Gil *et al.*
Journal of Electrical Systems and Inf Technol (2022) 9:1
https://doi.org/10.1186/s43067-022-00043-4

Journal of Electrical Systems and Information Technology

RESEARCH

Open Access

Converging IoT protocols for the data integration of automation systems in the electrical industry

Santiago Gil[1,2*], Germán D. Zapata-Madrigal[1], Rodolfo García-Sierra[3] and Luis Alberto Cruz Salazar[4,5]

*Correspondence: sagilar@unal.edu.co
[1] Grupo T&T, Facultad de Minas, Universidad Nacional de Colombia, Medellín, Colombia
Full list of author information is available at the end of the article

Abstract

The Internet of Things (IoT) plays an important role in the development of applications for the Electrical Industry. The data has become essential for the technological advances in this industry, changing abruptly due to the distributed energy resources and the smart grid concept. The data integration also represents a relevant matter to address when performing IoT projects for electrical industry applications. The electrical industry requires incorporating different IoT protocols to comply with the distinct scenarios and the interoperability. This work proposes integrating the HTTP REST, MQTT, LoRaWAN, and OPC UA open communications protocols into an IoT platform and interoperable architecture for smart grid applications. This approach intends to contribute to smart grid solutions and automation systems in the electrical industry, promotes further integration of communication protocols for this field, and enables additional data-based applications for their automation systems. A Multi-Agent System architecture based on the IoT integration is proposed as an application to show how implementable is this approach in current and technological electrical systems.

Keywords: IoT, Communication protocols, Data integration, Interoperability, Multi-agent systems, Smart grid

Introduction

The *Internet of Things* is a crucial factor for the development of vertical applications to cover different scenarios that involve connectivity coverage, energy consumption, costs, transmission capabilities, module size, among other criteria. The IoT is widely empowering the electrical industry in the context of *Smart Grids* and Smart Cities. The IoT acts as the enabler for the data acquisition and data integration in applications where several processing elements spread data, allowing the massification of Big Data approaches with distributed (geographical) data sources [1]. The comprehensive area coverage is an important matter in electrical applications due to the nature of the geographical distribution of the infrastructure for transmission, generation, and distribution of power; that is why the low power wide area networks (LPWAN) technologies are suitable to address the electrical industry [2] even when they are not too familiar for deployment in smart metering and smart grid communication [3]. There are several critical applications of LPWA connectivity for smart grids or systems.

The IoT can be employed for different purposes in the electrical engineering applications: for real-time monitoring, for asset tracking and management, demand-side management, for collecting data to train and test data models, for protection systems, electric vehicles integration, among others. There are several possible applications, but there is an essential matter to consider: data integration. The data integration in IoT applications is done through several available IoT protocols. The protocols focus on specific aspects of IoT communications. However, it is necessary to guarantee the horizontal integration to cover as many constrained and non-constrained devices for the applications as possible [4].

Therefore, interoperability plays an essential role in the Electrical Industry applications ready for smart grids empowered by the IoT [5]. The integration of several communication protocols into one approach provides a high interoperability degree for the things-machines which interact with one another. Thus, considering a flexible communication architecture, the corresponding deployment with multiple IoT communication alternatives, including protocols and technologies, helps to achieve the requirements of the different scenarios of the electrical industry, the data integration between the electrical processes (horizontal integration), and the integration between the electrical systems and other industrial sectors (vertical applications). With the proper deployment of IoT technologies and communication protocols in the smart grid, further applications of data analytics can be addressed, including fault detection, power quality monitoring, load forecasting, load forecasting, load disaggregation, non-technical loss detection, load profiling, among other applications [6]; thus, the automation systems of the electrical systems can embed data analytics applications in order to improve the performance of the processes.

In this project, the LoRaWAN, MQTT, HTTP, and OPC UA IoT protocols are covered. All of them are open-source communication protocols, a fact which is essential to highlight. According to [7], open communication standards are critical to Industry 4.0 (I4.0). The open-source communication protocols play essential roles in the development of the networks of the I4.0 and the IoT. These advances directly benefit automation systems. Consequently, the electrical industry's automation systems and the subsequent integration within an interoperability framework are composed of services, things, people, and the different industrial sectors [5].

This approach consists of an IoT platform with an architecture that includes integrating the stated protocols: LoRaWAN, MQTT, HTTP, and OPC UA. Four protocols are designed for IoT applications in different scenarios. The LoRaWAN protocol, based on the LoRa LPWAN technology, connects constrained devices distributed geographically in broad areas [8], a requisite communication protocol to target regional, national, or global networks, suitable when thinking of integrating the electrical industry with the smart cities [8]. MQTT is based on IP for lightweight publish/subscribe connections among devices, a communication protocol usually used for application layer protocols with adequate security considerations [9]. The HTTP, mostly used in software applications, is exploited for IoT web-based applications, in this case, using the REST services; this protocol enables the interoperability between the IoT services within the electrical industry and the conventional web services due to the massification of this protocol on the web [9]. The OPC UA based on IP to offer a Service Oriented Architecture (SOA) with an appropriate data model to represent objects, variables, methods, and services for automation networks; OPC UA also represents the opportunity to integrate the IEC 61850 and the automation systems on the smart grid applications [10]. These protocols guarantee the end-to-end communication between machine-to-machine and machine-to-user for multi-purpose communication in applying the electrical industry, e.g., smart grid applications. Additionally, all these protocols require structuring data models for the devices on the networks, such as the IEC 61850 operates; thus, the object notation becomes mandatory. Finally, the consolidation of these protocols into one platform enhances data integration and interoperability in the electrical industry systems, enabling applications and services for the smart grid, data analytics, and the subsequent integration with other industries and the customers.

This approach focuses on the electrical industry's automation systems, addressing the data integration for monitoring, control, and comprehensive services for the processes and the people involved.

The remainder of the paper is as follows: "Literature review" section presents the state of the art related to smart grids. Section "Methods" presents the methods and structure of the proposal. Section "Results and Discussion" presents the results and discussions of the approach and the mapping between IoT and a Multi-Agent System (MAS), and "Conclusions" section presents some conclusions and proposals for future work.

Literature Review

Al-Fuqaha et al. [4] reviewed some IoT technologies for connectivity, application protocols, and IoT gateways developed in the literature. They noticed a gap between existing IoT protocols and a divergence because each one focuses on specific aspects of IoT communications. Therefore, they proposed an intelligent rule based IoT gateway to reduce market fragmentation between IoT protocols and to guarantee an efficient horizontal integration of data and services in IoT networks. Their approach highlights the importance of converging IoT protocols for the integration of the IoT in vertical applications. Although they did not consider either the LPWAN technologies/protocols nor the OPC UA protocol for industries, they did present many other IoT protocols and features that should be considered for the complete integration of the IoT networks. According to the review of Boulogeorgos et al. in [11], the LPWAN technologies offer suitable capabilities to connect remote constrained devices and fit applications in the electrical systems which are not time-critical. When there is no need for low latency, e.g., smart metering, smart grid management, or street lighting, LPWAN technologies can be used for such applications. Thus, the LPWAN technologies should be considered in the IoT ecosystem for the electrical industry; LoRa/LoRaWAN as an open-source alternative allows easy integration for these purposes. As stated by Li et al. [2], NB-IoT is another right choice of LPWAN technology for smart grid applications. However, considering the technology's novelty and its difficulty being deployed (depends on the network service providers), the NB-IoT cannot be integrated into this ecosystem.

The review of Strasser et al. [12] presents a good point of view about applying the IoT in industrial systems. They highlight that the power and energy systems are changing and require incorporating automation with Energy IoT. They also mention the IEC 62541-OPC UA and MQTT as relevant protocols that comply with the interoperability, standardization, and requirements for the industrial IoT applied on power systems; such protocols are also compatible with the IIRA [13] and RAMI [14] architectural models for interoperability. Due to the robustness of the protocols, they are getting attention to the power and energy systems domain, just like proposed in this work, to address industrial IoT in power systems.

On the other hand, Bedi et al. [15] focused on IoT for electric power and energy systems. They stated that the IoT causes positive economic, environmental, and societal impacts in the electric power and energy systems. The transformation into the smart grids also benefits technical factors such as scalability and interoperability, sensing capabilities, and improved control. The digitization of the IoT's electrical systems involves multiple applications for generation, transmission, distribution, and customer-side solutions. These advantages require to overcome several challenges as well. The standards for communication in IoT, the coexistence of networks, energy-efficient wireless communication networks, and IoT computational requirements are challenges touched in their research, matters which this work intends to address by means of the integration of the LoRaWAN, MQTT, OPC UA, and HTTP REST communication protocols together with an IoT platform for electrical systems.

The proposal of Prudenzi et al. [16] exposes a promising approach to applying the IoT for power systems. They employed a Raspberry PI board and the HTTP REST protocol to create a supervisory system for distribution substations. Although their approach provides a proper alternative for power systems, constrained or remote devices could not work. This approach could not be extended to other electrical or power systems applications. If other protocols were considered, the approach could cover more application cases in the electrical industry, such as it is proposed in this work.

This work aligns with the proposal of Peniak and Franekova of using open communication protocols for systems within the I4.0 context [17]; our approach focuses on the electrical systems and adopts the LoRaWAN protocol for LPWA networks and OPC UA for automation networks of power systems. The Internet of Things Energy Platform IoTEP proposed by Terroso-Saenz et al. [18] also aligns with an IoT application's open-source contribution to integrating energy data in electrical systems. The proposed platform contains many complex components and layers. However, it is focused on the data analytics layer, and of course, the incorporation of more IoT protocols would enable more IoT devices to connect to the platform. Their approach provided a basis for future work when including data analytics features in the IoT ecosystem for the electrical industry. The proposal of Karpenko et al. [19] gives an essential point of view about the interoperability for data integration in IoT ecosystems. They employed the Open Messaging Interface (O-MI) and Open Data Format (O-DF) standards under the HTTP REST protocol for smart parking and electric vehicle charging stations. It is a correct approach to consider integrating the IoT protocols for the electrical industry. The approach of Kuzlu et al. [20] proposed an internet-based platform for automated demand response applications as an alternative for traditional metering infrastructure-based communications. The platform mainly operates over the HTTP REST protocol for the utility-side and the customer-side. They also considered ZigBee to implement the home energy management systems to connect the loads and collect the data.

The approach of Iglesias-Urkia et al. [21] implemented an IoT integration for communication in electrical substations using the IEC 61850 standard, Web Services, the Constrained Application Protocol (CoAP) protocol, which bases on the HTTP REST protocol, and the Concise Binary Object Representation (CBOR). The IEC 61850 is mapped into CoAP to enable lightweight communication instead of using the legacy suggested protocols. Finally, the substation network resources are available in web services, and the data is accessible using the JSON representation format. Similarly, Hossain et al. [22] implemented an IoT system to control and monitor substation equipment and resources using low-cost technologies. This system uses the ESP8266 module as the main microcontroller and IoT gateway implementing the Wi-Fi technology and the MQTT protocol. The resources are controlled and monitored via a web server. Pawar and Vittal [23] are also based on IoT to create a portable and flexible smart energy management system to optimize energy consumption and utilization of power generated by Distributed Energy Resources and implement remote monitoring and advanced analytics. In this case, the IoT gateway implements the ZigBee protocol with XBee modules and a WAMP Server (PHP + MySQL) for data acquisition and real-time monitoring.

Regarding security aspects, Khan and Salah [24], Yugha and Chithra [25], and Tournier et al. [26] did reviews for the analysis and assessment of security requirements, challenges, and issues in IoT networks. The three reviews agreed with analyzing the security aspects by splitting the network layers, either from low-level to high-level layers or mapping these layers into the OSI model layers (bottom to top). The three reviews also did a specific analysis of the security issues for some IoT wired or wireless technologies and protocols, either IP-based or non-IP-based. The review of Khan and Salah [24], besides analyzing security in IoT protocols, proposed the blockchain technology as a complementary technology for cybersecurity in IoT networks. In contrast, the other two reviews, by Yugha and Chithra [25] and Tournier et al. [26], focus on analyzing several IoT protocols in deep, including HTTP REST, MQTT, and MQTT, which are touched on in this work. In terms of security for OPC UA, Cavalieri and Chiacchio [27] analyzed performance and security for this specific industrial IoT protocol, which is commonly not included when analyzing other IoT protocols because of its industrial approach. Vargas-Martínez and Vogel-Heuser [28] addressed the issue of added connectivity in industrial automation systems. The authors propose a reactive protection concept to all devices in a production network that can suffer potential external attacks comparable to smart grid networks. Four requirements for the reactive protection were introduced [28]: configurability and Automatic or Semi-Automatic Reactions to Intrusions (Req1); Compliance with the ISA/IEC 62443 Series of Standards (Req2), Ensure Correct Operation of the Underlying Automation System (Req3); and Multi-Platform Support and Interoperability with Preexisting Solutions (Req4). Naturally, other issues of smart grids are the response to smart houses electricity consumption [29], demand and marketing of electric energy [30], voltage-type ideal transformer and real-time simulation [31], grid voltage sags [32], the impact of transmission technologies [33], photovoltaic reconfiguration [34], solar-panel power efficiency [35], among others. Table 1 summarizes the works referenced in this section, addressed by the smart grid layers introduced in [36].

According to the review, there are some gaps and opportunities to bring interoperable integration of the IoT communication protocols in the electrical industry. This

Table 1 Summary of the selected literature review of Smart grids

Approaches	Smart grid layers [36]		
	Consumers layer	**Communication layer**	**Restraining distribution layer**
Al-Fuqaha et al. [4]	IoT services	Intelligent rule based IoT gateway	IoT integration
Boulogeorgos et al. [11]	Not time electrical critical systems	LPWAN	Smart metering, smart grid management, street lighting
IIRA [13]/RAMI 4.0 [14]	I4.0 standardization	IEC 62541-OPC UA, MQTT	Architectural models for interoperability
Bedi et al. [15]	Electrical systems, Smart grids	IoT protocols	Scalability, interoperability, other of smart grids
Cavalieri and Chiacchio [27]	Smart grids	IEC 61850 SCL, OPC UA to SOA	Interoperability of Smart Grid
Dimeas et al. [29]	Smart grids	Internet protocol via a gateway	Electricity consumption in smart houses
Hossain et al. [22]	Substation with low-cost technology	IoT gateway, ESP8266 module, Wi-Fi, MQTT	Monitor substation equipment
Iglesias-Urkia et al. [21]	Electrical substation	IEC 61850, Web Services, CoAP, HTTP REST, CBOR	IoT integration
Benigni et al. [31]	Energy systems	Communication network (Wireless and Wired)	Real-time simulation in power systems
Karpenko et al. [19]	Electric vehicle charging station	HTTP REST (by O-MI, O-DF)	IoT integration
Khan and Salah [24]	IoT services	OSI model layers and security in IoT protocols	Security aspects
Kuzlu et al. [20]	An internet-based platform for automated demand	HTTP REST	Energy management systems
Li et al. [2]	Smart grids	NB-IoT to LPWAN	Transmission, generation, and distribution of power
Pawar and Vittal [23]	DER	IoT gateway, ZigBee protocol, XBee, WAMP Server (PHP + MySQL)	Energy management system
Peniak and Franekova [17]	A network of power systems	Based on I4.0 protocols	IoT integration
Prudenzi et al. [16]	IoT for power systems	Raspberry PI board to HTTP REST	Monitor substation equipment
Rey-Boué et al. [32]	Photovoltaic system	IEC 61400–21 norm	Control of grid voltage sags
Strasser et al. [12]	IoT in industrial systems	IEC 62541-OPC UA, MQTT	Automation with Energy IoT
Terroso-Saenz et al. [18]	Electrical industry	IoTEP	IoT integration
Tournier et al. [26]	IoT services	OSI model layers by HTTP REST, MQTT	Security aspects
Yugha and Chithra [25]	IoT services	OSI model layers by HTTP REST, MQTT	Security aspects
Vargas-Martínez and Vogel-Heuser [28]	Industrial automation systems	Industrial Gateway (also known as IoT Gateway)	Security aspects
This authors contribution	Electrical systems, Smart grids	LoRaWAN, OPC UA, HTTP REST, MQTT	Automation networks of power systems

industry is facing severe changes that require the adoption of different technologies to fulfill them. The proposed open communication protocols allow the way to deploy single-purpose or multi-purpose networks handled by own to provide suitable communication scenarios for the electrical industry's different applications and the smart grids. The data for such applications is fundamental; the IoT allows data acquisition. Other data-based strategies and services can be deployed to benefit the processes and the people involved in the electrical systems.

Methods

In this section, the design of the platform and the architecture is explained in detail. This approach relies on communication architecture, but the application protocols and the high-level interfaces take relevant places in the architecture. Also, the application architecture used for data management in the different components of the networks is introduced.

The communication architecture

The IoT platform was initially designed to work with the LoRaWAN protocol. After verifying the importance of the data integration which the IoT protocols offer, not only LoRaWAN, other IoT protocols were adopted. The complete LoRaWAN network stack has implicit use of the HTTP and MQTT protocols, then, extending them for non-LoRaWAN networks became very useful. Integrating data from constrained devices to non-constrained devices, vice versa, or making both available to clients to interact with them, gives more sense for the world of the IoT. The OPC UA is a communication protocol designed explicitly for automation networks, but it is intended to enhance the industrial IoT in traditional and modern automation systems. Thus, the explicit use of the HTTP, MQTT, and OPC UA protocols were implemented into the IoT platform along with the LoRaWAN protocol to provide a complemented IoT approach for the different scenarios of the automation systems of the electrical industry. The communication architecture consists of a flat architecture containing multiple decentralized "Things" with different processing capabilities and a centralized IoT application server. The architecture enables the data integration horizontally, provides a considerable interoperability degree for the systems and the nodes, contributes to the distribution of processing for applications, and considers the inclusion of industrial automation systems, complying with some requirements that the electrical industry of this era, such as the smart grids and the integration with the I4.0 requirements [5, 14, 37]. Figure 1 presents the proposed communication architecture to integrate the IoT protocols for electrical engineering and automation systems. The proposal is extensible for several automation engineering applications within the electrical engineering domain. It covers several purposes when remote monitoring and control is required.

The protocols which are included in the architecture are essential to integrate data in electrical systems when many applications are considered. The LoRaWAN protocol complies with the requirements of constrained devices geographically distributed, such as the DER, alternative generation, vehicle to grid integration, etc. The MQTT protocol complies with the requirements for remote or local constrained and non-constrained devices that work under the IP protocol with no large deployments, such as asynchronous publish/subscribe communication for monitoring and control, integration of local data analytics services based on microcontrollers, etc. MQTT protocol is also commonly used for industrial IoT applications. The HTTP-REST supports integrating unidirectional non-constrained devices that work under the IP protocol, integrating external web

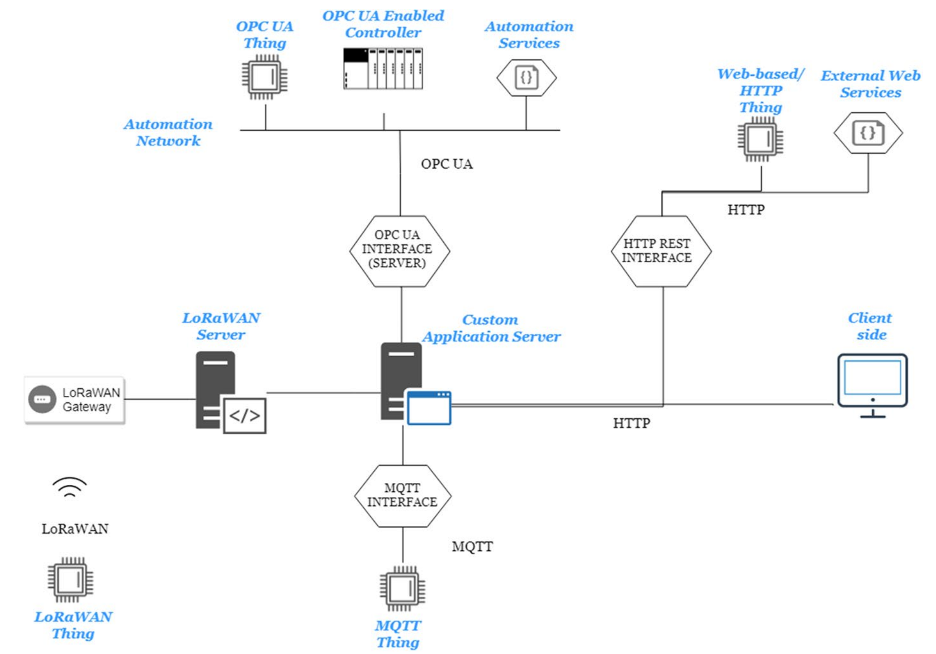

Fig. 1 The communication architecture to integrate IoT protocols

services and data visualization in the client-side. The OPC UA protocol complies with the most industrial part of the network. It is targeted to integrate controllers, sensors, SCADA systems, and other automation services in the factories, such as the automation of substations, automation of generation plants, etc. When the integration of these different protocols is completed, it is possible to create a robust ecosystem for machines in the automation systems and for people involved in the processes at the same time. The data integration interoperability, and distributed processing are some of the features that are provided by the network. Due to the LoRaWAN, MQTT, and OPC UA protocols' bidirectional capabilities, the data go across the network bidirectionally. The complementary integration of the REST services for the integration of external web services.

The application architecture

The interfaces to integrate the protocols are implemented in the application server, which is in charge of the IoT platform's functional features. The platform represents a means for the devices, machines, people, or things to interact with one another. It acts as a bridge to provide the transparency of the data in the processes. When integrating the IoT protocols into the platform, the dataflow converges into an interoperable approach. Finally, a powerful software resource is disposed to leverage automation systems through the IoT for several modern electrical engineering applications; the platform addresses the communication requirements for the consolidation of the real smart grids.

All the elements in the application layer, the "Things," are transparent in the network. According to a previously defined logic, the platform manages the dataflows stated by the software. The architecture was designed so the electrical things' messages enter into a transparent data integration core to allow interoperable information exchange between the protocols. The core is connected to the platform's business logic layer, where the system rules are performed. The objective of this approach of being applied to electrical systems demands a particular business logic in every component of the platform. Thus, the IoT platform, i.e., the network application, can be integrated with general-purpose IoT platforms (Google Cloud IoT, Azure IoT, AWS IoT, IBM IoT, etc.) to complement the functionalities and to avoid reinventing what such platforms already offer; then, more robust business logic for electrical systems can be developed instead. The integration capability with external IoT platforms is also complied by integrating the HTTP and MQTT protocols, which are often used for the connectivity in such applications.

The design of the application for the devices, the Electrical Things, is an essential matter. Thus, the application architecture considers the components for the device applications as well. Due to the processing capability of the things, regardless of whether constrained or non-constrained devices, they can perform light business logic. For example, the controllers can perform the automation processes; the sensors can give format to the variables; the meters can calculate the consumed energy; the multipurpose things can execute specific tasks. Once the devices have performed their tasks (reading or acting over the environment), the data is transmitted to the platform through the communication interfaces. Figure 2 presents the components of the application architecture for both the platform and the device applications. It shows the fundamental aspects that were considered for the integration of the IoT protocols in this approach.

The application server runs in an IoT platform that was designed using the Python programming language. Due to the web-based nature of the platform, the Django framework was used. Figure 3 exposes the pseudocodes of the IoT Platform's functionality and the structure of how the programming is developed to carry out of the IoT networks in the Django server in more detail. The Django Manager orchestrates the resources within the platform. It handles the views, resources, and models as an MVC web framework. However, it also runs on the OPC UA server's background and the MQTT integration via the client with the broker and the HTTP endpoints to integrate messaging with those protocols. Finally, the LoRaWAN server uses the HTTP endpoints or MQTT topics to send LoRaWAN messages to the platform, which runs as a standard web platform and

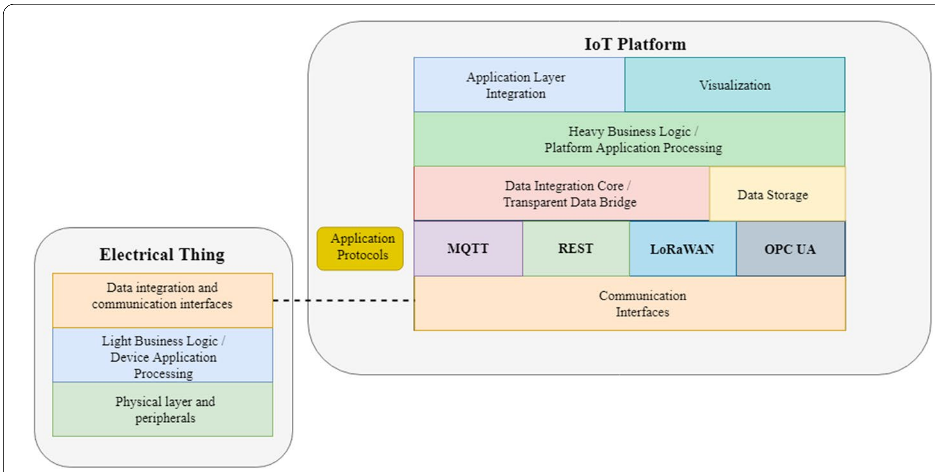

Fig. 2 The application architecture to integrate IoT protocols

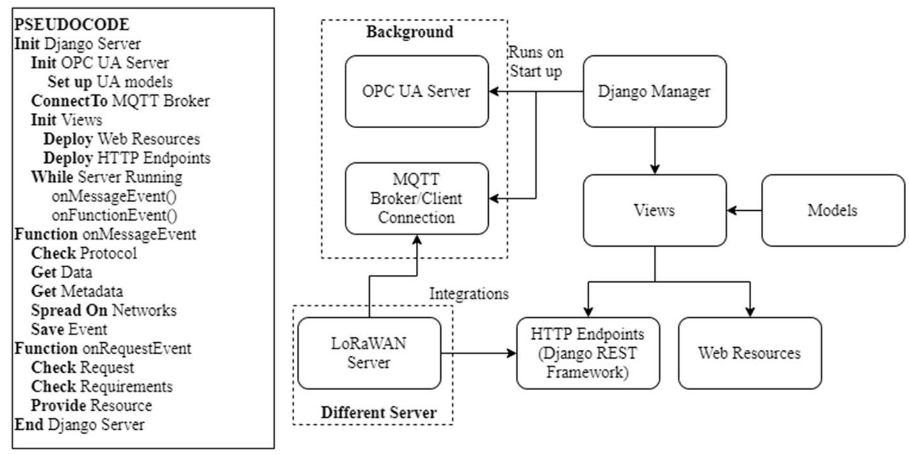

Fig. 3 Pseudocode and structure of resources of the IoT Platform

implements event handlers, asynchronous messages, and events. Works in [24–27] analyze the IoT security aspects which can be considered.

Results and Discussion

This approach is targeted as a first approach to the automation systems of the electrical industry. The approach can also be extended to fit any other automation system of other industries. The approach stated in [38] gives a valuable perspective on how smart grids' communications infrastructure can be used to integrate data and services for IoT applications in other industries.

The IoT can benefit the electrical industry in multiple applications [39]: for energy process control and monitoring, smart grids, DER, photovoltaic and wind generation systems, electric vehicles, demand-side management, demand response programs, and whatever application in which distributed sensors and controllers take place [40]. The automation systems are essential in critical electrical processes such as generation, transmission, and distribution; so, including multiple ways to integrate the data in systems which are geographically distributed by nature, and are composed of several process stages, makes the integration of IoT protocols a suitable approach to address systems. Figure 4 summarizes the possible IoT applications in the electrical industry when considering interoperable networks with IoT communication protocols. Each communication protocol fits specific applications; for example, OPC UA fits perfectly for power systems or industrial applications, but not too much for electric vehicles or street lighting. LoRaWAN fits for applications with constrained devices such as Street Lighting and can bring data from remote places such as the DER, the solar or wind generation farms, and distributed electric vehicles. MQTT and HTTP fit applications of multi-purpose IoT devices like home sensors or industrial/production devices; they also fit the integration with external web services. Once identified the applications and the IoT platform's suitability and its structure for the electrical industry, it is possible to deploy the networks with the different protocols.

Some microcontrollers equipped with the LoRa communication interface and some sensors in the peripherals to track interest variables in electrical applications are used.

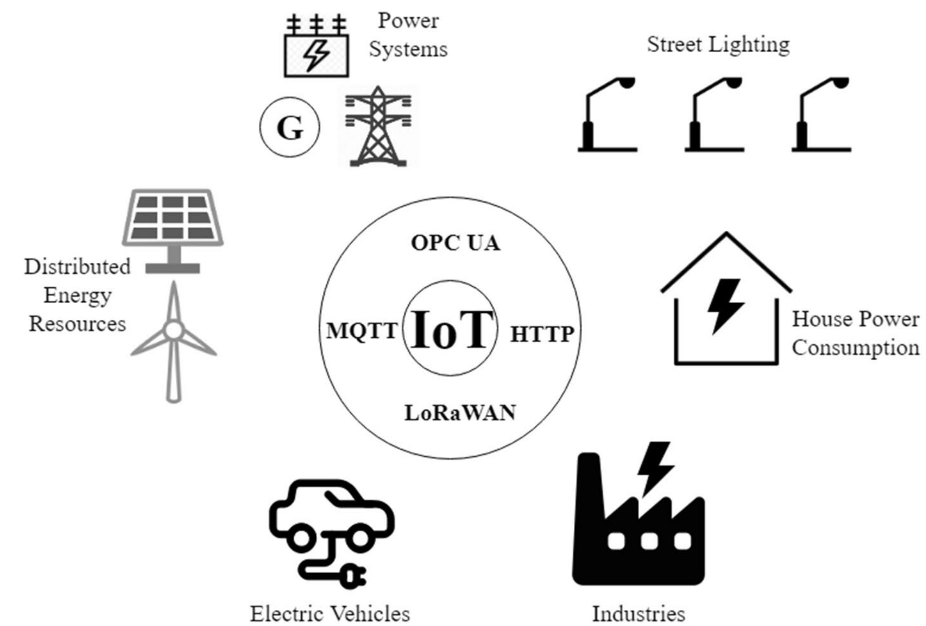

Fig. 4 IoT ecosystem for the electrical industry

The devices are coupled to different electrical elements, such as motors, dynamic lighting, refrigerators, transformers, etc. All of them are used for testing and prototyping purposes. It is possible to extract variables such as current, voltage, power, temperature, geolocation, fire detection, and on/off states. As mentioned before, the applications can be extended to whatever equipment and variables, according to the project's requirements, the novelty mainly relies on data integration.

The OPC UA protocol provides suitable networks for industrial IoT solutions or power systems in general. It can be interfaced with traditional automation systems; then, the IoT is integrated with the automation networks. An OPC UA network runs within the platform; it uses the Free OPC UA Client GUI software to check the network. The IoT data from the LoRaWAN nodes are available for the OPC UA network objects, discriminated by attributes, variables, and services. There are no services in this example, but if any IoT node had a service, it could be published on the OPC UA network and requested from other objects to perform the tasks. The ecosystem's nodes or things can request, acquire, or publish data or services available for the other objects, exploiting the service-oriented architectures' features.

The MQTT protocol provides a lightweight messaging service. The objects or devices can subscribe to receive the messages of interest and publish the newly available data for interesting objects and devices. Table 2 shows some MQTT messages which use the publish/subscribe method for some devices; the data is also available on the web interface of the IoT platform application, which allows the monitoring of the MQTT events with their respective timestamps. The MQTT protocol becomes useful even for human visualization. The objects can spread data across the IoT ecosystem while reaching constrained, and non-constrained devices with the publish/subscribe method by topics.

The same occurs with the HTTP protocol. It is widely used around the world for multi-purpose applications. The devices and web services are embedded with the

Table 2 MQTT messages by subscription topics

Topic	Message	Device	Units of measurement
iotplatform/eiot/Test-Application/EIoT-Node-2-LoRaWAN102	{"voltage":1.90}	EIoT LoRaWAN Node 2	[V]
iotplatform/eiot/Test-Application/EIoT-Node-4-LoRaWAN102	{"mean_current":0.32,"mean_power":38.42,"max_power":39.26,"fire_detector":0}	EIoT LoRaWAN Node 4	[A, W, W, Bool] respectively
iotplatform/eiot/Test-Application/EIoT-Node-1-LoRaWAN102	{"mean_current":0.32,"mean_power":38.42,"max_power":39.26,"refrig_temp":10.80,"freez_temp":47.47,"door_state":1}	EIoT LoRaWAN Node 1	[A,W,W,°C,°C, Bool] respectively
N/7c38665ac58c/system/0/Dc/Battery/Voltage	{"value": 52.909999847412109}	Battery Inverter/Charger Controller	[V]

HTTP protocol through the REST interfaces, allowing them to interact with web resources and data in a structured format. The REST interfaces' JSON format allows the representation through object-structured data, a suitable way to represent the data in the IoT.

The data objects represented by the JSON formats can vary depending on the specific development of the REST APIs. Incorporating the HTTP protocol inside the IoT ecosystem also enables web integration for the client-side using web integrations and external web services. Like the HTTP-REST, all the communications protocols proposed here allow bidirectional data exchange. The presented pictures only contain reading data information, but the interfaces to write data for the end devices are also available. Although the LoRaWAN protocol relies on the REST or MQTT protocols to represent the data, it is not the same protocol that any of them has many other considerations to deploy a LoRaWAN network test the JSON objects were used. The LoRaWAN packets on the server-side have JSON structures to handle the data—the LoRaWAN network server's local deployment based on ChirpStack.

The proposal of employing multiprotocol and interoperable networks in IoT applications benefits the industry with several connected devices, multiple processes, countless amounts of available data, and always presents the processes' geographical distribution and equipment. Something important to mention is that all the protocols proposed here can be deployed in private or local networks, in public networks, or a combination of both, due to the open-source nature of them. This feature helps deploy the IoT networks for the different environments of the electrical industry ecosystem. A qualitative analysis of performance for the implementation of the proposed protocols is shown in Table 2.

The electrical industry's data integration addresses the challenges of digitizing processes to go beyond the smart electrical grids and consolidate the electrical systems ready to integrate with the other industrial sectors under the IoT protocols. Subsequently, data-based services can be developed to make value-added solutions through artificial intelligence, data analytics, statistics, machine learning, and integrating such services with the traditional and modern automation systems. Table 3 shows selected performance efficiency based on ISO/IEC 25010 (Quality models to software product)

Table 3 Performance efficiency of the implemented IoT protocols

IoT protocol	Performance efficiency (based on ISO/IEC 25010)	
	Time-behavior	**Resource utilization**
LoRaWAN	− (its packets take from 0.2 s to more than 1 s to achieve the server)	+ (it implements a constrained device 20 KB RAM and lightweight server)
MQTT	+ (its lightweight packets require just a 2-byte header, achieving the fastest communication among the four implemented protocols)	+ (the broker and end devices are implemented seamlessly on constrained and small IP-enabled devices and its Pub/Sub feature enables bidirectionality)
OPC UA	+ (it can deal with hard real-time communication and Time Sensitive Networks for critical infrastructure)	– (It requires modeling the network before implementing and requires a dedicated server to manage all the events in the network)
HTTP REST	+ (Even if it is not a too lightweight protocol, its packets, depending on the payload, are fast to achieve the server)	– (its endpoints require a dedicated server and their corresponding development for the available options -POST, PUT, GET, DELETE-, which makes this protocol a little complex to use, especially in small deployments)

Notation: + means High performance, – means Low performance

to consider IoT protocols presented above in this section. The instrumentation, cybersecurity, business logic, redundancy, and other criteria are also essential in deploying IoT networks to electric power and energy systems [15]. The electrical systems domain is highly dependent on physical variables, which are usually complex to acquire. Then, a phase for the design and implementation of the instrumentation is suggested.

Mapping electric IoT to multi-agent systems for distributed control scenarios

IoT technology offers a suitable alternative to implement communication in distributed control systems for the electrical industry. The electrical systems have been positively affected by communication technologies, changing their traditional centralized communication functionalities into the diversification of nodes distributed along with power plants, cities, and rural spaces. Implementing MAS to coordinate all the electrical processes' resources becomes a useful strategy to manage the communication network and assist the operation with artificial intelligence using the smart agents [41]. Some previous works integrating MASs in electrical and power systems applications have been made by Srivastava et al. [42], Lagorse et al. [43], Singh et al. [44], and Tom et al. [45]. Readers are referred to [36] for more MAS approaches applications in smart grids and their agent's definitions in [46, 47]. Here is proposed a mapping between the IoT protocols previously mentioned, LoRaWAN, MQTT, HTTP, OPC UA, and a MAS to monitor and control a decentralized electric grid through four agents implement these protocols. This application simulation shows how these IoT protocols can be embedded into a simple and highly distributed electrical system in order to converge the data integration and the control into an interoperable and available platform, a MAS platform in this case. In this simulation, four agents have proposed: (1) the Grid Manager Agent, (2) the Distributed Resources Manager Agent, (3) the Smart City Integration Agent, and (4) the Market Agent. The system overview of the MAS applied is shown in Fig. 5. The legends refer to which protocol is used for actions and perceptions. This agent-based architecture is based on the Prometheus methodology [48]. A similar approach was carried out in previous work in [49].

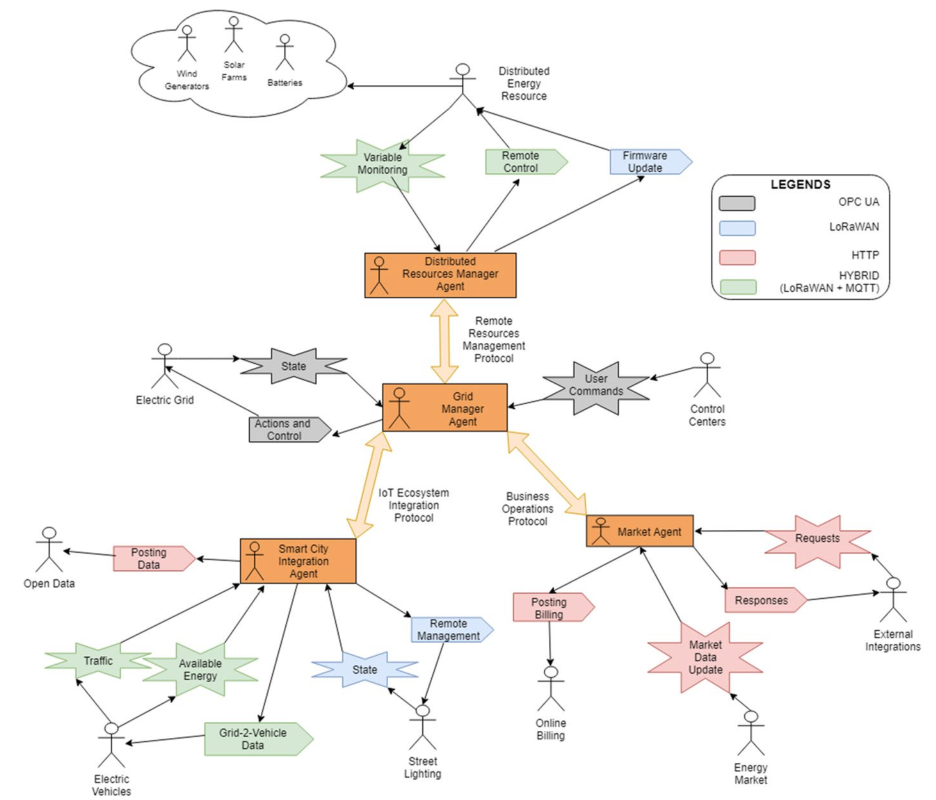

Fig. 5 Mapping between IoT protocols and a MAS to manage an electric grid

According to their name, every agent has specific capacities to deal with the environment, i.e., actions and perceptions with specific equipment. For example, the Smart City Integration Agent would interact with electric vehicles, smart light poles, and open city data portals. The Grid Manager Agent would integrate the other agents' data while managing the system's control center. The Distributed Resources Manager Agent would manage the Distributed Energy Resources, such as non-conventional renewable generators and distributed sensors. Finally, the Market Agent would be in charge of updating the energy market information, such as energy price continuously, required demand, availability, and other features. After defining the agents and their capacities/functionalities, the communication protocols are mapped to the agents. Firstly, the Grid Manager Agent, coupled with the control center and the grid management, use the OPC UA protocol to deal with its environment's actions and perceptions. The Distributed Resources Manager Agent, coupled to DER, uses a combination of LoRaWAN and MQTT to transmit and receive data in the form of actions and perceptions in its environment, composed of geographically distributed equipment, such as solar panels, wind generators, batteries, or energy meters. Correspondingly operates the Smart City Integration Agent, some actions and perceptions would use MQTT over IP, for example, electric vehicles using cellular modems, others would use LoRaWAN, for example, light poles with embedded LoRa modules, and some other integrations use HTTP because of its interoperability with other information systems. The Market Agent, on the other hand, does not perform operation tasks indeed, but it is designed to interact with the energy market (energy price, power demand, availability, etc.) and other integrations regarding the energy trading; then, this agent requires the implementation of HTTP, specifically REST requests, to interact with other servers and clients. Finally, the MAS coordination is done through the FIPA Agent Communication Language (ACL) with ACL protocols between agents [41], being the Grid Manager Agent the central agent, and the system's orchestrator in this approach.

Agents' development and pseudocodes

The MAS is launched using the Java Agent Development (JADE) framework [50]. Every agent is initialized and assigned its behaviors, in which the IoT protocols and the ACL communication are embedded. The agents' internal communication is carried out with the ACL messages, the integration with the LoRaWAN (MQTT backhaul) and MQTT protocols is done via the Eclipse Paho Java library, the HTTP protocol via HTTP requests in Java. All the protocols and messaging in this application converge to the OPC UA protocol, where it is possible to monitor and control every variable involved in the system. The OPC UA server is implemented in Python with the Free OPC UA stack, and the Grid Manager Agent connects to that server as a client with privileges using the OPC UA Java Legacy.

Once the networks are ready, the JADE container is deployed, and the MAS can begin the grid's operation. Figure 6 shows an ACL interaction between the proposed agents. The Grid Manager Agent subscribes to the Distributed Resources Manager Agent and the Smart City Integration Agent events. Then, these agents transmit the messages of their internal networks to the Grid Manager Agent, which confirms the message is

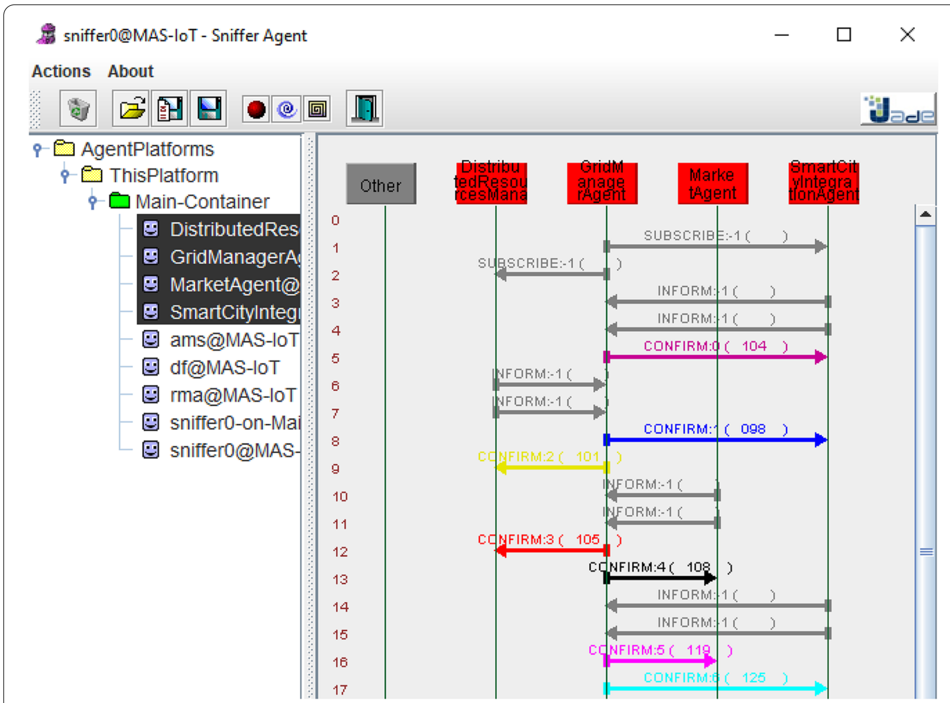

Fig. 6 Internal communication of MAS with ACL messages

receiving. The Market Agent, on the other hand, checks the energy market variables and transmits those updates to the Grid Manager Agent. Any time an agent has a new proposal, for example, a change in the operation, it asks the Grid Manager Agent, which verifies and accepts or denies the proposal. Finally, the Grid Manager Agent updates the nodes in the OPC UA network discriminated by agent network. Figure 7 presents the OPC UA network and takes advantage of the protocol's folder organization to discriminate the objects by interaction with agents. For instance, in Fig. 5, the Smart City Integration Agent acts over and receives electric vehicles and smart light poles' perceptions. The *SmartCity* folder includes an electric vehicle and a smart light pole that interact with this specific agent. This way, it is possible to integrate the data involved in controlling electrical systems via MAS in a convergent way and available for a central supervisory system of distributed resources. The *ControlCenter* folder contains the objects and variables regarding the Grid Manager Agent. The *DER* folder is the Distributed Resources Manager Agent, the *Market* folder the Market Agent, and the Smart City Integration Agent. A primary criterion to take all the information into OPC UA is that this protocol supports real-time required critical infrastructures, such as the electrical infrastructure, and coordinating the communications in distributed scenarios [41], including agent-based smart grids. OPC UA also supports several data types of representation and service orientation, an essential factor to consider when the distributed scenarios require distributed microservices in SOAs.

This application simulation exposes the suitability of integrating convergent IoT protocols for implementing communications and control systems in the different scenarios

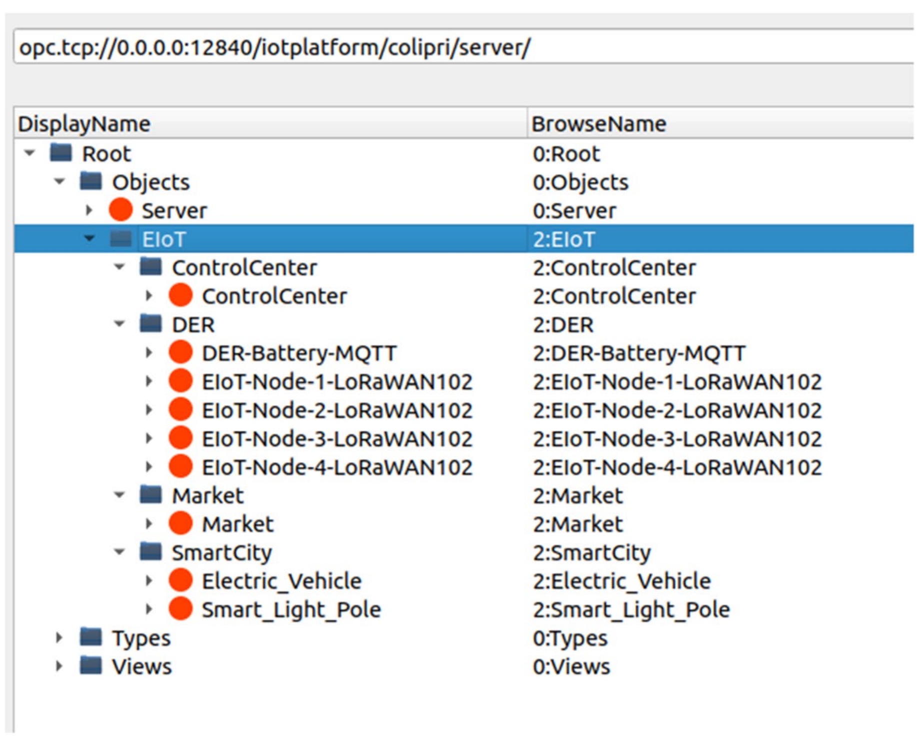

Fig. 7 OPC UA network discriminated by agent subnetwork

the smart grid has, this time via a MAS focused on handling the distributed resources of an electric grid. Implementing a MAS in this system depends on what will be represented and the MAS's scope indeed. In this case, the MAS is oriented to administrate and coordinate the messaging, data, and communications involved in the whole system. However, it could even be implemented to administrate certain functionalities of the system, interact directly with users, administrate databases, and perform inferences. Table 4 provides a brief explanation of the pseudocode used for every agent in the proposed MAS system, each designed with behaviors considering the Prometheus Methodology [47]. Then, no variables representative of power systems is shown, but they could be included seamlessly. Just consider a power generator. It could be a common generator located in a power plant or a wind generator located in a wind generator farm. The power plant's power generator can be integrated directly to the OPC UA network; it can be modeled and integrated with the next features: attributes, i.e., nominal frequency, nominal voltage, nominal current, peak current, peak RPM, number of poles, etc. Variables, i.e., voltage frequency, generated power, temperature, current, RPM, etc. Services (in case the system is integrated in a SOA with distributed control) – Start(), Release(), EmergencyStop(), etc. This for the generator located in a power plant. Now, for the wind generator, which is located far from a control center, the data can be acquired via LoRaWAN. The wind generator can also be modeled in the OPC UA network, but the data is acquired via LoRaWAN and then integrated into the OPC UA network, for this case, using smart agents. Thus, this approach shows an architecture and a methodology to implement communication in the electrical industry's distributed systems more than a specific application. Another great component of implementing a MAS and its ACL is the opportunity of using ACL protocols, tags, and serializations to deal with messages and objects which are necessary to be sent by the MAS network. Agent communication

Table 4 Agents' pseudocodes of the MAS proposed

PSEUDOCODE Grid Manager Agent **Init Agent** **Set up** Agent Parameters **Add** SubscribeBehavior **Add** ReceiveEventsBehavior **Add** ManageOPCUANetworkBehavior **Function** SubscribeBehavior **SubscribeTo** Pub/Sub Agents **Function** ReceiveEventsBehavior **FilterBy** ACL Performative **Performative**=="INFORM" **Save** Event **Performative**=="PROPOSE" **Check** Proposal **Accept** or **Deny** Proposal **Spread** Changes **Function** ManageOPCUANetworkBehavior **Update** OPC UA Network **Update** IoT Networks based on OPC UA **Spread** Central Commands **End** Agent	**PSEUDOCODE Distributed Resources Manager Agent** **Init Agent** **Set up** Agent Parameters **Add** ManageDERBehavior **Add** ReceiveCentralManagerBehavior **Function** ManageDERBehavior **Collect** Data and Events **Identify** DER changes **Execute** Internal Commands **PublishTo** Grid Manager Agent **Function** ReceiveCentralManagerBehavior **Check** External Commands **Execute** External Commands on DER **End** Agent
PSEUDOCODE Smart City Integration Agent **Init Agent** **Set up** Agent Parameters **Add** ManageCityOperationBehavior **Function** ManageCityOperationBehavior **Collect** Data and Events **Identify** Operation changes **Execute** Internal Commands **PublishTo** Grid Manager Agent **End** Agent	**PSEUDOCODE Market Agent** **Init Agent** **Set up** Agent Parameters **Add** CheckMarketBehavior **Function** CheckMarketBehavior **Search** Energy Market Data **Do** Web Scrapping on Energy Management Agencies **Search** Open Energy APIs **Analyze** Changes and Trends in Market **PublishTo** Grid Manager Agent **End** Agent

ontologies can also be applied to provide more rigor and structuration to the agents' messaging service.

Security aspects of the system

Regarding this approach's security aspects, authentication, encryption, and acceptable cybersecurity practices were focused. The MQTT security was addressed by implementing the user/password authorization mechanism, the OPC UA security by implementing the security policy with a sign and encrypt, but without a certificate, the HTTP security by implementing the JWT authentication method to access the services. The LoRaWAN security by implementing the AES 128 encryption and the Over The Air Activation (OTAA) with a 24-h reset mechanism to refresh the Network and Application security keys every day in the end nodes. Considering the security aspects of Vargas-Martínez and Vogel-Heuser [28] (see "Literature review" section), this work fulfills the requirements in terms of ensuring the correct operation of the underlying automation system (Req3). Moreover, by guaranteeing the real-time capabilities, high availability, and high performance of the communication network and the multi-platform support and interoperability (Req4) by providing an open and interoperable digital environment between the different resources of the entire network.

Conclusions

This work is aligned with the research trends in IoT for the electrical industry. It intends to comply with the existing challenges in smart grid applications, focusing on the interoperable integration of multiple processes and scenarios present in this industry. However, the electrical industry has many applications and scenarios that cannot be solved with just one IoT protocol or technology. It requires several communication alternatives that complement one another, and an integrated solution framed by the interoperability to address this industry. Therefore, four IoT protocols were applied in this work: (1) The WAN networks using the LoRaWAN protocol, (2) IoT networks through the HTTP REST, (3) the MQTT, and (4) the industrial approach by OPC UA. Moreover, an agent-based architecture was introduced using an open specification and software of LoRaWAN with the Mbed stack for the devices and ChirpStack for the network server; the Python Free OPC UA stack; the Paho Mosquitto libraries for MQT; and the Python-Django libraries for HTTP REST. It is essential to highlight that all the selected protocols are free to use and standardized by international organizations.

We conclude that integrating IoT communication protocols provides a straightforward way to integrate the data in applications where multiple data sources are available and required to guarantee monitoring and control. Specifically, in smart grids, each IoT protocol employed in this work has strengths for some types of applications and weaknesses for other types. LoRaWAN has offered an extended range and low power consumption, but few data rate and payload. HTTP REST has interacted with web-based applications but was more complex, heavier, and did not satisfy bidirectionality. The OPC UA has fitted particular applications for time-sensitive networks, service-oriented systems, and process control. Still, with this approach, it was much more complicated, heavier, and harder to deploy than the other IoT protocols. MQTT has offered a lightweight and straightforward bidirectional messaging service for IP-based devices, but it was not suitable for non-IP devices. However, according to its time-behavior and resource utilization, the MQTT protocol has been evaluated as the best performance efficiency. Finally, when combining all these protocols into one approach, a higher degree of smart grid's interoperability is achieved. This approach could be extended for different industries and applications seamlessly; this time, the electrical industry has been selected for the application case, but the core of the architecture and the data integration remains useful for any other automation or IoT system.

Thus, as future work is expected to include other IoT communication protocols in this architecture, standardized cellular LPWA networks and technologies/protocols such as NB-IoT and LTE-M are being researched to join them into this approach. Additionally, it is significant to integrate the IEC 61,850 standard communication protocols as additional protocols for domain-specific electrical systems applications. Other available IoT protocols presented in [4] would be considered, as well. It is also essential to carry out data-based applications and services: data analytics, machine learning, artificial intelligence proposals for predictive maintenance, detection of outliers, decision-makers for energy management systems, vehicle to grid integration, demand-side management, and demand response strategies, among others. The proposed architecture is expected to be extended for other domains as an IoT for I4.0 applications. This approach can be subsequently integrated with general-purpose IoT platforms (Google Cloud IoT, Azure IoT, AWS IoT, IBM IoT, etc.) to complement the systems' functionalities. Regarding security aspects, more robust mechanisms and strategies can be further applied to improve the electrical systems' cybersecurity (vulnerabilities, threats, attacks, and reactive protection), e.g., achieving Req1-2 from "Literature review" section.

Abbreviations
IoT: Internet of Things; DER: Distributed energy resources; LPWAN: Low power wide area networks; I4.0: Industry 4.0; SOA: Service-oriented architecture; MAS: Multi-agent system; O-MI: Open messaging interface; O-DF: Open data format; CoAP: Constrained application protocol; CBOR: Concise binary representation; ACL: Agent communication language; OTAA: Over the air activation.

Acknowledgements
Not applicable.

Authors' contributions
S.G. contributed with the implementation, analysis, validation of results, and writing the draft. G.Z. contributed with the supervision, project administration and the review and editing of the final document. R.G. contributed with the conceptualization, project administration, and supervision. L.C. contributed with conceptualization of multi-agent systems, analysis of performance, and review and editing of the final document. All authors have read and approved the manuscript.

Funding
Not applicable.

Available data and materials
Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Declarations

Competing interests
The authors declare that they have no competing interests.

Author details
[1]Grupo T&T, Facultad de Minas, Universidad Nacional de Colombia, Medellín, Colombia. [2]Department of Electrical and Computer Engineering, Aarhus University, Aarhus, Denmark. [3]Head of Innovation Observatory, Enel-Codensa S.A. E.S.P. (Enel Group), Energy Service Provider, Bogotá, Colombia. [4]Grupo de Investigación GEPRO, Universidad Antonio Nariño, Bogotá, Colombia. [5]Institute of Automation and Information System, Technical University Munich, Garching near Munich, Germany.

Received: 17 March 2021 Accepted: 26 January 2022
Published online: 10 February 2022

References

1. Bonomi F, Milito R, Natarajan P, Zhu J (2014) Fog computing: a platform for Internet of Things and analytics. In: Bessis N, Dobre C (eds) Big data and internet of things: a roadmap for smart environments Studies in Computational Intelligence, vol 546. Springer, Cham. https://doi.org/10.1007/978-3-319-05029-4_7
2. Li Y, Cheng X, Cao Y et al (2018) Smart choice for the smart grid: Narrowband internet of things (NB-IoT). IEEE Internet Things J 5:1505–1515. https://doi.org/10.1109/JIOT.2017.2781251
3. Kabalci Y (2016) A survey on smart metering and smart grid communication. Renew Sustain Energy Rev 57:302–318. https://doi.org/10.1016/j.rser.2015.12.114
4. Al-Fuqaha A, Khreishah A, Guizani M et al (2015) Toward better horizontal integration among IoT services. IEEE Commun Mag 53:72–79. https://doi.org/10.1109/MCOM.2015.7263375
5. Lu Y (2017) Industry 4.0: A survey on technologies, applications and open research issues. J Ind Inf Integr 6:1–10. https://doi.org/10.1016/j.jii.2017.04.005
6. Marlen A, Maxim A, Ukaegbu IA, Kumar Nunna HSVS (2019) Application of big data in smart grids: energy analytics. In: International conference on advanced communication technology, ICACT 2019, pp 402–407. https://doi.org/10.23919/ICACT.2019.8701973
7. B&R Automation (2014) Open communication standards. Key to success for Industry 4.0. br-automation.com
8. Bruneo D, Distefano S, Giacobbe M et al (2019) An IoT service ecosystem for smart cities: The #SmartME project. Internet Things 5:12–33. https://doi.org/10.1016/j.iot.2018.11.004
9. Čolaković A, Hadžialić M (2018) Internet of Things (IoT): a review of enabling technologies, challenges, and open research issues. Comput Netw 144:17–39. https://doi.org/10.1016/j.comnet.2018.07.017
10. Cavalieri S, Regalbuto A (2016) Integration of IEC 61850 SCL and OPC UA to improve interoperability in Smart Grid environment. Comput Stand Interfaces 47:77–99. https://doi.org/10.1016/j.csi.2015.10.005
11. Boulogeorgos A-AA, Diamantoulakis PD, Karagiannidis GK (2016) Low power wide area networks (LPWANs) for Internet of Things (IoT) applications: research challenges and future trends. arXiv:1611.07449
12. Strasser TI, Andrén FP, Vrba P, et al (2018) An overview of trends and developments of internet of things applied to industrial systems. In: Proceedings of IECON 2018—44th annual conference of the IEEE industrial electronics society, pp 2853–2860. https://doi.org/10.1109/IECON.2018.8591431
13. Shi-Wan L, Bradford M, Jacques D et al (2017) The industrial internet of things volume G1: reference architecture. Ind Internet Consort White Pap Version 1.:58 Seiten
14. Federal Ministry for Economic Affairs and Energy (2019) Plattform Industrie 4.0 - RAMI4.0 – a reference framework for digitalisation. Plattform Industrie 4.0. https://www.plattform-i40.de/IP/Redaktion/EN/Downloads/Publikation/rami40-an-introduction.html
15. Bedi G, Venayagamoorthy GK, Singh R et al (2018) Review of Internet of Things (IoT) in electric power and energy systems. IEEE Internet Things J 5:847–870. https://doi.org/10.1109/JIOT.2018.2802704
16. Prudenzi A, Fioravanti A, Regoli M (2018) Making electric distribution of industrial customers smarter with IoT. In: SPEEDAM 2018—Proceedings of international symposium on power electronics, electrical drives, automation and motion, pp 556–561. https://doi.org/10.1109/SPEEDAM.2018.8445253
17. Peniak P, Franekova M (2015) Open communication protocols for integration of embedded systems within Industry 4. In: International conference on electronic, pp 181–184
18. Terroso-Saenz F, González-Vidal A, Ramallo-González AP, Skarmeta AF (2019) An open IoT platform for the management and analysis of energy data. Futur Gener Comput Syst 92:1066–1079. https://doi.org/10.1016/j.future.2017.08.046
19. Karpenko A, Kinnunen T, Madhikermi M et al (2018) Data exchange interoperability in IoT ecosystem for smart parking and EV charging. Sensors (Switzerland). https://doi.org/10.3390/s18124404
20. Kuzlu M, Rahman MM, Pipattanasomporn M, Rahman S (2017) Internet-based communication platform for residential DR programmes. IET Netw 6:25–31. https://doi.org/10.1049/iet-net.2016.0040
21. Iglesias-Urkia M, Casado-Mansilla D, Mayer S et al (2019) Integrating Electrical Substations Within the IoT Using IEC 61850, CoAP, and CBOR. IEEE Internet Things J 6:7437–7449. https://doi.org/10.1109/JIOT.2019.2903344
22. Hossain MS, Rahman M, Sarker MT et al (2019) A smart IoT based system for monitoring and controlling the substation equipment. Internet Things 7:100085. https://doi.org/10.1016/j.iot.2019.100085
23. Pawar P, Vittal KP (2019) Design and development of advanced smart energy management system integrated with IoT framework in smart grid environment. J Energy Storage 25:100846. https://doi.org/10.1016/j.est.2019.100846
24. Khan MA, Salah K (2018) IoT security: Review, blockchain solutions, and open challenges. Futur Gener Comput Syst 82:395–411. https://doi.org/10.1016/j.future.2017.11.022
25. Yugha R, Chithra S (2020) A survey on technologies and security protocols: Reference for future generation IoT. J Netw Comput Appl 169:102763. https://doi.org/10.1016/j.jnca.2020.102763
26. Tournier J, Lesueur F, Le MF et al (2020) A survey of IoT protocols and their security issues through the lens of a generic IoT stack. Internet Things. https://doi.org/10.1016/j.iot.2020.100264
27. Cavalieri S, Chiacchio F (2013) Analysis of OPC UA performances. Comput Stand Interfaces 36:165–177. https://doi.org/10.1016/j.csi.2013.06.004
28. Vargas Martínez C, Vogel-Heuser B (2018) Towards industrial intrusion prevention systems: a concept and implementation for reactive protection. Appl Sci 8:2460. https://doi.org/10.3390/app8122460
29. Dimeas A, Drenkard S, Hatziargyriou N et al (2014) Smart Houses in the Smart Grid: Developing an interactive network. IEEE Electrif Mag 2:81–93. https://doi.org/10.1109/MELE.2013.2297032

30. Nakhodov V, Moreno G (2000) Métodos económicos para el manejo de la demanda de potencia eléctrica: aplicación en el mercado eléctrico de Ucrania. Rev Fac Ing Univ Antioquia 126–139. https://revistas.udea.edu.co/index.php/ingenieria/article/view/325926
31. Benigni A, Strasser T, De Carne G et al (2020) Real-time simulation-based testing of modern energy systems: a review and discussion. IEEE Ind Electron Mag 14:28–39. https://doi.org/10.1109/MIE.2019.2957996
32. Rey-Boué AB, Guerrero-Rodríguez NF, Stöckl J, Strasser TI (2021) Frequency-adaptive control of a three-phase single-stage grid-connected photovoltaic system under grid voltage sags. Int J Electr Power Energy Syst 125:106416. https://doi.org/10.1016/j.ijepes.2020.106416
33. Hernández-Callejo L, Arrinda A, De la Vega D et al (2019) A comprehensive review of the impact of transmission technologies on the electrical grid. Rev Fac Ing Univ Antioquia. https://doi.org/10.17533/udea.redin.20190515
34. Camarillo-Peñaranda JR, Ramírez-Quiroz FA, González-Montoya D et al (2015) Reconfiguration of photovoltaic arrays based on genetic algorithm. Rev Fac Ing Univ Antioquia. https://doi.org/10.17533/udea.redin.n75a10
35. Diazgranados-Garzón JD, Romero-Bravo JC, Navarro-Estrada LI et al (2019) Analysis of the soiling effect on solar-panel power efficiency in the Colombian Caribbean Region. Rev Fac Ing Univ Antioquia. https://doi.org/10.17533/udea.redin.20191156
36. Merabet GH, Essaaidi M, Talei H, et al (2014) Applications of multi-agent systems in smart grids: a survey. In: 2014 international conference on multimedia computing and systems (ICMCS). IEEE, pp 1088–1094
37. Vogel-Heuser B, Seitz M, Cruz SLA et al (2020) Multi-agent systems to enable Industry 4.0. Autom 68:445–458. https://doi.org/10.1515/auto-2020-0004
38. Chhaya L, Sharma P, Kumar A, Bhagwatikar G (2018) IoT-based implementation of field area network using smart grid communication infrastructure. Smart Cities 1:176–189. https://doi.org/10.3390/smartcities1010011
39. Stankovic JA (2014) Research directions for the internet of things. IEEE Internet Things J 1:3–9. https://doi.org/10.1109/JIOT.2014.2312291
40. Yun M, Yuxin B (2010) Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid. In: 2010 international conference on advances in energy engineering (ICAEE) 2010, pp 69–72. https://doi.org/10.1109/ICAEE.2010.5557611
41. LA Cruz S, Ryashentseva D, Lüder A, Vogel-Heuser B (2019) Cyber-physical production systems architecture based on multi-agent's design pattern—comparison of selected approaches mapping four agent patterns. Int J Adv Manuf Technol 105:4005–4034. https://doi.org/10.1007/s00170-019-03800-4
42. Srivastava I, Bhat S, Singh AR (2020) Fault diagnosis, service restoration, and data loss mitigation through multi-agent system in a smart power distribution grid. Energy Sources Part A Recover Util Environ Eff 00:1–26. https://doi.org/10.1080/15567036.2020.1817190
43. Lagorse J, Paire D, Miraoui A (2010) A multi-agent system for energy management of distributed power sources. Renew Energy 35:174–182. https://doi.org/10.1016/j.renene.2009.02.029
44. Singh VP, Kishor N, Samuel P (2017) Distributed multi-agent system-based load frequency control for multi-area power system in smart grid. IEEE Trans Ind Electron 64:5151–5160. https://doi.org/10.1109/TIE.2017.2668983
45. Tom RJ, Sankaranarayanan S, Rodrigues JJPC (2020) Agent negotiation in an IoT-Fog based power distribution system for demand reduction. Sustain Energy Technol Assess 38:100653. https://doi.org/10.1016/j.seta.2020.100653
46. Rohbogner G, Fey S, Hahnel UJJ et al (2012) (2012) What the term agent stands for in the Smart Grid definition of agents and multi-agent systems from an engineer's perspective. Fed Conf Comput Sci Inf Syst FedCSIS 2012:1301–1305
47. Cruz Salazar LA, Vogel-Heuser B (2017) Comparison of agent oriented software methodologies to apply in cyber physical production systems. In: 2017 IEEE 15th international conference on industrial informatics (INDIN). IEEE, Emden, pp 65–71
48. Padgham L, Thangarajah J, Winikoff M (2005) Tool support for agent development using the prometheus methodology. Proc Int Conf Qual Softw 2005:383–388. https://doi.org/10.1109/QSIC.2005.66
49. Gil S, Salazar OM, Ovalle DA (2018) A fuzzy-based multi-agent model to control the micro-grid operation based on energy market dynamics. In: Bajo J, Corchado JM, Navarro Martínez EM et al (eds) Highlights of practical applications of agents, multi-agent systems, and complexity: The PAAMS collection. Springer, Cham, pp 299–311
50. Bellifemine F, Bergenti F, Caire G, Poggi A (2005) JADE—a java agent development framework. In: Bordini RH, Dastani M, Dix J, El Fallah SA (eds) Multi-agent programming: languages, platforms and applications. Springer, Boston, pp 125–147

Publisher's note