Sustainable Energy, Grids and Networks 40 (2024) 101507

Contents lists available at ScienceDirect

Sustainable Energy, Grids and Networks

journal homepage: www.elsevier.com/locate/segan

Comprehensive analysis of smart grids functionalities virtualization

Laura Lázaro-Elorriaga [a,*], David Guerra [b], Imanol García-Pastor [c], Cristina Martínez [d], Eutimio Sanchez [a], Eugenio Perea [a]

[a] Tecnalia Research and Innovation, Derio, Biscay, Spain
[b] University of the Basque Country (UPV/EHU), Bilbao, Biscay, Spain
[c] Igeteam, Zamudio, Biscay, Spain
[d] ZIV Automation, Zamudio, Biscay, Spain

A R T I C L E I N F O

Keywords:
Virtualization
Smart grid
Containerization
IED
Primary substation
Secondary substations

A B S T R A C T

The implementation of advanced digital technologies in the conventional electric grid has triggered a transformation towards an intelligent network, known as Smart Grid. The associated benefits are diverse, ranging from more efficient energy management and demand response to the distributed integration of renewable energy sources. Ultimately, this transition promotes a more reliable, sustainable, and cost-effective energy supply. In this context, there is increasing recognition of the advantages of employing intelligent at edge to provide redundancy, virtualize functions that were previously in different proprietary hardware in the same device, or introduce new functionalities into the electric grid. This study focuses on conducting a comprehensive analysis on the key aspects to consider when implementing virtualized solutions in substations. Strategies have been sought to ensure the optimal deployment of virtualized nodes within the electrical sector, taking into account factors such as functional requirements, facility types, virtualization methodologies, and node specifications, among others. Furthermore, throughout the study, several virtualization tools have been analysed to determine their feasibility and the advantages they offer when integrated into the Smart Grid.

1. Introduction

The Smart Grid (SG) is an advanced electrical power network designed to enhance economic efficiency and promote sustainability in the power system. Its core objective is to seamlessly synchronize the functions of power generators, transmission lines, distribution utilities, and consumers. Key aims encompass curbing distribution losses, elevating the calibre and dependability of power provision, all while prioritizing the utmost safety and security of equipment and workers [1]. To accomplish these objectives, the digitization of the electricity grid stands as imperative, given the escalating demand for energy, the assimilation of intermittent renewable energy sources, and the imperative to refine operational efficiency. Moreover, digitalization is also necessary to ensure network reliability and security in an increasingly interconnected and technology-dependent environment.

The digitalization in the SG originated in the measuring, protection, and control equipment which evolved into Intelligent Electronic Devices (IEDs). Nowadays, the global trend of digitizing key facilities in the electrical grid means that both, secondary substations and primary substations, are in the spotlight for transformation. These nodes were originally designed for centralized generation and lack the automation and data analysis needed for intelligent distribution networks. Consequently, they have become bottlenecks for the integration of renewable energies and SG new functionalities.

Considering this issue, the increasing capacity of hardware platforms drives a significant trend in the digitization process, leading to the integration of functions that culminates in the concept of function virtualization. Virtualization in the SG, first introduced in [2], enables the

Abbreviations: SG, Smart Grid; IED, Intelligent Electronic Device; RT, Real Time; MV, Medium Voltage; LV, Low Voltage; RMU, Ring Main Units; LD, Logical Device; LN, Logical Node; MGMT, Management; MU, Merging Unit; SCADA, Supervisory Control and Data Acquisition; HMI, Human-Machine Interface; I/O, Input/Output; Comm., Communications; Tx, Transmission; RTU, Remote Terminal Unit; OLTC, On-Load Tap Changer; PMU, Phasor Measurement Unit; IT, Information Technology; OT, Operational Technology; VM, Virtual Machine; VPAC, Virtual Protection, Automation, and Control; CRI, Container Runtime Interface; SV, Sample Values; SDN, Software-Defined Networking; IPC, Inter-Process Communication; NCIT, Non-Conventional Instrument Transformers; NCC, Network Control Centres; NAT, Network Address Translation; AWS, Amazon Web Services; GCP, Google Cloud Platform.

* Correspondence to: Astondo Bidea, Edificio 700, Derio, Biscay 48160, Spain.
E-mail address: laura.lazaro@tecnalia.com (L. Lázaro-Elorriaga).

https://doi.org/10.1016/j.segan.2024.101507
Received 16 April 2024; Received in revised form 8 August 2024; Accepted 12 August 2024
Available online 15 August 2024
2352-4677/© 2024 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

transition from IEDs with specific functionality associated with hardware to a philosophy based on a powerful standard hardware platform and software module. This transformation results in a remarkable increase in interconnectivity and data exchanges, coupled with the consolidation of functions onto a considerably reduced number of devices. Indeed, implementing virtualized installations can lead to a reduction of 50 % or more in the number of hardware devices and a decrease of 76 % in operational and maintenance costs, as evidenced in [3]. This is primarily due to the enhanced potential for remote management. Moreover, virtualized solutions also promote scalability by distributing storage and data processing across multiple points, while allowing for the integration of new management, control, or monitoring algorithms. Furthermore, it enables real-time (RT) responses for certain algorithms, as data is processed on the same device (or very close) where it is generated, leading to reduced latency and faster response times [4].

However, given the high responsibility for the reliability of the electrical grid's operation, the electrical sector has always been very conservative when it comes to implementing changes to evolve towards a more digitalized and virtualized grid [5]. Even though, distribution network management is becoming more dynamic than ever, with a multitude of third-party tools developed, along with the need to respond to the increasing integration of distributed energy sources. So, utilities and energy companies view standardization as a necessary strategy to achieve efficient management of electrical networks. That is why they are beginning to see significant benefits in solutions that make use of virtualization as it allows them to decouple hardware from firmware, facilitating the integration of firmware from different manufacturers [6]. Indeed, the substation virtualization represents a significant stride toward achieving a more reliable, secure operating environment and is expected to continue evolving in the coming years, driven by key trends such as data aggregation, edge analytics, and the deployment of deep learning technology to optimize control algorithms [7].

Moreover, as the electrical grid becomes increasingly digitized and substations are virtualized, there emerges an opportunity to capitalize on the benefits offered by cloud and edge computing. Through the integration of these technologies with substation virtualization, electric companies can exploit the scalability and computational prowess of the cloud. This enables them to conduct extensive and prolonged optimization of control algorithms and accurately predict energy demand. Concurrently, edge computing facilitates swift and RT responses for critical tasks with stringent latency requirements, such as equipment monitoring and fault detection. Additionally, it aids in alleviating the workload on the cloud infrastructure.

The aim of this article is to explore the challenges and opportunities associated with the virtualization of critical infrastructures in the SG and to provide a guide for the effective implementation of virtualization solutions in this context. The main contributions of the study include the identification of the service requirements of the critical infrastructures in the SG that must be considered during virtualization. Based on these requirements, virtualizable elements associated with specific hardware resources have been identified. Additionally, an analysis of non-functional requirements has been conducted, with a particular focus on scalability models to forecast future needs. Finally, an evaluation of virtualization alternatives applicable to the SG has been carried out, which includes discussing appropriate architectures for specific applications within the SG.

The paper is organised in several sections. First, the paper identifies SG operational requirements and challenges that must be met and solved by virtualized functionalities, as detailed in Sections II, III, and IV. Second, it is necessary to compile a compendium of functionalities in the primary substations and secondary substations that can be virtualized, and associating them, with specific hardware resources, as described in Section V. Furthermore, a comparative analysis of scalability models is carried out in Section VI to allocate the necessary resources and anticipate future needs. Section VII compares the various virtualization alternatives and details the communication scenarios they pose. Finally, in Section VIII, the discussion of the most suitable virtualization architecture for the various SG applications is presented once all necessary elements have been described. The article concludes with the conclusions presented in Section IX. To provide proper context before starting the analysis, an introductory section is included.

2. Critical infrastructures for the SG

Understanding the functionalities and requirements of the key components within electrical installations is essential for implementing virtualization solutions and distributed systems. In the following section, an overview will be provided, offering insights into the roles, functions, and evolving technologies within secondary substations and primary substations. This will highlight the importance of virtualization in modernizing these critical components of the electrical system.

2.1. Secondary substations

The secondary substation is the point of connection between the central systems of the distribution company and smart meters, being the closest point of interaction with the customer. By definition, it is a facility that comprises one or more transformers, medium voltage (MV) and low voltage (LV) switchgear, connections, and auxiliary equipment to supply LV power from a high/medium voltage network. Within each secondary substation, there are sets of MV cells, also referred to as Ring Main Units (RMUs), which manage line input and output, providing power and protection for the distribution transformer that steps down voltage from MV to LV [5].

The introduction of the SGs into the LV/MV distribution network and in the secondary substations, requires additional functions to the existing infrastructure. Therefore, converting a conventional secondary substation into a digital one, involves installing new devices that integrate measurement systems and components to collect readings and data from LV/MV network elements. These devices then package the data and transmit it to network monitoring and operation systems. The overarching goals for digital secondary substation include implementing advanced telematics systems for customer metering, fault localization, monitoring LV networks for compliance and quality, detecting phase imbalances, identifying losses and fraud, optimizing existing installations through advanced monitoring, automating network processes, and enhancing facility management to improve operational efficiency and customer information within the modern electrical grid [5,8].

The main reason to consider the virtualization of secondary substation focuses on the need to accelerate the development of a standards-based, open, interoperable, and secure architecture to address the technical and business challenges faced by utility companies worldwide. Additionally, it addresses the issue of physical space constraints in some facilities and optimizes memory and CPU usage, enabling the deployment of new applications in this environment where communication may also be limited.

2.2. Primary substations

Primary substations are crucial nodes within electrical networks tasked with efficiently regulating the flow of energy in the grid. To achieve this, they act as connection points in the electrical system, modifying parameters such as voltage, frequency, phase number, or circuit connections to facilitate the transmission and distribution of energy. The equipment present at these points includes primary elements (transformers, switches, etc.) and secondary elements (protection relays, synchronizing relays, breaker protection, etc.). The secondary equipment is particularly crucial as it is dedicated to safeguarding and monitoring the operations of the primary equipment, ensuring the reliability and stability of the overall electrical system [9].

To adapt to the emerging needs of the SG, current primary substations must undergo modernization and transformation into digital primary substations. These digital primary substations play a crucial role in facilitating seamless coordination between substations, acquiring RT operational data, supporting RT control, detecting device interactions, and managing assets effectively. To achieve this, the primary focus of the digital primary substation is the digitization of communications, information management through optical fibre data networks, and the development of detailed engineering and telecontrol under the automation IEC 61850 standard [10]. This approach ensures interoperability across diverse electrical equipment and control systems, ultimately leading to enhanced operational efficiency [11].

Similarly to the secondary substations, virtualization constitutes a key innovation to consolidate the trend towards hardware integration into a virtualized platform in the primary substations. This implies that secondary elements, among which IEDs stand out, have the capability to virtualize the processing and communication functions previously managed by conventional secondary equipment [12]. In this scenario, it is worth noting the IEC 61850 device model shown in Fig. 1, where the physical device is the one that connects to the network, within which, there may be one or more logical devices (LDs). The IEC 61850 LD model allows a single physical device to act as a proxy or gateway for multiple devices, thus providing a standard representation of a data concentrator. Each LD contains one or more logical nodes (LNs). A LN is a named group of data and associated services which represent a real physical device and its functionality and are susceptible to virtualization [13].

3. Use cases for modernizing the electrical grid with virtualization

The distribution of electrical energy is evolving rapidly to adapt to a constantly changing environment, driven by the introduction of novel technologies and the necessity to implement advanced functionalities. These functionalities aim not only to improve operational efficiency but also to meet the changing demands of society and the electrical sector. Among the potential functionalities that would be integrated to effectively manage the electrical grid are [8]:

- Distributed Generation: Integration of small-scale renewable energy sources and management of locally generated energy, such as solar panels and wind turbines.
- Distributed Loads: Integration of electric vehicles and electric heat pumps, with intelligent load management to optimize energy consumption.
- Distributed Storage: Implementation of microgrids and energy storage systems at the local level to enhance grid stability and facilitate demand management.

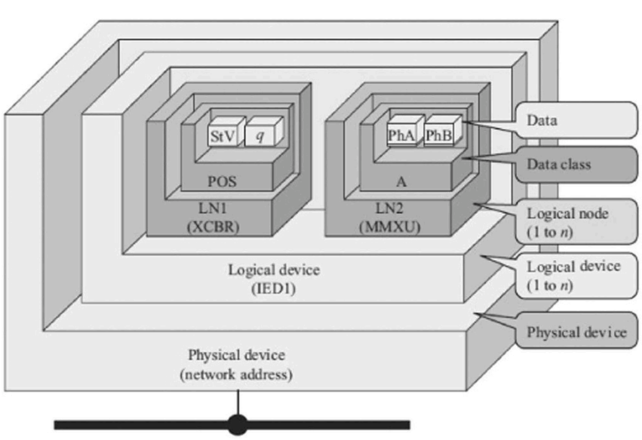

Fig. 1. Containment hierarchy of the IEC 61850 device model [14].

- Distributed Flexibility Mechanisms: Utilization of tools to manage flexibility in energy generation and consumption, enabling active participation of consumers in energy management.

These new functionalities require distributed processing to enable agile and RT responses to events in the electrical grid, thereby offering significant improvements in areas such predictive maintenance, operation, and the quality of electrical supply.

To address the challenges in managing and scaling the electrical grid, a dynamic and non-rigid solution is proposed using virtualization. Virtualization facilitates grid management, scalability and maintainability. Additionally, the application of virtualization in the SG has the potential to significantly improve the efficiency and management of the electrical grid by enabling the integration of new functionalities and redundancy mechanisms. Below are listed some of the SG related use cases, which can greatly benefit from virtualization to ensure an efficient and adaptable response to the needs of the modern electrical system [8]:

- Asset Management: Creating new functionalities to inventory assets and track their usage, which helps in detecting deterioration risks and forecasting incidents.
- Network Monitoring: Creating virtual control panels that display the status of the RT network, allowing for anomaly detection and alarm generation.
- Electrical Grid Prediction: Creating virtual models of electrical grids where the behaviour of the network can be predicted, and unmeasurable parameters adjusted.
- Network Analytics: Analysing large amounts of stored historical data, contributing to the optimization of bandwidth and processing capacity.
- Network Control: Enabling autonomous operation of operating elements. Additionally, it allows for simulation and testing of control actions on the electrical grid before implementation in the real environment, minimizing risks.
- Energy Management - Flexibility: Managing network capacity and interacting with active consumers, storage points, and distributed generators, facilitating the design of energy-efficient systems. It also enables the creation of simulations for network operations and maintenance, providing a secure environment for staff training and procedure testing.
- Cybersecurity and Security/Sustainability: Creating isolated and secure environments that meet the cybersecurity criteria of the SG. Additionally, new functionalities can be added such as evaluating system status, detecting anomalies in application execution, excessive consumption, and functionalities for controlling physical and environmental security, such as leaks or fires.

Furthermore, entire components and systems of the SG can also be digitally replicated through digital twins. By creating virtual replicas of physical infrastructures, digital twins enable RT monitoring, analysis, and optimization of network performance, facilitating early fault detection, predictive maintenance planning, and operational improvements [15].

4. Analysis of critical virtualization requirements for the SG

The application of virtualization in secondary substations and primary substations will enable a more efficient utilization of processing power, resulting in cost savings by reducing the amount of hardware used. However, virtualization is primarily constrained by the necessity to adhere to the requirements imposed by the reference standard of the SG, the IEC 61850. In this section, critical virtualization requirements for their application in substations and in the SG will be examined, addressing both general considerations and specific criteria for substation environments.

The overarching requirements for virtualization in SGs encompass [16,17]:

- Efficient management of bidirectional transmission of electricity and information to establish an automated and distributed network.
- RT capability for near-instantaneous balance between supply and demand management.
- Time synchronization and low latency for RT communications, enabling efficient data acquisition and rapid fault detection and correction.
- Robust fault detection, communication, and control capabilities to swiftly address deviations, prioritizing system security against various threats including deliberate attacks, espionage, user errors, equipment failures, and natural disasters, to ensure reliability and integrity in critical electrical environments. Additionally, the system should be able to monitor its own state and generate alerts for abnormal situations.
- Scalability to accommodate new users, deliver necessary information, and facilitate end-user interaction with RT monitoring.
- Quality of service for network and communication technologies throughout the grid.
- System availability and uninterrupted functionality, ensuring data is always available and accessible without delays, even in the event of failures or interruptions.
- Adequate bandwidth availability for managing a growing number of simultaneous messages.
- Interoperability among SG devices and systems to create conceptual models, reference architectures, and establish protocols and standards for information management.
- Efficient processing and analysis of large volumes of data, integrating different functions for predictive and operational analysis.
- Implementation of distributed storage systems that distribute data across multiple nodes to improve performance and availability, maximizing system performance and capacity.
- Technological uniformity through the adoption of an architecture based on open and interoperable standards, ensuring compatibility and flexibility.
- Modular and scalable software architecture based on independent services and communication through standard interfaces.

In addition to the general requirements, specific criteria are established for both secondary and primary substations. On the one hand, a key requirement for developing solutions for secondary substation is the isolation between the MV and LV networks, ensuring the safety and integrity of the electrical system by preventing the unwanted transfer of electric current between networks of different voltages. On the other hand, the most critical aspect for primary substation is latency, as some types of communication exchanges between the elements of the primary substation are only useful within a limited time frame. In terms of latency requirements, both IEEE 1646 [18] and IEC 61850 [19] standards define regulations related to the automation of electrical substations. While IEEE 1645 is a more general standard that addresses asset management and electrical energy systems in general, IEC 61850 specifically focuses on the automation of electrical substations, defining communication protocols and data models for this purpose.

Moreover, Table 1 and Table 2 specify industrial requirements that must be guaranteed in the secondary and primary substations for successful deployment of the use cases listed in the previous chapter. These indicative values are obtained from current physical equipment with similar functionality, provided by a member of the project consortium under the VIRTGRID project supported by the Basque Government. Similar values are known in other manufactures.

For secondary substations, as shown in Table 1, the most important functions to virtualize are those related to the automation and monitoring of the MV and LV network, voltage regulation, remote equipment management (MGMT), equipment MGMT, and other general services. These functions involve various requirements such as sensor inputs/outputs (I/O), signal processing needs, latency requirements, RAM memory, non-volatile memory, CPU, availability, communication interfaces, data transmission volumes, and redundancy. For example, automation and monitoring of the MV network requires 500 MB of RAM, a CPU with 1000 MHz, and 100 % availability, indicating high performance and reliability needs.

In primary substations, as indicated in Table 2, requirements are classified under the following functionality groups: analog/digital Merging Units (MUs), protection algorithms, the Supervisory Control and Data Acquisition (SCADA) Human-Machine Interface (HMI) or gateway, asset monitoring, service measurement/quality, and other general services. These functions are essential for the proper operation of each type of substation and, therefore, are prioritized for virtualization. For instance, protection algorithms require a CPU with 1000 MHz, 500 MB of RAM, and must adhere to IEC 61850 & IEEE 1646 standards for latency, highlighting the critical nature of these operations.

These tables provide a detailed breakdown of each requirement, ensuring that all aspects necessary for effective virtualization are considered. The values are crucial for guiding the definition of elements susceptible to virtualization in substations, enabling the infrastructure to adapt and grow with network changes. The inclusion of these specific values helps to ensure that the virtualized environment meets the high standards required for performance, reliability, and scalability in both secondary and primary substation settings.

5. Virtualizable elements in the SG

Based on the requirements mentioned previously, the elements, applications, and software nodes within secondary and primary substations that are susceptible to virtualization have been analysed for this

Table 1
Industrial requirements for secondary substations use cases functionalities deployment.

Specific Requirements	Auto. & Monitorization MV	Auto. & Monitorization LV	Voltage Regulation	Remote MGMT	Equipment MGMT	Other General Services
Sensors I/O	Analog channels + I/O	Analog channels + I/O	Analog channels + I/O	-	-	-
Signal Processing	YES	YES	YES	NO	NO	NO
Latency Requirements	ms	ms	s	mins	h	s
RAM Memory	500 MB	1 GB	500 MB	2 GB	-	-
Non-Volatile Memory	128 kB	2 GB	128 kB	8 GB	-	-
CPU	1000 MHz	1000 MHz	1000 MHz	1200 MHz	-	-
Availability	100 %	95 %	95 %	98 %	100 %	50 %
Comm. Interfaces	Control Systems Other IEDs (MOD-BUS)	Control Systems	Control Systems	HES PLC (Accountants)	HES	HES
Data Tx Volumes	-	5 MB /day + oscilos (20 KB/fault)	-	-	-	-
Redundancy	NO	NO	NO	NO	NO	NO

Table 2
Industrial requirements for primary substations use cases functionalities deployment.

Specific Requirements	Analog/Digital MUs	Protection Algorithms	SCADA HMI or Gateway	Asset Monitoring	Service Measurement/ Quality Systems	Other General Services
Sensors I/O	Sensors and digital I/O	Analog inputs and digital I/O	No	Receive data from the MUs through GOOSE	Analog inputs and digital I/O	NO
Signal Processing	YES	YES	NO	NO	YES	NO
Latency Requirements	IEC 61850 & IEEE 1646	IEC 61850 & IEEE 1646	IEC 61850 & IEEE 1646	IEC 61850 & IEEE 1646	IEC 61850 & IEEE 1646	IEC 61850 & IEEE 1646
RAM Memory	500 MB	500 MB	256 MB	1 GB	1 MB	-
Non-Volatile Memory	128 kB	128 kB	1 GB	2 GB	32 MB	-
CPU	1000 MHz	1000 MHz	1000 MHz	1000 MHz	500 MHz	-
Availability	100 %	100 %	100 %	90 %	90 %	50 %
Comm. Interfaces	Ethernet/FO	Ethernet/FO	IRIG-B Ethernet Ports	Ethernet/FO	Ethernet	Ethernet
Data Tx Volumes	100 Mbits/s - 1 Gbits/s	100 Mbits/s −1 Gbits/s	-	-	-	-
Redundancy	HSR/PRP	HSR/PRP	HSR/PRP	NO	Yes, at border point	NO

section.

The elements and functionalities suitable for virtualization in secondary and primary substations are [17]:

- Consolidation of functionalities from different LN of IEC 61850 into one or multiple virtualized nodes.
- Protocol translation: Transition to digitalization in facilities with communications based on protocols prior to IEC 61850.
- IEC 61850 protocol functions: such as load shedding to provide a systematic reduction of electrical load to prevent grid instability during critical situations, and thermal scanning of applications to monitor and assess the temperature of critical assets in RT.
- Algorithms for mapping meter-line and phase, fault detection algorithms in LV for secondary substations (using data from meters and supervisors), energy balance and loss detection algorithms, or monitoring algorithms for central elements, power supply systems, surveillance systems, etc.
- Data Storage and Alarm/Event Management: Creation of centralized databases for historical data storage, facilitating efficient analysis and decision-making, as well as managing notification functions and handling alarms and events generated by data processing.
- Graphic interface and visualization: IED graphic interfaces to provide a user-friendly HMI or console interface function, enabling easier access to information.
- Cybersecurity: Incorporating firewall, anomaly detection, fault detection, and cybersecurity functions for enhanced security. Additionally, effective credential management is essential to ensure the secure handling and authentication of user credentials and certificates.
- Fault detection and communication to the control centre. Control and signalling for the automatic isolation of faulty sections; switch opening and closing control.

In addition to these, the elements that can be found in the secondary substations and are suitable for virtualization are as follows:

- Data Concentrator for LV: Implemented by an IED with Remote Terminal Unit (RTU) functions, it collects current, voltage, energy, and power values for each phase of each secondary substation line.
- Network parameter monitoring for MV: Traditionally implemented through an RTU or IED, based on voltage and current measurements. This RTU or IED also incorporates signal conditioning, traditionally performed by MUs, and detection and communication to the control centre in case of faults.
- LV Monitoring and Advanced LV Monitoring: Information storage and transmission to remote management system, obtaining service quality values along with fault detection.
- On-Load Tap Changer (OLTC) for transformers: Activation of the monitored command for remote operation of the load regulator.

Similarly, in the primary substations, there is another set of elements and functions that are suitable for virtualization:

- Monitoring devices and equipment in RT.
- Equipment Control and Supervision: Involves the control and management the operation of electrical equipment, such as switchgear, transformers, and protection systems, from a centralized location. It includes tasks like equipment control, gathering data for network monitoring, maintenance, generating alarms, and executing automated protection actions. Traditionally, this function has been carried out using RTUs, or more recently, IEDs communicating with SCADA systems.
- Power Quality Analysis: Management and control of equipment to automatically adjust power factor based on network requirements.
- Phasor Measurement Unit (PMU) applications: leveraging RT synchronized measurements for wide-area monitoring, event analysis, and enhanced decision support.

6. Scalability models

When virtualizing, it is important to manage resources in a way that ensures the system's available capacity meets the requirements of all deployed applications. Therefore, special attention must be paid to available resources, considering not only the elements to be controlled but also the associated applications. Furthermore, when deploying virtualized nodes, the capability to allocate additional resources or nodes to the ecosystem should be carefully deliberated, especially as the network expands. This consideration ensures scalability and adaptability to accommodate growing demands and maintain optimal performance as the network scales. Therefore, both horizontal and vertical scalability strategies need to be thoroughly evaluated (See Fig. 2). Understanding horizontal scalability as the ability to increase the number of instances or servers, so that more computing, storage, or network resources are added to distribute the load among them without changing the individual capacity of each one. Vertical scalability is understood as the ability to increase the resources of an existing server, such as processing power, RAM, or storage, to handle growing workloads without the need to add more server.

It is crucial to recognize that the complexity and temporal demands of applications operating in virtualized environments might require adjustments in memory, processing time, or priority. A decrease in performance in a virtualized platform in Information Technology (IT) or in certain non-critical applications in Operational Technology (OT) may not be significant. However, increasing the number of critical

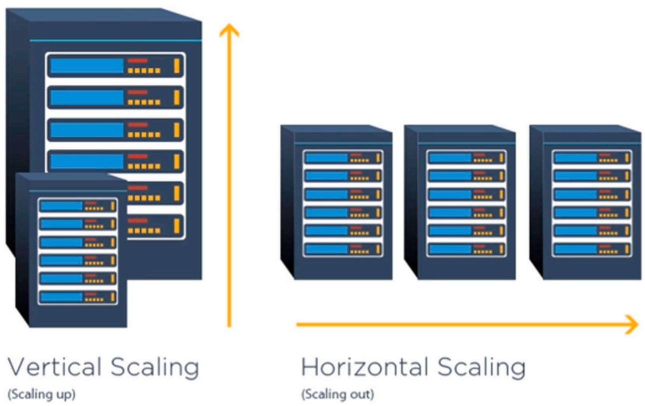

Fig. 2. Vertical Scaling vs. Horizontal Scaling [20].

applications with RT requirements, may result in a decline in performance potentially rendering them incapable of meeting specific demands. Furthermore, it will also be necessary to consider the number of LN modelled on the same physical device, as an increase in LN implies a higher overhead when virtualizing. On one hand, the available resources for each LN decrease, and on the other hand, the virtualization layer incurs overhead in managing the virtualized environment. As a result, prioritizing virtualized applications based on their criticality and considering the optimal number of virtualized LNs becomes indispensable to prevent resource consumption from adversely affecting the overall system performance.

As one of the scenarios to consider, due to the specified time requirements outlined in the IEC 61850 standard, it could be advisable to deploy containers with RT requirements, as virtualized protection, control and monitoring responsible IEDs, on dedicated nodes. These nodes could potentially be equipped with specialized hardware to effectively run RT applications. It is important to note that no additional RT applications can be introduced to a node if resource allocation would lead to temporal non-compliance for existing applications. Therefore, introducing a new RT application might require setting up a new node if it affects virtualization solutions response times. For this approach, a scalability model based on modularity is needed, adding more equipment to increase system power, that is, with a horizontal scalability model. In contrast, deploying containers without RT requirements, such as a data concentrator for LV, will be simpler, involving monitoring node occupancy and potentially leveraging vertical scalability where resources are added or adjusted within a single node to meet increasing demands. Taking this into account, there will be different ways to address scalability depending on the type and complexity of the substations.

6.1. *Secondary substations*

In a substation, the equipment and virtualized functionalities primarily depend on the properties and size of the substation. According to priority and security needs, data information sources can be categorized into two distinct zones: the control and operation division, and the data and management division. In the control and operation division, automation tasks with the highest priority and monitoring services are situated. These encompass RT applications requiring stringent latency and data transmission reliability. Conversely, the data and management division, while not as sensitive to latency, demands greater bandwidth and storage capacity.

In most cases, the secondary substation can be easily dimensioned due to the limited number of transformers and lines. Although it is foreseen that data and management RT capabilities may exist in the future, when active demand management mechanisms are incorporated, currently, all remote monitoring and billing processes do not require RT capabilities. Hence, considering the number of available cores in current machines, scalability appears non-critical, leading to the conclusion that vertical scalability is the most appropriate for secondary substations. Nevertheless, when dealing with numerous RT applications, the optimal approach would be to employ independent nodes, indicating a preference for horizontal scalability.

However, it is important to consider that vertical scalability comes with certain drawbacks. Investing in high-performance hardware can notably inflate costs, and timelines may be prolonged as certain components require time to significantly improve in power. This can affect both, expenses, and temporal planning. Additionally, vertical scalability presents the risk that if a node fails, it could lead to the suspension of all applications on that node, underscoring the need for security or redundancy mechanisms.

6.2. *Primary substations*

The main different between secondary and primary substations is that the primary substations protection, automation, and control systems process a large volume of data that is crucial for the operation of the system and requires ubiquitous, reliable, and RT communication [21]. Therefore, primary substations must be prepared to handle fast data flows from measurements in a scalable way, addressing deployments in an environment where changes occur unpredictably.

In this case, it will be necessary to improve the system's overall performance, which requires implementing a scalability model focused on the modularity of the system's functions. In this scenario, adopting horizontal scalability facilitates a gradual implementation of virtualization, as more equipment is added to provide more power to the system.

This solution involves robust interoperability at the software development level, encompassing considerations related to architecture and APIs, leading to elevated maintenance levels, and require extra efforts in standardization. Additionally, despite the initial absence of growth limitations in horizontal scalability, its effective implementation demands more extensive design and implementation efforts.

In addition to scalability, virtualization brings other non-functional requirements that must also be considered. On the one hand, it is a technology that promotes efficiency in resource usage, leading to cost reduction. By running multiple virtual machines (VMs) or containers on a single device, space and electrical energy are optimized, among other factors. Furthermore, it offers greater flexibility in interacting with hardware resources, allowing for quick reconfiguration based on changing network needs. This is particularly useful in a SG context due to fluctuations in energy demand, infrastructure changes, and the need to integrate new technologies.

On the other hand, virtualization also contributes to improving the maintainability of the electrical grid, as it allows the SG to be modified, updated, and repaired more efficiently. This is achieved by the ability to replace components without affecting the overall operation of the system.

7. Virtualization strategies in the SG

As described in [22], the natural progression to virtualization in substations involves transitioning from a digital substation, migrating from the original (physical) IEC 61850 structure towards a virtual infrastructure. In this new scenario, the techniques, mechanisms, and technologies of virtualization allow for the implementation of software applications to replace elements traditionally implemented in proprietary and closed systems using a fraction of the available hardware platform resources, thus isolating the applications from each other. However, it is necessary to consider that this change in hardware devices entails an economic cost for companies that must be evaluated based on the potential benefits in terms of flexibility, scalability, and operational efficiency that virtualization can provide.

The introduction of virtualization and cloud technologies as fundamental components of the infrastructure supporting electrical automation systems was initially proposed by Ferreira et al. in 2013 [2], and since then, numerous studies have been conducted to explore and advance the virtualization of SG. In Ferreira et al. subsequent work in 2017 [23], they proposed a physical to virtual solution for a particular application case involving substation automatic voltage control systems with the aim of replicating the functionality of traditional IEDs in virtualized environments. The paper not only discussed fundamental concepts of IEC 61850 but also introduced the notion of mapping physical components to virtual counterparts and outlined the system requirements for such an approach. Wojtowicz et al. [24], described the integration of virtualization technology within power system automation, with a specific emphasis on IEDs adhering to the IEC 61850 standard. They introduced the idea of establishing a virtual environment as a prospective alternative to conventional IEDs, focusing on the refinement of fundamental virtualization mechanisms and communication protocols tailored to the context of power system automation. These studies, among others, focused on the implementation of VMs using VMware software as a fundamental part of their development.

In more recent studies, Docker stands out as the predominant technology for containerization in SG virtualization due to its versatility, ease of use, and widespread adoption within the industry. Rösch et al. presented a co-simulation approach of an IEC 61850-based digital substation as a holistic representation of a highly automated power grid section [22]. This approach involved generating four virtual IEDs using custom Docker containers. Additionally, in another work by Rösch et al. [25], a comprehensive implementation for creating the specified virtual IEDs along with their respective LN was provided, detailing the exchange of sample data, all facilitated through Docker containerization. In 2023, an approach for the virtualization of DER communication using container technology was proposed in [26], where Docker container technology was also employed to virtualize each IED.

Within the context of secondary substations, the E4S Alliance is developing an Secondary Substation Platform (SSP) reference architecture, aiming to transition secondary substation into digital environments. By leveraging containerization on a unified platform, SSP will offer enhanced flexibility, simplifying the implementation of new use cases at the edge as they arise [27,28].

The main difference when making the initial decision of opting for virtualization or encapsulation is that, while VMs afford heightened control and flexibility for application testing, containers offer a streamlined deployment process, enhanced lightweight nature, and superior scalability. Research, such as studies by [29–31], exemplifies how container-based deployments can substantially diminish network-induced delays compared to VM-based setups. Given this, a recommended strategy entails utilizing VMs for preliminary configuration testing, then transitioning to containers to maximize storage efficiency and uphold consistency in application configurations [32].

Among virtualization technologies, Table 3 outlines the features of the three most prominent virtualization platforms in the market, all of which are well-suited for deployment within a SG environment.

Firstly, VirtualBox supports a range of host operating systems including Windows, Linux, macOS, Solaris, FreeBSD, and eComStation. It supports both x86 and x86–64 host and guest CPUs, with Intel VT-x or AMD-V for virtualization and is licensed under GPL version 2. This broad compatibility makes it a solid choice for diverse environments.

In contrast, QEMU, offers even wider CPU architecture support for both hosts and guests, including x86, x86–64, IA-64, PowerPC, SPARC 32/64, ARM, S/390, and MIPS. Its flexibility extends to its licensing under GPL/LGPL, making it an excellent option for test or pre-production environments due to its robust features and adaptability.

VMware ESX Server, on the other hand, is specifically designed for enterprise use, focusing on x86 and x86–64 host and guest CPUs. Unlike the other platforms, VMware ESX Server does not rely on a host operating system, which can enhance performance and reliability in a production environment. Its proprietary license reflects its commercial focus, and its impact on SCADA systems within the SG environment is significant, as highlighted by the Virtual Protection, Automation, and Control (vPAC) alliance [33], which aims to support substation virtualization and address future utility network needs.

On the other hand, Table 4 presents a detailed comparison of the most renowned solutions in the containerization environment. Each solution is distinguished by its unique approaches and suitability for implementation in a specific SG use case [34], [35]. In this context, it is important to highlight the importance of limiting and distributing resources among different groups of processes, and namespaces, which create isolated environments for processes. Docker and LXD follow a client-server architecture, while Podman and CRI-O are standalone tools without a centralized daemon server. Additionally, Docker primarily uses a layered image format, unlike Podman and CRI-O, which can

Table 3
Comparison of virtualization software platforms and capabilities.

	VirtualBox (Innotek)	QEMU (Fabrice Bellard and others)	VMware ESX Server (VMware)
CPU Host	X86, x86–64	X86, x86–64 IA–64, PowerP, SPARC 32/64, ARM, S/390, MIPS	X86, x86–64
Guest CPU	x86, x86–64, (Intel VT-x or AMD-V, and VirtualBox 2 or more)	x86, x86–64, Alpha, ARM, CRIS, LM32, M68k, MicroBlaze, MIPS, OpenRisc32, PowerPC, S/390, SH4, SPARC 32/64, Unicore32, Xtensa	X86, x86–64
OS Host	Windows, Linux, macOS, Solaris, FreeBSD, eComStation	Windows, Linux, macOS, Solaris, FreeBSD, OpenBSD, BeOS	No OS host
OS Guest	DOS, Linux, macOS, FreeBSD, Haiku, OS/2, Solaris, Syllable, Windows OpenBSD (with Intel VT-x o AMD-V	Changes regularly	Windows, Linux, Solaris, FreeBSD, OSx86 virtual apps, Netware, OS/2, SCO, BeOS, Haiku, Darwin
License	GPL version 2	GPL/LGPL	Proprietary

Table 4
Comparison of the most common containerization software (Docker, Podman, LXD and CRI-O). All of them feature multi-platform architecture and security based on user and groups.

	Docker (Docker, Inc)	Podman (Red Hat, Inc)	LXD (Canonical Ltd)	CRI-O (Kubernetes)
Architecture	Client-Server	Standalone	Client-Server	Standalone
Container Type	Application Containers	Application Containers	System Containers	Application Containers
Container Tech.	Docker Engine	Libpod	LXC	CRI-O Runtime
Language	Go	Go	C++	Go
Images	Docker Hub, Third-party Repositories	Red Hat Quay, Third-party Repositories	LXD Images	CRI-O Registry
Docker Comp.	Yes	Partial	No	No
Kubernetes Comp.	Yes	Yes	Yes	Yes
Network Config.	Default Routing for Docker	Native Network Configuration for Podman	Native Layer 2 Network	Container Network Interface
Isolation	Based on cgroups and namespaces	Based on cgroups and namespaces	Based on LXD	Based on cgroups and namespaces
License	Apache 2.0	Apache 2.0	LGPL v3	Apache 2.0

handle both layered and flat images. It is worth mentioning that CRI-O, being an implementation of the Kubernetes Container Runtime Interface (CRI) specifically designed for Kubernetes, is an interesting alternative if working with Kubernetes container orchestration is desired. Although not an independent tool like Docker or Podman, it follows a similar model to Podman.

Regarding encapsulation, due to its ease of use, intuitive command-line interface, extensive documentation, mature ecosystem including a wide variety of tools, and compatibility with a broad range of operating systems and architectures, it is worth noting that Docker is the most widely used container technology in the works conducted to date. The use cases under study are based on the IEC61850 protocol, where the starting point is the virtualization of IEC61850 LNs on a general-purpose hardware platform applicable in the field of substations. Examples of these use cases could be the containerization of a protection LN, which, subscribed to Sample Values (SV), monitors overvoltage and overcurrent conditions, as well as a LN that responds to GOOSE messages to perform relevant actions.

In SG context, containers can function as the complete representation of an IED, a complete LD, encompassing protection, measurement, and control functions, or each specific LN, such as switches, transformers, or input and output devices. This architectural approach employs micro-services, enabling flexible groupings tailored to system requirements; however, due to the intricacy and diversity of substation components, virtualizing all LNs within a single virtualized node is impractical. Consequently, deploying multiple virtualized nodes becomes necessary for effective management of IEC 61850 devices and their associated functionalities within the substation. Although there are no clear guidelines in the literature on this topic, three deployment strategies for virtualized LN are conceivable:

- IED functionalities sharing the same container. The configuration would be equivalent to deploying LNs on the same native hardware but in a virtualized mode.
- IED functionalities sharing the same hardware equipment but virtualized on different containers. LNs are decomposed into containers based on functionalities. This deployment mode suits the validation of vertical scalability.
- IED functionalities virtualized on different containers located on different hardware platforms. Oriented towards verifying both distributed deployment modes and horizontal scalability.

However, in order to ensure seamless integration and adherence to established standards, it is imperative that virtualization remains completely transparent for IEC 61850-based operations. Therefore, the virtualization platform must provide mechanisms such as container orchestration platforms, well-defined data transfer schemes and robust software-defined networking (SDN) networks to support efficient communication and management.

7.1. Container orchestration platforms

The stringent communication requirements, including bandwidth, latency, availability, and redundancy, make it essential to limit the number of applications with hard-RT requirements to the available host resources to prevent breaches. This entails allocating CPU cores exclusively to processes within containers for applications with hard-RT requirements, along with ensuring sufficient RAM allocation for each process and application with hard-RT requirements when necessary. Meanwhile, applications with soft-RT needs or without RT requirements can share the remaining CPU cores. Additionally, the network must be prepared to handle the requirements and priorities of new containers. Achieving this requires dynamic resource orchestration between containers to meet demand based on workload. Therefore, effective container orchestration becomes crucial to help manage and coordinate the deployment, scaling, and operation of containerized applications across multiple hosts.

In this context, container orchestration platforms play a fundamental role in automating the deployment or commissioning of the entire platform in an installation. The orchestration platforms offer features such as RT scheduling, resource isolation, task prioritization, and run-time guarantees to ensure that applications with hard-RT requirements are executed within the established time limits. They also manage, scale, interconnect, and ensure the availability of applications, considering both vertical and horizontal scalability, as well as remote updating. Two typical container orchestrators are Kubernetes and Docker Swarm. Kubernetes, being broader and more versatile, offers advanced scalability suitable for managing and updating complex and larger-scale application sets. K3s, as a lightweight distribution of Kubernetes, can be an interesting option for orchestration in SG environments, as it is a simplified version designed for constrained environments that retains most of Kubernetes' core functionalities [36]. On the other hand, Docker Swarm is a native solution specifically developed for Docker, providing simpler scalability and management [37]. As shown in Table 4, Docker, Podman, LXD and CRI-O are compatible and can be orchestrated using Kubernetes. Among them, CRI-O provides an optimized environment for running containers within a Kubernetes cluster [38]. However, only Docker has all integration with Docker orchestration.

A comprehensive comparison and evaluation of the performance of Docker Swarm and Kubernetes is presented in [39],. The study investigates differences in latency within containerization environments on the same host. The findings suggest that utilizing orchestration tools could substantially decrease latency compared to simpler methods. This is attributed to their ability to optimize resource allocation, automate tasks related to managing the virtualized environment (such as provisioning, scaling, and load balancing), and facilitate dynamic resource scaling based on workload demands. Regarding the results of the experiments and evaluations carried out to compare the performance of Docker Swarm and Kubernetes, overall, both have comparable performance, but it may vary in different environments and require different technical approaches. Additionally, it is highlighted that major cloud service providers now offer managed Kubernetes services.

7.2. Well-defined data transfer schemes

With virtualization, even if the IEC 61850 requirements remain in force, communications no longer occur solely between IEDs or hardware nodes connected to the Ethernet LAN. Instead, they take place among virtualized elements within the virtualized environment. As a result, well-defined data transfer schemes should be established within the host or hardware node where multiple virtualized devices are located (intra-host), as well as between virtualized devices residing on different hosts (inter-host), to ensure efficient communication and data exchange between applications.

On the one hand, intra-host communications can correspond to:

- GOOSE messages between IEDs, both for status and burst messages triggered by processing anomalous values of SMV. These messages are sent over the process bus in the absence of virtualization.
- GOOSE messages to local telecontrol platforms, such as SCADA systems. These messages are sent over the station bus in the absence of virtualization.
- MMS messages between local telecontrol platforms and IEDs, which are also sent over the station bus if there is no virtualization.

  When virtualizing, it is not essential to map individual IEDs to distinct virtualized elements. Instead, they should be abstracted to the level of LN and grouped, as much as possible, so that a function becomes an application in a container. Within the host, there is no Ethernet LAN network, so both the process bus and the station bus are replaced by communications between processes. Consequently, communications between two LN of two IEDs that have been virtualized within the same element are no longer necessary; the information is directly available to both LN.

Given that the design of containers should not be overly complicated, if it is not possible to have two LN in one container, there will be communication between two virtualized elements that, due to the RT requirements, should be two containers. Thus, in this case, communications would involve the complete implementation of the IEC 61850 protocols, but this would not imply communication over a bus per se, but rather a transfer of data through memory. While it would be feasible to replace the messages with lighter Inter-Process Communication (IPC) communications in this scenario, doing so would deviate from the IEC 61850 standard and could be seen as a regression in terms of interoperability, which is one of the key issues that the standard aims to address.

To carry out intra-host communications between virtualized containers, it is essential to enable one or more of the following networking modes [40]:

- Bridge: Assigns a switch operating at layer 2 of the OSI model. It is the default networking mode for a Docker or Podman container when created. With a bridge, containers can connect to the host or communicate directly with each other within the same created internal virtual subnet. Derived from bridge mode, in Kubernetes, one container acts as a proxy or bridge for an entire set of containers (Pod).
- Macvlan: It is a network virtualization technology that creates virtual interfaces that directly connect to physical interfaces on the host and assigns individual MAC addresses to each container. This enables direct communication between containers and between them and the physical network without going through a bridge, which can result in high transfer speeds and good scalability.
- Host Network: The container directly joins the host operating system's network instead of creating a separate internal network. By using the host's network, the container shares the host's IP address, network interfaces, and network connectivity.

In general, when working with containerization, it is not necessary for the user to explicitly activate the network mode. This is because container orchestrators, such as Kubernetes or k3s, handle the network configuration for containers in the environment. However, although in most cases it is the orchestrators that take care of this task, in some cases, especially in highly customized or specific environments, it may be necessary for the user to manually configure the network mode or make additional adjustments to the network configuration.

In the case of Docker, which uses the bridge network mode by default, each container is assigned an IP address for every IP subnet it connects to. The Docker daemon dynamically allocates and subdivides IP addresses for containers. Each network also has a subnet mask and a default gateway. On the other hand, in a Kubernetes Pod, containers within the same Pod share the same IP address and namespace, which simplifies communication within the Pod while maintaining network isolation. [41].

On the other hand, inter-host communications can be classified into two main groups. The first group comprises communications involving virtualized elements distributed across two hardware platforms for horizontal scalability reasons. In addition to this type of communication, there are flows of SMVs originating from MUs or Non-Conventional Instrument Transformers (NCITs) at the bay or core level of the OT segment of the power installations. Within the IT segment, there are communications with remote elements, including Network Control Centres (NCCs) or specific Cloud applications.

Similar to intra-host communications, on the one hand, all flows of SMVs and GOOSE messages between virtualized elements hosted on different platforms must comply with the IEC 61850 standard, with the added difficulty of having to traverse the external Ethernet LAN network, with its bandwidth, latency, synchronization, etc., limitations. Therefore, one of the main criteria for distributing virtualized elements must be to minimize inter-host communications, especially of the GOOSE type, so that the topology of the Ethernet LAN network remains as simple as possible. Therefore, although some horizontal scalability is necessary to provide redundancy to the SG, vertical scalability should be prioritized whenever possible to avoid the additional complications that come with horizontal scalability communications. Additionally, in inter-host communications, the requirement for internal orchestration increases, along with the need for proper resource allocation on each hardware platform or host. Furthermore, orchestrating between multiple hosts becomes essential, necessitating efficient network management to guarantee access to network infrastructure for communications with more demanding requirements and to avoid congestion due to inefficient information routing.

For inter-host communications, NAT (Network Address Translation) or an overlay network can be added to intra-host modes. Overlay networking facilitates communication by establishing a virtual network layer that overlays the underlying physical network infrastructure. They allow configuring the logical network topology, defining virtual LAN subnets, and adding communication management capabilities for both inter-host and intra-host communications. However, this entails the addition of additional headers and processing times. In these cases, the macvlan mode becomes ipvlan [42] and docker has adopted the VXLAN overlay network [43].

7.3. SDN

Secondary and primary substations play a crucial role in the energy generation and distribution process. Therefore, the communication networks associated with these substations require high levels of availability and reliability, along with a management platform that is functional, secure, scalable, and easy to administer [44]. In this context, SDN introduces a more flexible and automatable approach to managing and controlling LAN networks by separating the control plane from the data plane. This enables dynamic and centralized configuration, easing network adaptation to RT changes and optimizing traffic based on requirements and facilitating information exchange among applications, regardless of their deployment on different nodes. It also offers enhanced scalability and performance optimization by automatically prioritizing critical traffic for IEC 61850, which improves the quality of service and reduces response time. [45].

Additionally, SDN can manage redundancy to optimize the use of mesh topologies and ensure the availability of control and monitoring applications within secondary and primary substations services using protocols such as, OpenFlow, OSPF, or VXLAN networks, that allow an external controller to configure multiple redundant paths between devices with multiple network interfaces.

There are great number of application cases where the incorporation of SDN networks as key elements of power substation communication networks could improve the operation, management, availability, and reliability within the networks. In their study [46], the authors enumerate several applications, such as RT monitoring of grid health to facilitate informed decision-making, energy distribution optimization, and the integration of renewable energy sources. Additionally, they analyse how SDN facilitates active demand management and efficient load administration, involving consumers in decision-making processes and fostering energy efficiency.

However, even if the virtualization of network management through SDN networks provides greater flexibility and dynamic management capabilities, it may lead to increased delays depending on its optimization level. The virtualization of network management through SDN introduces an additional layer of abstraction between physical network devices and control applications. This can lead to increased delays due to the need to process and translate network commands and policies through the SDN controller before reaching the underlying network devices. Furthermore, the efficiency and speed of this translation can vary depending on the controller's capabilities and the complexity of the network policies. Additionally, network optimization in SDN environments can also affect delays if routing policies and network management are not properly optimized. Therefore, it is crucial to design effective optimization strategies that balance network flexibility and efficiency in SDN environments to minimize delays and ensure optimal network performance.

There are several SDN solutions available in the market, each with its own features and capabilities. The choice between them will depend on a prior assessment of the specific needs of the electrical substation environment and network requirements.

8. Functions allocation for SG virtualization

To define the necessary architectures for the SG virtualization, it is essential to consider the possibility of massive deployments, the need for system management and supervision, as well as their impact on criticality and RT demands. Therefore, cloud applications and solutions play a crucial role in the virtualization of SG, providing a flexible, scalable, and secure infrastructure that supports efficient management and the implementation of new technologies. Cloud platforms offer extensive data storage and processing capabilities, allowing for the handling of large volumes of information generated by the grids. Additionally, they can easily adjust as the demand for resources in the SG grows and provide a centralized view of the entire network, enabling efficient management and supervision. Moreover, this also reduces the initial investment in physical infrastructure.

However, a centralized cloud architecture poses challenges such as network and central server saturation due to incoming information, heightened latency, and reduced flexibility in failure response. Consequently, there is a trend towards deploying edge nodes to shift the network towards distributed management, allocating appropriate functions to each component. This shift brings information processing closer to the assets, thus reducing latency and enhancing response speed [47]. Additionally, it enables virtualization to facilitate the transition from a centralized energy system to a more decentralized, localized, and efficient one [48]. Within this framework, each edge node can autonomously execute multiple diverse applications and communicate with other nodes, thereby mitigating the costs and security risks associated with centralized infrastructures. However, the distribution of functions between the edge and the cloud is not predetermined; it depends on the chosen computing strategy in each scenario.

In the design of such an infrastructure, it is necessary to foresee not only scalability to accommodate new operations/functions and increased data flow, but also flexibility to enable function reallocation and data flow control. In an SG network architecture based on edge nodes and a centralized cloud, each component would serve distinct functions to ensure efficient grid operation and management. Here are the main functions that each could acquire:

- The edge node will tend to perform more specific functions, those closest to the systems. It should connect using the main protocols used by the equipment in the substations and transformer stations of the power grid (such as Modbus, OPC-UA, IEC 61750) and manage three types of communications: between hard-RT or soft-RT applications located within the same host; with applications that have hard-RT requirements and are running on other hosts or edge nodes within the same installation, as part of horizontal scalability; and with other cloud nodes in the management system. In all cases, the latency requirements of process-level messages demand that the hosts function as edge nodes situated within their respective secondary or primary substation.

- The cloud will have connectivity with the edge nodes to obtain significant data that may influence decision-making at the level of the entire power grid and to act on equipment if necessary. Additionally, it will centralize all equipment management functions.

While cloud computing has traditionally leaned on VM for resource allocation and user isolation, this method faces challenges with big data workloads, like weak resilience and inefficient resource management [49]. As a result, there is a growing trend towards adopting container-based solutions [50–52], due to containers bring several benefits related to deployment, operation, isolation, and efficient resource sharing. In the case of edge nodes, the latency and RT requirements imposed by the SG make containerization emerge as a more suitable solution [53].

Currently, Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure are prominent leaders in providing cloud infrastructure and services. These industry leaders facilitate seamless connectivity with devices or edge nodes through standard protocols. Alongside their IoT services in the cloud, these providers offer fully integrated edge services to distribute computing functions across the entire data chain. In addition to these major cloud providers, there are independent solutions available for deploying tools both in the cloud and at the edge. Notably, Minsait by Indra has emerged as a prominent player in this space. Leveraging various open-source services, Minsait has developed a versatile platform that offers integration and flexibility to meet diverse use cases, including those within the electrical grid sector. Moreover, specific platforms tailored for edge computing are gaining traction. Among them, EdgeXFoundry stands out as an open-source service architecture standard specifically designed for edge implementation, further enhancing the landscape of edge computing solutions. In [5], a comparative table is presented summarizing the main features of the IoT Edge-Cloud platforms from the three major public cloud providers, Minsait, and EdgeXFoundry, among others.

When considering market share and connectivity between hubs, AWS boasts the greatest market share, as well as the highest number of connections between devices, and between devices and cloud hubs. Therefore, in the study conducted by [54], it was determined that AWS emerges as the optimal IoT cloud platform vendor, fulfilling all user requirements regarding hub connectivity, analytics, and security services. However, the decision-making process for choosing a cloud solution is not straightforward. The choice will depend on the characteristics and requirements, as well as the cost and preferences of the team.

9. Illustrative example: containerized applications in a SG PS

In this conceptual case study, two identical hardware units, each comprising two Docker containers representing LNs in an SG primary substation, are considered. The hardware specifications for each unit include a Quad-core ARM A57 CPU, a 128-core Maxwell GPU, 4 GB of LPDDR4 RAM, two 1 GB Ethernet ports (NIC #1 and NIC #2), and additional connectivity options such as 4 USB ports, I2C, SPI, UART, and GPIO interfaces. These specifications provide the necessary processing power, memory, and connectivity for the effective operation of the containerized protection and breaker IEDs within the primary substation scenario described.

As shown in Fig. 3, both hardware elements are equally configured and have the same capabilities. On each piece of hardware unit, one containerized protection IED LN subscribes to SV and monitors overvoltage and overcurrent conditions. In case any of these conditions occur, the protection IED LN sends a GOOSE message to notify the situation to other IEDs within the substation in the bay level or across the substation network. On the other hand, we have a containerized breaker IED LN that waits to receive these GOOSE messages. When it receives a relevant GOOSE message from the protection IED LN, the breaker IED LN performs the corresponding action, such as activating or deactivating a switch. This approach was conceptually chosen to ensure that each function is managed by dedicated processing units, which helps meet the strict RT requirements typical in substation environments.

In this conceptual model, since we are virtualizing functionalities with strict RT requirements, we have opted for horizontal scalability.

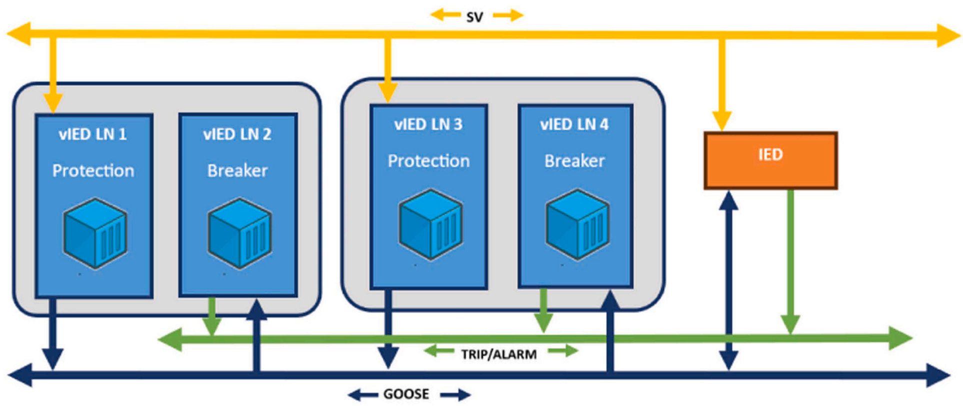

Fig. 3. IEDs LNs and message exchange between the actors.

This means that, as defined in Section Scalability Models, instead of overloading existing devices, we add new devices, thus ensuring that each device has its own dedicated processing capacity.

As the orchestrator, k3s has been considered a suitable option, as it is lightweight and easy-to-install distribution designed specifically for resource-constrained environments, which is compatible with Docker (See Section Container orchestration platforms). The k3s orchestrator is configured to establish a private virtual network so that the containers within the electrical substation can communicate with each other and with other devices in the substation. For containers running on the same node (or hardware) within the k3s cluster, they can communicate with each other through the bridge network provided by k3s without the need for additional configuration. Therefore, in this case, it is not necessary to enable intra-host communications using bridge networking mode. On the other hand, when we refer to inter-host communications or containers running on different nodes within the k3s cluster, even if K3s does support overlay networks, the user needs to enable and configure them as part of the cluster setup to enable communication between nodes within the k3s cluster.

Docker has adopted VXLAN overlay networks, which provide a virtual network layer above the underlying physical infrastructure, allowing communication between containers distributed across different edge nodes. To enable VXLAN overlay network in k3s, it is necessary to configure it on all nodes of the K3s cluster, both physical and virtualized ones between which communication is desired. Configuring the VXLAN overlay network should be done prior to deploying containers and nodes in the cluster. So, during k3s installation, it will be necessary to select the appropriate options to enable network features like VXLAN overlay. Once the network plugin is installed and configured, an overlay network will be created spanning all nodes within the K3s cluster, allowing communication between containers running on different nodes. For our scenario, the containerized protection IED LN and breaker IED LN should be deployed on each hardware element within the K3s cluster, ensuring that the containers are configured to use the overlay network for communication. Additionally, the additional devices we want to be part of the VXLAN network must also be deployed and configured for it.

In Section SDN, we also have highlighted the potential benefits of working with SDN, which can improve operation, management, availability, and reliability within networks by providing greater flexibility and centralized control over the network infrastructure. Therefore, the application of SDN networks would be something to consider as long as the network performance is not affected. To effectively implement an SDN in the described electrical substation environment, it is essential to begin by carefully assessing the specific needs and network requirements. This allows for the selection of an SDN solution that perfectly suits those needs. Once the appropriate SDN solution has been chosen, the next step is the installation and configuration within the electrical substation environment. This involves deploying SDN controllers, compatible switches, and other necessary components, ensuring they are properly integrated with existing hardware devices and control systems. Given its potential in flexibility, scalability, and support for standard protocols, OpenDaylight emerges as a solid option for this implementation [55]. Its ability to manage the electrical substation network and ensure interoperability with existing systems makes it an attractive choice. However, conducting a thorough evaluation before making a final decision is crucial.

Finally, it is important to note that these hardware represents devices located at the edge of the network with RT requirements, which handle functions more related to the control and management of each specific electrical installation. On the other hand, the cloud would manage more general functions related to a set of installations or the entire network, such as updates, software verification, configuration of edge nodes or installations, etc. For this function allocation to be successful, connectivity between edge nodes and the cloud is essential for data transmission. The communication between the edge and the cloud is carried out through a combination of communication protocols (such as MQTT, CoAP, AMQP, HTTP/HTTPS or WebSocket), gateways, IoT protocols, and cloud services, with the aim of efficiently and securely transferring data between edge devices and cloud services for processing and analysis.

In summary, this conceptual case study outlines a theoretical framework for virtualizing IED functionalities within a primary substation. Future implementation and testing will be necessary to validate these design choices and to address potential challenges that may arise during practical deployment.

10. Conclusion

The digitization of electrical grids has been a growing trend in recent years, aimed at optimizing processes, improving efficiency, and enabling better information management, leading to what is known as SG. As technology advances and hardware gets stronger, the trend to combine functions leads to virtualizing functions and putting them onto fewer devices. However, this transition comes with its challenges. To ensure that the SG continues to operate effectively and meets the requirements established in the IEC 61850 standard, it is crucial to ensure that virtualization solutions meet the necessary criteria.

In this paper, the most critical requirements for ensuring the proper functioning of the SG have been outlined, as well as the specific requirements that the critical infrastructures, secondary and primary substations, must meet to comply with SG standards. For secondary substations, the priority is the separation between MV and LV networks, while for primary substations, latency is crucial for timely communication exchanges. Additionally, the use cases that can benefit from virtualization and critical functions for virtualization for each type of substation have been determined, with detailed requirements ranging from sensors I/O to communication interfaces, ensuring an effective implementation that meets the specific needs of each environment.

Based on these requirements, the elements and functionalities suitable for virtualization in substations have been identified with the aim of improving efficiency in the management of the electrical system. Once the elements and functions that can be virtualized in secondary or primary substations have been established, along with the requirements they must meet, scalability studies have been carried out to ensure the system's adaptability to network changes. It has been concluded that elements and functionalities susceptible to virtualization in secondary substations, typically characterized by a smaller number of elements and less strict time or latency demands, probably favour vertical scalability. In contrast, primary substations, where stricter timing requirements are common, will tend to lean toward horizontal virtualization.

To complete the study, an evaluation has been conducted on the most suitable virtualization platforms (VirtualBox, QEMU, VMware) and containerization tools (Docker, Podman, LXD, and CRI-O) currently available for use in SG environments. Virtualization platforms like VMware were found to have a significant impact on SG environments, particularly in SCADA systems. Regarding encapsulation, Docker emerged as the most widely used container technology due to its ease of use and compatibility. Furthermore, as virtualization must be transparent for IEC 61850-based operations to ensure smooth integration and compliance with established standards, mechanisms such as container orchestration platforms must be offered by the virtualization platform. In the case study, it was concluded that K3s could be an interesting option, given its compatibility with Docker and its design for constrained environments, typical of substation elements. Additionally, well-defined data transfer schemes, such as bridges to facilitate intra-host communications between virtualized containers, and robust SDN networks are required to support efficient communication and management.

Finally, it is necessary to establish specific requirements for designing the infrastructure and distributing functions between the cloud and the edge within the context of SGs. An appropriate approach could involve deploying a virtualized solution in the cloud using any of the analysed platforms (such as AWS, GCP, Microsoft Azure, Minsait, or EdgeXFoundry), while implementing applications with stricter latency and RT requirements on containers at the edge nodes.

However, it is important to highlight some limitations of this work. The virtualization solutions and proposals presented still need validation in real environments to ensure their effectiveness. Although studies and simulations have been developed, implementation in real environments could reveal unforeseen challenges. Therefore, additional prototypes and tests are required to ensure that the virtualized solutions function adequately under various operating conditions. Furthermore, although efforts have been made to comply with IEC 61850 standards, compatibility with other systems and standards could present challenges. The security of virtualized solutions, the implications for latency and real-time performance, and the infrastructure requirements also need further investigation. Thus, there is still work to be done to ensure the successful and sustainable implementation of the proposed solutions.

CRediT authorship contribution statement

Laura Lázaro-Elorriaga: Writing - Original Draft, Writing - Review & Editing, Investigation, Conceptualization. **David Guerra:** Writing - Review & Editing, Investigation. **Imanol García-Pastor:** Investigation. **Cristina Martínez:** Investigation. **Eutimio Sanchez:** Supervision, Project administration. **Eugenio Perea:** Writing - Review & Editing, Supervision, Conceptualization.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The authors are unable or have chosen not to specify which data has been used.

Acknowledgment

The present work is supported by the Basque Government under the project VIRTGRID (ELKARTEK program KK-2022/00069). We would like to recognize the ELKARTEK project consortium for their collaboration and support throughout this research endeavour, as well as to the contributions and expertise of the participating organizations: TECNALIA, INGETEAM R&D EUROPE, ZIV I+D SMART ENERGY NETWORKS, GISEL and TSR from the University of the Basque Country and ACE.

References

[1] P. Rai, A. Mishra and A. Lal, Smart Grid and IEC 61850, in *2021 International Conference on Intelligent Technologies (CONIT)*, 2021.
[2] R.D.F. Ferreira, B. Fontes, H. Samaniego, M. Mendes and A. Apostolov, Cloud IEC 61850, in *PAC World Conference*, Dublin, 2013.
[3] C. Weber and S. Kumar, Modernized Grids Require Substation Virtualization," July 2021. [Online]. Available: ⟨https://www.advantech.com/en/resources/white-papers/modernized-grids-require-substation-virtualization⟩.
[4] S. Attarha, A. Narayan, B. Hage Hassan, C. Krüger, F. Castro, D. Babazadeh, S. Lehnhoff, Virtualization management concept for flexible and fault-tolerant smart grid service provision (no), Energies vol. 13 (2020) 2196.
[5] Grupo de Trabajo de Centro de Transformación Inteligente, Centro de Transfomación Inteligente: Fundamentos para Distribución de Funcionalidades," 2021. [Online]. Available: ⟨https://www.futured.es/grupo-trabajo-ct-inteligente/⟩.
[6] H. Niveri, Virtualization: A Key Enabler of the Future Power Grid," *Mission Critical Magazine,* 2023.
[7] The Virtualized Substation: No, Really," Directors, Clarion Energy Content, 2018. [Online]. Available: ⟨https://www.power-grid.com/der-grid-edge/the-virtualized-substation-no-really/#gref⟩. [Accessed October 2023].
[8] Grupo de Trabajo de Centro de Transformación Inteligente, Visión FUTURED hacia 2050," Futured, 2020. [Online]. Available: ⟨https://www.futured.es/wp-content/uploads/2020/06/20200626_libro-Vision-FUTURED-hacia-2050.pdf⟩.
[9] S. Babu, P. a J. Hilber and J. Henning, On the status of reliability studies involving primary and secondary equipment applied to power system," in 2014 International Conference on Probabilistic Methods Applied to Power Systems (PMAPS), 2014.
[10] TC 57 - Power systems management and associated information exchange, IEC 61850:2023 Series. Communication networks and systems for power utility automation - ALL PARTS," 2023.
[11] La subestación digital: un acelerador de la transición ecológica," Red Electrica de España, 2021. [Online]. Available: https://www.ree.es/es/sala-de-prensa/actualidad/especial/2021/07/la-subestacion-digital-un-acelerador-de-la-transicion-ecologica.
[12] E. Torres, P. Eguia, O. Abarrategi, D. Larruskain, V. Valverde and G. Buigues, Trends in Centralized Protection and Control in Digital Substations, in 21st International Conference on Renewable Energies and Power Quality (ICREPQ'23), Madrid, 2023.
[13] R.E. Mackiewicz, Overview of IEC 61850 and Benefits, in 2006 *IEEE Power Engineering Society General Meeting*, 2006.
[14] A. Schumilin, C. Düpmeier, K.-U. Stucky and V. Hagenmeyer, A Consistent View of the Smart Grid: Bridging the Gap between IEC CIM and IEC 61850, pp. 321-325, 08 2018..
[15] D. Purón, Gemelos digitales de una red eléctrica inteligente, barbara, 12 07 2022. [Online]. Available: ⟨https://www.barbara.tech/es/blog/gemelos-digitales-de-una-smart-grid⟩. [Accessed 01 07 2024].
[16] Y. Yan, Y. Qian, H. Sharif, D. Tipper, A survey on smart grid communication infrastructures: motivations, requirements and challenges, IEEE Commun. Surv. Tutor. vol. 15 (1) (2013) 5–20.
[17] E. Ancillotti, R. Bruno, M. Conti, The role of communication systems in smart grids: architectures, technical solutions and research challenges, Comput. Commun. vol. 36 (2013) 1665–1697.
[18] IEEE Standards Association, «IEEE Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation,» IEEE, 2004. [En línea]. Available: ⟨https://standards.ieee.org/standard/1646-2004.html⟩. [Último acceso: 04 October 2003].

[19] IEC 61850 Website, IEC 61850 Website, 2004. [Online]. Available: ⟨https://iec61850.dvl.iec.ch/⟩. [Accessed 04 October 2023].
[20] C. Slingerland, «Horizontal Vs. Vertical Scaling: How Do They Compare?,» Cloud Zero, 05 May 2023. [En línea]. Available: ⟨https://www.cloudzero.com/blog/horizontal-vs-vertical-scaling/⟩. [Último acceso: May 2024].
[21] N.K. Morais, M.O.N. Belaid, M. Gibescu, L.R. Camargo, J. Cantenot, T. Coste, V. Audebert and H. Morais, Towards Software-Defined Protection, Automation, and Control in Power Systems: Concepts, State of the Art, and Future Challenges, *energies,* 2023.
[22] D. Rösch, S. Nicolai and P. Bretschneider, Combined simulation and virtualization approach for interconnected substation automation, in Proceedings of the 2021 6th International Conference on Smart and Sustainable Technologies (SpliTech), Croatia, 2021.
[23] R.D.F. Ferreira, D. Oliveira and R. Silva, Cloud IEC 61850: DDS performance in virtualized environment with opendds, in 2017 *IEEE International Conference on C*omputer and Information Technology (CIT), 2017.
[24] R. Wojtowicz, R. Kowalik, D.D. Rasolomampionona, Next generation of power system protection automation - virtual power system protections, IEEE Trans. Power Deliv. (2017).
[25] D. Rösch, O. Farghaly, R. Suri, P. Dahane, S. Nicolai, P. Bretschneider, VirtualSubstation: an IEC 61850 framework for a containernet based virtual substation, 57th Int. Univ. Power Eng. Conf. (UPEC) 2022 (2022).
[26] S. Chen, J. Morris, Z. Lu and G. Heilscher, Concept and implementation of a grid simulation framework utilizing containerized IEC 61850 compatible IED, in 27th International Conference on Electricity Distribution (CIRED 2023), 2023.
[27] M. Gorlan, E4S Alliance | Secondary Substation Platform – SSP, October 2020. [Online]. Available: ⟨https://merytronic.gorlan.com/en/e4s-alliance-plataforma-del-centro-de-transformaci/⟩. [Accessed February 2024].
[28] E4S Alliance, «Edge for Smart Secondary Substation (E4S) Alliance,» E4S Alliance, 2023. [En línea]. Available: ⟨https://www.e4salliance.com/⟩. [Último acceso: February 2024].
[29] V.-G. Nguyen, K.-J. Grinnemo, J. Cheng, J. Taheri, A. Brunstrom, On the use of a virtualized 5G core for time critical communication in smart grid, 8th IEEE Int. Conf. Mob. Cloud Comput., Serv., Eng. (Mob.) 2020 (2020).
[30] J. Fontenla-González, C. Pérez-Garrido, F. Gil-Castiñeira, F.J. González-Castaño and C. Giraldo-Rodriguez, Lightweight container-based OpenEPC deployment and its evaluation, in *2016 IEEE NetSoft Conference and Workshops (NetSoft)*, 2016.
[31] H.-C. Chang, B.-J. Qiu, J.-C. Chen, T.-J. Tan, P.-F. Ho, C.-H. Chiu, B.-S. Lin, Empirical experience and experimental evaluation of open5gcore over hypervisor and container, Wirel. Commun. Mob. Comput. (2018) 1–14.
[32] Q. Zhang, L. Liu, C. Pu, Q. Dou, L. Wu, W. Zhou, A comparative study of containers and virtual machines in big data environment, IEEE 11th Int. Conf. CLOUD Comput. (CLOUD) 2018 (2018).
[33] «Utility Substation Virtual Protection,» vmware, 2023. [En línea]. Available: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-utility-substation-virtual-protection-automation-and-control-ready-infrastructure.pdf. [Último acceso: May 2024].
[34] S. Kaiser, M.S. Haq, A.Ş. Tosun, T. Korkmaz, Container technologies for ARM architecture: a comprehensive survey of the state-of-the-art, IEEE Access vol. 10 (2022) 84853–84881.
[35] R. Riley, X. Jiang and D. Xu, Guest-transparent prevention of kernel rootkits with vmm-based memory shadowing, in *Recent Advances in Intrusion Detection: 11th International Symposium*, Cambridge, 2008.
[36] S. Böhm and G. Wirtz, Profiling Lightweight Container Platforms: MicroK8s and K3s in Comparison to Kubernetes," in *ZEUS*, 2021.
[37] Y. Pan, I. Chen, F. Brasileiro, G. Jayaputera, R. Sinnott, A performance comparison of cloud-based container orchestration tools, IEEE Int. Conf. Big Knowl. (ICBK) 2019 (2019).
[38] .«¿Qué es CRI-O?,» Digital Guide IONOS, 23 March 2021. [En línea]. Available: ⟨https://www.ionos.es/digitalguide/servidores/know-how/que-es-cri-o/⟩. [Último acceso: 06 May 2024].
[39] M.A. Rodriguez, R. Buyya, Container-based cluster orchestration systems: a taxonomy and future directions, Softw.: Pract. Exp. vol. 49 (5) (2019) 698–719.
[40] J. Struye, B. Spinnewyn, K. Spaey, K. Bonjean, S. Latre, Assessing the value of containers for NFVs: a detailed network performance study, 13th Int. Conf. Netw. Serv. Manag. (CNSM) 2017 (2017).
[41] J. Shah, D. Dubaria, Building modern clouds: using docker, kubernetes & Google cloud platform, 2019 IEEE 9th Annu. Comput. Commun. Workshop Conf. (CCWC) (2019).
[42] L. Zhang, Y. Wang, S. Liang, R. Jin, Container network architecture and performance analysis of Macvlan and IPvlan, SHS Web Conf. (2023).
[43] Y. Haruna, A.A. Lawan, K.I. Yarima, M.M. Ahmad, M.A. Sani, Analysis of docker networking and optimizing the overhead of docker overlay networks using OS kernel support, Networks vol. 10 (2) (2022) 15–30.
[44] A. Leal, J.F. Botero, An architecture for power substationscommunication networks based on SDN andvirtualization paradigms, Rev. Fac. De. Ing. ía, Univ. De. Antioquia (100) (2021) 48–66.
[45] M.H. Rehmani, A. Davy, B. Jennings, C. Assi, Software defined networks-based smart grid communication: a comprehensive survey, IEEE Commun. Surv. Tutor. vol. 21 (3) (2019) 2637–2670.
[46] W. Velasquez, G.Z. Moreira-Moreira, y, M.S. Alvarez-Alvarado, Smart grids empowered by software-defined network: a comprehensive review of advancements and challenges, IEEE Access (2024).
[47] Y. Huang, Y. Lu, F. Wang, X. Fan, J. Liu, V.C. Leung, An edge computing framework for real-time monitoring in smart grid, IEEE Int. Conf. Ind. Internet (ICII) 2018 (2018).
[48] Q. Ou, Y. Wang, W. Song, N. Zhang, J. Zhang and H. Liu, Research on network performance optimization technology based on cloud-edge collaborative architecture, in 2021 *IEEE 2nd International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE)*, 2021.
[49] Q. Zhang, L. Liu, C. Pu, Q. Dou, L. Wu, W. Zhou, A comparative study of containers and virtual machines in big data environment, IEEE 11th Int. Conf. CLOUD Comput. (CLOUD) 2018 (2018).
[50] S. Hardikar, P. Ahirwar, S. Rajan, Containerization: cloud computing based inspiration Technology for Adoption through Docker and Kubernetes, Second Int. Conf. Electron. Sustain. Commun. Syst. (ICESC) 2021 (2021).
[51] A. Celesti, D. Mulfari, M. Fazio, M. Villari, A. Puliafito, Exploring container virtualization in IoT clouds, IEEE Int. Conf. Smart Comput. (SMARTCOMP) 2016 (2016).
[52] A. Bhardwaj, C.R. Krishna, Virtualization in cloud computing: moving from hypervisor to containerization—a survey, Arab. J. Sci. Eng. vol. 46 (9) (2021) 8585–8601.
[53] Á. Kovács, Comparison of different Linux containers, in *In* 2017 40th International Conference on Telecommunications and Signal Processing (TSP), 2017.
[54] A.S. Muhammed and D. Ucuz, Comparison of the IoT Platform Vendors, Microsoft Azure, Amazon Web Services, and Google Cloud, from Users' Perspectives, in 2020 8th International Symposium on Digital Forensics and Security (ISDFS), 2020.
[55] A. Aydeger, K. Akkaya y A. S. Uluagac, «SDN-based resilience for smart grid communications,» 2015 *IEEE Conference on Network Function Virtualization and Software Defined Network (NFV-SDN),* pp. 31-33, 2015.