energies

MDPI

Article

Virtualization Management Concept for Flexible and Fault-Tolerant Smart Grid Service Provision

Shadi Attarha *, Anand Narayan, Batoul Hage Hassan, Carsten Krüger, Felipe Castro, Davood Babazadeh and Sebastian Lehnhoff

OFFIS—Institute for Information Technology, 26121 Oldenburg, Germany; anand.narayan@offis.de (A.N.); batoul.hage.hassan@offis.de (B.H.H.); carsten.krueger@offis.de (C.K.); felipe.castro@offis.de (F.C.); davood.babazadeh@offis.de (D.B.); Sebastian.Lehnhoff@offis.de (S.L.)

* Correspondence: shadi.attarha@offis.de; Tel.: +49-441-9722-361

Received: 18 March 2020; Accepted: 22 April 2020; Published: 2 May 2020

Abstract: In modern power systems, reliable provision of grid services (e.g., primary and ancillary services) are highly dependent on automation systems in order to have monitoring, processing, decision making and communication capabilities. The operational flexibility of automation systems is essential for the reliable operation of power systems during and after disruptive events. However, this is restricted by integrated hardware-software platforms. Therefore, it will be difficult to reconfigure control strategies during run time. This paper presents the concept of Grid Function Virtualization (GFV) as a potential approach to improve the operational flexibility of grid automation systems. GFV has been proposed to offer a new way to deploy and manage grid services by leveraging virtualization technology. The main idea of GFV is to run grid services (i.e., software implementation of services) independently from underlying hardware. To realize the important design considerations, the GFV architecture and its building blocks is elaborated in details. To this end, an exhaustive review of applications of virtualization in several domains is provided to show the importance of virtualization in improving flexibility and resource utilization. Finally, the advantages of the proposed concept to deal with disruptions in power systems is demonstrated in a proof of concept based on a CIGRE MV benchmark grid.

Keywords: virtualization; power system automation; communication; grid services; flexibility; smart grids

1. Introduction

The power system is a safety critical infrastructure which has to supply electricity constantly and reliably in order to support its consumers. To ensure its reliable operation, system operators, among others, use a set of grid services (e.g., ancillary and primary services), that include real-time balancing, frequency control, voltage control, reactive power management and system restoration. These services can be used during disruptive events in order to bring-back parameters like frequency and voltage to their nominal values. During normal operation of power systems, these grid service also aid in improving operational efficiency and economy. Therefore, the reliable provision of these grid services is of utmost importance. However, this becoming challenging considering the current structure of power systems with stochastic power flows as well as large number of actors, e.g., active consumers and Distributed Energy Resources (DER). These services are typically comprised of different grid functions such as measuring, analysis, communication and control, which are highly dependent on Information and Communication Technologies (ICTs) [1,2].

With the increasing digitalization of power systems, there is also an increased risk of disruptive events with large consequences. This increases the system complexity making it more unpredictable [3]. In order to provide grid services reliably, the automation or the ICT system as a significant integrated

part of the power system must be designed to cope with these disruptive events, irrespective of their origin (i.e., both cyber and physical side). For this purpose, several methods and recommendations such as re-configurable control and protection function on standard hardware based on IEC 61850 substation configuration [4], advanced ICT monitoring and anomaly detection mechanisms [5] and digital-twin-based simulation system [6] have been suggested. The automation or ICT system can also improve the survivability of power systems in case of disruptive events [3,6]. However, the operational flexibility of automation systems is currently restricted by integrated hardware-software setups and vendor-locked solutions [4]. In other words, the provided functionalities have to be typically fixed during the design phase. This makes it difficult to reconfigure or change the control strategies during run-time in order to counteract the disruptive events in a timely manner. For instance, if an analysis on a finer time scale is required, grid services can request automation devices like Phasor Measurement Units (PMUs) to measure and transfer data at various predefined sampling rates [7]. Thus, there exists a trade-off between performance and resiliency in the paradigms with limited flexibility. Virtualization is a well-established concept that can be used in Cyber-Physical Energy Systems (CPES) to improve its operational flexibility.

The commonly applied definition of virtualization, which refers to hardware-level virtualization, is 'the logical abstraction of the underlying hardware devices, through decoupled software implementation' [8]. Virtualization allows dynamic reallocating of computing resources (e.g., Memory, CPU, Network) among a multitude of processes. In other words, virtualization is a technology that provides the ability to create services and run them independently from underlying hardware which have been bound to hardware traditionally. As a result, services can be relocated among devices or reconfigured freely. It helps increasing a flexibility of the system, reducing cost and optimizing resource utilization [9]. Nowadays, virtual machine and containerization techniques are mostly used both in industry and academy for employing virtualization [10].

In CPES or smart grids, current researches on the use of virtualization have been focused on improving the performance and reliability of the communication networks, as part of smart grids, using technologies such as Network Function Virtualization (NFV) or Software Defined Networks (SDN) [2,11]. A systematic approach and structure towards virtualizing grid functions for reliable provision of grid services running on the computational resources of power systems (e.g., IEDs, PMUs and servers) is not yet investigated. This paper distinguishes between the well-researched NFV concept which is used by communication network operators in their infrastructure (i.e., to optimize deployment and control of network functions such as load balancer and firewall) and the use of virtualization in power grid (i.e., for grid services such as state estimation and voltage control, which run on computational resources of the power system).

This paper introduces the concept of GFV and elaborates its capability to improve the operational flexibility of automation systems for reliable provision of grid services. In this approach, by using virtualization technology, grid services (i.e., software implementation of service) are decoupled from underlying hardware and provided as chains of different virtual entities called Virtual Grid Functions (VGFs). The VGFs could be deployed on virtual resources such as containers or virtual machines and run on computational resources of power grid (e.g., IEDs, PMUs) independently. This enables the ability to reconfigure grid services as well as relocate VGFs based on real-time power system requirements. To explore the important design considerations that must be considered in this approach to make grid components (i.e., infrastructure and grid services) compatible for virtualization, the GFV architecture is proposed. The remainder of this paper is organized as follows. A detailed literature survey on the applications of virtualization in different domains including smart grids is discussed in Section 2. Then, the proposed Grid Function Virtualization (GFV) architecture and its building blocks are described in details. Finally, a simulation-based proof of concept is presented using an ICT-enriched CIGRE MV benchmark grid to demonstrate the advantages of GFV concept. Three exemplary grid services, namely State Estimation (SE), Coordinated Voltage Control (CVC) and Unit Commitment

(UC) are considered in the proof of concept; all of which are vital grid services for the operation of the power system.

2. State-Of-The-Art in Virtualization

Virtualization is a technology that provides a reduction in complexity and cost by abstracting computing resources into logical partitions [12]. It helps to increase resource utilization and system flexibility [13]. Virtualization is a well defined concept and there are several reasons to show how it can be effective in different domains. Using virtualization in smart grids is a new topic, so it is worthwhile to find out a virtualization usage in other domains where its benefits are well used. This section provides the state-of-the-art of virtualization in several domains such as wireless sensor networks, avionics systems and data center as well as smart grids. Furthermore, the goals, applications and technologies based on virtualization are addressed as well as its requirements and implementation approaches.

2.1. Virtualization in Smart Grids

Virtualization has been applied in communication networks within smart grids for different purposes. The ability of SDN to enhance the resiliency of smart grids is presented in [11,14]. This is done by rerouting the communication network paths in case of communication failures or network congestion—thereby mitigating their effects. The SDN platform using Internet of Things to improve resiliency in smart grids under communications fault situations using real-time monitoring techniques is presented in [2]. However, the allocation of communication network resources—in case of power system failures—for grid services with different QoS requirements using industrial protocols is not considered. A survey on SDN architecture in smart grids along with case studies is presented in [15]. Furthermore, based on SDN, an architecture using Power Line Communication (PLC) infrastructure in [16] is proposed for providing resiliency against cyber attacks. In this approach, measurements data are transferred by wireless channel while control information is carried by PLC infrastructure. All in all, the goal of using SDN in power system is to improve the management of communication networking architecture of smart grids ,which is nowadays more and more complicated [17–19]. While in GFV approach, the main purpose is to provide an ability to reconfigure/relocate grid services based on power system status by leveraging the virtualization technology. This makes power systems more reliable in case of disruptions either in ICT (e.g., link congestion in communication networks) or power systems (e.g., hardware failure) side.

Virtualization is also proposed as a core technology behind NFV to enhance operational flexibility by providing the ability of sharing resources such as infrastructures, software and applications [20]. Complex communication services can be built with several virtualized functions which are connected in certain sequences. These functions can be executed on commodity hardware or standard server; thereby making them independents from proprietary underlying hardware [21]. In [22], virtualizing PMUs for provide a certain degree of local logic is proposed. It considers the smart data transmission and implements a bandwidth-efficient mechanism to meet the QoS requirements possible. However, the concept and architecture of virtualization of grid services in power systems have yet to be developed. Cloud computing and server virtualization has also been implemented in smart grids [23]. This approach provides reliable acquisition of timely data from the power system, with immense computing and storage resources.

Deploying grid services (e.g., state estimation and coordinated voltage control) in cloud environments results in a lot of communication overhead as all power systems measurements that are gathered from the field must be transmitted over the network to the cloud (where services are located). This is because most services require a global view of the system. Compared to cloud approach, in the presented GFV approach, grid services such as data acquisition or state estimation are deployed in field devices (e.g., in IEDs or COTS hardware) that are near to the field. Therefore, the communication redundancy is significantly reduced and in terms of costs, it is more economical.

2.2. Virtualization in Other Domains

The continuously increasing number of communication network functions that are coupled with underlying hardware results in poor network management and higher costs [24]. NFV is a framework where Network Functions (NF), e.g., firewall, encryption, and decryption, which traditionally run on various specialized hardware appliances, are now implemented on general-purpose hardware and are referred to as Virtual Network Functions (VNF) [25]. The aim of NFV is to bring deployment flexibility and cost reduction to the network domain by decoupling NFs from dedicated hardware [26]. In the meantime,to manage and secure a communication network which involve integration and interconnection of diverse devices, network operators are responsible for implementing increasingly network policies [27]. Software Defined Networking (SDN) decouples the network control functions (control plane) from the underlying hardware (data plane) for better management, faster innovation and network flexibility [28]. This allows the control functions to become directly programmable via an open interface and the underlying infrastructure to become simple packet forwarding devices [29].

Recently, by emerging the Internet-of-Things, Wireless Sensor Networks (WSNs) have become pervasive and gains popularity. Generally, WSNs have been deployed domain-specific and task-oriented. It means the WSNs deployment are designed to support a specific application which is bundled with the sensors [30]. In this environment, there is no possibility to re-use sensors or change the application. Improvement of WSNs nodes hardware leads to motivating developers to find a solution how multiple applications can be deployed on the same infrastructure [13]. Virtualization technology by providing the ability to share resources/infrastructure can aid in solving this issue. Executing several applications simultaneously on a node and sharing data collected from sensors with multiple applications are virtualization advantages. This provides the ability to access sensors concurrently from different independent applications [31].

Nowadays, with the growth of data volumes, data centers are considered as a cost-effective solution for storing data. However, previous data center architectures can not support several applications, which are have different resource demands. This lack of flexibility leads to poor QoS, manageability and cyber-security issues. Furthermore, the number of data centers are growing exponentially. Consequently, their energy consumption and performance have become even more important. Virtualized data centers provide better management, flexibility, scalability, better resources utilization and energy efficiency. In virtualized data centers, virtual machines which contain services are allowed to move freely among physical machines (PMs) with negligible downtime. This is done by using specific software (e.g., a hypervisor) that divides single physical servers into several independent virtual servers with different resources for services [32]. Virtualization plays a primary role in efficiently delivering Infrastructure-as-a-Service (IaaS) solutions for cloud computing and unifies resources of multiple servers that can be used by different services in cloud computing [33].

Many automotive innovations are based on embedded systems and the number of software-based functionality is rapidly increasing which has led to an increase of Electronic Control Units (ECU) and software with less resources and modifiability [34]. Updating the ECUs is a long and complicated process causing issues in security and complexity in terms of cost, installation space and energy consumption [35]. The ability to run multiple functions concurrently as well as software isolation make virtualization into an attractive solution to fulfill the automotive requirements [36]. This makes it easier to program/configure ECUs [37]. Dynamic distribution of functions and virtualization of ECU are in the future road map of automotive system architectures [38].

In avionic systems, the life-cycle costs are increasing and force equipment manufacturers to migrate toward the solution that provides the possibility to run multiple applications concurrently on platform. Integrated modular avionics approach is introduced to overcome this problem in current avionics system [39]. In this concept, current avionics applications that are executed until now on separate devices, should be executed on one hardware and managed by a dedicated special real time operating system [40].

2.3. Summary

The investigation of the state-of-art indicates that virtualization has been applied in several domains with different goals. For example, in WSNs, it is used to enhance deployment flexibility whereas in virtual data centers, it is used to improve data center's performance. Table 1 summarizes results along with different methods employed in different domains. It can be seen that the typical goals of using virtualization are to improve deployment flexibility, enhance resource utilization and reduce cost; all of which are vital aspects in smart grids as well. This research suggests the use of virtualization in order to enhance the overall performance of grid services (e.g., voltage control, reactive power control). By leveraging virtualization in smart grid a number of differences in the way grid service provisioning is implemented in comparison to current operation will be introduced. Therefore, this needs two aspects: an architectural framework to make grid components (i.e., infrastructure and services) compatible for virtualization and a management layer for effectively allocating and managing computational resources of power grid among grid services.

Table 1. Summary of Virtualization in other domains.

Domain	Literature	Goals	Methods
Communication—NFV	[20–22,24–26]	Scalability, Cost reduction, Fast integration	Implementing network functions as pure software elements that can be run in standardized hardware
Communication—SDN	[2,11,14,15,28,29]	Resiliency, Easy management	Abstracting network control function into logical programmable entity
WSN	[13,31,41,42]	Flexibility in deployment	Virtual sensor networks, Sensing as a service model
Data Center	[32,33,43]	Performance improvement, Cost reduction	Server consolidation, Cloud based
Avionics Systems	[39,40,44]	Cost reduction	Embedded hypervisor technology

3. Grid Function Virtualization

Current grid operators have the responsibility for managing grid services, which includes monitoring and responding to the wide range of power system events that may occur. At distribution system level, grid operators typically use a shared communication infrastructure with a certain QoS level provided by communication network operators via service level agreements in order to exchange information. Similar to another domains such as communication that network operators use SDN and NFV to manage their networks, virtualization technique can be used in power systems to decouple physical power systems equipment from grid services that run on them. It means the grid services (e.g., state estimation, unit commitment) can run independently from underlying hardware and grid operator can take the advantage of the resulting flexibility to cope with abnormal situations more efficiently. Figure 1 shows how virtualization can be applied to power systems. In this approach, grid functions are deployed on virtual resources such as containers or virtual machines and called Virtual Grid Functions (VGF). A set of VGFs constitute a grid service. The aim of detachment of software from hardware in power systems by leveraging virtualization is to provide a basis for flexible as well as cost effective reallocation of the available computational resources among grid services based on their requirements (e.g., computational resources, required bandwidth). Furthermore, this allows to update grid services and relocate them freely among grid computational resources (e.g., PMUs, IEDs, servers). It is to be noted that field sensors and actuators, because of their physical interface with the power grid can not be virtualized and are connected via the communication links to commodity hardware. The primary challenge for introducing the virtualization concept in smart grids is the lack of a standardized architecture. In this paper, the Grid Function Virtualization (GFV) architecture, which is a structure that explores important design considerations, is elaborated in details.

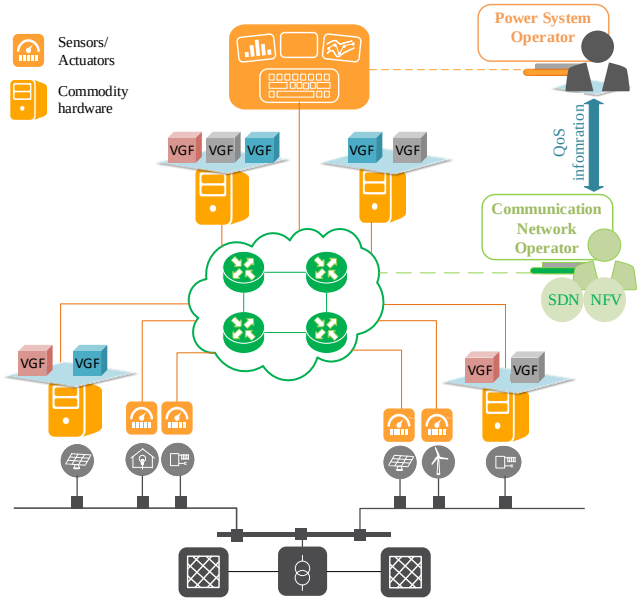


Figure 1. Grid Function Virtualization in smart grids.

3.1. Grid Function Virtualization Architecture

This section explains the proposed architecture (shown in Figure 2) for GFV along with its building blocks. It intends to provide a structure for deploying and managing VGFs instances across available computational resources of grid. The GFV architecture consists of three layers—Infrastructure, Service and Management.

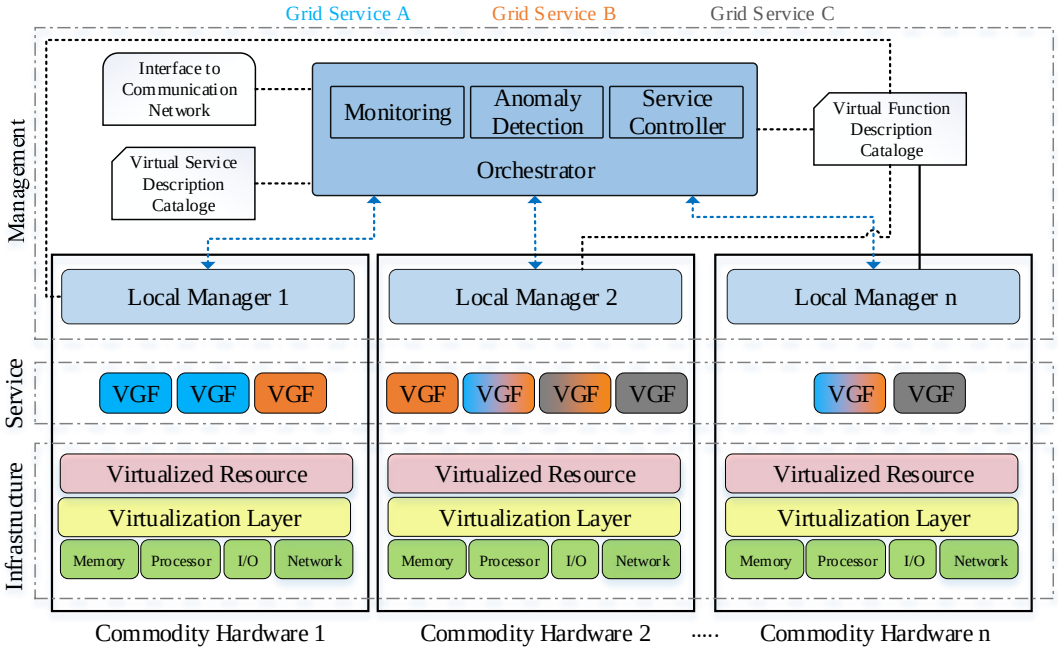


Figure 2. Grid function virtualization architecture.

3.1.1. Infrastructure

The ability to run grid services on computational resources of power grid (e.g., processor and memory) is provided by the Infrastructure layer. In order to have an ability to allocate resources among VGFs in a flexible manner and use them efficiently, this resources must be virtualized. It can be

realized by the Virtualization Layer applying software like a Hypervisor or Container Engine. It is worth mentioning, in additional to the computational resources (e.g., network, processor and memory), the I/O is considered to bring in a grid service-specific resource, which is the connection point for sending and receiving data to sensors and actuators respectively. All in all, each hardware and software resources that provide an operational environment for grid services are covered by Infrastructure layer.

3.1.2. Service

In order to be able to deploy and configure grid services flexibly, software implementation of them (i.e., the standard grid service code) will be considered as an independent layer from the underlying hardware. Owing to complexity of grid services (e.g., SE, CVC), they can be divided into different grid functions (i.e., breaking grid service code down into smaller functions) such as data acquisition and control algorithm. Virtual Grid Function (VGF), which is introduced in this paper, is a software package that represents the implementation of the current non-virtual grid function and can be deployed in virtual entities (e.g., containers or virtual machines) which are run on computational resources of power grid (e.g., PMUs, IEDs, servers). In other words, virtualizing grid functions and implementing them inside containers or virtual machines makes them independent from underlying hardware. Therefore, based on virtualization features (e.g., live migration of virtual entity, updating in run-time), the ability to reconfigure grid functions or relocate them from one device (i.e., computational resources of power grid) to another based on power system status can be achieved. These VGFs can be combined in specific sequences to constitute the grid services. Furthermore, VGFs can be shared between different grid services to reduce resource usage. Each VGF and grid service have a specific configuration file which comprises all required information for implementing them (e.g., their resource requirements). These are called Grid Function Descriptor (GFD) and Grid Service Descriptor (GSD) that are part of Management layer and used to deploy and control VGFs and grid services.

3.1.3. Management

The Management layer, which is the most critical part of this architecture, is responsible for the management and orchestration of all virtualization-specific tasks required throughout the life-cycle of grid services and VGFs. It includes five modules—Virtual Service Description Catalog and Virtual Function Description Catalog, Interface to Communication Network, Orchestrator and Local Managers.

The Virtual Service Description Catalog and Virtual Function Description catalog are repositories that store GSD and GFD respectively. The GSD references all grid service configuration parameters that are essential for grid service life-cycle management. It includes grid service QoS requirements (e.g., data rate and delay) as well as constitutive VGFs and their order. Each VGF has a certain configuration parameters such as minimum resource requirements (e.g., CPU, memory) and required input/output data with reference to deployment and configuration behavior which are represented in GFD. The information which is represented by GSD and GFD is used by Local Manger and Orchestrator to deploy and manage grid services and VGFs. Furthermore, because of dependencies between VGFs in a grid service and the possibility of putting them on different commodity hardware, the Management layer needs certain information from the communication networks (e.g., bandwidth, delay) in order to guarantee the required QoS. Thus, this QoS information can be provided, e.g., by an interface to a communication network operator.

Since VGFs which are part of a grid service can be located in different independent infrastructures, there are two levels of management to orchestrate grid services, VGFs and resources in dispersed smart grid environment. In the first level of management, each commodity hardware has its own Local Manager to handle several tasks related to its resources and VGFs. The Local Manager can instantiate, terminate and update VGFs by receiving management commands such as deploy, update and stop from the Orchestrator. Moreover, it can monitor resources and VGFs performance continuously. In other words, the Local Manager operates on the level of VGFs and it is considered as a first level of management.

The Orchestrator, which is considered as second layer of management, acts as an unified interface that can talk to all Local Managers and collects system information in order to provide a global view of all available grid services in smart grids. Generally, it has a responsibility regarding service life-cycle and its associated procedures. In coordination with Local Managers, Orchestrator can deploy, update and terminate grid services based on GSDs.

The Orchestrator responsibilities can be categorized through three main sub-modules: Monitoring, Anomaly Detection and Service Controller. These modules collaborate with each other to observe the operational environment, detect anomalies and provide reasonable reactions for tuning power systems. Observing the performance of computational resources of grid and collecting stats to achieve a set of objectives defined as QoS is fulfilled by Monitoring. It can be implemented in two different ways: sending request periodically to Local Managers and gathering metrics related to their computational resources or using monitoring software tools such as Zabbix, Check Mk and Prometheus.

Continuously monitoring grid service performance and controlling correlation of collected metrics for each grid service can help to detect disruptive events. Anomaly Detection module by analysing the information collected by Monitoring module detects anomalous behaviors such as cyber attack, hardware failure and power outage and provides accurate notifications. In order to distinguish normal and abnormal behavior, machine learning-based anomaly detection models and statistical methods can be used in Anomaly Detection module [45].

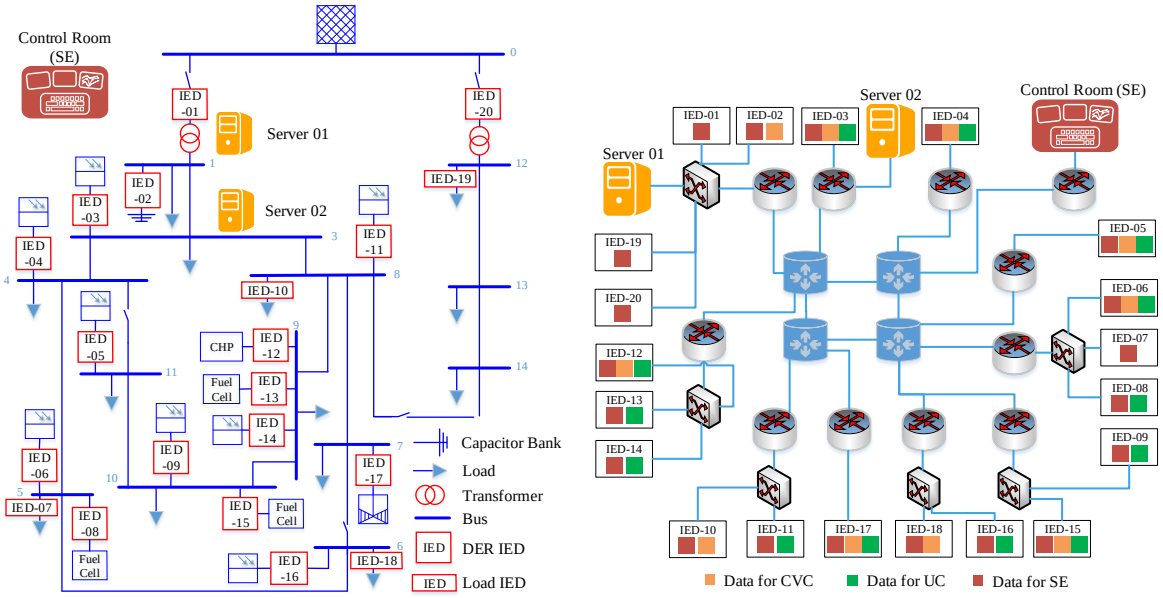
Service Controller provides actions associated with grid services life-cycle such as initializing, updating and terminating. In other words, the Service Controller is responsible to distribute VGFs based on the available network and computational resources. In the case of disruptive events, which influence the power system performance, alarms from the Anomaly Detection module are used to activate the Service Controller. Then, the Service Controller can decide on remedial actions such as changing configuration parameters of related VGFs or shifting them to another commodity hardware. To this end, Service Controller considers acquired metrics from Monitoring module and real-time information from the communication network as well as GFDs and GSDs, then it makes decision based on this information about changing operating environment. Afterwards, Service Controller triggers related Local Manager(s) to start/stop/update intended VGFs. The compliance of all requirements according to the available resources, network QoS parameter and dependencies between VGFs can be formalized as Problem. To solve such a problem several solution concepts are available such as optimization algorithm and Rule-based Expert Systems. For instance, if a commodity hardware fails, Service Controller can move VGFs from failed hardware to another proper Commodity hardware immediately to keep system reliable.

4. Proof of Concept

The goal of the introduced Grid Function Virtualization (GFV) concept is the reliable provision of grid services by enabling the flexible reconfiguration as well as relocation of their constituting grid functions. This is important when certain grid services are required to diminish the effect of disruptive events in the power system. In such cases, the GFV approach can ensure the reliable operation of these critical grid services by providing their grid functions with required computational resources (e.g., CPU. memory) and network (e.g., bandwidth) resources. This section presents two simulation-based proof of concepts to demonstrate the benefits of GFV for mitigating the impact of disruptive events either in ICT or power system. This is done by reconfiguring the grid services or relocating them in run-time, which can be done using the proposed GFV concept. In order to present the effect of this approach to counteract the impact of disruptions in the ICT side (e.g., link congestion on communication network), in use-case 1, the communication network is modeled and simulated by Exata (https://www.scalable-networks.com/exata-network-emulator-software). The power system in this use-case is abstracted and just edge nodes (IEDs, RTUs) are modeled. The size of packets that transmit over network is 117 bytes. All nodes have been connected via wired Ethernet connections. The capacity of links located at the edge is 2 Mbits/s and core link capacity is 10 Mbits/s.

Furthermore, the protocol which is used for this simulation is IEC 60870-5-104 [46]. Then, in use-case 2, for approving the benefit of using GFV in case of disruption in the power system side (e.g., hardware failure), the power system is modeled by DIgSILENT PowerFactory software and the communication part is abstracted in this use-case. It is worth remarking that simulations (i.e., use-case 1 and use-case 2) were done sequentially to achieve these results.

Both simulations are carried out considering the CIGRE medium voltage benchmark grid, which is augmented with grid automation components as shown in Figure 3a. The modified 14-busbar CIGRE distribution model has been adjusted to consider only its residential area which corresponds to busbars 1 to 11 (Figure 3a). This part of the system feeds a total load of 24.8 MW (with power factor 0.97 lag) and a total injection of 10.0 MW from the DERs. The key performance indicators considered for use-case 2 are keeping the voltage of the bus between a range of [0.95, 1.05] p.u and the reactive power flowing through the transformer between a range of $[-5, 5]$ MVAr. IEDs are placed at loads as well as DERs. Load IEDs perform only monitoring as the loads are not controllable; whereas the DER IEDs perform both monitoring and control as DERs are controllable. Since distribution grids are typically under-determined, the IEDs are only located at certain arbitrarily chosen loads. The IEDs measure data from the power system and send them to the server via the communication network, which is shown in Figure 3b. The IEDs are interfaced with the backbone network via routers and switches. Routers are located at each bus, to which all the IEDs of that bus are connected.



(**a**) CIGRE MV grid (**b**) ICT System Model

Figure 3. Simulated cyber-physical energy system.

Three exemplary grid services are considered, namely Coordinated Voltage Control (CVC), State Estimation (SE) and Unit Commitment (UC). It is worthwhile to mention that UC, in this paper, is related to real-time generation balancing. Table 2 shows the QoS requirements for the considered grid services. Note that these requirements were taken from C37.1—IEEE Standard for SCADA and Automation Systems [46]. This could however vary from one system operator to another. Violation of these requirements may cause the corresponding service to fail. A central architecture is considered for Coordinated Voltage Control (CVC) and State Estimation (SE), where all IEDs send measurement data to the server. The server does the required processing corresponding to the CVC or SE algorithm. The server (Server 01) which holds the CVC algorithm is located at Bus-1, whereas the server for SE is located in the external control room. Server 02 located at Bus-3 is a back-up server. A distributed

multi-agent architecture is considered for UC, where the DER IEDs communicate with each other to achieve consensus. This does not require a server. It is to be noted that in this proof of concept the grid services are considered only based on their architecture and their QoS requirements (see Table 2). Their actual implementation is yet to be considered.

Table 2. QoS requirements of grid services [46].

Grid Service	Acceptable Delay (s)	Update Periodicity (s)	Data Rate (pps)
Coordinated Voltage Control (CVC)	1	2	0.5
State Estimation (SE)	10	15	0.067
Unit Commitment (UC)	0.4	1.5	0.67

4.1. Use-Case 1

In this use-case, three scenarios are simulated considering the aforementioned grid services to demonstrate the benefits of the proposed GFV concept in case of disruption in ICT side. Scenario-1 represents normal operation of the power system. Here, since there are no disruptive events, the grid as well as the grid services operate normally. Scenario-2 is assumed to have a disruptive event in the power system causing the voltage to rise (e.g., a sudden gush of wind causing the wind farm at Bus-7 to generate more power). This makes the CVC service critical because it has to remedy the voltage increase. This can potentially be done by changing the set points of the DERs or by changing the transformer tap position. In this case, according to the current state-of-the-art (refer to Section 1), the IEDs will sense this voltage increase and will in-turn increase the sampling rate for CVC measurements to a certain pre-configured value. This is because, during voltage disruptions, the CVC algorithm requires more data samples to have observation on a finer time-scale in order to give a better control decision [47]. Thus, the sampling rate for CVC is assumed to increase five times and the interval time between each measurements updating will be decreased. Additionally, since the role of the SE service is to provide better grid observability, especially during disruptive events, its measurement sampling rate is also assumed to increase five times. The measurement sampling rate for UC service remains unchanged.

Figure 4 shows the simulation results for the scenarios considered. Since Scenario-1 represents normal operation, it can be seen that the average delay of all grid services are within their respective delay requirements (refer Table 2). However, in Scenario-2, the delay requirement for CVC is violated, which can cause the CVC service to fail. This can hamper the remedial action for the voltage disruption potentially resulting in grid instability. This is due to the unchecked increase in the sampling rates of CVC and SE services, which cause congestion in the communication network due to its limited bandwidth resource.

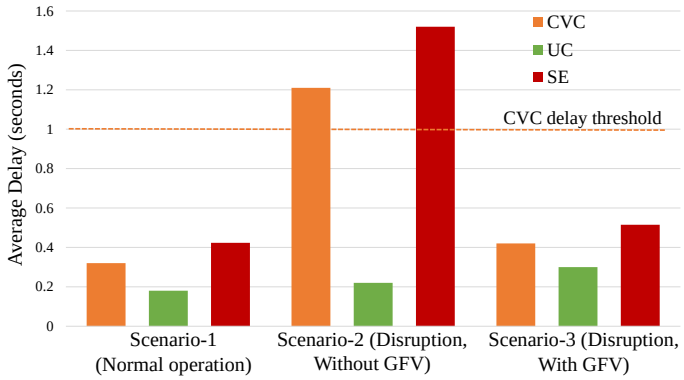


Figure 4. Average delay for the scenarios considered.

The proposed concept of GFV can provide a solution by monitoring and reallocating resources as well as reconfiguring VGFs, in order to detect and remedy anomalies. This is done by virtualizing

the grid functions as VGFs, which are deployed on containers or virtual machines and run on the commodity grid hardware to perform specific task (e.g., data acquisition and CVC algorithm). During the voltage disruption, ensuring grid stability has more priority compared to economic operation. Therefore, the UC service is reconfigured and updated with the decreased sampling rate. The sequence diagram in Figure 5 shows the actions of the modules in the proposed GFV architecture (refer Figure 2), which is used to remedy the disruption. First, the performance of the VGFs as well as the computational resources are monitored continuously. Once an anomaly is detected i.e., delay of CVC exceeds its threshold, the Anomaly Detection module sends an alarm to the Service Controller module. Next, the Service Controller module requests the computational resources information from the Monitoring module and the QoS information from the communication network operator. Additionally, it also requests the requirements of the VGFs (i.e., data acquisition and CVC algorithm) and requirements of the grid services (i.e., CVC, SE and UC) from the Virtual Function Description Catalog and Virtual Service Description Catalog respectively. Then, the Service Controller makes a suitable decision by considering all these information. In this proof of concept, it decides the new sampling rate for UC and reconfigures the data acquisition function of UC with the new sampling rate (i.e., the update periodicity will be 10s), which not only prevents network congestion but also fulfils the QoS requirements of the three grid services. This means the GFD of data acquisition that contains configuration parameters is updated with a new sampling rate. The Service Controller then instructs the relevant Local Manager(s) to update the related VGF (i.e., data acquisition) in run-time, which then apply the decision. Updating VGFs in run time with zero downtime is one of facilities provided by virtualization. Figure 4 also shows that, with the concept of GFV (Scenario-3), the QoS requirement thresholds for all three grid services are satisfied. The CVC service now operates normally to potentially remedy the voltage disruption.

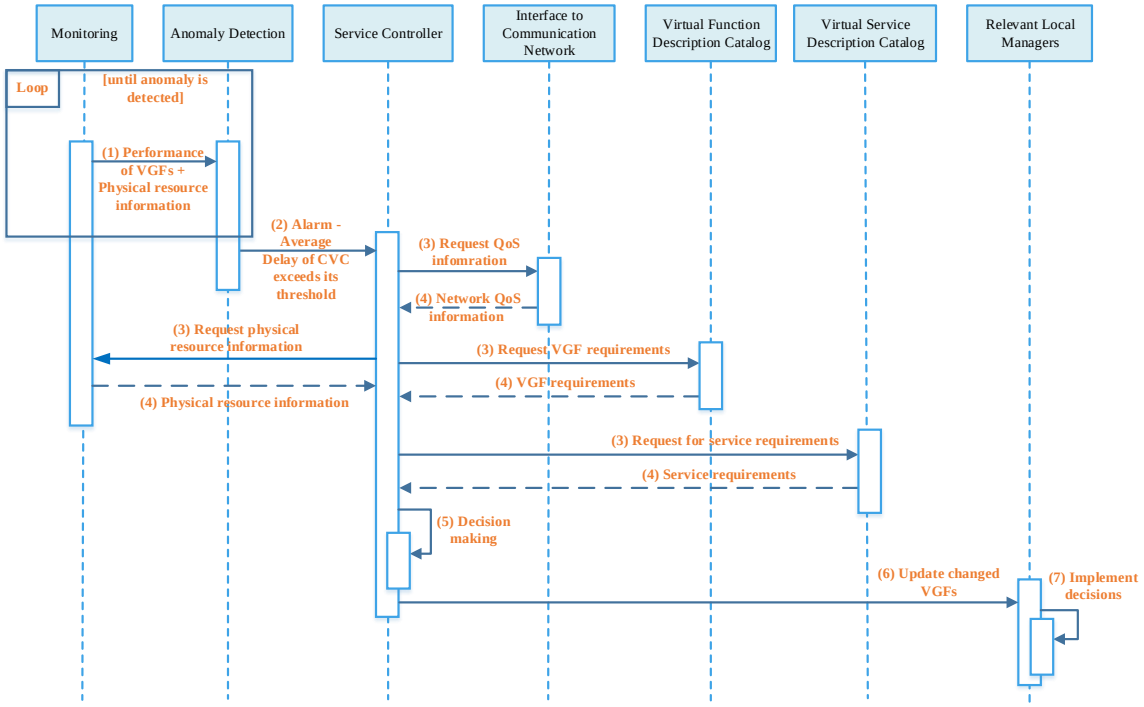


Figure 5. Sequence diagram for use-case 1.

4.2. Use-Case 2

This use-case shows a scenario where two disruptive events causes the power system be in a sub-optimal operating point. The events considered are the failure of the capacitor bank located at

Bus-1 and the failure of Server 01 which hosts the CVC algorithm (refer Figure 3a). The former directly leads to an operational limit violation in the power system, whereas the latter impacts the CVC service. The use of the proposed GFV concept as a remedial solution is then demonstrated. It is noted that this scenario just considers the consequences of these events in the power system, and therefore the ICT domain is not modeled nor simulated. This scenario shows only the effects of not counting with virtualized smart grid services on the power system variables.

The CVC service, which is running on Server 01, periodically determines the optimal adjustments of the controllable elements in the power system so as to comply with the given operational objectives. One of these objectives is to limit the reactive power flow through the transformer within the range of $-5/5$ MVAr. To achieve this, the CVC service (on Server 01) requires information from different parts of the power system. This would be possible using a communication network, which transmits all the required field data to Server 01. With this information, the CVC service can determine new set-points for the controllable elements throughout the system. These include the tap position of the transformer, the step of the capacitor bank and the reactive power set-points of all the DERs. Contrary to the previous use-case, this use-case focuses more on the power system variables instead of communication network characteristics. The power system operating points are determined through load-flow calculations (performed in the DIgSILENT PowerFactory) considering the following sequence of events.

1. The power system operates in an optimal point determined by the CVC service.
2. The power system is subjected to the disruptive disconnection of the capacitor bank. This causes the reactive power flow through the transformer to violate the acceptable operation limits, i.e., $-5/5$ MVAr.
3. Considering this, the CVC service determines new set-points for the transformer tap position and the reactive power set-points of the DERs. The reactive power flow through the transformer is then restored within its acceptable operation range.
4. The system is then subjected to the failure of Server 01 resulting in the interruption of the CVC service. This causes the power system to be in a sub-optimal operating point because the controllable elements can no longer receive optimal set-points from the CVC service. Their control is now based on local measurements.
5. The proposed GFV concept can be used to solve this problem. The CVC service can be relocated to another server, i.e., Server 02. Once the CVC service is running again, it can continue to determine set-points of the controllable elements, which can then restore the system to its optimal operating point.

Figure 6 shows the reactive power flow though the transformer at various considered operating points. The failure of the capacitor bank causes reactive power flow violation though the transformer. The CVC service can solve this by issuing set-points to various available control elements. In the case of CVC server failure, without the proposed GFV concept, the system will only undergo operating points 1, 2, 3 and 4; resulting in a sub-optimal operating point. As a result of decoupling software from underlying hardware by using virtualization, the use of GFV makes it possible for the system to have the operating point 5, i.e., the power system can be reverted to its optimal operating point as soon as the CVC service is restored and run in the new proper device (i.e., server 02). This is possible because the CVC in GFV approach is represented as a software package that is decoupled from hardware and can relocate from one device to another. However, it is important to mention that the sub-optimal operating point 4 can be avoided if the CVC service restoring process (i.e., deciding the new proper place for running CVC by Service Controller and applying this to related Local manager to run CVC) is faster than its action period.

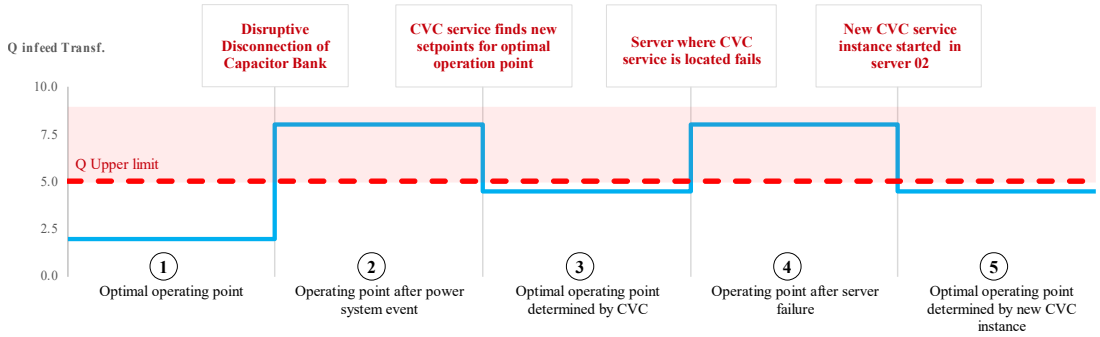


Figure 6. Reactive power flow through transformer in operating points of the use-case 2.

As mentioned in the previous section, with GFV, the functionalities of grid services (i.e., standard grid services code) are virtualized (i.e., deployed on virtual resources such as containers or virtual machines) and represented as VGFs. Similar to the Use-case 1 (see Section 4.1), the Monitoring module continuously monitors the performance of VGFs and the grid computational resources. When the anomaly is detected, i.e., failure of Server 01, the Anomaly Detection module notifies the Service Controller. From here, the sequence of events is similar to Figure 5. However, the reaction from the Service Controller to the anomaly is different. It will now initiate the VGFs corresponding to the CVC service on Server 02. Using the Interface to the Communication Network, the communication network will then be instructed to reroute all data from the field to Server 02, which now hosts the CVC service. This shows how the proposed GFV approach can enhance the operational flexibly of grid automation systems by providing the ability to re-locate grid services, making it independent from underlying hardware.

The proposed concept of GFV differs from communication network mechanisms such as SDN and NFV. The former can handle certain disruptive events in the power grid whereas the latter can only handle the communication networks disruptions. Additionally, GFV performs reconfiguration of the grid services (i.e., Software implementation of services), which are on the application layer; whereas SDN and NFV operate on the network layer.

5. Conclusions

In this paper, a concept of Grid Function Virtualization has been introduced for the first time to improve the operational flexibility of grid automation systems. In this approach the software implantation of grid services (i.e., standard grid service code) can be encapsulated in virtual entities such as containers or virtual machines. This makes grid services independent from underlying hardware and can be reconfigured or relocated in run-time. Furthermore, owing the lack of standard for using virtualization in smart grid, GFV architecture with its building blocks is proposed to realize the important design considerations. With the aid of virtualization, flexible reconfiguration of virtualized grid functions as well as reallocation of computational resources during the normal and abnormal situations in power systems can be enabled. The advantages of proposed approach to mitigate the effect of disruptions both in ICT and power systems side have been shown in two use cases based on the CIGRE MV benchmark grid, where flexible reallocation of computational resources assures that requirements of grid services are properly responded. As the future research direction, the proposed GFV architecture and its building blocks will be investigated in terms of potential deployment tools and interfaces. Moreover, a (co-)simulation framework that includes the virtualization process will then be analyzed and implemented. Furthermore, decoupling grid services from underlying hardware using virtualization imposes software reliability concerns that must be considered in future.

Author Contributions: Conceptualization, S.A., D.B. and C.K.; Simulation, A.N., B.H.H. and F.C.; Methodology, S.A. and B.H.H.; Validation, B.H.H., D.B. and A.N.; Writing—review & editing, S.A., A.N., B.H.H., C.K., D.B. and S.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work is funded partially by the European Community's Horizon 2020 Program (H2020/2014–2020) under project "ERIGrid" (Grant Agreement No. 654113) and also by German Federal Ministry for Economic Affairs and Energy (BMWi) under agreement no. 03EI6001B (i-Autonomous).

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

Abbreviations

The following abbreviations are used in this manuscript:

CIGRE	Conseil International des Grands Réseaux Électriques
CPU	Central Processing Unit
CVC	Coordinated Voltage Control
DER	Distributed Energy Resource
ECU	Electronic Control Units
GFD	Grid Function Descriptors
GSD	Grid Service Descriptors
GFV	Grid Function Virtualization
IaaS	Infrastructure-as-a-Service
ICT	Information and Communication Technology
IED	Intelligent Electronic Devices
IIoT	Industrial Internet of Things
IMA	Integrated Modular Avionics
IoT	Internet of Things
NF	Network Function
NFV	Network Function Virtualization
PLC	Power Line Communication
PMU	Phasor Measurement Unit
QoS	Quality of Service
SCADA	Supervisory Control and Data Acquisition
SDN	Software-Defined Networking
SE	State Estimation
UC	Unit Commitment
VGF	Virtual Grid Function
VNF	Virtual Network Function
WSN	Wireless Sensor Network

References

1. Mallet, P.; Granstrom, P.; Hallberg, P.; Lorenz, G.; Mandatova, P. Power to the People!: European Perspectives on the Future of Electric Distribution. *IEEE Power Energy Mag.* **2014**, *12*, 51–64. [CrossRef]
2. Al-Rubaye, S.; Kadhum, E.; Ni, Q.; Anpalagan, A. Industrial internet of things driven by SDN platform for smart grid resiliency. *IEEE Internet Things J.* **2017**, *6*, 267–277. [CrossRef]
3. Narayan, A.; Klaes, M.; Babazadeh, D.; Lehnhoff, S.; Rehtanz, C. First Approach for a Multi-dimensional State Classification for ICT-reliant Energy Systems. In Proceedings of the International ETG-Congress 2019, Esslingen, Germany, 8–9 May 2019; pp. 1–6.
4. Krüger, C.; Velasquez, J.; Babazadeh, D.; Lehnhoff, S. Flexible and reconfigurable data sharing for smart grid functions. *Energy Inform.* **2018**, *1*, 43. [CrossRef]
5. Brand, M.; Ansari, S.; Castro, F.; Chakra, R.; Hage Hassan, H.; Krüger, C.; Babazadeh, D.; Lehnhoff, S. Framework for the Integration of ICT-relevant Data in Power System Applications. In Proceedings of the 2019 IEEE PES PowerTech, Milan, Italy, 23–27 June 2019; pp. 1–6.
6. Narayan, A.; Krueger, C.; Goering, A.; Babazadeh, D.; Harre, M.C.; Wortelen, B.; Luedtke, A.; Lehnhoff, S. Towards Future SCADA Systems for ICT-reliant Energy Systems. In Proceedings of the International ETG-Congress 2019; ETG Symposium, Esslingen, Germany, 8–9 May 2019; pp. 1–7.
7. Stewart, E.M.; von Meier, A. Phasor measurements for distribution system applications. In *Smart Grid Handbook*; Wiley: Hoboken, NJ, USA, 2016; pp. 1–10.
8. Alam, I.; Sharif, K.; Li, F.; Latif, Z.; Karim, M.M.; Nour, B.; Biswas, S.; Wang, Y. IoT Virtualization: A Survey of Software Definition & Function Virtualization Techniques for Internet of Things. *arXiv* **2019**, arXiv:1902.10910.

9. Blenk, A.; Basta, A.; Zerwas, J.; Kellerer, W. Pairing SDN with network virtualization: The network hypervisor placement problem. In Proceedings of the 2015 IEEE Conference on Network Function Virtualization and Software Defined Network (NFV-SDN), San Francisco, CA, USA , 18–21 November 2015; pp. 198–204.
10. Plauth, M.; Feinbube, L.; Polze, A. A performance survey of lightweight virtualization techniques. In Proceedings of the European Conference on Service-Oriented and Cloud Computing, Oslo, Norway, 27–29 September 2017; pp. 34–48.
11. Dong, X.; Lin, H.; Tan, R.; Iyer, R.K.; Kalbarczyk, Z. Software-defined networking for smart grid resilience: Opportunities and challenges. In Proceedings of the 1st ACM Workshop on Cyber-Physical System Security, Singapore, 14–17 April 2015; ACM: New York, NY, USA, 2015; pp. 61–68.
12. Loveland, S.; Dow, E.M.; LeFevre, F.; Beyer, D.; Chan, P.F. Leveraging virtualization to optimize high-availability system configurations. *IBM Syst. J.* **2008**, *47*, 591–604. [CrossRef]
13. Khan, I.; Belqasmi, F.; Glitho, R.; Crespi, N.; Morrow, M.; Polakos, P. Wireless sensor network virtualization: A survey. *IEEE Commun. Surv. Tutor.* **2015**, *18*, 553–576. [CrossRef]
14. Lee, C.; Shin, S. Fault Tolerance for Software-Defined Networking in Smart Grid. In Proceedings of the 2018 IEEE International Conference on Big Data and Smart Computing (BigComp), Shanghai, China, 15–17 January 2018; pp. 705–708.
15. Rehmani, M.H.; Davy, A.; Jennings, B.; Assi, C. Software defined networks based smart grid communication: A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2637–2670. [CrossRef]
16. Danzi, P.; Angjelichinoski, M.; Stefanović, Č.; Dragičević, T.; Popovski, P. Software-defined microgrid control for resilience against denial-of-service attacks. *IEEE Trans. Smart Grid* **2018**, *10*, 5258–5268. [CrossRef]
17. Abdella, J.; Shuaib, K. Peer to peer distributed energy trading in smart grids: A survey. *Energies* **2018**, *11*, 1560. [CrossRef]
18. Rinaldi, S.; Ferrari, P.; Brandão, D.; Sulis, S. Software defined networking applied to the heterogeneous infrastructure of smart grid. In Proceedings of the 2015 IEEE World Conference on Factory Communication Systems (WFCS), Palma de Mallorca, Spain, 27–29 May 2015; pp. 1–4.
19. Ghosh, U.; Chatterjee, P.; Shetty, S. A security framework for SDN-enabled smart power grids. In Proceedings of the 2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW), Atlanta, GA, USA, 5–8 June 2017, pp. 113–118.
20. Hans, M.; Phad, P.; Jogi, V.; Udayakumar, P. Energy Management of Smart Grid using Cloud Computing. In Proceedings of the 2018 International Conference on Information, Communication, Engineering and Technology (ICICET), Pune, India, 29–31 August 2018; pp. 1–4.
21. Cankaya, H.C. Software Defined Networking and Virtualization for Smart Grid. In *Transportation and Power Grid in Smart Cities: Communication Networks and Services*; Wiley: Hoboken, NJ, USA, 2018; pp. 171–190.
22. Meloni, A.; Pegoraro, P.A.; Atzori, L.; Castello, P.; Sulis, S. IoT cloud-based distribution system state estimation: Virtual objects and context-awareness. In Proceedings of the 2016 IEEE International Conference on Communications (ICC), Kuala Lumpur, Malaysia, 22–27 May 2016; pp. 1–6.
23. Cosovic, M.; Tsitsimelis, A.; Vukobratovic, D.; Matamoros, J.; Anton-Haro, C. 5G mobile cellular networks: Enabling distributed state estimation for smart grids. *IEEE Commun. Mag.* **2017**, *55*, 62–69. [CrossRef]
24. Mijumbi, R.; Serrat, J.; Gorricho, J.L.; Bouten, N.; De Turck, F.; Boutaba, R. Network function virtualization: State-of-the-art and research challenges. *IEEE Commun. Surv. Tutor.* **2015**, *18*, 236–262. [CrossRef]
25. European Telecommunications Standards Institute (ETSI). *GS NFV-MAN 001 V1. 1.1 Network Function Virtualisation (NFV); Management and Orchestration*; ETSI: Sophia Antipolis, France, 2014.
26. Yi, B.; Wang, X.; Li, K.; Huang, M. A comprehensive survey of network function virtualization. *Comput. Netw.* **2018**, *133*, 212–262. [CrossRef]
27. Kim, H.; Feamster, N. Improving network management with software defined networking. *IEEE Commun. Mag.* **2013**, *51*, 114–119. [CrossRef]
28. Kreutz, D.; Ramos, F.M.; Verissimo, P.; Rothenberg, C.E.; Azodolmolky, S.; Uhlig, S. Software-defined networking: A comprehensive survey. *Proc. IEEE* **2015**, *103*, 14–76. [CrossRef]
29. Attarha, S.; Hosseiny, K.H.; Mirjalily, G.; Mizanian, K. A load balanced congestion aware routing mechanism for Software Defined Networks. In Proceedings of the 2017 Iranian Conference on Electrical Engineering (ICEE), Tehran, Iran, 2–4 May 2017; pp. 2206–2210.

30. Toyonaga, S.; Kominami, D.; Murata, M. Virtual wireless sensor networks: Adaptive brain-inspired configuration for internet of things applications. *Sensors* **2016**, *16*, 1323. [CrossRef] [PubMed]
31. Liu, R.; Srivastava, M. VirtSense: Virtualize Sensing through ARM TrustZone on Internet-of-Things. In *Proceedings of the 3rd Workshop on System Software for Trusted Execution*; ACM: New York, NY, USA, 2018; pp. 2–7.
32. Varasteh, A.; Goudarzi, M. Server consolidation techniques in virtualized data centers: A survey. *IEEE Syst. J.* **2015**, *11*, 772–783. [CrossRef]
33. Nishiguchi, Y.; Yano, A.; Ohtani, T.; Matsukura, R.; Kakuta, J. IoT fault management platform with device virtualization. In Proceedings of the 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 5–8 February 2018; pp. 257–262.
34. Broy, M.; Kruger, I.H.; Pretschner, A.; Salzmann, C. Engineering automotive software. *Proc. IEEE* **2007**, *95*, 356–373. [CrossRef]
35. Rajan, A.K.S.; Feucht, A.; Gamer, L.; Smaili, I. Hypervisor for consolidating real-time automotive control units: Its procedure, implications and hidden pitfalls. *J. Syst. Archit.* **2018**, *82*, 37–48. [CrossRef]
36. Herber, C.; Reinhardt, D.; Richter, A.; Herkersdorf, A. HW/SW trade-offs in I/O virtualization for Controller Area Network. In Proceedings of the 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), San Francisco, CA, USA, 8–12 June 2015; pp. 1–6.
37. Morabito, R.; Petrolo, R.; Loscri, V.; Mitton, N.; Ruggeri, G.; Molinaro, A. Lightweight virtualization as enabling technology for future smart cars. In Proceedings of the 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Lisbon, Portugal, 8–12 May 2017; pp. 1238–1245.
38. Bello, L.L.; Mariani, R.; Mubeen, S.; Saponara, S. Recent Advances and Trends in On-board Embedded and Networked Automotive Systems. *IEEE Trans. Ind. Inform.* **2019**, *15*, 1038–1051. [CrossRef]
39. Parkinson, P.; Kinnan, L. Safety-critical software development for integrated modular avionics. *Embed. Syst. Eng.* **2003**, *11*, 40–41.
40. Kleidermacher, D.; Wolf, M. Mils virtualization for integrated modular avionics. In Proceedings of the 2008 IEEE/AIAA 27th Digital Avionics Systems Conference, St. Paul, MN, USA, 26–30 October 2008.
41. Kaiwartya, O.; Abdullah, A.H.; Cao, Y.; Lloret, J.; Kumar, S.; Shah, R.R.; Prasad, M.; Prakash, S. Virtualization in wireless sensor networks: Fault tolerant embedding for internet of things. *IEEE Internet Things J.* **2018**, *5*, 571–580. [CrossRef]
42. Champa, H. An Extensive Review on Sensing as a Service Paradigm in IoT: Architecture, Research Challenges, Lessons Learned and Future Directions. *Int. J. Appl. Eng. Res.* **2019**, *14*, 1220–1243.
43. Yedder, H.B.; Ding, Q.; Zakia, U.; Li, Z.; Haeri, S.; Trajkovic, L. Comparison of virtualization algorithms and topologies for data center networks. In Proceedings of the 2017 26th International Conference on Computer Communication and Networks (ICCCN), Vancouver, BC, Canada, 31 July–3 August 2017, pp. 1–6.
44. Horváth, Á.; Varró, D. Model-driven development of ARINC 653 configuration tables. In Proceedings of the 29th Digital Avionics Systems Conference, Salt Lake City, UT, USA, 3–7 October 2010, pp. 6.E.3-1–6.E.3-15.
45. Magableh, B.; Almiani, M. A Self Healing Microservices Architecture: A Case Study in Docker Swarm Cluster. In Proceedings of the International Conference on Advanced Information Networking and Applications, Matsue, Japan, 27–29 March 2019; Springer: Berlin, Germany, 2019; pp. 846–858.
46. PE/PSRCC. *IEEE Standard for SCADA and Automation Systems, IEEE Std C37.1 (Revision of IEEE Std C37.1-1994)*; IEEE: Piscataway, NJ, USA, 2008.
47. Zhu, K.; Chenine, M.; Nordstrom, L. ICT architecture impact on wide area monitoring and control systems' reliability. *IEEE Trans. Power Deliv.* **2011**, *26*, 2801–2808. [CrossRef]