Internet of Smart Grid Things (IoSGT): Prototyping a Real Cloud-Edge Testbed

Hugo Santos[1], Paulo Eugênio[2], Leonardo Marques[2], Helder Oliveira[1]
Denis Rosário[1], Eduardo Nogueira[2], Augusto Neto[2], Eduardo Cerqueira[1]

[1]Federal University of Pará (UFPA) – Belém – PA – Brazil

[2]Federal University of Rio Grande do Norte (UFRN) – Natal – RN – Brazil

{hugosantos, heldermay, denis, cerqueira}@ufpa.br

{paulo.filho.071, leonardo.augusto.103}@ufrn.edu.br

eduardo.nogueira@ufrn.br, augusto@dimap.ufrn.br

Abstract. *This paper presents the Internet of Smart Grid Things (IoSGT) architecture, which is understood as an ecosystem of cutting-edge technologies that work together to enable advanced SG applications, which run at core/edge cloud datacenter premises connecting an underlying IoT networking infrastructure. The IoT-to-Edge-to-Cloud continuum paradigm that the IoSGT architecture yields aim to accelerate a plethora of Smart Grid (SG) new generation systems, which will advance current facilities at unprecedented levels. We materialized the proposed architecture in the form of a prototype atop a testbed entailing real-world technologies to lay high-accurate experiments assessments. The IoT-to-Edge-to-Cloud continuum of the IoSGT testbed extends from edge datacenter facilities running at the Federal University of Pará (UFPA), and the Federal University of Rio Grande do Norte (UFRN) premises, interconnected by RNP. An IoT-based off-the-shelf Smart Meter has been built by our group to provide a low-cost IoSGT Advanced Metering Infrastructure (AMI) use case. In addition to presenting the IoSGT architecture, our work includes prototyping and exercise on the testbed.*

1. Introduction

Smart Grid (SG) can be understood as an ecosystem of Information and Communication Technologies (ICT) that make up a disruptive approach to yield monitoring and management of electricity distribution features in real-time [Tom and Sankaranarayanan 2017]. This approach is based on the bidirectional flow of energy and information data between Intelligent Electronic Device (IED) installed in the subscriber's premises and backend systems in the power grid operator's control center [Risco et al. 2021]. In this way, an SG ecosystem allows software applications to carry out real-time telemetries on the IEDs, analyze the gathered IED data, and efficiently understand the system's behavior as a whole.

On conventional SG systems (with decades of installation), IEDs massively implement legacy protocols so that they are accessible to remote systems running in the SG operation center premises, such as the well-known Supervisory Control and Data Acquisition (SCADA) [Pliatsios et al. 2020]. SCADA are based on specific software approaches prepared for monitoring and supervising measurements that IEDs publish, in their specific

access technologies, across the SG domain. As a critical system, the power grid adopts a massively composed approach of proprietary technologies, which goes against the current trends of modern ICT for easier interaction and flexible data usage [Li et al. 2019].

Most of the SG operation center architecture relies on a centralized cloud datacenter to deal with a vast number of IEDs [Moraes et al. 2021]. With the expected high-dense number of IEDs that SG expects to realize, several concerns about scalability, data protection, agile response, and other key features that the power grid system requires to accomplish over time unavoidably, will come up. The literature proposes extending the central cloud computing features to edge facilities in an attempt to offer the hereinabove benefits [Pliatsios et al. 2020]. Currently, the cloud/edge and Internet of Things (IoT) computing paradigms stand out as key enabling technologies in the perspective of consolidating the new generation of SG systems [Modesto et al. 2021, Mota et al. 2019].

Modern datacenter network domains, which employ central cloud and edge server interplay to provide a cooperative computing approach, seek to outperform the classical centralized SG systems in several benefits (depending on the application workflow) [Moraes et al. 2021]. In IoT environments, the continuum of cloud/edge computing will pave the efficient and seamless integration of SG-specific services and applications (including third-parties solutions) across multi-vendor computing and networking converging platforms. Therefore, the local premises of edge datacenters running applications provide greater agility in monitoring and control operations, avoid security and privacy threats, and leverage the scalability and energy efficiency of the central cloud datacenter, among many other reported benefits [Modesto et al. 2021].

Indeed, the IoT-to-Edge-to-Cloud continuum increases complexity in the SG, requiring new and appropriate management tools to achieve the expected improvements fully [Pliatsios et al. 2020]. To efficiently tackle the challenges described above, related to monitoring and managing a high dense SG sub-systems across an IoT-to-Edge-to-Cloud continuum, we explored cutting-edge ICTs to design an ecosystem with a cloud-native approach denoted here as Internet of Smart Grids for IoT (IoSGT), the central contribution of this research. In the IoSGT, the ICTs work together to enable advanced SG applications running at core/edge cloud datacenter premises and interconnected through Internet networking infrastructure to offer a fully integrated environment with flexible access to IEDs. Through the IoT-to-Edge-to-Cloud continuum paradigm that the IoSGT architecture yields by principle, we foresee accelerating a plethora of SG new generation services and applications that will advance current facilities at unprecedented levels. Our proposal also aims to afford processing and storage resources for large-scale volumes of data in a cost-effective and scalable fashion for SG applications. Thus, the IoSGT aims to benefit the power energy player with several innovations within the value chain and a wide range of new business opportunities while reducing CAPItal EXpenditure (CAPEX) and OPerational EXpenditure (OPEX).

In addition to the IoSGT ecosystem, this work also contributes with a low-cost Advanced Metering Infrastruture (AMI) solution, by means of building IEDs to actuate as SG equipment. These IEDs are accessible within the IoSGT domain through the Message Queuing Telemetry Transport (MQTT) [1] protocol, the most prominent IoT communication protocol standard. Moreover, we design an experimental testbed using AMI

[1] http://mqtt.org/mqtt-specification/

based on IEDs installed at two residences (one in Belém/PA and another in Natal/RN), two at lab premises (GERCOM@UFPA and REGINA@UFRN) and one at a building premise (nPITI@UFRN). All IEDs publish their telemetries simultaneously at both edge datacenters (i.e., UFPA and UFRN) targeting two FIWARE[2] IoT plataform instances (one running at GERCOM and another at the REGINA).

The rest of this paper is organized as follows. Section 2 presents a study on the main related works in the context of this research. Section 3 describes our distributed edge-cloud IoSGT datacenters and details about our low cost AMI testbed prototype. The 4 section provides proof-of-concept results by prototyping on a real laboratory testbed. Finally, Section 5 concludes the paper and proposes future work.

2. Related Works

Enabling a flexible and secure option for communication mechanism between IEDs and the distributed edges is essential. MQTT stands out as an efficient IoT protocol due to low complexity and easy implementation [Tightiz and Yang 2020]. [Tom and Sankaranarayanan 2017] proposed an IoT-based SCADA system that afford edge-supported power distribution automation, but the placement of additional routers on the power lines is needed and Wi-Fi communication play this role without additional costs. [Risco et al. 2021] proposed a SG stability monitoring system that connects SCADA interface of the company to a central cloud. The system uses a decentralized SG control to get electricity prices and encourage users to reduce their consumption. However, residential IEDs can provide important information for electrical system providers who were not considered in the paper.

Solutions harnessing legacy SG protocols rely on gateways with off-the-shelf hardware architecture to afford connection between the power grid network backhaul and border datacenters. Most solutions are based on proprietary platforms, such as Dell Edge Gateway [Nugur et al. 2019]. Therefore, managing communication infrastructure depends on third-parties tools, which come up with concerns about privacy, acquisition costs, and higher complexity to adapt to cheaper and more flexible wireless communication protocols. The integration of SG Cloud with legacy SG protocols prevents the previous concerns of proprietary system through an IoT-to-Edge-to-Cloud [Modesto et al. 2021]. However, integrating cloud-based architectures with IEDs can further improve data storage management [Moraes et al. 2021]. IED can publish more useful information by extract more information during specific period than upload raw data to be centrally processed, which impacts scalability for tenths of thousands users.

As a critical system, the entire SG demands reliable communication along with the IoT-to-Edge-to-Cloud continuum facilities in order to assure operations with high accuracy over time. Based on the related work analysis, the IoSGT proposal advances a step ahead of the state-of-the-art by yielding data gathering to be executed at different DC premises along the edge-to-cloud continuum. The decentralized approach that IoSGT yields aims at supporting legacy and prominent IoT communication protocol (*e.g.*, the IoT widely-used MQTT), making possible multi-site deployment (*i.e.*, at edge facility, at central cloud facility, or even leveraging edge-cloud facilities interplay) as a non-unique point of service within the IoT-to-Edge-to-Cloud continuum. Moreover, the IoSGT proof of concept is based on an open prototyping (based on the FIWARE framework) with our

[2]https://www.fiware.org/about-us/

adaptable low-cost AMI real use case, which are lacking in previous works and can improve the system scalability.

3. IoSGT Prototype

This work is supported by the research and development project entitled "IoT-Cloud Systems for Centralized Energy Measurement Aimed at the Equatorial Grid", under the coordination of Federal University of Pará (UFPA), in close collaboration with Federal University of Rio Grande do Norte (UFRN). In this project, we consider the IoSGT ecosystem, which aims to provide means for controlling and monitoring IEDs with high agility and efficiency by harnessing the IoT-to-Edge-to-Cloud continuum. Specifically, IoSGT integrates these physical devices into a FIWARE-enabled domain for achieving a more flexible, monitorable, and adaptable environment to accommodate new SG services and applications without causing significant changes to the adjacent landscape.

We split the task of IoSGT prototyping into two parts: (i) the first part deals with IEDs targeting a low-cost AMI, being primarily responsible for reading energy-consuming units and transmitting respective data towards the Edge Cloud, via available Internet connectivity; and, (ii) the second part focus on the infrastructure location of edge servers (Edge Cloud), responsible for storing and aggregate data, and extract more useful information with applications. IoSGT is independent of specialized router installed in powerlines, thus avoid additional costs for supporting Wi-Fi communication. In the following, we give detailed information about these two parts.

3.1. Low-Cost AMI Solution

The AMI is a key technology enabler to pave energy efficiency, sustainability, or conscious energy use. An AMI system has the role of automatically interconnecting end users and the energy provider through a two-way communication channel. Smart metering is the classic AMI use case, which presupposes the use of smart meters IEDs that are prepared to measure electricity consumption on a regular granularity basis at the end-user premises. As far as AMI is concerned, it must comply with strict quality standards, and thus, sampling and data periodicity is significant for efficient measurement. Most smart meters IEDs available on the market do all their sampling in hardware. End users, unlike corporate consumers, require low-cost solutions for widespread adoption, which is very challenging to tackle.

We designed low-cost smart meters IEDs that leverage off-the-shelf technologies capable of gathering voltage and current signal conditioning at the electronic circuit level. To achieve this, the IED employs an ESP32 micro-controller with two 12-bit analog-to-digital converters (ADCs) divided into 18 measurement channels. We adjusted the quality of the readings performed by the ADC by the following parameters: sampling frequency, ADC clock, ADC timer, attenuation, number of cycles per sample, and samples. Accurate representation is unavoidable for reliable readings and analysis.

For this, a bench calibration was performed to represent the entire reading range for voltage and current. A varistor with voltage variation between 0 to 420 V phase by phase and a resistive circuit were used for the voltage and current reading. The voltage response was linear and satisfactory, while the current had slightly quadratic behavior at the edges and linear in the middle range. This behavior is expected due to a primary

meter, the current transformer. We made a Python script capable of generating polynomial regression to correct the readings performed.

The smart meter PCB has an electronic circuit that converts the voltage directly from the electrical network to the levels established by the microcontroller. This board has four pins for the voltage input, one for the respective analyzed phase and one for the neutral, and six other pins representing the current input, where each pair represents the input of a current transformer. The PCB project was prototyped, adequately welded, and installed in the Research and Innovation Center in Information Technology (IMD/UFRN), building parallel with another meter. Figure 1(a) shows the arrangement of the printed circuit elements.

The printed circuit board was stored in a plastic case with openings to allow connections to the electrical network. As a way of validating the readings, we installed the IED developed by us in parallel with the CW500 Power Quality Analyzer meter from the Chinese company Yokogawa. The meters are constantly connected to the mainboard due to the difficulty of reconnection. The data is stored every 20 seconds inside a microSD card, where the data is removed manually. On the other hand, the IED sends the data online so that the IoSGT platform can carry out an analysis. Figure 1(b) exemplifies the arrangement of meters in the general picture. The gauge developed by us is the orange element on the right, and CW500 is in the lower-left position.

(a) Data acquisition PCB prototype

(b) Field assembly of the meter developed in parallel with CW500

Figure 1. PCB prototype and field assembly

3.2. Edge and Cloud Data Center

Figure 2 depicts the IoSGT Testbed, which considers an architecture divided into three main layers, namely Extreme Edge, Edge Cloud Data Center (DC), and Central Cloud DC. The Extreme Edge layer is composed of IEDs (described in Section 3.1) that have the role of gathering energy-consuming information at pre-defined granularity. These IED devices embed ESP32 boards prepared to fetch voltage, current, active and reactive power, among other measures. After fetching, the IEDs transmit the data to the Edge Cloud DC destination by considering the MQTT protocol. In our testbed, we have 4 IEDs in different geographical locations, *i.e.*, two deployed at UFRN, and two deployed at UFPA. It is worth noting that the IEDs transmission lifecycle is configurable: for our experiments, we set them for sending energy data to both UFPA and UFRN Edge Cloud DC FIWARE instances.

The Edge Cloud DC layer works as a gateway and acts as a manager in each set of IEDs, intermediating data from devices to be forwarded to atop applications and IoT platforms through MQTT protocols. In our testbed, the Edge Cloud DC layer is accommodated through two Dell Edge Servers model PowerEdge R540, with Intel Xeon Octa-Core processor, 64Gb of memory, and 6TB of storage, one located at UFPA, and the other at UFRN. Both servers virtualize an Ubuntu 20.04 machine to serve as a host for the IoSGT applications.

For instance, each Edge Cloud DC layer considers the FIWARE ecosystem deployed on Docker containers, enabling greater scalability. Specifically, the FIWARE is an open-source platform that entails an extensive catalog of generic components to enable IoT environments development. The Edge Cloud DC layer makes it possible to interact with FIWARE for triggering different functions, *e.g.*, device creation, devices adding to the cloud, device data publishing, and device properties updating. FIWARE aims to make IoT development simpler, by means of driving key standards to break the information silos, transforming Big Data into knowledge, enabling data economy, and ensuring sovereignty on IoT data. In our testbed, the setup of each FIWARE environment contains six Docker containers, namely, Eclipse Mosquitto, Internet of Things Agent (IoTA), context Broker (Orion), Connector framework (Cygnus), MySQL, and MongoDB.

Eclipse Mosquitto is a free software messaging agent that implements the MQTT protocol, which is lightweight and suitable for use on all devices, from low-power computers to full servers. IoTA is responsible for publishing data from the IEDs devices to the Context Broker, which is based on Ultralight 2.0 protocol (with Advanced Message Queuing Protocol, HTTP, and MQTT transports). IoTA relies on the IoT agent's Node.js library, which was designed to be a bridge between ultralight and the Next Generation Service Interfaces (NGSI) interface of a context broker. The Orion Context Broker implements Publish/Subscribe Context Broker GE, providing an NGSI interface that allows querying context information. For instance, context information consists of entities and their attributes. The Context Broker in the application intercepts incoming messages and provides data storage and processing, thus allowing local access if there is no connection to the cloud.

Cygnus is a connector responsible for persisting contextual data sources in third-party databases and storage systems, creating a history of the context. It was built to automate and manage the flow of data between systems. Cygnus is based on Apache Flume, where Flume is a dataflow system based on the concepts of flow-based programming. Each data persistence agent within Cygnus is composed of three parts, a listener, the source responsible for receiving the data, a channel where the source places the transformed data in a Flume event, and a sink, which receives the Flume events from a channel to keep the data inside its body in a third-party store. MySQL is an open-source relational database management system (RDBMS) used to store data from IEDs persistently. On the other hand, MongoDB is an open-source and cross-platform document-oriented NoSQL database program that uses documents with JSON-like schemas to store IEDs data temporarily.

Each IED makes a publish in the broker (Orion) on each server, so the information is written to both servers simultaneously via MQTT communication protocol, following the publish/subscribe process of the broker model present in the backend FIWARE. Each server has two independent databases, MongoDB, responsible for storing the last reading

of the IEDs, overwriting the old data with the most current information, and MySql, which stores all data persistently. The Cygnus component is a Connector Framework responsible for guaranteeing the broker's integration with the databases, performing the proper storage of the information of each IED. It connects to the broker doing the subscribe process, following all the changes of elements and attributes present in Orion; upon detecting any change in the data, Cygnus immediately stores these changes in the databases.

Finally, within the IoT-to-Edge-to-Cloud continuum, the Central Cloud DC layer complements the IoSGT with a higher cloud computing level role, entailing powerful processing and storing capabilities and leveraging a broader view of the SG system as a whole. For instance, the Central Cloud DC can collaborate with the Edge Cloud DCs applications with powerful analytics and decision-making schemes, high-performance and high-accurate Artificial Intelligence training, per-IED domains predictions according to the respective Edge Cloud DCs, and others. Our prototyping employs an edge-based approach, and therefore, the Central Cloud DC instance will be used in future works and therefore is not in the scope of our current prototype.

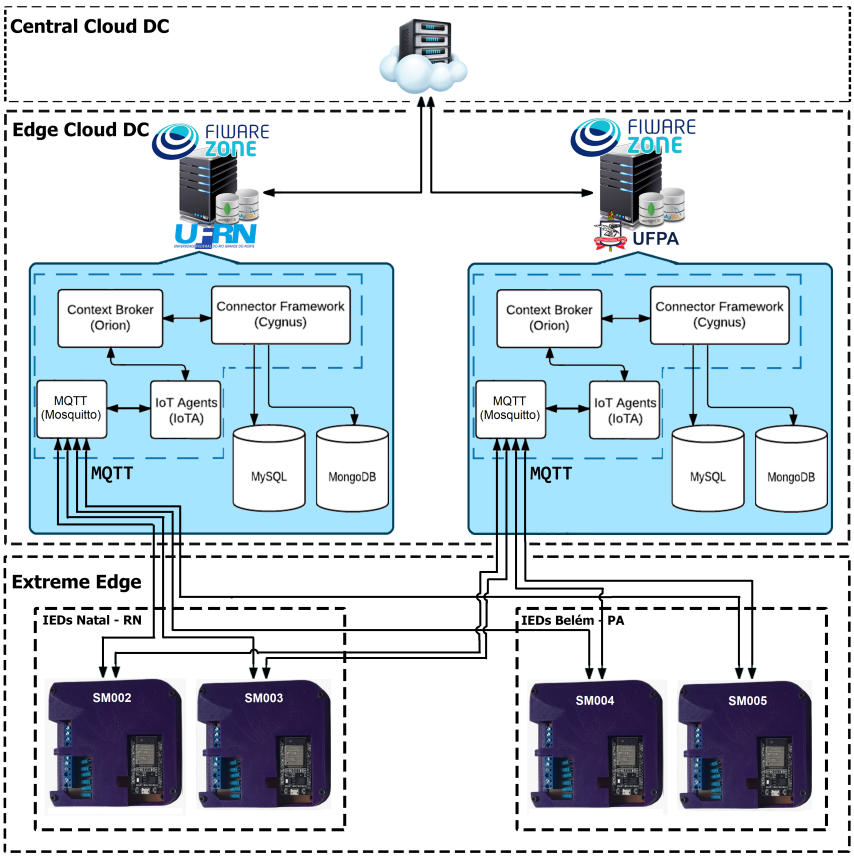


Figure 2. IoSGT testbed based on FIWARE backend in edge datacenters

4. Evaluation Results

This section introduces the results of how our IoSGT receives information in the front-end of our architecture. In addition, we introduce the results of our low-cost AMI measurements collected via our IoSGT prototype and compare the results of our AMI measurements to commercial meters.

4.1. IoT Cloud-Edge Communication

Based on the IoSGT prototype introduced in Section 3, we initially show data received from the IEDs via the MQTT protocol supporting Wi-Fi communication, which avoids additional routers installed in powerlines. We register each device and publish its data in JSON format to both Edge Clouds (UFPA and UFRN) to store data. Specifically, we identify the IEDs Smart Meter with the prefix SM and the number identifiers. Therefore, the full identifiers are SM002, SM003, SM004, and SM005. The first two are installed at UFRN and the remaining ones at UFPA. We send 26 attributes as float variables encoded in a MQTT message from IED SM002 to Eclipse Mosquitto instances of both FIWARE instances. The IoTA intermediates the context changes of the readings with Orion. Data temporarily remain on MongoDB as the last reading. Then, all different values from the last reading are written in the persistent database MySQL. Listing 1 shows the output variables and reading from a single sample written at REGINA@UFRN.

```
REGINA@UFRN
    SM002
        voltA|25.81|voltB|19.64|voltC|30.01|correnteA|-3.44|correnteB|
        -1.12|correnteC|-1.13|potenciaAtiva|0.00|potenciaReativa|0.10|
        potenciaAparente|-0.14|fatorDePotencia|-0.00|voltTHDA|460.45|v
        oltTHDB|125.64|voltTHDC|206.15|correnteTHDA|306.61|correnteTHD
        B|293.05|correnteTHDC|186.35|frequencia|340.28|anguloVoltAB|0.
        00|anguloVoltBC|98.05|anguloVoltAC|-458.05|energiaAtiva|0.065|
        energiaReativa|-2.243|energiaAparente|24.188|reservado1|164909
        7856.00|reservado2|1.00|reservado3|20.00
```

Listing 1. Attributes of MQTT message

We sent data from IEDs towards the IoSGT instances of both edges at the same time, UFPA and UFRN. Ideally, none of the samples should be lost if servers and network availability are in good condition. In this way, Figure 3 shows the collected data from four SM between March 1st and March 30th, 2022. We noted sample losses mainly because of network unavailability for short periods during the day. However, the lack of energy supply of the edge nodes side due to prolonged maintenance of energy distribution can easily cause losses of many readings of the IEDs. The network availability of the UFPA edge was slightly better and could store more data than the one at UFRN. In summary, we expected to receive 51.4 MB of data on each IoSGT instance, but UFPA had 10.2%, and UFRN had 12.8% of data loss.

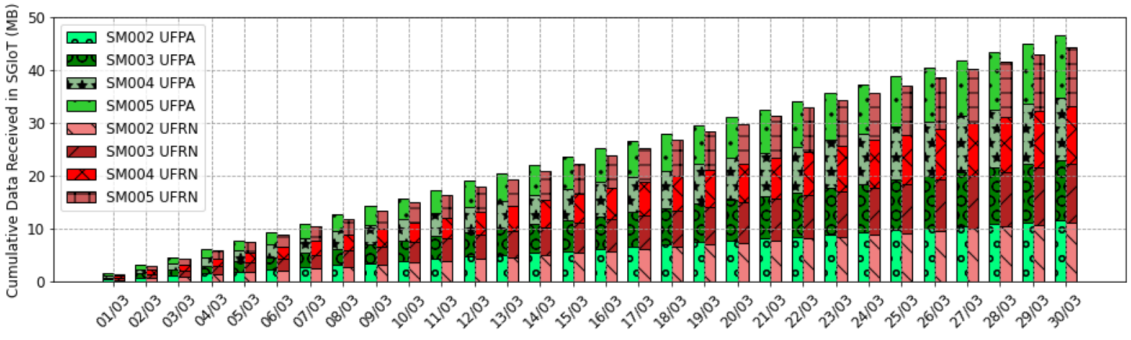


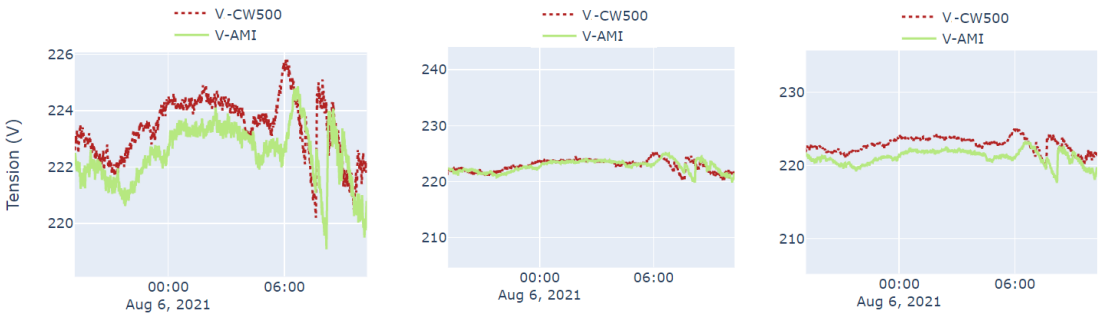
Figure 3. Cumulative Data Received in both IoSGT Edges

4.2. Low-cost AMI measurements

The IEDs take voltage-to-current readings in a three-phase system. These metrics allow the system to detect frauds and defective devices when the energy consumption profile varies beyond the usual. The methodology of the readings considered ten days with collections every 20 seconds directly in the database of our IoSGT platform. We compared the readings of the 2 meters connected in parallel for comparison with the IED developed by us. Each meter has its voltages identified as V-CW500 and V-AMI, and the currents are identified as I-CW500 and I-AMI.

Voltage values generally show smooth variations around the nominal value of 220 V. The smoothness is due to regulations in energy supply to end customers. All phases had smooth variations up to 10 V, less than 5% of the nominal values. In addition, all meters had the same dynamics compared to each other, meaning that they vary in the same order for similar stimuli, as shown in Figure 4(a).

Voltage B and C exhibit a bond order pattern with linear voltage at A, as can be confirmed in Figure 4(b) and 4(c).



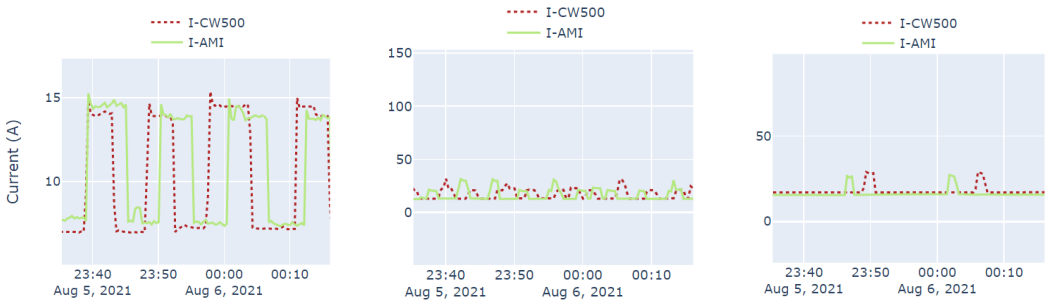
(a) Voltage A (b) Voltage B (c) Voltage C

Figure 4. Triphase voltage measurements

The current outcomes raise a more chaotic behavior when compared to voltage due to the energy load of the building. The most significant changes in current happen to load switching, mainly due to air conditioners with constant on-off cycles to stabilize room temperature. The current measurement results have similar values between meters. Figures 5(a), 5(b) and 5(c) show several moments of overlay between the measurements of all three meters.

5. Conclusion

This paper proposed an IoT solution capable of reading and monitoring SG safely and efficiently using the lightweight IoT protocol MQTT. We obtained real-time data from IEDs into two Edge-Cloud infrastructures with a low-cost smart meter. The meter costs around $60, while the CW500, used in the comparison, has a market value of around $7150. The proposed meter has a value of about 0.85% of the commercial one, though . The measurements of our developed smart meter had a similar reading to commercial ones in terms of linearity for both voltages and current. In the future, we aim to integrate the sensors reading and our FIWARE deployment with Artificial Intelligence (AI) techniques to detect and react to power consumption anomalies. Moreover, we aim to avoid data loss due to Edge-cloud unavailability synchronizing both FIWARE databases.



(a) Current A (b) Current B (c) Current C

Figure 5. Triphase current measurements

Acknowledgments

This study was financed by the R&D project entitled "Sistema IoT-Cloud de Medição Centralizada de Energia Voltado a Rede CEA - 001/2021", and in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Finance Code 001.

References

Li, Y., Kang, Z., Wang, Y., and Shi, Z. (2019). A study on development and evolution of the intelligent power grid information communication architecture. In *Journal of Physics: Conference Series*, volume 1345, page 052047. IOP Publishing.

Modesto, W., Neto, A. V., Rosário, D., and Cerqueira, E. (2021). Sg2iot - uma arquitetura para integracao de dispositivos eletricos inteligentes de abordagem legada em sistemas smart grid baseados na iot. In *Anais do XIII Simposio Brasileiro de Computacao Ubiqua e Pervasiva*, pages 31–40, Porto Alegre, RS, Brasil. SBC.

Moraes, J. et al. (2021). Implementação de um cluster kubernetes com a plataforma dojot para aplicações de internet das coisas. In *Anais do XLVIII Seminário Integrado de Software e Hardware*, pages 1–8. SBC.

Mota, R., Riker, A., and Rosário, D. (2019). Adjusting group communication in dense internet of things networks with heterogeneous energy sources. In *11th Brazilian Symposium on Ubiquitous and Pervasive Computing (SBCUP)*. SBC.

Nugur, A., Pipattanasomporn, M., Kuzlu, M., and Rahman, S. (2019). Design and development of an iot gateway for smart building applications. *IEEE Internet of Things Journal*.

Pliatsios, D. et al. (2020). A survey on scada systems: secure protocols, incidents, threats and tactics. *IEEE Communications Surveys & Tutorials*.

Risco, A. B. et al. (2021). Iot-based scada system for smart grid stability monitoring using machine learning algorithms. In *2021 IEEE XXVIII International Conference on Electronics, Electrical Engineering and Computing (INTERCON)*, pages 1–4. IEEE.

Tightiz, L. and Yang, H. (2020). A comprehensive review on iot protocols' features in smart grid communication. *Energies*, 13(11):2762.

Tom, R. J. and Sankaranarayanan, S. (2017). Iot based scada integrated with fog for power distribution automation. In *2017 12th Iberian Conference on Information Systems and Technologies (CISTI)*, pages 1–4. IEEE.