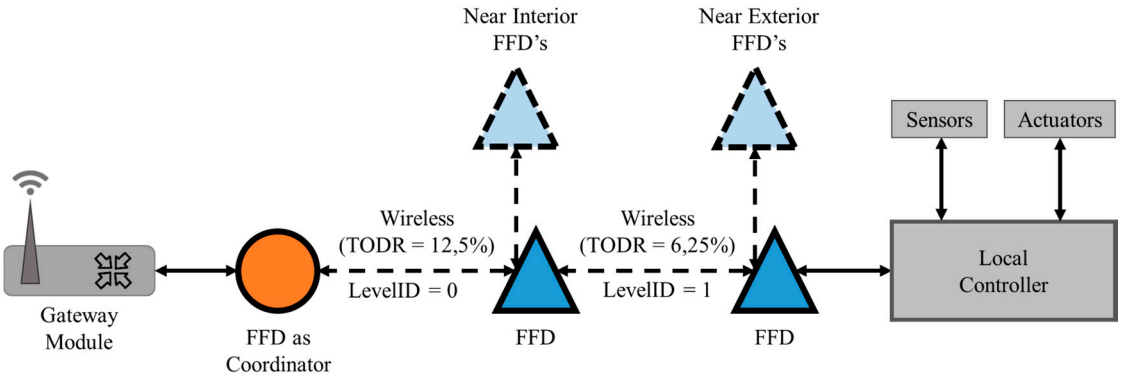

Figure 20. Manufacturing cell exterior connections example diagram with TODR values.

5.4. Distance Measurement Test

The location information of the materials, parts, products, platforms, robots and other assets inside an industrial plant is extremely valuable. Using the communication drivers and applying the Shadowing model [38,39], it's possible to use the received signal strength indication (RSSI) to estimate de distance between the drivers inside a network.

The strength of signal falls off with distance over transmission medium. Using the Shadowing model, the wireless signal transmission is given by:

$$P_{r(d)} = P_{r(d_0)} - 10\, n\, log_{10}\left(\frac{d}{d_0}\right) + X \tag{5}$$

Where in (5), d is the distance from the transmitter to receiver and its unit is meter, d_0 is a reference distance and usually equals 1 m, $P_{r(d)}$ is the signal power received from the transmitter and its unit is dBm, $P_{r(d_0)}$ is the signal power measured at the reference distance, X is a Gaussian random variable whose mean value is 0 and it reflects the change of the received signal power in certain distance, n is the path loss index and relates to the environment.

Simplifying the Shadowing model (5) results (6) given by:

$$P_{r(d)} = P_{r(d_0)} - 10\, n\, log_{10}\left(\frac{d}{d_0}\right) \tag{6}$$

Applying mathematical transformations in (6), the pretended distance value d is given by:

$$d = d_0\, 10^{\left(\frac{P_{r(d_0)} - P_{r(d)}}{10\ n}\right)} \tag{7}$$

A line-of-sight situations range test was made to verify the, approximate, maximum distance that the modules can communicate ones among the others and the estimated distance is calculated using (7). To implement the test a microcontroller was used, connected to a communication driver module in Router API mode, transmitting a message within a one second period. With another communication driver connected via USB to a laptop it was possible to register the local RSSI given by the X-CTU program. The results of distance estimation obtained in the test for the wireless device are presented in Table 3.

Table 3. Results of distance estimation obtained in the test for the wireless device.

Measurement	Linear Distance (m)	RSSI ZigBee (dBm)	Estimated Distance (m)	Percentual Error (%)
0	0.0	−45	–	–
1	3.9	−47	3.9	Reference
2	9.8	−53	9.0	−7.52
3	18.2	−58	18.1	−0.63
4	24.5	−57	15.7	−35.75
5	32.7	−65	47.7	45.93
6	39.3	−63	36.2	−7.97
7	50.4	−68	72.3	43.46
8	59.4	−65	47.7	−19.63
9	72.7	−66	54.8	−24.58
10	84.6	−66	54.8	−35.19
11	94.0	−69	83.1	−11.57
12	103.1	−70	95.5	−7.45
13	113.5	−71	109.7	−3.34
14	123.3	−72	126.0	2.22
15	136.9	−74	166.3	21.47
16	148.3	−74	166.3	12.15
17	158.6	−76	219.4	38.32
18	168.4	Lost	–	–

Although having some points with an excessive error, the mean value of 0.66% is pretty good taking into consideration that there were used only two FFD's. Increasing the number of devices used and applying other equations to make a triangulation for the position the estimated distances would be more precise.

For better explanation of the results obtained, a plot was made containing the real distance of the measurements and the estimation using (7) is shown in Figure 21.

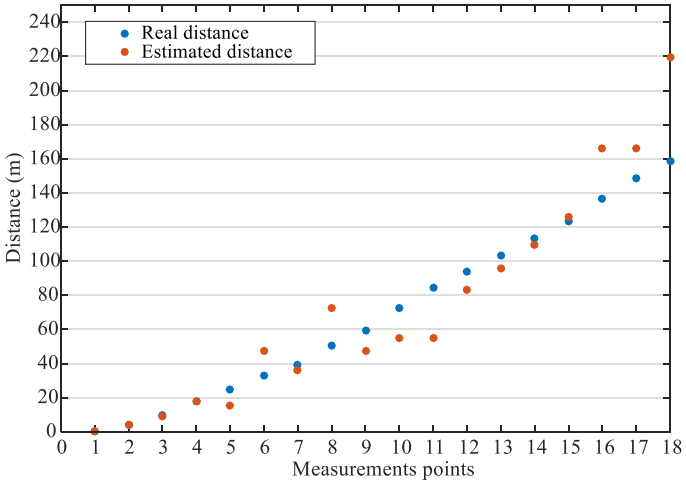

Figure 21. Communication Drivers Distance Measurement and Estimation.

6. Conclusions

This paper focused on the study and development of an IoT architecture for Smart Industry services providers. The study was applied to a legacy manufacturing cell. The architecture is aware of the main technologies, protocols and services in order to be an enabler of integrated services empowering the interrelationship of heterogeneous technologies of the present and future IoT.

The heterogeneity of available technologies and solutions brings obstacles and challenges when supported by the same architecture. The prototypes facilitate these technologies and services integration addressing the concerns of integration in an industrial cell. They offer extra security measures that are important to cover in a professional situation, added to overcome existing threats and overseen future risks. The modularity of the system offers the ability to integrate in the platform different technologies solutions and security measures. The implementation of all the IoT devices proposed simplifies, facilitates and enhances business intelligence and operators' activity.

The generalization of this work to other manufacturing cells presents some advantages but also many challenges: one challenge is related to the more complex cells, such as aeronautics construction, where the number of machines largely surpasses the number of machines analyzed in this work. Nevertheless, the IoT architecture defined was tested for seven machines simultaneously and the load did not go over 12.5% of the maximum load. So, in a very rough estimation, the number of machines may be four time higher and the load will still be in the order of 50%, which is relatively safe. Moreover, the architecture assumes that many gateways can be created for handling several groups of nodes. Generating too much data may be difficult to handle on the management mainframes, so these mainframes will probably need to be upgraded.

Other challenge is related to the legacy equipment that have no sort of communications interfaces and, in many cases, are still operated manually. The existence of IoT sensors in the machine may provide smooth integration of the machine operations, namely on-off, loading, processing, unloading. The sensors installation highly depends on the availably of opening the equipment. In a less ambition phase, pressure sensors may be put over the operating buttons to sense and transmit the operator commands. In an even less ambition phase, the operators have a board where they log the operations. The integration proposed in the two previous phases are smooth as they do not deviate the operator from productive work. This last phase is the less smooth integration as it requires the operators to enroll other activities deviating then from the productive work.

Anyway, as long as data is acquired, the IoT architecture proposed handles all the remaining to integrate the legacy cell into an Industry 4.0 system.

The cloud platform chosen was tested and relevant details are achieved. Some important measures were proposed to avoid some existent bottlenecks. Other free platforms could be used such as Carriots, among others [36], but this drawback can only be overcome by the development of own platform using free tools such as Kaa [36].

Author Contributions: J.C. made this work under his MSc (Master of Science) Thesis and is mainly involved in the Implementation, Software Validation, Data Collecting and Analysis. N.B. is mainly involved in the Communications Protocol and Software Design and Implementation. C.C. and R.M. are supervisors of this work. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Acknowledgments: This work was supported by FCT, through IDMEC, under LAETA, project UIDB/50022/2020; FCT through ICT (Institute of Earth Sciences) project, project UIDB/04683/2020.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Diallo, M.; Pierreval, H.; Quilliot, A. Manufacturing cells design with flexible routing capability in presence of unreliable machines. *Int. J. Prod. Econ.* **2001**, *74*, 175–182. [CrossRef]
2. Trujillo-Toledo, D.A.; López-Bonilla, O.R.; García-Guerrero, E.E.; Tlelo-Cuautle, E.; López-Mancilla, D.; Guillén-Fernández, O.; Inzunza-González, E. Real-time RGB image encryption for IoT applications using enhanced sequences from chaotic maps. *Chaos Solitons Fractals* **2021**, *153 Pt 2*, 111506. [CrossRef]
3. Da Costa, F. *Rethinking the Internet of Things: A Scalable Approach to Connecting Everything*; Apress Media: New York, NY, USA, 2013; pp. 95–141.
4. Godoy, A.J.C.; Pérez, I.G. Integration of sensor and actuator networks and the SCADA system to promote the migration of the legacy flexible manufacturing system towards the industry 4.0 concept. *J. Sens. Actuator Netw.* **2018**, *7*, 1–21.
5. Rupprecht, B.; Trunzer, E.; König, S.; Vogel-Heuser, B. Concepts for retrofitting industrial programmable logic controllers for industrie 4.0 scenarios. In Proceedings of the 22nd IEEE International Conference on Industrial Technology, Valencia, Spain, 10–12 March 2021; pp. 1034–1041.
6. Kelepouris, T.; McFarlane, D. Determining the value of asset location information systems in a manufacturing environment. *Int. J. Prod. Econ.* **2010**, *126*, 324–334. [CrossRef]
7. Bosman, H.H.W.J.; Iacca, G.; Tejada, A.; Wörtche, H.J.; Liotta, A. Spatial anomaly detection in sensor networks using neighborhood information. *Inf. Fusion* **2017**, *33*, 41–56. [CrossRef]
8. Vermesan, O.; Friess, P. *Internet of Things: From Research and Innovation to Market Deployment*; River Publisherss: Aalborg, Denmark, 2014; pp. 1–6.
9. Silvestri, L.; Forcina, A.; Introna, V.; Santolamazza, A.; Cesarotti, V. Maintenance transformation through industry 4.0 technologies: A systematic literature review. *Comput. Ind.* **2020**, *123*, 103335. [CrossRef]
10. Zanella, A.; Bui, N.; Castellani, A.; Vangelista, L. Internet of things for smart cities. *IEEE Internet Things J.* **2014**, *1*, 22–32. [CrossRef]
11. Liu, J.; Yan, Z.; Yang, L.T. Fusion—An aide to data mining in internet of things. *Inf. Fusion* **2015**, *23*, 1–2. [CrossRef]
12. Zhao, F.; Sun, Z.; Jin, H. Topic-centric and semantic-aware retrieval system for internet of things. *Inf. Fusion* **2015**, *23*, 33–42. [CrossRef]
13. Cunha, J.; Cardeira, C.; Melicio, R. Traffic lights control prototype using wireless technologies. *Renew. Energy Power Qual. J.* **2016**, *1*, 1031–1036. [CrossRef]
14. Cunha, J.; Batista, N.C.; Cardeira, C.; Melicio, R. Wireless networks for traffic light control on urban and aerotropolis roads. *J. Sens. Actuator Netw.* **2020**, *9*, 1–17. [CrossRef]
15. Cunha, J.P.P.; Cardeira, C.; Batista, N.C.; Melicio, R. Wireless technologies for controlling a traffic lights prototype. In Proceedings of the IEEE 17th International Conference on Power Electronics and Motion Control, Varna, Bulgaria, 18–23 September 2016; pp. 866–871.
16. Cardeira, C.; Colombo, A.W.; Schoop, R. Wireless solutions for automation requirements. *ATP Int. Autom. Technol. Pract.* **2006**, *2*, 51–58.
17. Dhanjani, N. *Abusing the Internet of Things: Blackouts, Freakouts, and Stakeouts*; O'Reilly Media: Sebastopol, CA, USA, 2015.
18. Qiu, X.; Luo, H.; Xu, G.; Zhong, R.; Huang, G.Q. Physical assets and service sharing for IoT-enabled supply hub in industrial park (SHIP). *Int. J. Prod. Econ.* **2015**, *159*, 4–15. [CrossRef]
19. De la Fraga, L.G.; Mancillas-López, C.; Tlelo-Cuautle, E. Designing an authenticated Hash function with a 2D chaotic map. *Nonlinear Dyn.* **2021**, *104*, 4569–4580. [CrossRef]
20. García-Guerrero, E.E.; Inzunza-González, E.; López-Bonilla, O.R.; Cárdenas-Valdez, J.R.; Tlelo-Cuautle, E. Randomness improvement of chaotic maps for image encryption in a wireless communication scheme using PIC-microcontroller via Zigbee channels. *Chaos Solitons Fractals* **2020**, *133*, 109646. [CrossRef]
21. Perera, C.; Liu, C.H.; Jayawardena, S.; Chen, M. A survey on internet of things from industrial market perspective. *IEEE Access* **2015**, *2*, 1660–1679. [CrossRef]
22. Batista, N.C.; Melicio, R.; Matias, J.C.O.; Catalão, J.P.S. ZigBee wireless area network for home automation and energy management: Field trials and installation approaches. In Proceedings of the 3rd IEEE PES Europe Conference on Innovative Smart Grid Technologies, Berlin, Germany, 14–17 October 2012; pp. 1–5.
23. Batista, N.C.; Melicio, R.; Matias, J.C.O.; Catalão, J.P.S. ZigBee standard in the creation of wireless networks for advanced metering infrastructures. In Proceedings of the 16th IEEE Mediterranean Electrotechnical Conference, Yasmine Hammamet, Tunisia, 25–28 March 2012; pp. 220–223.
24. Batista, N.C.; Melicio, R.; Matias, J.C.O.; Catalão, J.P.S. ZigBee devices for distributed generation management: Field tests and installation approaches. In Proceedings of the 6th IET International Conference on Power Electronics, Machines and Drives, Bristol, UK, 27–29 March 2012; pp. 1–5.
25. Huang, L.-C.; Chang, H.-C.; Chen, C.-C.; Kuo, C.-C. A ZigBee-based monitoring and protection system for building electrical safety. *Energy Build.* **2011**, *43*, 1418–1426. [CrossRef]
26. Gomes, I.L.R.; Melicio, R.; Mendes, V.M.F. A novel microgrid support management system based on stochastic mixed-integer linear programming. *Energy* **2021**, *223*, 120030. [CrossRef]
27. Bonifácio, T.G.; Pantoni, R.P.; Brandão, D. SMAC multi-hop mesh routing protocol using IEEE 802.15.4. *Comput. Electr. Eng.* **2012**, *38*, 492–509. [CrossRef]

28. Han, D.-M.; Lim, J.-H. Smart home energy management system using IEEE 802.15.4 and ZigBee. *IEEE Trans. Consum. Electron.* **2010**, *56*, 1403–1410. [CrossRef]
29. Batista, N.C.; Melicio, R.; Matias, J.C.O.; Catalão, J.P.S. Photovoltaic and wind energy systems monitoring and building/home energy management using ZigBee devices within a smart grid. *Energy* **2013**, *49*, 306–315. [CrossRef]
30. Batista, N.C.; Melicio, R.; Mendes, V.M.F. Layered smart grid architecture approach and field tests by ZigBee technology. *Energy Convers. Manag.* **2014**, *88*, 49–59. [CrossRef]
31. Batista, N.C.; Melicio, R.; Mendes, V.M.F. Services enabler architecture for smart grid and smart living services providers under industry 4.0. *Energy Build.* **2017**, *141*, 16–27. [CrossRef]
32. Shuaib, K.; Alnuaimi, M.; Boulmalf, M.; Jawhar, I.; Sallabi, F.; Lakas, A. Performance evaluation of IEEE 802.15.4: Experimental and simulation results. *J. Commun.* **2007**, *2*, 29–37. [CrossRef]
33. Yi, P.; Iwayemi, A.; Zhou, C. Frequency agility in a ZigBee network for smart grid application. In Proceedings of the IEEE Innovative Smart Grid Technologies, Gaithersburg, MD, USA, 19–21 January 2010; pp. 1–6.
34. Yi, P.; Iwayemi, A.; Zhou, C. Developing ZigBee deployment guideline under WiFi interference for smart grid applications. *IEEE Trans. Smar* **2011**, *2*, 110–120. [CrossRef]
35. Betta, G.; Capriglione, D.; Ferrigno, L.; Miele, G. Influence of Wi-Fi computer interfaces on measurement apparatuses. *IEEE Trans. Instrum. Meas.* **2010**, *59*, 3244–3252. [CrossRef]
36. Zdravković, M.; Trajanović, M.; Sarraipa, J.; Jardim-Gonçalves, R.; Lezoche, M.; Aubry, A.; Panetto, H. Survey of internet-of-things platforms. In Proceedings of the 6th International Conference on Information Society and Techology, Barcelona, Spain, 18–20 March 2016; pp. 1–5.
37. Setiawan, M.A.; Shahnia, F.; Rajakaruna, S.; Ghosh, A. ZigBee-based communication system for data transfer within future microgrids. *IEEE Trans. Smart Grid* **2015**, *6*, 2343–2355. [CrossRef]
38. Botta, M.; Simek, M. Adaptive distance estimation based on RSSI in 802.15.4 network. *Radioengineering* **2013**, *22*, 1162–1168.
39. Jianwu, Z.; Lu, Z. Research on distance measurement based on RSSI of ZigBee. In Proceedings of the ISECS International Colloquium on Computing, Communication, Control, and Management, Sanya, China, 8–9 August 2009; pp. 210–212.