




Review

Towards Software-Defined Protection, Automation, and Control in Power Systems: Concepts, State of the Art, and Future Challenges

Nadine Kabbara ^{1,2,*}, Mohand Ouamer Nait Belaid ^{1,3,*} , Madeleine Gibescu ², Luis Ramirez Camargo ² , Jerome Cantenot ¹, Thierry Coste ¹, Vincent Audebert ¹ and Hugo Morais ^{4,*} 

¹ EDF R&D, 91120 Palaiseau, France

² Copernicus Institute of Sustainable Development, Utrecht University, 3584 CB Utrecht, The Netherlands

³ LIGM Lab, Gustave Eiffel University, 77420 Champs-sur-Marne, France

⁴ Inesc-ID, 1049-001 Lisboa, Portugal

* Correspondence: nadine.kabbara@edf.fr (N.K.); mohand-ouamer.nait-belaid@edf.fr (M.O.N.B.); hugo.morais@tecnico.ulisboa.pt (H.M.)



Citation: Kabbara, N.; Nait Belaid, M.O.; Gibescu, M.; Camargo, L.R.; Cantenot, J.; Coste, T.; Audebert, V.; Morais, H. Towards Software-Defined Protection, Automation, and Control in Power Systems: Concepts, State of the Art, and Future Challenges. *Energies* **2022**, *15*, 9362. <https://doi.org/10.3390/en15249362>

Academic Editor: Abu-Siada Ahmed

Received: 17 November 2022

Accepted: 8 December 2022

Published: 10 December 2022

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



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Abstract: Nowadays, power systems' Protection, Automation, and Control (PAC) functionalities are often deployed in different constrained devices (Intelligent Electronic Devices) following a coupled hardware/software design. However, with the increase in distributed energy resources, more customized controllers will be required. These devices have high operational and deployment costs with long development, testing, and complex upgrade cycles. Addressing these challenges requires that a 'revolution' in power system PAC design takes place. Decoupling from hardware-dependent implementations by virtualizing the functionalities facilitates the transition from a traditional power grid into a software-defined smart grid. This article presents a survey of recent literature on software-defined PAC for power systems, covering the concepts, main academic works, industrial proof of concepts, and the latest standardization efforts in this rising area. Finally, we summarize the expected future technical, industrial, and standardization challenges and open research problems. It was observed that software-defined PAC systems have a promising potential that can be leveraged for future PAC and smart grid developments. Moreover, standardizations in virtual IED software development and deployments, configuration tools, performance benchmarking, and compliance testing using a dynamic, agile approach assuring interoperability are critical enablers.

Keywords: PAC systems; IT/OT convergence; software-defined/virtualized PAC; virtualization technology; interoperability; IEC 61850; smart grids

1. Introduction

Today, power systems face rising challenges that motivate their development into smart grids. The numerous challenges include: reaching carbon neutrality goals, electrification of end-uses, and the energy transition into renewables [1]. The integration of Distributed Energy Resources (DERs) at both Medium Voltage (MV) and Low Voltage (LV) levels is actively transforming the traditional centralized design of power systems; from a mostly static, uni-directional grid into a grid supporting bidirectional flows of energy and information between different energy actors with much faster operating dynamics and limited predictability [2,3]. Therefore, maintaining the supply–demand balance and avoiding grid congestion becomes an increasingly complex task with significant uncertainties [4].

As the power system evolves, introducing novel improved Protection, Automation, and Control (PAC) systems supporting its operation becomes a necessity [5]. In this paper, we formally define PAC systems as a cohesive set of power system functionalities that allow to protect, automate, and control the electrical grid, spanning the field, process, and operational zones. Examples include substation voltage controller, under/overvoltage

protections, differential protection, Supervisory Control And Data Acquisition (SCADA) systems, wind farm controllers, etc.

PAC systems are based on three main components spread across the power grid [6]: (i) Protection functions located as close as possible to the monitored structures (e.g., line or a transformer); (ii) Control for coordinated actions by local automation/control software (e.g., in an electrical substation or DER plants); (iii) Optimization by the grid operator's control center (e.g., set of monitoring software, management systems) requiring a global macroscopic system view.

However, the possibility of massive DER integration was rarely considered during conventional PAC design schemes with limited coordination between PAC systems' three-layer hierarchy. This could lead to several cascading events triggered by faults in the High Voltage (HV) level and unwanted tripping of DER protections. For example, a recent event around London in 2019 resulted in the disconnection of approximately 1.1 million customers, where many DER generators disconnected due to underperforming protection settings and mechanisms (e.g., low voltage ride-through) [7].

1.1. Motivation

Following the energy transition paradigm, the digital transformation of the power industry is thought to 'revolutionize' its management, reliability, and efficiency [3]. As a result, more and more energy stakeholders are getting interested in implementing adaptive systems such as those offered by the Information Technology (IT) field (e.g., Virtualization Technology, Cloud/Edge Computing), with the reliability and security required for Operational Technology (OT) power assets [8]. In the particular case of PAC systems, this concerns field deployments of the numerous hardware devices (otherwise known as Intelligent Electronic Devices IEDs) embedding the functional logic and the associated information systems monitoring and operating them.

Conventional PAC systems' hardware infrastructure is currently costly to evolve (e.g., to integrate new advanced functions), maintain (e.g., during hardware failure events), and operate in face of long-term system specification uncertainties and reliability concerns [9,10]. Furthermore, deployments require significant manual and inconsistent efforts that are highly error-prone when not automatically validated.

In light of the problems facing PAC implementations, the concept of software-defined PAC systems recently gained popularity; it is the result of the convergence efforts between IT and power system communities. The idea, which was first mentioned by Lo et al. [11], can be formally defined based on [12], as *"an approach to decouple PAC software from their dedicated hardware using efficiently managed architectures supporting heterogeneous, time-deterministic protection, automation (e.g., SCADA), and control (e.g., closed- or open-loop) applications"*.

1.2. Related Work: Trends and Evolutions of Protection, Automation, and Control Systems for Smart Grids

Recent growth in communication, information, and networking technologies has led to a shift in PAC design and supported architectures. This tendency has also been observed in several previous research works reviewed in the following paragraphs. Bo et al. [13] performed a survey on protection and control evolutions in power systems covering the impacts of advancements in communication, information, and networking technologies (as presented in Figure 1). The survey addressed hybrid, wide area (regional), and local (substation-level) protection and control architectures that can be coordinated to enhance system performance. The work presented in [13] also discusses the implementation of this concept on a distributed real-time computing platform they name 'power cloud'. Despite suggesting the importance of interoperability (Defined by the International Electrotechnical Commission (IEC) as: *"The capability to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units"* [14]) and openness of the platform, Bo et al. [13] do not

discuss the integration of such platform and architectures with existing protection and control standards.

Phadke et al. [15] presented some opportunities and motivations related to the recent development of Wide Area PAC systems including: monitoring the suitability of relay characteristics, supervision of backup zones, adaptive protections, managing wide area disturbance. Similarly, the IEEE Power System Relaying Committee [16] reviewed recent advances in centralized protection and control architectures. The authors summarize the main results comparing traditional (distributed) and different centralized architectures in terms of qualitative metrics (security, interoperability) and quantitative metrics (availability, reliability, cost) with experience from a test trial.

Regarding the concept of distributed intelligence in power systems, Strasser et al. [17] surveyed the needs of future smart grids (e.g., hardware/controller levels, local/coordinated optimizations). The survey also covered the application of software technologies for power system automation and control. However, trends towards decentralization with specific implementation technology were outside the scope of [16,17].

Furthermore, Birman et al. [18] discussed the cloud computing model's suitability for smart grid applications. The topics addressed included scalability, real-time operation, consistency, fault tolerance, privacy, and security. All these aspects remain highly relevant despite the research dating back to 2011. Authors in [18] declared that a dedicated data center or private dedicated internet for power systems is not cost-beneficial enough and thus analyzed an integrated cross-sectoral solution. The concept of 'grid function virtualization' was detailed by Kruger et al. in [19] based on similar concepts developed by the telecommunication industry. However, the authors focus on examples of flexible distribution automation (e.g., state estimation) without covering trends towards protection and control in digital substations or mentioning practical feedback from the telecommunication industry's virtualization experience.

Summarizing, observations in the literature show that the desired properties of future PAC systems include: flexibility, portability, resilience, and interoperability. Typical trends are to move towards improving the operational efficiency of future power systems by leveraging the best implementation practices from the IT world (e.g., virtualization technology). However, a detailed survey on the concepts of software-defined PAC systems for power grids, covering both the academic and latest industrial research, and assessing their potentials and challenges is still missing.

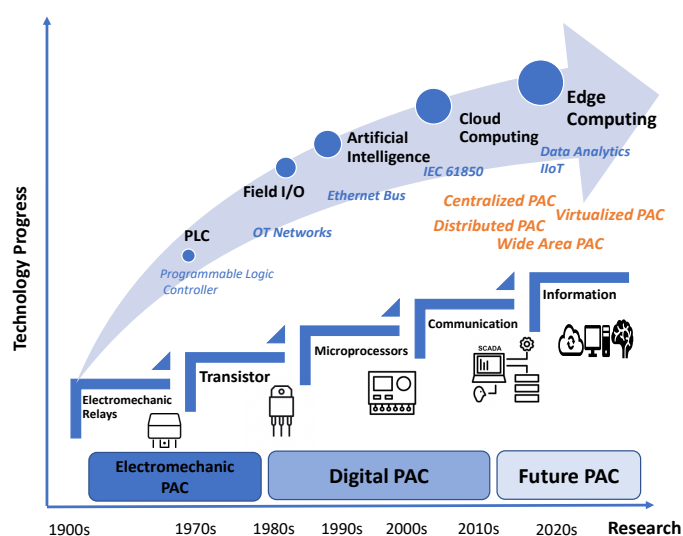


Figure 1. Evolution of PAC systems based on [13].

1.3. Contributions and Paper Organization

The main contributions of this paper are the following:

- **First:** Survey on the concepts of software-defined PAC systems for power grids clarifying its elements based on relevant academic research.
- **Second:** Survey on latest industrial research, test trials, and standardization works assessing the current maturity of software-defined PAC.
- **Third:** Lessons learned from the use of software-defined systems by telecommunication industry and their relevance for software-defined PAC systems in smart grids.
- **Fourth:** Identification of the major issues and barriers for the adoption of software-defined PAC systems.

The rest of the article is organized as follows: The current challenges related to PAC deployments in heterogeneous IEDs are highlighted in Section 2. We then introduce the communication requirements of PAC systems in Section 3, and interoperability needs (detailing IEC 61850) in Section 4. Next, we explain the concepts of ‘Cloud IEC 61850’ and software-defined PAC systems in more detail by presenting an overview of virtualization technology in Section 5, and Cloud/Edge computing architecture relevance for PAC systems in Section 6. A survey (academic, industrial, and standardization) on PAC systems deployments using virtualization technology is detailed in Section 7. An industrial feedback from the telecommunication world regarding network function virtualization and its relevance for software-defined PAC is presented in Section 8. We finally close with the main technical and industrial stakeholders’ challenges based on the current maturity of software-defined PAC concepts and present our main conclusions in Sections 9 and 10 respectively.

2. Challenges Related to the Deployment of PAC Systems in Intelligent Electronic Devices

2.1. IED Design Requirements

PAC systems are currently deployed by numerous IEDs (defined in IEC 61850-5 ED 2.0 [20] as: “a device incorporating one or more processors with the capability to execute application functions, store data locally in a memory, and exchange data with other IEDs over a digital link”). Examples include: protection relays, automation controllers, and data gateways spread across substations, power plants, and DERs. These communicating devices result from technological advancements in communication and processing power from originally electro-mechanical, electronic static/solid-state relays to today’s digital era of microprocessor-based devices (seen in Figure 1). According to [21,22], an IED should respect the requirements characterized by its governing PAC system including:

- **Reliability:** Reliability can be decomposed into (1) dependability, which is defined as the degree of assurance that a PAC system will work correctly when required; (2) security, refers to the assurance that a PAC system will operate correctly during failure for which it is not responsible.
- **Speed:** The time delay to receive, treat, and issue a response for a data stream from physical assets. The response time should be respected in order to minimize damage caused by equipment and system failures.
- **Selectivity:** In the specific case of protection functions, the ability to determine and disconnect the minimum possible parts of the network necessary for fault elimination and disconnect the minimum number of customers.
- **Redundancy:** Required at both hardware and communication network levels.
- **Interoperability:** Allows to support multi-vendor deployments.
- **Cost:** Keeping the implementation and operating costs low while achieving the PAC system goals. This is tightly related to the ‘interoperability’ feature.
- **Simplicity:** Keeping operations as straightforward as possible to recover rapidly during emergency events. This is also tightly related to the ‘interoperability’ feature.

2.2. Current IED Design Requirements Limitations

A missing, yet vital, characteristic that has yet to be considered so far is flexibility. Flexibility in engineering scope can be described as: “the ability of a system to respond to internal or external changes affecting its service, in a timely and cost-effective manner” [23]. In

the context of IEDs, research tackling this topic is limited to [24–27]. The primary use cases include: (i) reducing initial manual deployments efforts; (ii) capability to modify or add new functionalities; (iii) system recoveries in case of hardware failures or maintenance.

Moreover, the number of IEDs currently present in electricity grids is rather significant (could reach hundreds in a HV substation) with a mixture of both outdated and novel digital devices [9] (seen in Figure 2). Each IED is usually based on proprietary vendor hardware, coupled with different operating systems and firmware that require managing vendor-specific hardware configuration and maintenance tools.

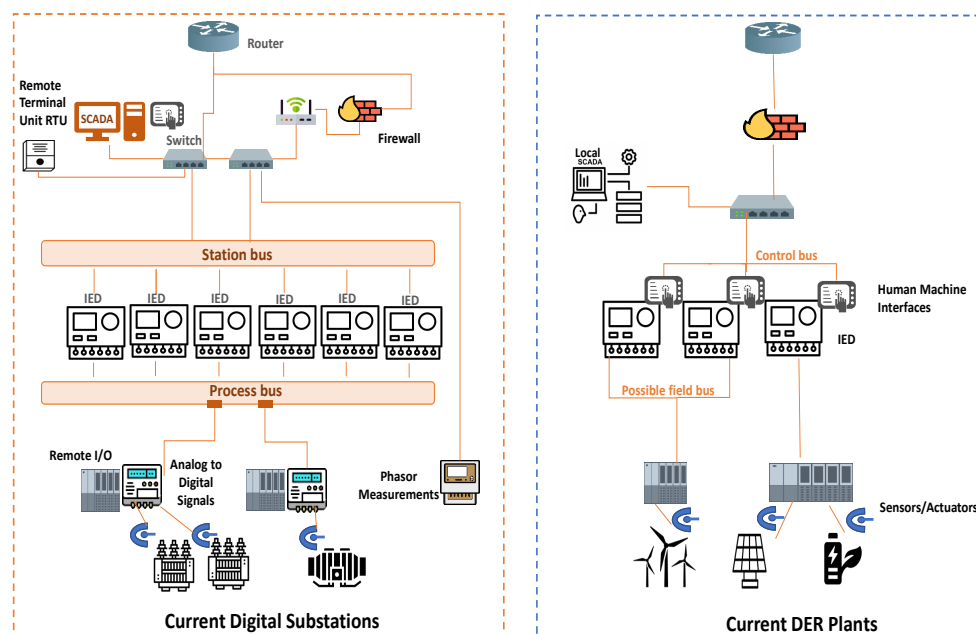


Figure 2. Current Digital Substation and DER Plant architectures based on [28,29].

This number is projected to increase further as more innovative digital solutions are developed. Active research exists on optimal placement of control devices that enhance grid reliability and reduce investment costs in the electrical infrastructure itself, as studied in [30,31]. Such complexity burdens utilities and grid operators with expensive CAPEX and OPEX for the ICT infrastructure. In some cases, this might even push them into establishing a functional dependency on a single vendor solution (hoping to reduce operational costs).

Projecting into a future with high uncertainties from renewables, the lack of agile methodologies for IEDs developments and deployments, and solutions to easily monitor, upgrade and manage the digital life cycles of IEDs introduces more operational constraints against smart grid developments. In Section 5, we will introduce the concept of virtual IEDs as a possible solution to the challenges presented. Nevertheless, we first present future PAC systems' communication requirements in the next section.

3. Communication Needs for Future PAC Systems

PAC systems process numerous data for applications that can be critical to power system operation and require ubiquitous, reliable, and real-time communication. PAC systems' communication architecture is hierarchical, governing two extremities: a central-slow level and a local-fast level.

- **Local level:** ensuring simple, safe functions based on local information acting on very fast timescales
- **Central level:** allowing coordinated actions at the scale of the whole system, with complex algorithms, slower action times, and the need to collect information from dispersed network components

The downsides of such hierarchy were studied extensively by an IEEE Smart Grid Research group [5] with a recommendation to move part of the ‘intelligent control’ from the central-regional level to an intermediate-zonal level as a future vision by 2030. This new control architecture defines stringent communication requirements to ensure robust coordination of heterogeneous smart grid components.

Assuring real-time exchange of information from different electrical grid components will permit power system actors to monitor, control, and manage grid operations more efficiently, reliably, and flexibly [32]. Wide Area Networks (WAN), Neighborhood/Field Area Network (NAN/FAN) and Local Area Networks (LAN) are basic communication categories in smart grids. The three categories are interconnected hierarchically as illustrated in Figure 3. The content of this section is summarized in Table 1, which illustrates communication requirements of various PAC applications. Many research studies have detailed the wired and wireless communication technologies cited in Table 1, including [33–36].

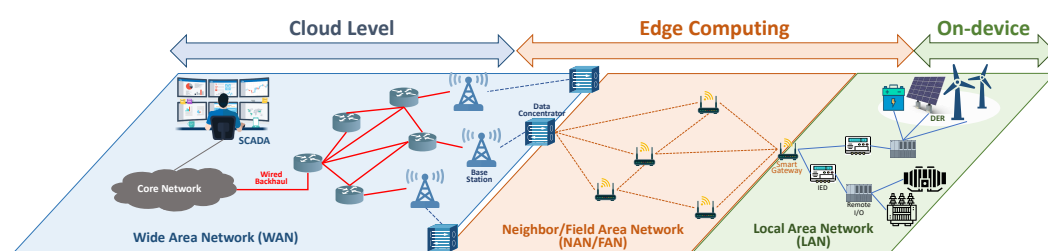


Figure 3. Communication categories interconnection [34,35,37].

Table 1. PAC application communication requirements [20,35,38–41].

Category	Communication Link		Application	Throughput	E2E Delay	Reliability
	Wired	Wireless				
LAN	Coaxial Cable, Ethernet	Bluetooth, ZigBee, Wifi, Z-wave	Transfer tripping	<10 kbps	3–10 ms	>99.99%
			GOOSE	-	4 ms	>99.99%
			Sample Value SV	80, 256 samples per 20 ms	-	>99.99%
			IED to IED interlocking	9.6–64 kbps	<10 ms	>99.99%
			IED to IED, reverse blocking	9.6–64 kbps	<10 ms	>99.99%
NAN FAN	Coaxial Cable, Ethernet, DSL, Fiber optic	ZigBee Pro, WiFi, Cellular, LPWAN, Satellite	Meter reads	10 kbps	2–10 s	>98%
			Distribution system monitoring and maintenance	10–30 kbps	<5 s	>99.5%
			Volt/VAR control	10–30 kbps	<5 s	>99.5%
			DSDR	10–30 kbps	<4 s	>99.5%
			Distribution grid FLISR	10–30 kbps	few 100 ms	>99.9%
			Optimization for distribution grids	2–5 Mbps	25–100 ms	>98%
			Protection for microgrids	-	0.1–10 s	>99%
WAN	Coaxial Cable, DSL, Fiber optic	Cellular, LPWAN, Satellite	Distribution Management System	9.6–100 kbps	0.1–2 s	>99%
			Wide-Area Situational Awareness (WASA)	600–1500 kbps	15–200 ms	>99.9%
			Outage management	56 kbps	2 s	>99.9%
			Wide-Area Monitoring PAC	10–100 kbps	<10 ms	>99.99%
			Adaptive islanding	-	<100 ms	>99.9%
			Cascading failure control	-	<5 s	>99.9%
			Wide-area voltage stability control	-	<5 s	>99.9%
			SCADA	1–10 kbps	<100 ms	>99.99%
			Phasor Measurement Unit-based state estimation	<1 Mbps	10–200 ms	>99.9%
			Dynamic state estimation	-	100 ms	>99.9%
			Fault location	<10 kbps	10 ms	>99.99%

3.1. Local Area Network

LAN-based applications of PAC systems enable data exchange between IEDs and a controller close to the power grid (for example, in the substation). A LAN can be connected to other smart grid stakeholders, such as an electric utility or third-party energy service provider, through a gateway. Since all data exchange occurs close to the power grid, the communication requirements for LAN applications of PAC systems are low

latency, high reliability, low cost, simplicity, and security. LAN networks can also allow the Distribution System Operator (DSO) to perform NAN/FAN applications close to the IEDs.

3.2. Neighborhood/Field Area Network

NAN and FAN are networks in the distribution domain, supporting the flow of information between WAN and LAN using either wireless or wired communications. They allow data collection from various components on the distribution grid for transmission to a central processing point or, in the reverse direction, to transmit commands from the central processing point to distribution grid components. NANs/FANs capacities (i.e., data rates in the range of 100 kbps–10 Mbps and a coverage up to 10 Km) enable the implementation of various services on the distribution grid [42,43] such as: smart metering, fault management, distribution grid control and automation, Fault Location, Isolation, and Service Recovery (FLISR) for distribution grids, distribution system demand response (DSDR), etc.

3.3. Wide Area Network

The Wide Area Network (WAN) offers communication resources for intelligent backbone networks, and spans long-haul distances from the control center to NAN/FAN. This supports applications such as wide-area PAC and high-frequency data transmission from many measurement points. As a result, an efficiently coordinated control is allowed, improving the stability of the power system. Moreover, managing various IEDs can enable various application, such as dynamic state estimation, distribution management system, and cascading failure control.

Wide-area PAC applications leverage information on the overall state of the system and locally collected data to limit the spread of significant disturbances [44]. These applications, compared to conventional SCADA and Energy Management (EMS) systems, reduce response time and provide higher data resolution. Real-time measurements are taken across the entire electrical network by IEDs and transmitted to control centers. Conversely, orders and commands are transmitted from control centers to IEDs [43].

WAN applications collect a large amount of data at high data rates (10 Mbps–1 Gbps) while covering a wide perimeter of the electrical network (10–100 km). Various communication means can meet the requirements of WAN applications:

- Optical fiber network: Often used due to its high capacity, security, and low latency.
- Cellular Network: Used for its wide coverage range and high data rate.
- Satellite Network: Provide backup communications through redundant communications at critical nodes of the power grid (i.e., transmission/distribution substations).

However, ensuring a good performance of the communication network is not sufficient for the requirements of PAC systems. In the next section, the importance of “interoperability” for future PAC systems is presented.

4. Interoperability Needs for Future PAC Systems

Integrating Information and Communication Technologies (ICT) in the power system promises to ensure an automated, self-healing smart grid model preventing unnecessary blackouts caused by human errors [17]. However, correctly describing and configuring the necessary data (e.g., primary asset data, IEDs) by different interoperable ICT tools becomes a tedious task. Traditional practices involve highly complex documentation to interpret grid data (mainly saved on memory registers), thus lacking inherent interoperability properties.

In order to simplify access to grid data, the IEC published the main standards semantically defined for power systems: (1) IEC 61850 for power automation; (2) power system operation and planning standards bundled in Common Information Model (CIM) (parts IEC 61970, IEC 61968, IEC 62325) [45]; (3) IEC 62056 for metering [46]. The standards aim to provide a more efficient, and reliable electrical grid where large scale information can be shared without lock-ins from proprietary vendor definitions [47].

The standardized information can then be transmitted over multiple IEDs or hosts over the communication channels with no additional mapping of essential meta-data (e.g.,

value, unit, scale). Protocols (communication rules), Semantics (data meaning), and Syntax (data format) interoperability are all indispensable for future PAC systems operations. We particularly focus on IEC 61850 standard as we generally (but not fully) limit the scope of the PAC applications considered in this research to those that can be embedded and formally modeled within IEDs (especially in digital substations and distribution grid control systems). In the next subsection, we introduce the main concepts of IEC 61850 that will be utilized and referred to in the survey conducted in Section 7.

Fundamental Components of IEC 61850

IEC 61850 is an international, well-established standard for specifying communication networks and systems in power utility automation. Its primary goals are to ensure interoperability between multiple vendor IEDs and the data exchange between physically separated subsystems performing different functionality [28]. Interoperability as per IEC 61850 is often a pre-condition to interchangeability and portability but does not automatically imply them [48]. Interchangeability includes behavioral and performance characteristics in contrast to portability which solely concerns hardware and platform level modifications [28].

Most importantly, IEC 61850 is not just a communication protocol; it also does not describe the “behavior” of IEDs. For example, how each piece of equipment should operate and be implemented to perform its expected function(s) is outside the standard’s scopes [28].

IEC 61850 consists of three main elements:

- **Data Model:** Partitioning each IED into modular object-oriented components (using Logical Devices (LD), Logical Nodes (LN), Data Objects (DO), and Data Attributes (DA)) which allows performing independent replacements [49]. The standard defines the common ‘Classes’ to specify different semantic data objects. This permits modeling and describing several electrical network information (including electrical protections, electro-technical equipment, power quality equipment, DER, etc.) homogeneously.
- **Communication:** Describing Abstract Communication Service Interfaces (ACSI) (IEC 61850-7-2 [50]), based on the functional requirements in IEC 61850-5 [20], facilitates the information exchange between IEDs, and towards external remote information systems. The standard specifies the procedures to map the abstract stack to the final communication protocol stack, including Sample Value (SV), Manufacturing Messaging Specification (MMS), and Generic Object-Oriented Substation Event (GOOSE) protocols (IEC 61850-8-1 [51]/IEC 61850-9-2 [52]).
- **Engineering and Testing:** The standard specifies engineering tools for the specification, configuration, and testing of IEDs (IEC 61850-6 [53]). The files exchanged with the vendors are in standardized digital eXtensible markup language (XML) format.

In recent years, the idea of ‘Cloud IEC 61850’ based on the cloud computing model emerged. Ferreira et al. [11] were the first to demonstrate the migration concept of the original (physical) IEC 61850 structure into a (virtual) infrastructure. The study proposes a mapping from the ‘logical’ IEC 61850 specification (LD, LNs) to a portable virtual machine environment connected to process interfaces benefiting as much as possible from traditional IEC 61850 engineering design. The study also proved the important contribution of IEC 61850 when transitioning into software-defined PAC systems.

In the next two sections, we present the principle of virtualization technology and the Cloud/Edge computing architecture for future PAC systems in relation with the concept of Cloud IEC 61850.

5. Virtualization

Virtualization, a well-established practice in the IT field, is claimed to have emerged in the late 1960s as a robust time-sharing solution for mainframe computers [54]. This breakthrough concept increased the efficiency of expensive, shared computing resources among different users. Over the years, the idea of having computing servers supporting

the simultaneous running of multiple isolated runtimes with legacy support (operating systems, libraries) grew into a necessity. This led to the wide adoption of virtualization techniques in the early 2000s, becoming a computing industry standard [54].

Virtualization uses software (represented by the virtualization hypervisor/container engine layer in Figure 4) to emulate different hardware-level functionalities and create an equivalent 'virtual' or 'software-based' computing system. A hypervisor is responsible for partitioning a single physical (host) hardware and allocating the system resources (computing, networking, storage) between the isolated partitions. The 'virtual' computing system is formally known as a 'virtual machine' or VM. Each VM encapsulates a self-contained environment with a (guest) operating system and running software applications decoupled from its underlying host. Another variation of VMs gaining interest is container technology. The main difference is that containers share the host's kernel (hence are constrained to the host operating system with less isolation) and are orchestrated by a container engine, which is more lightweight than classical VMs with better scalability support [55].

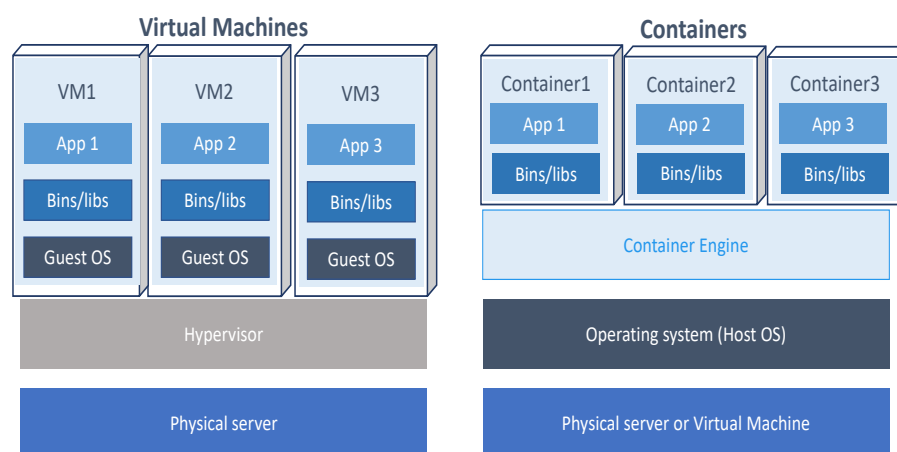


Figure 4. Generic Virtualization Architecture based on [56].

Different types of virtualization exist ranging from: desktop, server (mainly for data centers), operating system, networking, and network functions or NFV in telecommunications [57]. The multidisciplinary adoption stems from the added benefits of virtualization compared to legacy IT systems which can be summarized as [55,57]:

- Optimize compute resource usage
- Increase the flexibility of processing and storage resources
- Reducing overall deployment costs (CAPEX) by using software-based applications running on low-cost "off-the-shelf" processing equipment instead of dedicated hardware
- Reduce maintenance, operations and management (OPEX) costs through centralized remote monitoring
- Enabler of Infrastructure as a Service (IaaS) [58] and cloud computing paradigms
- Supporting legacy applications
- Disaster recovery, High availability support
- Backup, Cloning, Snapshots

Virtualization for Critical Real-Time Systems and the vIED Concept

More recently, the interest in virtualization for real-time systems gained popularity with applications in industrial control systems (with virtualized Programmable Logic Controllers PLCs). Results by [59] showed the suitability of virtualized PLC (i.e., a VM or container with a PLC software runtime) with response times in the ranges of 5–10 ms.

Interested readers can refer to the works of [29] for a state-of-the-art on virtual PLC concepts and their real-time performance with consolidated (dummy traffic) workloads.

Latest versions of VMware [60] hypervisor ESXi Real Time (RT) showed promising deterministic latency (i.e., the time difference between the actual thread wake-up and the intended wake-up time [61]) averaging at 3.5 microseconds for a total cycle time of 120 microseconds [62]. These results fit into the stringent hard RT (“*real-time system whose operation is incorrect (totally fails) if results are not produced according to specified timing requirements*”—ISO/IEC TR 23188 [63]) requirements of protection and process control applications as an upgrade from the already supported soft RT (“*real time system whose operation is degraded if results are not produced according to specified timing requirements*”—ISO/IEC TR 23188 [63]).

Similarly, a software-defined (or hereby virtualized) PAC system relies on different IEDs bundled into logical/software entities running on standardized hardware. As shown in Figure 5, a virtual IED (vIED) instance represents a VM or container with functional business logic (e.g., overvoltage protection, tap voltage regulator, or droop control algorithms) and an IEC 61850 communication stack. The physical grid data are gathered by remote I/O modules and, possibly, Merging Units (MU), which digitalize the analog signals and transmit them through Ethernet connections. The physical network adapters receive the digital data where redirection and treatment within the logical levels occur. In the next section, we introduce the concepts of Cloud/Edge computing, enabled by virtualization technology, in relevance with the software-defined PAC systems concept.

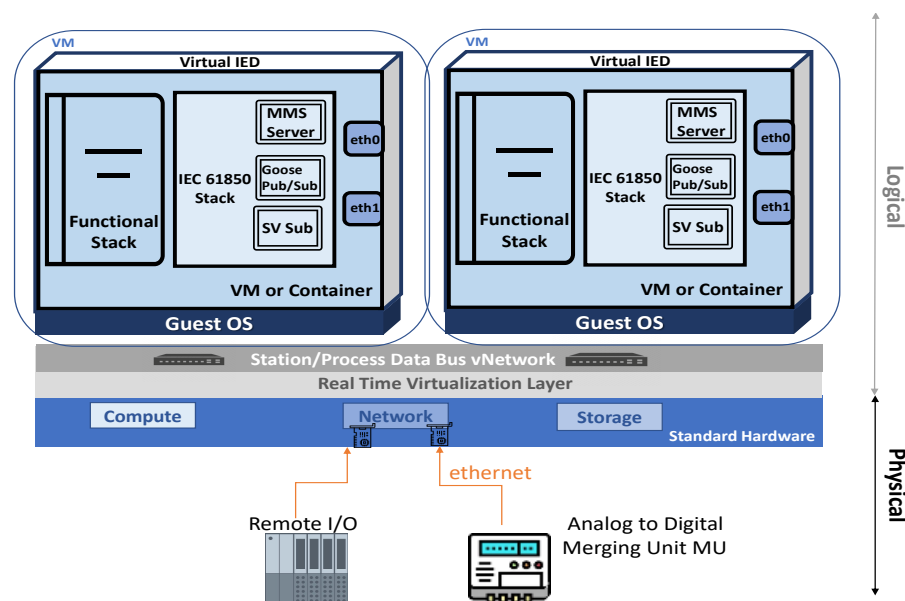


Figure 5. Virtual IED concept based on [64,65].

6. Cloud/Edge Computing Architecture for Future PAC Systems

In order to improve their operation, smart grids are integrating additional connected IEDs and sensing nodes (often Internet of Things, or IoT-based) collecting large amounts of data which become challenging to manage. In the case of critical PAC systems, traditional architectures, based on cloud computing, fail to meet processing requirements as presented in Section 3.

Data processing near devices, known as *edge computing* or *fog computing*, is a new data processing architecture where data are no longer exploited in a public or private cloud data center but rather locally in the device or a nearby gateway. By treating data as close as possible to their source (e.g., primary/secondary substation, DER plant), edge computing supports new services requiring wide bandwidth, high reactivity, and low latency while respecting data security and confidentiality. Edge computing also enables high application

availability, allowing operations with low-quality connection to the Cloud, or even in some cases with no connectivity at all (which is the case of critical PAC). Table 2 presents a comparison between cloud and edge architectures based on [66–68].

Table 2. Comparison between edge and cloud architectures based on [66–68].

Evaluation Parameter	Edge Computing Architecture	Cloud Architecture
Latency	Ensures low latency to handle real-time applications such as: monitoring frequency and verifying VAR (Voltage-Ampere Reaction) regulation to avoid power factor penalties.	Given the distance that separates the connected devices from the cloud servers, a multi-hop communication is necessary, imposing a high communication delay. This exceeds the maximum delay tolerated by some real-time applications.
Bandwidth	Thanks to data filtering and pre-processing on the edge, it would no longer be necessary to send vast amounts of non-treated data to the cloud; it would be possible to collect more information on the grid and enrich forecasting models without increasing the cost of communication service.	To ensure precise control of the grid, communicating devices (e.g., IoT based) transmit large amounts of real-time raw data to the cloud. This increases the load on the communication network, thereby creating congestion and increasing the transmission delay, the error rate, and the OPEX of the telecommunication network.
Security	PAC systems handle an increasing volume of private and sensitive information on the power grid. Data processing in the edge allows selecting which data must go through the cloud and which must remain local.	The cloud can be managed by third parties, so sending sensitive or private user data (collected by connected IoT devices) raises privacy and security concerns.
Storage	Limited	Abundant

6.1. Hierarchical Relationship between Cloud and Edge Computing for PAC Systems

As presented in Figure 6, the PAC system architecture mapped to the Cloud/Edge computing model consists of three main layers. The lower (on-device) layer represents the wide-area measurement system. It sends collected data to a processing point located at the middle (edge) layer that can be on-site or distributed throughout the communication network. The edge layer stores and analyzes the collected data to transmit corrective orders to resolve local issues. Aggregated data are then sent to the central (cloud) processing point in the upper layer, which has system-wide visibility to solve problems requiring coordination. However, edge or cloud computing system model requires extensive management and monitoring capabilities.

6.2. Management of a Fleet of vIEDs

Using the Cloud/Edge architecture to manage a fleet of virtual IEDs can help reduce deployment efforts and optimize system performance. For example, the tool can quickly deploy new virtual PAC applications on edge nodes from a central remote station with no need for on-site interventions (with a precondition that physical I/O cabling is already done). In addition, if the virtual IEDs require an upgrade (e.g., firmware, configuration files) or hardware maintenance, the application can be temporarily redeployed to a different edge node redirecting the I/O streams as required. However, the deterministic compute resource behavior and the need for robust state and time synchronization techniques are the main research points. Having introduced the different constituting elements of software-defined/virtualized PAC systems, we next present a detailed survey on this topic.

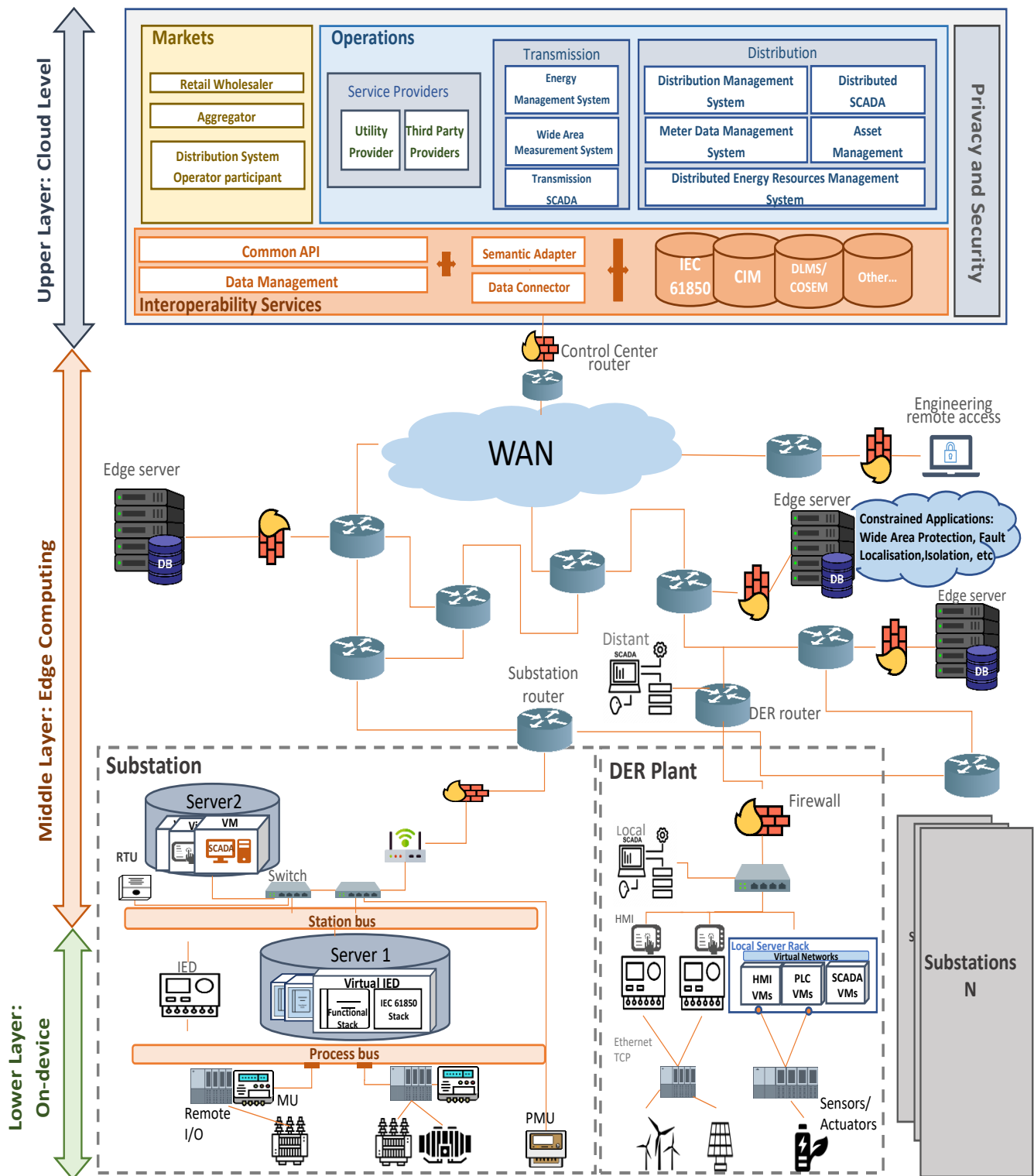


Figure 6. Cloud/Edge Computing Architecture mapped to future PAC systems in Smart Grids based on [69,70].

7. Survey on Software-Defined PAC

The survey aims to assess the maturity of software-defined/virtualized PAC systems in smart grids by analyzing: (1) the latest academic research, (2) first industrial prototypes, (3) as well as relevant standards works. For the rest of the paper, we use virtualized PAC systems and software-defined PAC systems interchangeably.

7.1. Methodology

This survey was conducted by mainly referring to Google Scholar [71] and IEEE Xplore [72] databases for all academic references. The keywords used include: software-defined PAC; software-defined smart grid; virtualized PAC; virtualized IED; cyber-physical energy system virtualization; flexible PAC; substation virtualization; Cloud IEC 61850; containerized IEC 61850. The selected research articles date from the 2010s till 2022. We neglected papers dealing purely with software-defined communication networks for power systems. Moreover, we focused on papers with case studies conforming to our definition of PAC applications and requirements (refer to Sections 1 and 3). As for the industrial references, we mainly used similar keywords aggregated with some power system vendors' names on the google search engine, which led us to some industry White Papers. Furthermore, the IEEE, IEC, and CIGRE standards' websites were used to find relevant standards based on the same keywords.

7.2. Virtualized PAC Systems Main Academic Works

A summary of previous academic works can be seen in Table 3. The criteria to distinguish the works include:

- research scope
- the use of IEC 61850
- the need for deterministic latency (Hard real-time or Soft real-time) based on the tested case study
- communication networking covered
- application domain of case study

Table 3. Academic Research Articles on virtualized PAC systems.

Reference	Research	IEC 61850	RT	Networking	Domain
Yufeng Xin et al. [73]	Concepts Only	-	-	Virtual Networking	Generic Smart Grid
Ferreira et al. [74]	Followup of [11]	Only Transfer Time Requirements (TTR)	Hard Real-Time	Open DDS	Digital Substation
Ferreira et al. [75]	Followup of [74]	Limited to Data modelling/TTR	Hard Real-Time	Open DDS	Digital Substation
Dayabhai et al. [76,77]	Architectures/ Design Considerations	-	-	-	Digital Substation
Wojtowicz et al. [78]	Concepts/Testbed	VM-Based IEC 61850 Server	Hard Real-Time	Virtual Networking	Digital Substation
Wojtowicz et al. [79]	Followup of [78]	VM-based IEC 61850 Server	Hard Real-Time	Virtual Networking	Digital Substation
Rosch et al. [65]	Concepts/Testbed	Containerized IEC 61850 Server	Soft Real-Time	SDN	Digital Substation
Rosch et al. [80]	Followup of [65]	ogy/Containerized IEC 61850 Server	Soft Real-Time	SDN	Digital Substation
Wang et al. [81]	Architecture/ Simulation	Limited to data modelling	-	-	Generic Smart Grid
Attarha, Kurger et al. [19,24,82]	Concepts/Testbed	MMS	-	-	Distribution Grid Automation
Hage Hassan et al. [83]	Concepts/ Simulation	-	-	-	Distribution Grid Automation
De Din et al. [84]	Concepts /Simulation	Proprietary data model	-	-	Distribution Grid Automation
Jablkowski et al. [85]	Testbed	-	Soft Real-Time	SDN	Digital Substations/ Distribution Grid Automation
Wang et al. [10]	Concepts/Testbed	-	-	-	Microgrids

Yufeng Xin et al. [73] initially introduced the concept of decoupling smart grid control applications from their underlying computing infrastructure back in 2011. The authors in [73] argued against the inefficiency of classical fixed-feature designs for complex smart grid application deployments. Three affected smart grid levels were recognized: sensors/

phasor measurement units (PMUs), substation, and inter-substation, which were centrally orchestrated by a broker. However, the study by [73] was purely conceptual and did not deal with interoperability considerations.

The works of Ferreira et al. [11] were followed up in [74,75], where the concept of ‘software-defined PAC systems’ made its first appearance (see Figure 7). The focus of the works in [74,75] was to test the end-to-end performance of virtualized PAC system architectures. Benchmark testing using a Data Distribution Service (DDS) middleware (simulating an IEC 61850 communication) in VMs validated performance for soft real-time PAC applications with transfer time latencies (e.g., VM to VM, Host to VM) varying from 1 to 5 ms.

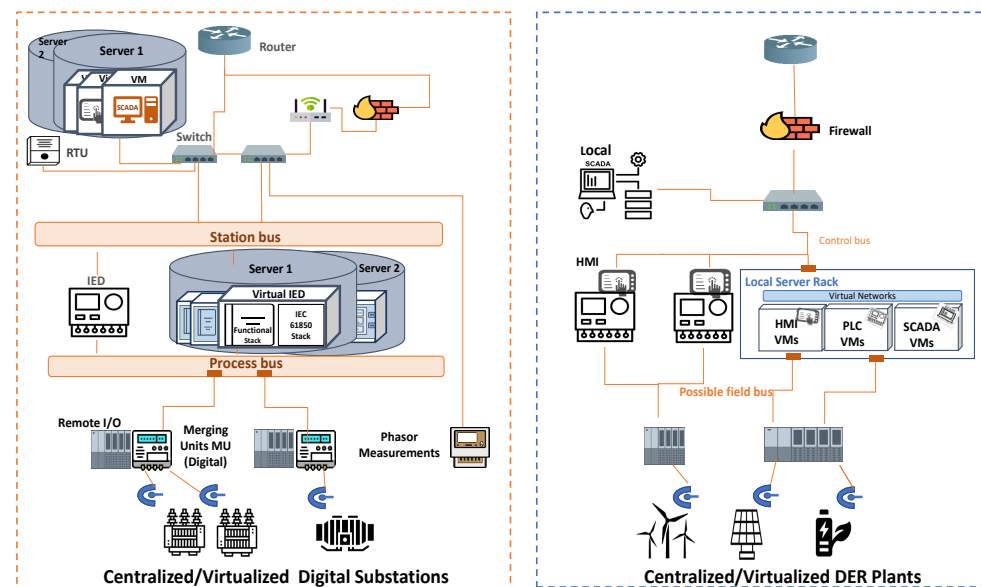


Figure 7. Possible Future Centralized/Virtualized Digital Substation and DER Plant architectures based on Table 3 references where ‘Centralized’ refers to the architecture and ‘Virtualized’ refers to the implementation.

The design considerations of a high-performance computing substation platform with support for virtualization were evaluated by Dayabhai et al. [76,77]. The analyzed areas ranged from hypervisor features (VM management, supervision, and network access), redundancy against disaster recovery scenarios, hardware specifications, and virtual networking (VLAN, vSwitch). Moreover, the authors in [76] detailed the expected industrialization and technical challenges beholding virtualized substation automation solutions with recommendations to help bridge the IT/OT technical gap and cybersecurity by design considerations. However, the study did not explicitly deal with process-level PAC system applications and was limited to station-level generic applications (e.g., Human Machine Interface (HMI), gateway, and data concentrators).

Wojtowicz et al. [78] presented the concept of an IED based on virtualization technology. Authors in [78] built a virtual environment and performed system tests on different virtual machines simulating IEC 61850 client/server services (including MMS, SV, and GOOSE). The tests in [78] focused on communication delays and time synchronization performances without simulating any particular PAC application logic. The work of [78] is continued in [79] by testing a generic overcurrent protection application subscribed to SV streams from a Merging Unit (MU). Furthermore, the environment in [79] was scaled and benchmarked to around 171 virtual machines (Linux and Windows based) running on three different physical servers. Results showed an average of 7–8 ms tripping time, validating the potential and preliminary reliability of virtualized protection systems.

The works of Rosch et al. [65] were the first to test container-based virtualization of an IEC 61850 communication network based on Software Defined Networking (SDN)

principles [86]. The authors in [65] proposed a novel co-simulation setup covering both the physical electrical grid and a realistic process network traffic (running as docker containers [87]) in the host server. The evaluation was performed on a simplified overvoltage protection algorithm and modeling of the affected latency. The criteria were primarily based on transfer times (delays) specified in IEC 61850-5. Again, the first results showed no violations of the fixed requirements in all different scenarios (averaging at around 21 ms delay).

The follow-up by [80] focuses on proposing a framework for automating the creation of containerized IEDs from existing IEC 61850 configuration files. The containerized virtual IEDs are set up after parsing the System Configuration Language (SCL) file and configuring their base image with the IEC 61850 communication services (from open source libIEC61850 [88]). Rosch et al. [80] conclude on the possibility of scaling the framework to fully represent a real substation network in the future. No particular performance (technical or qualitative) evaluations were performed in the scope of the framework testing.

Both Attarha et al. [24] and Wang et al. [81] propose a smart grid function virtualization framework inspired by the ETSI MANO [89] telecommunication architecture. Wang et al. explicitly included an IEC 61850 component in the framework to ensure interoperability. The concepts in [24] were validated by simulating the mitigation of a hardware and telecom networking anomaly thanks to a containerized coordinated voltage controller and state estimator case study. The scenarios helped demonstrate the advantages of virtual IEDs for disaster recovery. Moreover, the cybersecurity risks and threats analysis of the proposed virtualization-based smart grid architecture were later investigated in Attarha et al. [82].

Hassan et al. [83] tested flexible execution modes (centralized, distributed) for virtualized state estimators (on docker containers) to address system disturbances. Similarly, a study by De Din et al. [84] focused on a flexible distributed voltage controller (on docker containers) with a coordinated data exchange mechanism between the container nodes resolving voltage limits and assuring communication network scalability.

Another testbed was prototyped by Jablkowski et al. [85] as an open source platform based on the XEN hypervisor [90] which was optimized for cyber-physical systems. Support of the developed testbed was verified by coupling to a real-time grid simulator. A server running a virtual tap changer control received data from a phasor measurement unit through a software-defined network open switch.

Wang et al. [10] presented a software-defined control architecture for microgrids to tackle the challenges of hardware dependencies and reducing costs. The study proposed the concepts of a flexible software-defined controller with a control function library (e.g., droop, secondary, tertiary control) and a generalized orchestrated workflow for ensuring controller management. A proof-of-concept testbed for a virtual droop controller was set up where results showed no performance degradation compared to a traditional (embedded) controller. Wang et al. [10] mention the possibility of utilizing virtual machines to run the virtual controllers; however, the chosen setup was based on a single physical remote server without mentioning any data modeling aspects. Furthermore, the general orchestration workflow was not fully demonstrated in the case of secondary and tertiary controllers nor in terms of remote control management.

Summarizing, the majority of previous papers can be considered purely conceptual, non-experimental papers. This can be justified as this research area is still in its early stages, thus the need to start with proper concept definitions. Regarding the few experimental works, most focused primarily on benchmarking performance requirements (mainly as specified in IEC 61850-5) with stress tests on the telecom network to validate bottlenecks and latency. Both virtual machines and container technologies were utilized, where the latter was favored for soft real-time performances (greater than 10 ms). In general, full support for hard RT performance is still lacking due to the virtualization hypervisors' limitations, especially in containers. The IEC 61850 standard was used in most previous studies, especially for virtual protection. Moreover, the concept of orchestration tools for centralized lifecycle management was evaluated to mitigate failure events and ensure

automated disaster recovery of virtualized PAC systems. In the next section, we extend our survey and summarize the latest industrial proof of concepts in the area of virtualized PAC systems.

7.3. Virtualized PAC Systems Main Industrial Works

More recently, industrial pilots and proof of concepts have emerged in the field of virtualized PAC systems (seen in Table 4). The research aims varied from proposing reference architectures and specifications, and integrated hardware/software platform solutions.

Table 4. Industrial proofs of concepts for virtualized PAC systems.

Project Name	Lead	Scope	Virtualization Technology Used	Domain	Applications	RT
SOGNO [69]	EU/LF Energy	Reference concept of a modular, interoperable service-oriented design of data-driven distribution automation systems	Docker Kubernetes	Distributed Automation	State Estimation, Power Control, Quality, Fault Localization, Load Forecasting	Soft RT
EU projects [70,91]	EU	Re-utilizing [69]'s reference platform for virtual power plants and market based data exchanges	Docker Kubernetes [92]	Distributed Automation	Voltage, Frequency control	Soft RT
SEAPATH [93]	LF Energy	Reference concept/design and real time platform for industrial electricity system operators to execute their virtualized applications for automation and protection.	KVM [94]	Digital Substation	-	Hard RT
Centralized Substation Platform [95]	EPRI	Virtual computing platform for electric substations to support SCADA and management applications while meeting cybersecurity requirements	-	Digital Substation	-	-
Grid Management platform common design architecture GMP [96]	Dell, Intel, VMWare	Virtual computing platform running in edge substation or control center supporting legacy applications and security standards	VMware	Digital Substation, Distribution Grid Automation	-	-
Edge for Smart Secondary Substations [97]	Consortium	Reference architecture design for open, interoperable standards-based platform for digital secondary substations	-	Digital Substation	Secondary Substation Automation	Soft RT
Virtual Protection Relay (VPR) [98]	Kalkitech, Intel	VPR reference architecture hosting protection applications to benchmark against legacy applications and a framework to support onboarding of VPR	VMware	Digital Substation	Protection	Hard RT

A docker-based platform for containerized distribution grid automation domain was developed as part of the European project SOGNO [69], now part of the open-source Linux

Foundation (LF) Energy. The SOGNO project demonstrated the benefits of microservices, a lightweight, scalable software development architecture [99,100], for distribution system operators' control center information systems. Several advanced soft RT functionalities (e.g., LV state estimator, fault isolation, power control) were validated in different field trials. The architecture proposed in [69] also envisioned an interoperability layer, with IEC 61850 protocol gateways and support of grid topology based on CIM data. Several European projects utilized the SOGNO reference architecture as part of their advanced smart grid platform implementations (e.g., EdgeFlex [70], Platoon [91]). However, SOGNO does not directly deal with virtualized IEDs at process levels or within substation domains.

Another project led by LF Energy, the SEAPATH project [93], mainly focused on providing a reference hard real-time platform running virtualized substation automation systems (and beyond). KVM [94], an open-source hypervisor, forms the base of the platform with docker support, advanced data processing technologies (e.g., Data Plane Development Kit DPDK [101]), and several integrated administration and security services. Testing the availability, performance, and reliability of the platform and virtualized automation applications based on lab measurements (with IEC 61850 communications) are within the envisioned scope of SEAPATH.

The Electric Power Research Institute (EPRI) surveyed specific considerations for centralized digital substation platforms [95]. The areas covered among others were cybersecurity support, intrusion detection, access control, network support, fault tolerance, firmware management, and scalability. A collaboration between Dell, Intel, and VMware aims to develop the proper hardware servers responding to the needs of centralized/virtualized substation PAC systems and power system operators' modernized control centers [96].

Recently, an international consortium of utilities, distribution grid operators, integrators, and IT technology experts was developed as part of the 'Edge for Smart Secondary Substations' project [97]. This consortium focuses on specifying reference technical hardware/software requirements and end-to-end application management for proactive secondary substations.

The Virtual Protection Relay (VPR) solution for hard RT requirements in substation automation was jointly developed by Intel, and Kalkitech [98]. The research analyzed response time (referring to IEC 61850 requirements) against different network configurations and resource allocations with parameter sensitivity studies. Furthermore, virtual networking redundancy and time synchronization requirements were discussed. Promising results were shown with time delays equivalent to existing protection systems.

Moreover, industrial products specialized in providing hardware-level centralization and virtualization of IEDs are being researched by leading vendors [102–104]. The interest in a microservice architecture (container-based) for substation protection applications was analyzed by [105]. Preliminary results showed multiple practical issues (mainly compatibility, resources, dependencies, and overhead) which made the transition to containerized protection non-straightforward. Industrial standardized servers (compliant with IEC 61850-3 [106]) that can run virtualized IEDs have emerged, yet still lack proper installation and operation frameworks.

Summarizing, the current maturity of industry solutions for virtualized PAC systems is at its early stages (mainly through pilots and proofs of concept). The areas covered both deterministic latency (hard RT protection and control) as well as soft RT (mainly automation and SCADA, secondary substations). Some market-ready solutions exist but are limited to specific vendor implementations and hence do not fully harvest the advantages of virtualized PAC systems. The tool interfaces remain proprietary and easy to use frameworks are still lacking. Moreover, the maintainability and support of the platform itself and the responsibilities of the involved stakeholders (e.g., grid operators, virtualization platform maintainers, certification bodies) have yet to be explicitly addressed. Another observation concerns the proposals of different 'reference' architectures within these projects. Unless these diverse 'references' somehow converge, a significant complexity will be added for future PAC systems deployments. In the next section, we extend

our survey and summarize the latest standardization efforts in the area of virtualized PAC systems.

7.4. Virtualized PAC Systems Main Standardization Groups Works

Recently, many standardization groups in the research area of future PAC system developments have been emerging, driven by the rising industry interest (as seen in Table 5). The working groups mainly from IEC, IEEE, and CIGRE aim to cover specific digital substation requirements and architectures, as well as IT/OT convergence specifications relevant for future PAC systems. We observe involvement from power system experts, distribution and transmission system operators, software vendor providers, and IT experts within these working groups.

It would be in the best interest of the power community if the standardization works highly consider feedback from the aforementioned industries and pilot projects in Section 7. Moreover, reaching a comprehensive or relative convergence between all standardization parties is key to avoiding closed visions creating added complexity. Having presented our comprehensive survey spanning academic, industrial, and standards works, in the next Section 8, the survey's domain is extended. We share a summary of the telecommunication industry's experience with a concept that we believe is relevant for virtualized PAC systems.

Table 5. Standards Groups in relation with virtualized PAC systems.

Origin	Research Scope	Type	Publishing
IEEE PSCC P21 [107]	System requirements and architecture for supporting the virtualization of substation protection and control applications	Study Group/ Technical Report	2022
IEEE PSCC P11 [107]	Cloud Computing, uses and Requirements of Electric Power Utilities	Task Force	-
CIGRE B5.60 [108]	Protection, Automation, and Control Architectures with Functionality independent of hardware	Working Group/ Technical Report	2022
CIGRE B5.73 [109]	Experiences and Trends related to Protection Automation and Control Systems Functional Integration	Working Group/ Technical Report	2023
CIGRE D2.43 [110]	Enabling software defined networking for electric power utilities	Working Group/ Technical Brochure	2022
CIGRE B5.77 [111]	Requirements for Information Technologies (IT) and Operational Technology (OT) managed of Protection, Automation, and Control Systems (PAC systems)	Working Group/ Technical Report	2025
ISO/IEC JTC1 WG24 [112]	IIoT and digital twin applications in power system's management	Joint WG with IEC TC 57	-
ISO/IEC TR 23188/IEC TS 23167 [63]	Information technology — Cloud computing — Edge computing landscape/Common technologies and techniques	Standard	2020

8. Relevance of Telecommunication Industry Experience in Network Function Virtualization When Virtualizing PAC Systems

In early 2012, the European Telecommunications Standards Institute (ETSI) group first released a white paper explaining the next paradigm shift in the telecommunication world [113]. The paper unveiled the concept of "Network Function Virtualization" shortly known as NFV. The 'revolutionary' idea came after telecom network operators became bombarded with hundreds of different single-function hardware they had to maintain. Each network vendor provided a dedicated hardware appliance embedded with a network application (e.g., router, firewall, radio access nodes), resulting in complex manual efforts with high costs. Consequently, the basic idea behind NFV was to uncouple network application hardware dependencies by using IT virtualization practices. The previously

hardware-tied network functions would be run inside the well-established IT virtual machines on top of standardized commodity hardware. The benefits of NFV according to [113–115] included:

- increased flexibility over network deployments
- CAPEX/OPEX savings
- faster innovation cycles (time to market)
- simpler integration and controllability over network operations (orchestration)

The NFV community was closely followed by ETSI, which established different working group areas (from virtualization infrastructure, management and orchestration, reliability and availability, as well as security and ecosystem strategies) with over 100 s of specification documents already published [116]. ETSI subsequently proposed a reference architectural framework for NFV to homogenize solutions that can be reused by industry [117].

Nevertheless, this section highlights the latest market observations and industry implementation experiences of NFV that might be of high relevance to consider for virtualized PAC systems. The resemblances are the implementation choices based on IT virtualization for hardware/software decoupling and the promised long-term benefits and opportunities. A recent industry survey summarized in Table 6 depicted some of the most common challenges faced by network operators when switching to NFV architectures. Despite a relative technology readiness and maturity, several non-technical factors led to the slow evolution of NFV and prevented it from becoming mainstream today [118,119].

Table 6. Challenges of Network Function Virtualization NFV as identified by network operators in [120] survey that are relevant for virtualized PAC systems. ✓ = confirmed, - = not applicable

Identified Challenge/Enterprise	AT & T	China Mobile	DTelecom	Orange	Verizon	Vodafone	Rautken
Lack IT Skills	✓	-	✓	-	-	-	-
Performance Differences	-	✓	-	-	-	-	-
Integrating Multi-Vendor Solutions	-	✓	-	✓	-	-	-
Lacking Integration Standards/Interoperability	-	-	-	✓	✓	✓	-
Too Complex Architecture	-	-	✓	-	✓	-	-
Support for Orchestration/Automation	-	-	✓	✓	-	✓	-
Move to Cloud-Native (containers)	-	-	✓	✓	✓	✓	✓
Vendor Support	✓	-	-	-	✓	-	✓
Need Support for Open Collaborations	✓	-	✓	✓	-	-	-

In general, the issues faced ranged from modest CAPEX and OPEX reductions, which were offset by high software licensing costs. A typical reasoning was given by [118] as: “The device vendors say that the cost and value of their product are more tied into things such as the R&D for the software and support of software-hosted features than it is in the ‘hardware’ boxes”. Furthermore, finding suitable business cases to justify significant upfront investment costs was problematic [118,121]. Given the long-established critical nature of networks, finding the right balance between legacy and NFV adoption was also a main challenge.

Moreover, onboarding of NFV was a rather difficult process due to lacking common integration frameworks and Application Programming Interfaces (APIs) (e.g., support connection to SDN/Core controllers) [121,122]. This resulted in numerous customized approaches locking operators into vendor-specific virtualization platforms. Inconsistencies in performance and compliance testing validations, especially in the case of orchestration, were observed. With limited metrics standardization, cross-vendor and cross-architecture results become difficult to analyze [123].

We expect that most of the NFV adoption issues mentioned in this section, especially regarding interoperability, software licensing, onboarding, and deployment efforts will also be faced in the case of software-defined PAC architectures. However, by having clearly defined objectives, the power industry can at least avoid some hurdles and prevent unnecessary operational issues thanks to the lessons learned from the telecommunication

world experience in NFV. In the next section, we discuss the future challenges for software-defined PAC systems' adoption in more detail.

9. Challenges for Software-Defined PAC Systems Adoption

Based on the surveys conducted in the previous sections, we expect the following future challenges awaiting software-defined PAC systems. These include both technical, as well as industry stakeholders challenges before widespread adoption takes place.

9.1. Technical Challenges

- **Interoperability:** In the case of software-defined systems, we can see that communication interoperability will no longer be sufficient; Rather, interoperability at software development levels is required (architectures, APIs). New standardization efforts, as presented in Section 7.4, are the first steps in this direction. However, it is also necessary to have proper engineering tools and frameworks that abstract the underlying technology platform running the (cross-vendor) virtualized IEDs. For example, a hardware descriptor and networking model with an IEC 61850 configuration file (including functional setting parametrization) can describe the virtual IED needs independently of a specific hypervisor or container engine. Furthermore, as internal communication (on the same physical server) between the virtual IEDs replaces physical GOOSE messaging, standard API developments to access a shared memory or a shared GOOSE service need to be considered [98].
- **Determinism, Networking, and Time Synchronization:** Mission-critical hard RT applications (e.g., substations protection and control and distribution automation) will fail if maximum delay requirements are not respected. Currently, state-of-the-art performances are limited to 5–20 ms response times. Support for hard real-time deterministic virtualization is still not fully mature yet. Advancements in last-level cache, time sensitive networking [124], and deterministic networking are possible enablers [29]. Moreover, support is needed for deterministic live VM migration [125], and synchronized redundant virtual network interface cards (e.g., parallel redundancy protocol and single root I/O virtualization (SR-IOV)) [98]. Avoiding networking bottlenecks, especially for consolidated workloads with different resource priority requirements, is essential. This shall allow benefiting from the high availability and disaster recovery mechanisms offered by virtualization for real-time systems.
- **Reliability & Availability:** Virtualized PAC systems are composed of numerous sub-components between the physical power asset and the logical environment controlling the asset. Traditional failure risks are at the physical networks (switches), I/O modules, and server operating systems. vPAC systems include failure risks from the hypervisor or container engine as well as virtual networking cards in internal networks. Extensive reliability, including all sub-components, must be studied to ensure robustness equivalent to physical PAC systems.
- **Scalability:** Solution performance at scale has both technical (networking bottlenecks, determinism) and economic (hardware footprint reductions) implications that need to be considered. Examples of testing include scale-ups of LD/LN IEC 61850 data model per VM/container and its effect on performance, especially in the case of GOOSE and SV.
- **Security:** Need for security by design and intrusion detection studies. This also includes users' authentication, secure protocols (Transport Layer Security TLS certificates, De-Militarized Zones DMZ), data at rest encryption, and isolation [82].

9.2. Industry Stakeholders Challenges

- **Brownfield Implementations:** Addition to existing legacy systems is an important consideration. It is necessary to develop new tools supporting software-defined PAC systems with an interface that can be integrated within legacy system aspects (e.g., built

upon IEC engineering tools [53]). This will enable the developed frameworks to better co-exist within conventional systems and reduce integration and transition efforts.

- **Solutions Maturity:** Uncertainties in technology/IT-based solutions that are constantly evolving (at a much faster pace than PAC evolution) can impact the final maturity. For example, by the time a solution based on virtualization technology is mature enough for power experts to use, a newer IT technology may be released, making the previous solution possibly obsolete or less maintained. Furthermore, the software developed needs to operate physical power grid assets that have lifetimes of over 50 years.
- **Certified Solutions:** Availability of market-ready solutions by IT and OT vendors have to be certified and tested for performance and compliance with standards (security, hardware, software, etc.). Certificates provided by IEC 61850 currently exist for the full IED (hardware/software product) and not the software function individually. It would be interesting to test individual virtualized IEDs and their certified performance with standardized testing setups; otherwise, bench-marking performances on cross-platforms becomes cumbersome.
- **Cost Constraints:** Investment studies should focus on long-term benefits (compared to current IED lifecycles). Moreover, some specific cost considerations include: the electrical consumption of hardware servers running the virtualized IEDs, their backup battery systems, costs of digital stand-alone merging units, and remote Ethernet input/output modules. In general, identifying integration costs is non-straightforward and highly dependent on the specific case study, the equipment deployed, and the required support level. Moreover, cost-benefits vs. reliability studies are further needed.
- **Integrating new IT Actors and defining responsibilities:** Need for regulations, mind-set change, clear responsibility scope, and new IT skills in the PAC stakeholder environment will be necessary. These shall be one of the challenges that will need the longest time to set place.

10. Conclusions

In this paper, we explained the concepts of software-defined PAC systems and performed a survey to assess the current academic and industrial maturity of this emerging set of technologies. We started by detailing the trends in PAC systems developments (at both hardware and software levels) motivated by the current problems faced including: (1) deployment time and costly efforts, (2) complexity of system upgrades lacking flexibility, (3) as well as interoperability (focusing on IEC 61850). IT virtualization and cloud/edge computing paradigms were mapped to PAC systems' communication and operational needs, and the virtual IED concept was detailed.

Current state-of-the-art shows that software-defined PAC systems have a promising potential that can be further exploited for the needs of future PAC and smart grid developments. It was observed that such a concept is no longer completely burdened by technology constraints (e.g., insufficient computational capacity, and networking performance). The potential offered by virtualized PAC has been demonstrated beyond theoretical designs in the case of multiple simulation platforms and industrial proof of concepts.

Performances showed compliance with the critical time requirements of PAC systems (between 5 ms to 20 ms) showcasing early stages of maturity especially in the case of soft real-time. As for hard real-time (e.g., for protection or process control), progress to overcome the deterministic latency hurdles, mainly at the software virtualization layer, is still needed before attaining full maturity levels. A few of the demonstration project's developments have been shared as open-source software allowing interested researchers and developers to rapidly adopt, test, and provide improvements in the area of virtualized PAC frameworks.

As with most technology solutions, such a concept is not a 'one size fits all' solution. It is thus important to first start with the specific power system and PAC system development needs which can be mapped to what the technology offers; the transition can then be

justified by the economic, reliability, and operational gains provided. However, as observed in Section 9, the transition is not straightforward. It requires significant upfront efforts to first overcome the gaps for converged IT/OT systems and, eventually, respond to the initial problems of traditional PAC deployments (Section 2). Moreover, from Section 8, it can be concluded that the main hurdles against industry adoption for virtualized systems are the stakeholders (involved in PAC exploitation) and interoperability challenges. Therefore, standardizations following an agile and dynamic approach in the areas of virtual IED software developments and deployments, configurations tools, APIs, as well as performance benchmarking and compliance testing are essential enablers.

The power grid operation is experiencing a major transformation by the advent of DERs, the multiplication of actors involved, new protection schemas, and cyber-security requirements. PAC systems must be able to adapt more dynamically in response to such changes. Therefore, grid modernization efforts in the area of software-defined PAC can help respond to the needs of a more resilient and efficient future power system.

Author Contributions: Conceptualization, N.K. and M.O.N.B.; Methodology, N.K. and M.O.N.B.; Formal Analysis, N.K. and M.O.N.B.; Writing—original draft preparation, N.K. and M.O.N.B.; Review and Editing, N.K., M.O.N.B., M.G., L.R.C., J.C., T.C., V.A. and H.M.; Supervision, M.G., L.R.C., J.C., T.C., V.A. and H.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research has received funding from the European Union’s Horizon 2020 research and innovation programme under the InnoCyPES project (Innovative tools for Cyber Physical Energy Systems) and the Marie Skłodowska-Curie grant agreement No 956433. H. Morais was partially funded by Portuguese national funds through Fundação para a Ciência e a Tecnologia (FCT) with reference UIDB/50021/2020.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to acknowledge the research engineer colleagues at EDF R&D group (control and automation of smart grids) for their help with IEC 61850 concepts and real life projects experience with the standard. We thank B. Hage Hassan for the discussion regarding her work on grid services virtualization. Finally, we acknowledge P. Khajuria for sharing his industrial experience and journey in PAC system virtualization in power grids as well as discussing the main standardization challenges in this area.

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

References

1. Allgöwer, F.; Sousa, J.; Kapinski, J.; Mosterman, P.; Oehlerking, J.; Panciatici, P.; Prandini, M.; Rajhans, A.; Tabuada, P.; Wenzelburger, P. Position paper on the challenges posed by modern applications to cyber-physical systems theory. *Nonlinear Anal.* **2019**, *34*, 147–165. [[CrossRef](#)]
2. Cao, J.; Yang, M. Energy internet—towards smart grid 2.0. In Proceedings of the 2013 Fourth International Conference on Networking and Distributed Computing, Los Angeles, CA, USA, 21–24 December 2013; pp. 105–110.
3. ENTSO-E. The Cyber Physical System for the Energy Transition Digitalisation Challenges, Opportunities and Projects from TSOs and ENTSO-E 2019. Report 2019. Available online: https://eepublicdownloads.entsoe.eu/clean-documents/Publications/Positionpapersandreports/digital_report_2019.pdf (accessed on 7 December 2022).
4. Kafle, Y.; Mahmud, K.; Morsalin, S.; Town, G. Towards an internet of energy. In Proceedings of the 2016 IEEE International Conference on Power System Technology (POWERCON), Wollongong, Australia, 28 September–1 October 2016; pp. 1–6.
5. Annaswamy, A.M. Institute of Electrical and Electronics Engineers; IEEE Standards Association. In *IEEE Vision for Smart Grid Controls: 2030 and Beyond*; Institute of Electrical and Electronics Engineers: New York, NY, USA, 2013. OCLC: 861074253.
6. CAP R&D FEUILLE DE ROUTE R&D 2021/2024; RTE Report; France’s Transmission System Operator 2021. Available online: https://assets.rte-france.com/prod/public/2021-10/RTE-Feuille_route_RD_2021-2024.pdf (accessed on 7 December 2022).
7. Investigation into 9 August 2019 Power Outage. Available online: <https://www.ofgem.gov.uk/publications/investigation-9-august-2019-power-outage> (accessed on 7 December 2022).
8. Power Sector to Spend \$5 Billion on Software by 2025. Available online: <https://about.bnef.com/blog/power-sector-to-spend-5-billion-on-software-by-2025/> (accessed on 2 September 2022).
9. Khajuria, P.; Samara-Rubio, D. *Power of Infrastructure Modernization*; Intel Corporation 2021. Available online: <https://gridwise.org/wp-content/uploads/2021/09/Power-of-Infrastructure-Modernization-Ebook.pdf> (accessed on 2 September 2022).

10. Wang, L.; Qin, Y.; Tang, Z.; Zhang, P. Software-Defined Microgrid Control: The Genesis of Decoupled Cyber-Physical Microgrids. *IEEE Open Access J. Power Energy* **2020**, *7*, 173–182. [[CrossRef](#)]
11. Lo, T.B.; Mendes, M.F.; Samaniego, H.A.L.; Silva De Oliveira, R. Cloud IEC 61850: Architecture and Integration of Electrical Automation Systems. In Proceedings of the 2014 Brazilian Symposium on Computing Systems Engineering, Manaus, Brazil, 3–7 November 2014; pp. 13–18. [[CrossRef](#)]
12. IEEE PSCC Subcommittee Study Group Meeting Minutes: “System Architectures Supporting the Virtualization of Substation Protection and Control Applications”. Available online: <https://site.ieee.org/pes-pscc/files/2022/07/SG-P21-Meeting-Minutes-2022-01-10.pdf> (accessed on 3 November 2022).
13. Bo, Z.Q.; Lin, X.N.; Wang, Q.P.; Yi, Y.H.; Zhou, F.Q. Developments of power system protection and control. *Prot. Control Mod. Power Syst.* **2016**, *1*, 7. [[CrossRef](#)]
14. ISO. *International Technology for Learning, Education, and Training*; International Electrotechnical Commission Standard: Geneva, Switzerland, 2003.
15. Phadke, A.G.; Wall, P.; Ding, L.; Terzija, V. Improving the performance of power system protection using wide area monitoring systems. *J. Mod. Power Syst. Clean Energy* **2016**, *4*, 319–331. [[CrossRef](#)]
16. IEEE. PSRC “Advancements in Centralized Protection and Control Within a Substation”. *IEEE Trans. Power Deliv.* **2016**, *31*, 1945–1952. [[CrossRef](#)]
17. Strasser, T.; Andren, F.; Kathan, J.; Cecati, C.; Buccella, C.; Siano, P.; Leitao, P.; Zhabelova, G.; Vyatkin, V.; Vrba, P.; et al. A Review of Architectures and Concepts for Intelligence in Future Electric Energy Systems. *IEEE Trans. Ind. Electron.* **2015**, *62*, 2424–2438. [[CrossRef](#)]
18. Birman, K.P.; Ganesh, L.; van Renesse, R. Running Smart Grid Control Software on Cloud Computing Architectures. In *Workshop Computational Needs for the Next Generation Electric Grid*; Cornell University: Ithaca, NY, USA, 2011.
19. Kruger, C.; Narayan, A.; Castro, F.; Hage Hassan, B.; Attarha, S.; Babazadeh, D.; Lehnhoff, S. Real-time Test Platform for Enabling Grid Service Virtualisation in Cyber Physical Energy System. In Proceedings of the 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Vienna, Austria, 8–11 September 2020; pp. 109–116. [[CrossRef](#)]
20. IEC 61850-5; Communication Networks and Systems for Power Utility Automation—Part 5: Communication Requirements for Functions and Device Models. International Electrotechnical Commission: Geneva, Switzerland, 2013.
21. Blackburn, J.L.; Domin, T.J. *Protective Relaying: Principles and Applications*; CRC Press: Boca Raton, FL, USA, 2014; p. 639.
22. Gers, J.M.; Holmes, E. *Protection of Electricity Distribution Networks*, 2nd ed.; Institution of Electrical Engineers: London, UK, 2004.
23. Wikipedia: Flexibility. Available online: [https://en.wikipedia.org/wiki/Flexibility_\(engineering\)](https://en.wikipedia.org/wiki/Flexibility_(engineering)) (accessed on 1 September 2022).
24. Attarha, S.; Narayan, A.; Hage Hassan, B.; Krüger, C.; Castro, F.; Babazadeh, D.; Lehnhoff, S. Virtualization Management Concept for Flexible and Fault-Tolerant Smart Grid Service Provision. *Energies* **2020**, *13*, 2196. [[CrossRef](#)]
25. Strasser, T.; Andren, F.; Lehmann, F.; Stifter, M.; Palensky, P. Online Reconfigurable Control Software for IEDs. *IEEE Trans. Ind. Informatics* **2013**, *9*, 1455–1465. [[CrossRef](#)]
26. Zavoda, F.; Abbey, C.; Brissette, Y. The ideal IED for smart distribution applications. In Proceedings of the 2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies, Manchester, UK, 5–7 December 2011; pp. 1–5. [[CrossRef](#)]
27. Gruner, S.; Malakuti, S.; Schmitt, J.; Terzimehic, T.; Wenger, M.; Elfaham, H. Alternatives for Flexible Deployment Architectures in Industrial Automation Systems. In Proceedings of the 2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA), Torino, Italy, 4–7 September 2018; pp. 35–42. [[CrossRef](#)]
28. IEC 61850-7-1; Communication Networks and Systems for Power Utility Automation—Part 7-1: Basic Communication Structure—Principles and Models. International Electrotechnical Commission: Geneva, Switzerland, 2011. OCLC: 861074253.
29. Elchuev, T. Implementation of a Consolidated Virtual Industrial Control System. Master’s Thesis, Technical University of Munich, Munich, Germany, 2022.
30. Armendáriz, M.; Paridari, K.; Wallin, E.; Nordström, L. Comparative study of optimal controller placement considering uncertainty in PV growth and distribution grid expansion. *Electr. Power Syst. Res.* **2018**, *155*, 48–57. [[CrossRef](#)]
31. Goyel, H.; Swarup, K.S. Cyber-Physical System Enabled Smart Grid Based Optimal Controller placement. In Proceedings of the 2020 21st National Power Systems Conference (NPSC), Gandhinagar, India, 17–19 December 2020; pp. 1–6. [[CrossRef](#)]
32. Gungor, V.C.; Sahin, D.; Kocak, T.; Ergut, S.; Buccella, C.; Cecati, C.; Hancke, G.P. Smart Grid Technologies: Communication Technologies and Standards. *IEEE Trans. Ind. Inform.* **2011**, *7*, 529–539. [[CrossRef](#)]
33. Shaukat, N.; Ali, S.; Mehmood, C.; Khan, B.; Jawad, M.; Farid, U.; Ullah, Z.; Anwar, S.; Majid, M. A survey on consumers empowerment, communication technologies, and renewable generation penetration within Smart Grid. *Renew. Sustain. Energy Rev.* **2018**, *81*, 1453–1475. [[CrossRef](#)]
34. Alam, S.; Sohail, M.F.; Ghauri, S.A.; Qureshi, I.; Aqdas, N. Cognitive radio based smart grid communication network. *Renew. Sustain. Energy Rev.* **2017**, *72*, 535–548. [[CrossRef](#)]
35. Kuzlu, M.; Pipattanasomporn, M.; Rahman, S. Communication network requirements for major smart grid applications in HAN, NAN and WAN. *Comput. Netw.* **2014**, *67*, 74–88. [[CrossRef](#)]
36. Usman, A.; Shami, S.H. Evolution of communication technologies for smart grid applications. *Renew. Sustain. Energy Rev.* **2013**, *19*, 191–199. [[CrossRef](#)]

37. Yu, R.; Zhang, Y.; Gjessing, S.; Yuen, C.; Xie, S.; Guizani, M. Cognitive radio based hierarchical communications infrastructure for smart grid. *IEEE Netw.* **2011**, *25*, 6–14. [[CrossRef](#)]
38. Al-Ali, A.R.; Aburukba, R. Role of Internet of Things in the Smart Grid Technology. *J. Comput. Commun.* **2015**, *3*, 229–233. [[CrossRef](#)]
39. Tightiz, L.; Yang, H. A Comprehensive Review on IoT Protocols' Features in Smart Grid Communication. *Energies* **2020**, *13*, 2762. [[CrossRef](#)]
40. Faheem, M.; Shah, S.; Butt, R.; Raza, B.; Anwar, M.; Ashraf, M.; Ngadi, M.; Gungor, V. Smart grid communication and information technologies in the perspective of Industry 4.0: Opportunities and challenges. *Comput. Sci. Rev.* **2018**, *30*, 1–30. doi: 10.1016/j.cosrev.2018.08.001. [[CrossRef](#)]
41. IEC 61850-90-12; Communication Networks and Systems for Power Utility Automation—Part 90-12: Wide Area Network Engineering Guidelines. International Electrotechnical Commission: Geneva, Switzerland, 2020. OCLC: 861074253.
42. Lo, C.H.; Ansari, N. The Progressive Smart Grid System from Both Power and Communications Aspects. *Commun. Surv. Tutorials* **2012**, *14*, 1–23. [[CrossRef](#)]
43. Wang, W.; Xu, Y.; Khanna, M. A survey on the communication architectures in smart grid. *Comput. Netw.* **2011**, *55*, 3604–3629. [[CrossRef](#)]
44. Terzija, V.; Valverde, G.; Cai, D.; Regulski, P.; Madani, V.; Fitch, J.; Skok, S.; Begovic, M.M.; Phadke, A. Wide-Area Monitoring, Protection, and Control of Future Electric Power Networks. *Proc. IEEE* **2011**, *99*, 80–93. [[CrossRef](#)]
45. Uslar, M.; Specht, M.; Rohjans, S.; Trefke, J.; Gonzalez Vazquez, J.M. *The Common Information Model CIM: IEC 61968/61970 and 62325—A Practical Introduction to the CIM*; Springer: Berlin/Heidelberg, Germany, 2012; Volume 66. [[CrossRef](#)]
46. *Smart Grid Coordination Group Smart Grid Reference Architecture*; CEN-CENELEC-ETSI Smart Grid Coordination Group 2012. Available online: https://www.cencenelec.eu/media/CEN-CENELEC/AreasOfWork/CEN-CENELEC_Topics/SmartGridsandMeters/SmartGrids/reference_architecture_smartgrids.pdf (accessed on 13 September 2022).
47. Schwarz, K.; Eichbaeumle, I. IEC 61850, IEC 61400-25, and IEC 61970: Information Models and Information Exchange for Electric Power Systems. 2004. Available online: https://www.nettedautomation.com/download/Paper_IEC61850_Distributtech_2004-02-10.pdf (accessed on 13 September 2022).
48. Uslar, M.; Specht, M.; Dänekas, C.; Trefke, J.; Rohjans, S.; González, J.M.; Rosinger, C.; Bleiker, R. *Standardization in Smart Grids*; Springer: Berlin/Heidelberg, Germany, 2013. [[CrossRef](#)]
49. Huang, W. Learn IEC 61850 configuration in 30 minutes. In Proceedings of the 2018 71st Annual Conference for Protective Relay Engineers (CPRE), College Station, TX, USA, 26–29 March 2018; pp. 1–5. [[CrossRef](#)]
50. IEC 61850-7-2; Communication Networks and Systems for Power Utility Automation—Part 7-2: Basic Communication Structure for Substation and Feeder Equipment—Abstract Communication Service Interface (ACSI). International Electrotechnical Commission: Geneva, Switzerland, 2003. OCLC: 861074253.
51. IEC 61850-8-1; Communication Networks and Systems for Power Utility Automation—Part 8-1: Specific Communication Service Mapping (SCSM)—Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3. International Electrotechnical Commission: Geneva, Switzerland, 2011. OCLC: 861074253.
52. IEC 61850-9-2; Communication Networks and Systems for Power Utility Automation—Part 9-2: Specific communication Service Mapping (SCSM)—Sampled values over ISO/IEC 8802-3. International Electrotechnical Commission: Geneva, Switzerland, 2011. OCLC: 861074253.
53. IEC 61850-6; Communication Networks and Systems for Power Utility Automation—Part 6: Configuration Description Language for Communication in Electrical Substations Related to IEDs. International Electrotechnical Commission: Geneva, Switzerland, 2009. OCLC: 861074253.
54. Oracle. Brief History of Virtualization. Available online: https://docs.oracle.com/cd/E26996_01/E18549/html/VMUSG1010.html (accessed on 13 September 2022).
55. Zhang, Q.; Liu, L.; Pu, C.; Dou, Q.; Wu, L.; Zhou, W. A Comparative Study of Containers and Virtual Machines in Big Data Environment. In Proceedings of the 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), Zurich, Switzerland, 17–20 December 2018; pp. 178–185. [[CrossRef](#)]
56. Dua, R.; Raja, A.R.; Kakadia, D. Virtualization vs. Containerization to Support PaaS. In Proceedings of the 2014 IEEE International Conference on Cloud Engineering, Boston, MA, USA, 10–14 March 2014; pp. 610–614. [[CrossRef](#)]
57. Redhat. What is Virtualization? Available online: <https://opensource.com/resources/virtualization> (accessed on 13 October 2022).
58. IaaS. Available online: <https://www.redhat.com/en/topics/cloud-computing/what-is-iaas> (accessed on 1 September 2022).
59. Perez, D.J.; Waltl, J.; Prenzel, L.; Steinhorst, S. *How Real (Time) Are Virtual PLCs?* 2022. Available online: https://tum-esi.github.io/publications-list/PDF/2022-ETFA-How_Real_Time_Are_Virtual_PLCs.pdf (accessed on 1 December 2022).
60. VMware. Available online: <https://www.vmware.com/> (accessed on 1 September 2022).
61. The Linux Foundation Wiki CyclicTest. Available online: <https://wiki.linuxfoundation.org/realtime/documentation/howto/tools/cyclictest/start> (accessed on 11 October 2022).
62. Welotech. Substation Modernization: Current to Future. Online Webinar 2022. Available online: <https://vmware-industry.com/substation-modernization-current-to-future> (accessed on 11 October 2022).
63. ISO. ISO/IEC TR 23188:2020(en) 'Information Technology—Cloud Computing—Edge Computing Landscape'. Available online: <https://www.iso.org/obp/ui/#/> (accessed on 8 September 2022).

64. Kalkitech. Centralized IED management: Substation Fault Record Collection. Available online: <https://kalkitech.com/products/control-room-software/ied-management/> (accessed on 20 August 2022).
65. Rösch, D.; Nicolai, S.; Bretschneider, P. Combined simulation and virtualization approach for interconnected substation automation. In Proceedings of the 2021 6th International Conference on Smart and Sustainable Technologies (SpliTech), Bol and Split, Croatia, 8–11 September 2021; pp. 1–6. [CrossRef]
66. Bagherzadeh, L.; Shahinzadeh, H.; Shayeghi, H.; Dejamkhooy, A.; Bayindir, R.; Iranpour, M. Integration of cloud computing and IoT (CloudIoT) in smart grids: Benefits, challenges, and solutions. In Proceedings of the 2020 International Conference on Computational Intelligence for Smart Power System and Sustainable Energy (CISPSSE), Keonjhar, Odisha, 29–31 July 2020; pp. 1–8.
67. Samie, F.; Bauer, L.; Henkel, J. Edge computing for smart grid: An overview on architectures and solutions. *IoT for Smart Grids*; Springer International Publishing: Cham, Switzerland, 2019; pp. 21–42.
68. How Can Smart Grids Benefit from Edge Computing? Available online: <https://stlpartners.com/articles/edge-computing/smart-grids-edge-computing/> (accessed on 14 September 2022).
69. Pau, M.; Mirz, M.; Dinkelbach, J.; McKeever, P.; Ponci, F.; Monti, A. A Service Oriented Architecture for the Digitalization and Automation of Distribution Grids. *IEEE Access* **2022**, *10*, 37050–37063. [CrossRef]
70. EdgeFLEX, E.H. EdgeFlex. Available online: <https://www.edgeflex-h2020.eu/> (accessed on 30 September 2022).
71. Google Scholar. Available online: <https://scholar.google.com/> (accessed on 1 September 2022).
72. IEEE Xplore. Available online: <https://ieeexplore.ieee.org/Xplore/home.jsp> (accessed on 1 September 2022).
73. Xin, Y.; Baldine, I.; Chase, J.; Beyene, T.; Parkhurst, B.; Chakraborty, A. Virtual smart grid architecture and control framework. In Proceedings of the 2011 IEEE International Conference on Smart Grid Communications (SmartGridComm), Brussels, Belgium, 17–20 October 2011; pp. 1–6. [CrossRef]
74. Ferreira, R.D.F.; De Oliveira, R.S. Cloud IEC 61850: DDS Performance in Virtualized Environment with OpenDDS. In Proceedings of the 2017 IEEE International Conference on Computer and Information Technology (CIT), Helsinki, Finland, 21–23 August 2017; pp. 231–236. [CrossRef]
75. Ferreira, R.D.F.; de Oliveira, R.S. Cloud IEC 61850 A Case Study of a Software Defined Protection, Automation & Control System. In Proceedings of the 2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA), Turin, Italy, 4–7 September 2018; pp. 75–82. [CrossRef]
76. Dayabhai, S.; Prestwich, J. A Substation Automation Solution That Uses Virtualization to Reduce Cost While Ensuring Redundancy and Security Compliance. In Proceedings of the Power and Energy Automation Conference, Spokane, WA, USA, 6–7 March 2018.
77. Dayabhai, S. *The Role of Virtualization in a Smart-Grid Enabled Substation*; Conco Group: 2015. Available online: <https://www.concogrp.com/downloads/white-papers/The-role-of-virtualization-in-a-smart-grid-enabled-Substation-Automation.pdf> (accessed on 1 September 2022).
78. Wojtowicz, R.; Kowalik, R.; Rasolomampionona, D.D. Next Generation of Power System Protection Automation—Virtualization of Protection Systems. *IEEE Trans. Power Deliv.* **2018**, *33*, 2002–2010. [CrossRef]
79. Wojtowicz, R.; Kowalik, R.; Rasolomampionona, D.D.; Kurek, K. Virtualization of Protection Systems Part 2: Tests Performed on a Large Environment Based on Data Center Solutions. *IEEE Trans. Power Deliv.* **2021**, *37*, 3401–3411. [CrossRef]
80. Rosch, D.; Nicolai, S.; Bretschneider, P. Container-based Virtualization of an IEC 61850 Substation Co-Simulation Approach. In Proceedings of the 2022 10th Workshop on Modelling and Simulation of Cyber-Physical Energy Systems (MSCPES), Milan, Italy, 3 May 2022; pp. 1–6. [CrossRef]
81. Wang, K.; Wu, J.; Zheng, X.; Jolfaei, A.; Li, J.; Yu, D. Leveraging Energy Function Virtualization With Game Theory for Fault-Tolerant Smart Grid. *IEEE Trans. Ind. Inform.* **2021**, *17*, 678–687. [CrossRef]
82. Attarha, S.; Krüger, C.; Kamsamrong, J.; Babazadeh, D.; Lehnhoff, S. A comprehensive analysis of threats and countermeasures in virtualized cyber-physical energy systems. In Proceedings of the CIRED 2021—The 26th International Conference and Exhibition on Electricity Distribution, Virtuell, Switzerland, 20–23 September 2021; Volume 2021, pp. 1525–1529. [CrossRef]
83. Hassan, B.; Narayan, A.; Brand, M.; Lehnhoff, S. Virtualization for performance guarantees of state estimation in cyber-physical energy systems. *Energy Inform.* **2022**, *5*, 30. [CrossRef]
84. De Din, E.; Pitz, M.; Ponci, F.; Monti, A. Implementation of the online distributed voltage control based on containers. In Proceedings of the 2022 International Conference on Smart Energy Systems and Technologies (SEST), Eindhoven, The Netherlands, 5–7 September 2022; pp. 1–6. [CrossRef]
85. Jablkowski, B.; Kuech, M.; Dorsch, N.; Kubis, A.; Spinczyk, O.; Wietfeld, C.; Rehtanz, C. Poster Abstract: vGridLab—A testbed for virtualized smart grids. *Comput. Sci. Res. Dev.* **2018**, *33*, 245–246. [CrossRef]
86. Yan, Q.; Yu, F.R.; Gong, Q.; Li, J. Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges. *IEEE Commun. Surv. Tutor.* **2015**, *18*, 602–622. [CrossRef]
87. Docker. Available online: <https://www.docker.com/> (accessed on 30 September 2022).
88. libIEC61850. Available online: <https://libiec61850.com/> (accessed on 1 September 2022).

89. ETSI. *ETSI GS NFV-MAN 001 V1.1: Network Functions Virtualisation (NFV); Management and Orchestration*; ETSI: 2014. Available online: https://www.etsi.org/deliver/etsi_gs/nfv-man/001_099/001/01.01.01_60/gs_nfv-man001v010101p.pdf (accessed on 1 September 2022).
90. Xen-Hypervisor. Available online: <https://xenproject.org/> (accessed on 6 September 2022).
91. Platoon EU Project. Available online: <https://platoon-project.eu/> (accessed on 30 September 2022).
92. Kubernetes. Available online: <https://kubernetes.io/> (accessed on 30 September 2022).
93. SEAPATH, Linux Foundation. Available online: <https://www.lfenergy.org/projects/seapath/> (accessed on 30 September 2022).
94. Linux KVM. Available online: https://www.linux-kvm.org/page/Main_Page (accessed on 30 September 2022).
95. EPRI. Common Substation Platform: Utility Requirements Assessment—Part 1,2. 2022. Available online: <https://www.epri.com/research/products/000000003002015877> (accessed on 30 September 2022).
96. Dell Technologies Grid Management Platform Common Design Architecture. Available online: <https://www.delltechnologies.com/asset/en-gb/solutions/business-solutions/briefs-summaries/dell-technologies-grid-management-common-design-arch-h18551.pdf> (accessed on 23 October 2022).
97. E4S Alliance: Secondary Substation Platform—SSP. Available online: <https://www.ariadnagrid.com/blog/e4s-alliance-secondary-substation-platform-ssp/> (accessed on 3 August 2022).
98. Samara-Rubio, D.; McKenzie, G.; Khajuria, P. *White Paper: “A Paradigm Shift in Power System Protection”*; Intel Corporation: Mountain View, CA, USA; Kalkitech: Bengaluru, India, 2022. Available online: <https://kalkitech.com/wp-content/uploads/2022/05/Virtual-Protection-Relay-WP-V051222.pdf> (accessed on 3 August 2022).
99. Balalaie, A.; Heydarnoori, A.; Jamshidi, P. Microservices architecture enables devops: Migration to a cloud-native architecture. *IEEE Softw.* **2016**, *33*, 42–52. [CrossRef]
100. Jaramillo, D.; Nguyen, D.V.; Smart, R. Leveraging microservices architecture by using Docker technology. In Proceedings of the SoutheastCon 2016, Norfolk, VA, USA, 30 March–3 April 2016; pp. 1–5.
101. LinuxFoundation DPDK. Available online: <https://www.dpdk.org/> (accessed on 30 September 2022).
102. Valtari, J.; Joshi, S. *White Paper: Centralized Protection and Control*; ABB: 2019. Available online: https://library.e.abb.com/public/6b20916a4d2e412daabb76fbada1268e/Centralized_Protection_and_Control_White_paper_2NGA000256_LRENA.pdf (accessed on 3 August 2022).
103. Björklun, H. Experiences with the deployment of centralized protection systems using virtual protection relays for substations with large power electronic converters. *CIGRE 2022 Paris Session.* **2022**.
104. Kreuzer, P.; Oliveira, J. Virtualization as an enabler for digital substation deployment. *CIGRE 2022 Paris Session.* **2022**.
105. Hokkanen, A. Scalable Software Platform Architecture for the Power Distribution Protection and Analysis. 2020. Available online: <https://core.ac.uk/download/pdf/304703496.pdf> (accessed on 23 September 2022).
106. IEC 61850-3; Communication Networks and Systems for Power Utility Automation—Part 3: General Requirements. International Electrotechnical Commission: Geneva, Switzerland, 2013.
107. Protocols and Communication Architecture Subcommittee (P0), ‘System Architectures Supporting the Virtualization of Substation Protection and Control Applications’, ‘P11 TF: Cloud Computing, uses and Requirements of Electric Power Utilities’ IEEE PES Technical Committee on Power System Communications and Cybersecurity PSCC. Available online: <https://site.ieee.org/pes-pssc/protocols-and-communication-architecture-subcommittee-p0/> (accessed on 8 August 2022).
108. CIGRE, Study Committee B5.60. Protection, Automation and Control Architectures with Functionality Independent of Hardware. 2022. Available online: https://www.cigre.org/userfiles/files/News/2018/TOR_WG_B5_60_Protection_Automation_and_Control_Architectures_with_Functionality_Independent_of_Hardware.pdf (accessed on 8 August 2022).
109. CIGRE, Study Committee B5.73. Experiences and Trends related to Protection Automation and Control Systems Functional Integration & Working Group. 2023. Available online: <https://www.cigre.org/> (accessed on 8 August 2022).
110. CIGRE, Study Committee B2.43. Enabling Software Defined Networking for Electric Power Utilities. 2022. Available online: <https://e-cigre.org/publication/866-enabling-software-defined-networking-for-electric-power-utilities> (accessed on 8 August 2022).
111. CIGRE, Study Committee B5.77. Requirements for Information Technologies (IT) and Operational Technology (OT) managed of Protection, Automation, and Control Systems (PACS). 2025. Available online: <https://www.cigre.org/> (accessed on 8 August 2022).
112. TC 57, ‘IIoT and Digital Twin Applications in Power Systems Management’, ISO/IEC JTC 1/SC 41. Available online: <https://www.iec.ch> (accessed on 17 October 2022).
113. White Paper: ‘Network Functions Virtualisation An Introduction, Benefits, Enablers, Challenges & Call for Action’. Available online: http://portal.etsi.org/NFV/NFV_White_Paper.pdf (accessed on 18 August 2022).
114. Rehman, A.U.; Aguiar, R.L.; Barraca, J.P. Network Functions Virtualization: The Long Road to Commercial Deployments. *IEEE Access* **2019**, *7*, 60439–60464. [CrossRef]
115. Zhang, T.; Qiu, H.; Linguaglossa, L.; Cerroni, W.; Giaccone, P. NFV Platforms: Taxonomy, Design Choices and Future Challenges. *IEEE Trans. Netw. Serv. Manag.* **2021**, *18*, 30–48. [CrossRef]
116. Dahmen-Lhuissier, S. Our Group Network Functions Virtualisation (NFV). Available online: <https://www.etsi.org/committee/1427-nfv> (accessed on 13 August 2022).
117. NFV Architectural Framework: The ETSI Architectural Framework Explained. Available online: <https://stlpartners.com/articles/telco-cloud/nfv-architectural-framework/> (accessed on 11 November 2022).

118. CIMI, A. What Went Wrong with NFV: The Operator View. Available online: <https://blog.cimicorp.com/?p=3821> (accessed on 12 November 2022).
119. TELCO CLOUD: Why It hasn't Delivered Yet and What Must Change for 5G. Available online: <https://www.juniper.net/content/dam/www/assets/white-papers/us/en/stl-white-paper-telco-cloud-why-it-hasnt-delivered-and-what-must-change-for-5g.pdf> (accessed on 24 August 2022).
120. '2020 State of NFV Report', Avid Think LLC and Converge! 2020. Available online: https://www.equinix.es/content/dam/eqxcorp/en_us/documents/resources/analyst-reports/ar_avidthink_2020_state_of_nfv_en_oct2020.pdf (accessed on 24 August 2022).
121. ETSI NFV Evolution Event, TelecomTV. Available online: <https://www.telecomtv.com/content/etsi-nfv-evolution-event/> (accessed on 13 October 2022).
122. *White Paper: 'Streamlining VNF On-Boarding Process: Learnings from over 200 VNFs on-Boarded by HPE, Intel, TechMahindra and VMware'*; Intel: Mountain View, CA, USA, 2017. Available online: <https://www.intel.in/content/dam/www/public/us/en/documents/white-papers/vnf-on-boarding-process-white-paper.pdf> (accessed on 13 October 2022).
123. *White Paper: 'NFV Testing and Automation Research and Methodologies A Telecom Operator's Perspective'*; Linux Foundation Networking: San Francisco, CA, USA, 2021. Available online: https://lfnetworking.org/wp-content/uploads/sites/7/2022/06/LFN_NFV_TestingandAutomation_ResearchMethodologies_Whitepaper_033021.pdf (accessed on 13 October 2022).
124. *White Paper: "Implementing Real-Time System Using Intel Time-Sensitive Networking Capable Ethernet Controller on Linux Operating System"*; Intel Corporation: Mountain View, CA, USA, 2022. Available online: <https://www.intel.com/content/dam/www/central-libraries/us/en/documents/2022-10/tsn-real-time-profinet-linux.pdf> (accessed on 7 December 2022).
125. Gundall, M.; Stegmann, J.; Reichardt, M.; Schotten, H.D. Downtime Optimized Live Migration of Industrial Real-Time Control Services. *arXiv* **2022**, arXiv:2203.12935.