Computers and Electrical Engineering xxx (2014) xxx–xxx

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

Using Software Defined Networking to manage and control IEC 61850-based systems ☆

Elias Molina *, Eduardo Jacob, Jon Matias, Naiara Moreira, Armando Astarloa

Department of Communications Engineering, University of the Basque Country UPV/EHU, Alameda de Urquijo s/n, 48013 Bilbao, Spain

ARTICLE INFO

Article history:
Received 15 May 2014
Received in revised form 22 October 2014
Accepted 22 October 2014
Available online xxxx

Keywords:
IEC 61850
Monitoring
OpenFlow
sFlow
Smart Grid
Software Defined Networking

ABSTRACT

Smart Grid makes use of Information and Communications Technology (ICT) infrastructures for the management of the generation, transmission and consumption of electrical energy to increase the efficiency of remote control and automation systems. One of the most widely accepted standards for power system communication is IEC 61850, which defines services and protocols with different requirements that need to be fulfilled with traffic engineering techniques. In this paper, we discuss the implementation of a novel management framework to meet these requirements through control and monitoring tools that provide a global view of the network. With this purpose, we provide an overview of relevant Software Defined Networking (SDN) related approaches, and we describe an architecture based on OpenFlow that establishes different types of flows according to their needs and the network status. We present the implementation of the architecture and evaluate its capabilities using the Mininet network emulator.

1. Introduction

In industrial networks or, in general, mission-critical environments, it is necessary to develop mechanisms for ensuring network performance such that the provided services are not jeopardized. Currently, the Smart Grid concept is a relevant critical use case, which includes the protection, automation and control of electric power systems, and that is supported by ICT facilities that must meet the real-time requirements of these applications with high dependability and security. However, according to [1], "communication technologies are not yet mature for the revolution of transmission grids, and the existing grids lack enough compatibility to accommodate the implementation of spear-point technologies in the practical networks". The same authors predict that "adaptive networks will allow open-standardized communication protocols to operate on a unique platform. Real-time control based on a fast and accurate information exchange in different platforms will improve system resilience by enhancing the reliability and optimization of the transmission asset utilization".

The International Electrotechnical Commission (IEC) is the most important standardization body in this area, being noteworthy the emerging IEC 61850 standard for power utility applications, which proposes a series of specifications that globally define the configuration of a power substation (either internally or externally), including new communication services, requirements and priorities. For the purpose of developing ICT facilities that enable substation automation, the

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Associate Editor Dr. Ziya Arnavut.

* Corresponding author.

http://dx.doi.org/10.1016/j.compeleceng.2014.10.016
0045-7906/

management and control planes have to be aware of the network resources and requirements mentioned to maintain proper network performance.

In this paper, we provide a description of the IEC 61850 protocol stack, and a framework that uses the Software Defined Networking (SDN) paradigm in which "the control and data planes are decoupled, network intelligence and state are logically centralized, and the underlying network is abstracted from the applications" [2]. The proposed platform establishes monitoring and management tasks that build a global view of network utilization, allowing it to act quickly and accurately. Consequently, a deeper and more flexible control is achieved by implementing traffic engineering in IEC 61850-based systems, to enhance network robustness.

Regarding the use of SDN as an enabling technology for the development of Smart Grid solutions, we review several studies that have recently perceived opportunities for this integration, along with other SDN-related research applicable to IEC 61850 compliant systems.

The rest of this paper is organized as follows: Section 2 provides an overview of the IEC 61850 specification; Section 3 describes the main control and management technologies used in the proposal; Section 4 analyzes the services offered by the architecture, whose results are shown in Section 5; Section 6 contains related and future work; and finally, in Section 7, we present the conclusions.

2. IEC 61850

The IEC 61850 specification, entitled "Communication Networks and Systems for Power Utility Automation", covers many topics related to the equipment and interfaces with the substation automation systems. For this work, the relevant parts of the standard are those focused on the definition of the information model and communication services.

2.1. Formal configuration language

The information model is included in IEC 61850-7-x documents, which lead to design substations in logical nodes, and characterize their data inputs and outputs. With this goal, IEC 61850-6 [3] defines the Substation Configuration Language (SCL), based on eXtensible Markup Language (XML) schema, allowing us to model and share substation parameters, e.g., system topology or Intelligent Electronic Device (IED) configuration. Different SCL files are available depending on their objectives. Specifically, we highlight the Substation Configuration Description (SCD), intended to design and configure a whole substation. Particularly, the communication section of an SCD file allows the setting of device parameters such as IP address, destination MAC addresses, VLAN-ID and VLAN-PRIORITY. However, the current information model is not complete enough to represent the communication network in detail; for example, it does not describe the physical network topology. According to [4], the specification should integrate the network configuration in the unified engineering process of substation automation.

2.2. Communications

IEC 61850-8-1 and 61850-9-2 describe communication profiles for teleprotection, measurement and control signals over packet-switched networks. These are mapped to the following protocol stack:

- TCP/IP traffic: it includes, among other data applications, the Manufacturing Messaging Specification (MMS) Protocol that defines unicast messages in a client-server model. This traffic normally flows from the IEDs to the substation administrator, such as the Supervisory Control And Data Acquisition (SCADA).
- Non-IP traffic: it is mapped directly to the Ethernet Link layer to reduce protocol overhead, and consequently, to increase the performance. It allows the sending of time-critical high-priority information within the maximum allowable latency according to the application. It specifies the use of multicast frames, and there are two types of messages generated by the Merging Units (MU) or IEDs:
  - Generic Object Oriented Substation Event (GOOSE) for protection messaging (interlocking, control, and tripping signals).
  - Sampled Values (SV), which carry voltage and current samples.

Outside the substations, GOOSE and SV messages can be transmitted through tunnel technologies (IEC/TR 61850-90-1 and 61850-90-2) or by using Routable-GOOSE and Routable-SV (IEC/TR 61850-90-5), which are based on TCP or UDP over IP multicast.

It is noteworthy that an IEC 61850 compliant system must ensure that the requirements specified in IEC 61850-5 are met. They depend on the protection and control applications (performance class) thereof; for instance, the most stringent message accepts a maximum delay of three milliseconds, which must be guaranteed independently of the network condition.

Please cite this article in press as: Molina E et al. Using Software Defined Networking to manage and control IEC 61850-based systems. Comput Electr Eng (2014), http://dx.doi.org/10.1016/j.compeleceng.2014.10.016

3. Decoupled control and management planes

In the SDN paradigm, control and management (C&M) are decoupled from the data plane. Thus, in this section, several C&M technologies are analyzed to determine the best choice to build an SDN platform suitable for our target application.

3.1. Control protocol

Regarding the control plane, the most significant technology is OpenFlow, which is a protocol promoted and standardized by the Open Networking Foundation (ONF) [2]. In this technology, a controller can access and define the data path of an OpenFlow switch by adding, updating and deleting flow entries in forwarding tables. These tables contain multiple match fields (ingress port, metadata and packet headers), priorities and actions associated with each flow entry [5]. It is important to emphasize that the establishment of forwarding rule entries can be performed in different ways:

- *Reactive mode*: the controller can dynamically insert entries in response to switch requests.
- *Proactive mode*: the flow tables are statically prepopulated, thereby reducing latency.

Though a more centralized structure seems to contradict with features identified in critical time-sensitive environments, these possible drawbacks can be overcome as summarized below:

- OpenFlow centralized operation may pose scalability problems; however, since version 1.2, switches can communicate with multiple controllers so that they can balance the load or set backup controllers. This enables a distributed control plane that avoids single points of failure.
- Minimal latencies: because the control plane is decoupled, being communicated via the OpenFlow protocol that runs over TCP, it may experience higher latencies than in monolithic approaches. Accordingly, time-sensitive scenarios require a proactive behavior that does not introduce additional delays. For other traffic, such as MMS or HTTP, this mode of operation may not be required.
- Reliability schemes: starting on version 1.1, OpenFlow tables support a fast failover group entry as a protection mechanism [5]. Thus, it is possible to accelerate the detection and fault recovery by acting directly on the OpenFlow switches without involving the controller. Moreover, it can be combined with a backup path computation, which is proactively installed by the controller, so that the switchover time is reduced. Additionally, the use of Operations, Administration and Maintenance (OAM) tools improves network resilience, fault management or congestion problems.

3.2. Monitoring techniques

Among the main tools for traffic monitoring, we highlight the sFlow standard (IETF RFC 3176), which operates via packet sampling, such that sFlow agents (switches or routers) push their interface counters and sampled packets to an sFlow collector that is able to report packet headers for each flow. sFlow relies on a sampling-based method whose accuracy depends on the reporting interval specified in the agents. The estimation of the expected error can be extracted from [6]. Additionally, these authors concede that sFlow is suited to real-time traffic engineering, providing flexibility, scalability, low latency and advantages over other monitoring protocols such as:

- *OpenFlow*: the OpenFlow protocol itself allows the controller to retrieve counters per flows, ports and queues from controlled switches, so it could be an option for implementing the network monitoring task. Nevertheless, these statistics are tightly associated with every flow entry installed on switches and this is an inconvenience for anomaly detection processes, as discussed in [7].
- *NetFlow/IPFIX*: NetFlow is a push-based monitoring technology developed by Cisco that has been superseded by the IP Flow Information Export (IPFIX) as a standard (IETF RFC 7011). For our target application, one of the main advantages of sFlow is that it allows us to monitor flows defined by layer 2 to layer 7 information of the OSI reference model, while on the contrary, NetFlow and IPFIX are oriented to collect IP traffic information, not allowing us to determine flows with layer 2 headers. Moreover, NetFlow is not suitable for low-latency network measurements [6]. These features are indispensable for monitoring SV and GOOSE messages in substation local area networks (LANs).
- *SNMP/RMON*: on the one hand, the Simple Network Management Protocol (SNMP, IETF RFC 1157) offers a widely accepted protocol, and its use for polling statistics in substations is suggested by IEC 61850-90-4 [8]. However, according to [9], "SNMP is not well suited for end-to-end measurements that are needed for performance metrics". Additionally, the analysis of [10] is remarkable in showing a "passive flow monitoring framework for OpenFlow enabled experimental facilities" and discussing the advantages of sFlow over SNMP, such as "pushing counters is much more efficient than retrieving them using SNMP". In addition, sFlow uses XDR (IETF RFC 1832) as the data representation protocol, which is simpler than that used in SNMP (ASN.1, IETF RFC 3641), "hence significantly reducing CPU overhead in switches and collectors", being more advantageous to monitor large networks.

Please cite this article in press as: Molina E et al. Using Software Defined Networking to manage and control IEC 61850-based systems. Comput Electr Eng (2014), http://dx.doi.org/10.1016/j.compeleceng.2014.10.016

On the other hand, the Remote Network MONitoring (RMON, IETF RFC 2819) specification is based on SNMP to improve network monitoring and traffic analysis. Nevertheless, as stated in [9], "the use of RMON by service providers has been limited due to the complexity and cost of the RMON probes".

3.3. Management protocols

Despite the fact that MMS allows us to obtain the status of communication parameters, this information is very limited and does not provide "any way to control the settings of these functions" [4]. This prevents the information model of a switch from being viewed as an individual IED. Additionally, its use is not widespread in network elements; thereby, MMS is not a suitable alternative to traditional management protocols. Typically, network elements are managed by proprietary Command Line Interfaces (CLIs) or SNMP-based configuration tools. In the case of SNMP, it allows us to manage systems through exposed Management Information Base (MIB) parameters.

In addition to the emergence of OpenFlow, different proposals have been published to operate the management plane. However, currently, there is no unified standard for managing all aspects of an OpenFlow device. This lack of interoperability is an important issue to support multi-vendor networks. In our case, because the implementation is performed with Open vSwitch (software switch that supports OpenFlow and sFlow [11]), the resources are provisioned by the Open vSwitch Database Management Protocol (OVSDB, standardized in IETF RFC 7047), which uses a remote procedure call encoded in JavaScript Object Notation (JSON-RPC).

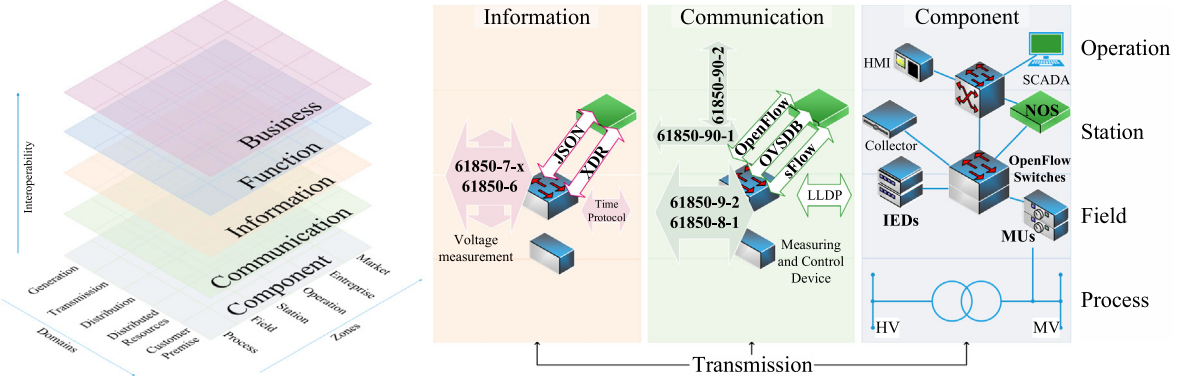
Among other options for configuring OpenFlow switches, we highlight the OpenFlow Management and Configuration Protocol (OF-Config), developed by ONF [2], which uses NETCONF (IETF RFC 6241), that is, an XML-RPC-based network management approach (RPC encoded in XML). Nevertheless, the OF-Config protocol appeared recently and its degree of deployment is reduced (currently, it is not supported by Open vSwitch).

4. Architecture

Obviously, the transmission of measurement and control data takes time and depends on network features and configuration in addition to its current status. Our approach integrates different services that help guarantee a more deterministic behavior for an IEC 61850-based network. For the elaboration of the proposal, we have applied the reference Smart Grid Architecture Model (SGAM) defined by the CEN–CENELEC–ETSI Smart Grid Coordination Group [12], whose methodology expedites the design of new structured power system developments. As outlined subsequently, this method has facilitated the identification of the Smart Grid use case and the design of a complete Network Operating System (NOS) that can support the requirements set forth.

4.1. SGAM framework

SGAM describes the mapping of the use case in question into an entire Smart Grid architecture decomposed in a layered three-dimensional model (Fig. 1(a)). Each layer (interoperability dimension) includes the activities and actors in a plane with vertical (zones) and horizontal (domains) dependencies. Because our interest is focused on ICT within IEC 61850 substations, we underline the relations in information, communication and, to a lesser extent on component layers [12]:



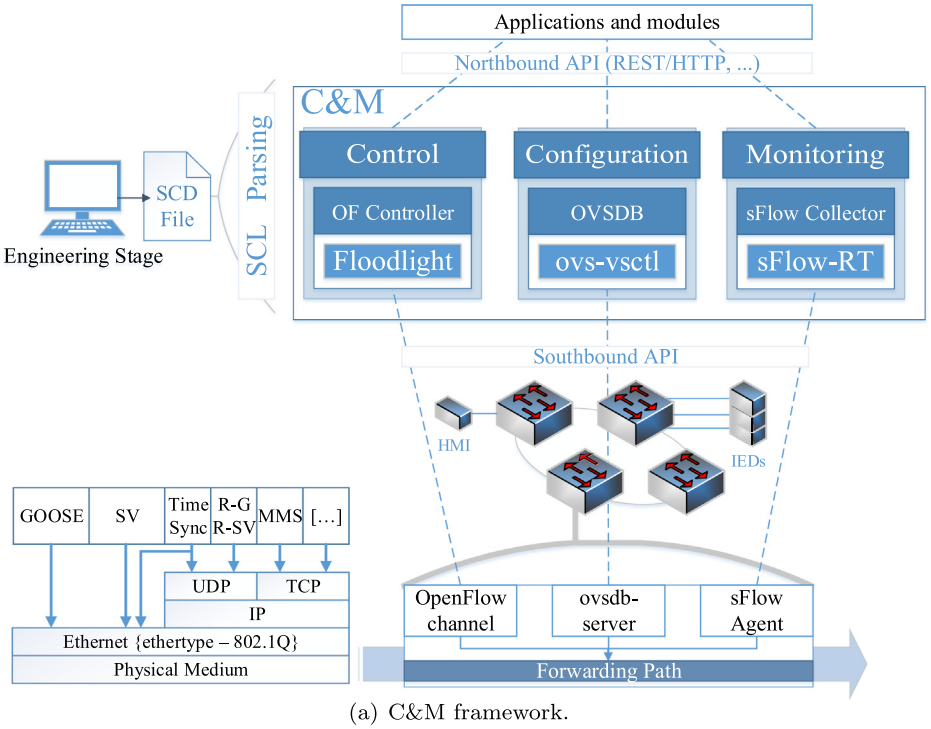
(a) Entire layered three-dimensional model. (b) Information, communication and component layers for transmission domain.

Fig. 1. SGAM framework.

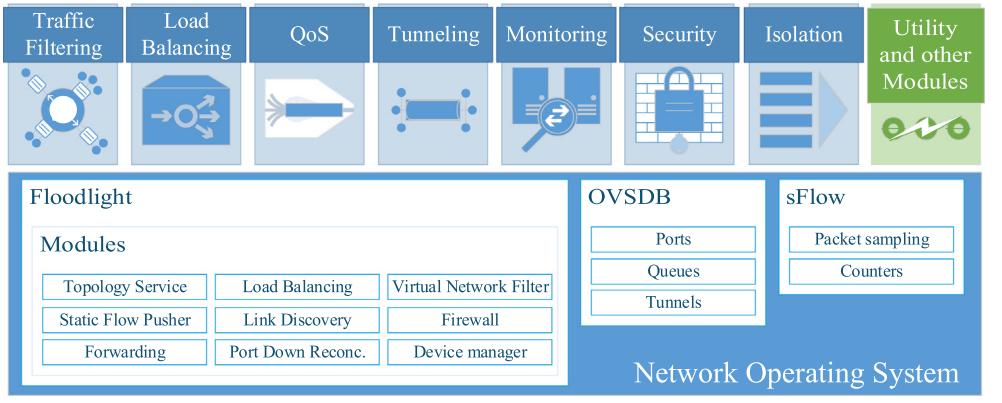
Please cite this article in press as: Molina E et al. Using Software Defined Networking to manage and control IEC 61850-based systems. Comput Electr Eng (2014), http://dx.doi.org/10.1016/j.compeleceng.2014.10.016

- The first layer represents the data exchanged between functions, services, and components. They can be identified by analyzing the information exchanged between the actors.
- The second layer consists of suitable protocols and mechanisms for exchanging that information and the data models allocated in the upper layer. It has to take into account the communication requirements.
- Finally, the component layer is derived from the actors involved in the use case, comprising physical components such as assets, devices, grid equipment and operators.

According to the domains that form the energy conversion chain, the use case is placed in the transmission domain, including high-voltage (HV) and medium-voltage (MV) equipment; whereas among the zones of power system management, the use case is situated on the station zone that encompasses the aggregation of the field level (equipment to monitor, protect and control) and connects with the operation zone (power control operation). Subsequently, the model comprises a heterogeneous communication infrastructure disaggregated into data models, protocols, and control functions. Fig. 1(b) shows the resulting transmission domain in the zones and layers of interest.



(a) C&M framework.



(b) NOS and applications.

Fig. 2. SDN architecture.

Please cite this article in press as: Molina E et al. Using Software Defined Networking to manage and control IEC 61850-based systems. Comput Electr Eng (2014), http://dx.doi.org/10.1016/j.compeleceng.2014.10.016

4.2. Network operating system

As shown in Fig. 2(a), the proposed development is formed by the above-mentioned components (Section 3) along an IEC 61850 protocol stack. The elements require cooperation among themselves so that communication with network elements is performed through so-called southbound APIs, whereas applications written on top of the C&M architecture connect to each other via Northbound APIs, specifically based on the JSON Representational State Transfer (REST). All of this is summarized in the following way:

- With respect to the OpenFlow controller, the development relies on the Floodlight open source software [13], and many of the employed features are closely related to it.
- The sFlow agent reports sFlow datagrams (over UDP) to the monitoring system. In our case, it is implemented with the sFlow-RT collector.
- Each Open vSwitch executes a software application (ovsdb-server) responsible for processing the OVSDB configuration protocol messages from ovs-vsctl and configuring the switch accordingly.

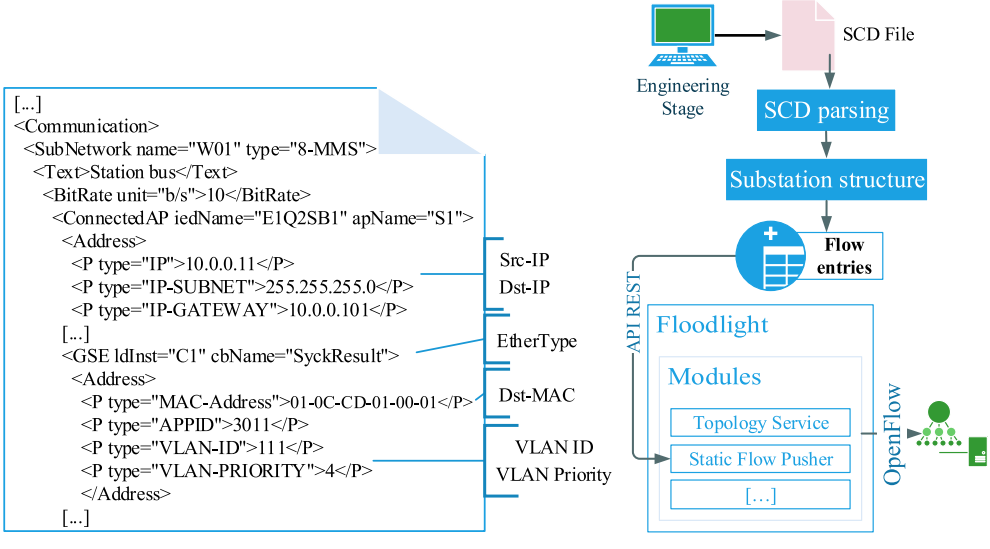
In summary, Fig. 2(b) illustrates the different elements of the network intelligence residing in the C&M framework. Our specific implementation of all features provided by the platform is described in Sections 4.4 to 4.6.

4.3. OpenFlow and IEC 61850 integration

To integrate the IEC 61850 communication and data models, the proposed architecture benefits from the programmability feature of OpenFlow. Thus, SCL parsing provides a mapping method between the engineering stage and C&M platform. In this process, SCD files are translated into information that can be handled by the OpenFlow controller, obtaining accurate information about the substation configuration (Fig. 3). Thus, the controller can know the existing devices and their data flows in managed substations, so it may automatically determine the logical topology of the substation. The controller has to decide how to route, modify or discard traffic flows, providing exactly the required performance. In this case, we have incorporated static rules with the highest priority for critical traffic flows, using the Static Flow Pusher Floodlight module (Fig. 3(a)).

Several properties are obtained after an appropriate SCD file parsing. These allow us to build flow forwarding entries that are installed in switches, enabling IEDs to publish and subscribe information. Specifically, we parse each IED section, for which there are a series of *input* subsections that define all external signals of interest identified by the name of the publisher IED (*iedName*). Fig. 3(a) partially illustrates an SCD file, where we can identify elements and values that are mapped on OpenFlow fields.

To establish the flows correctly, the controller has to know the connection between the switches and the IEDs (ports and physical topology). In our case, we consider that the connection of each device with each switch in a network is known, so this information is statically incorporated in the controller logic. Namely, the controller has an a priori knowledge of IED



(a) Mapping of SCL parameters in OpenFlow fields. (b) Parsing process flow.

Fig. 3. OpenFlow and IEC 61850 integration.

Please cite this article in press as: Molina E et al. Using Software Defined Networking to manage and control IEC 61850-based systems. Comput Electr Eng (2014), http://dx.doi.org/10.1016/j.compeleceng.2014.10.016

connections, associating a particular IED with a concrete edge switch. This involves installing rules, which associate a publisher-subscriber flow to the corresponding input/output switch ports. We prefer to choose this inflexible choice, where a particular port is assigned to an IED, making it difficult the port swapping once the network is deployed. Another alternative to obtain the physical connection of IEDs is the approach described in [14], where the controller communicates proactively with IEDs by ICMP; likewise, this is suitable because static IP addresses are recommended [8]. Nevertheless, this restricts the use of simpler devices that only implement SV and GOOSE (layer 2 only devices), which is very common in process bus equipment.

In summary, this proposal may be an appropriate tool to automate network administration, which is a need reinforced by [15], where the authors suggest that "the complexity of the data network configuration for a large substation makes automated management of network switches an attractive option [...] automated tools could be developed to extract this information to streamline the VLAN and multicast address filter configuration of Ethernet switches from multiple vendors". Moreover, proposals for enhancing IEC 61850 as found in [4], where several extensions related to network parameters and communication monitoring are defined to be included in IEC 61850-6. Consequently, processing these new SCL parameters may enable future scenarios that can be handled centrally.

4.4. Data path control

Below, we describe the implemented features that process the data path of a network, allowing us to forward flows according to their requirements, for example, for latency or Quality of Service (QoS).

4.4.1. Shortest path forwarding

In IEEE 802.3, there is no mechanism to discard duplicate frames or a time-to-live field, implying that loops should be avoided. Thus, the more widely used protocols in IEC 61850 substations are based on a Spanning Tree approach such as Rapid Spanning Tree Protocol (RSTP, IEEE 802.1D-2004), whose performance is studied in [8]. This approach employs a distributed algorithm to disable certain ports and obtain loop-free topologies. These resulting topologies do not take advantage of all physically redundant links; therefore, data do not have to follow the shortest path without achieving the optimal delay, which is considered useful for time-sensitive services.

In our case, the OpenFlow controller is able to perform unicast data traffic forwarding across the shortest path. This is possible because the Floodlight controller is aware of the network topology through discovery services (Fig. 2(b)) based on the Link Layer Discovery Protocol (LLDP, IEEE 802.1AB).

Recently, several proposals have been developed as an alternative to the Spanning Tree-based protocols, highlighting the Transparent Interconnection of Lots of Links (TRILL, IETF RFC 6325) and IEEE 802.1aq. Both are based on the IS–IS Link State Protocol, allowing them to compute the shortest paths by avoiding loops and do load balancing through multiples paths. Ref. [16] shows that TRILL results in "an enhanced alternative to RSTP"; however, it "is still unable to meet the required convergence time claimed by the Smart Grid requirements".

4.4.2. Traffic filtering

Because GOOSE and SV are both multicast frames, the IEDs should be configured to subscribe or not to subscribe to certain frames according to the SCD files. Additionally, on the other hand, the switches should [8] be configured to filter specific multicast MAC addresses and VLAN IDs only to determined ports, to reduce the network load. In our architecture, the forwarding rules are automatically generated from SCD parsing and are installed into controlled switches. Therefore, this automatic and static behavior facilitates the deployment and implementation of a network, allowing the more critical traffic (only GOOSE and SV messages are predetermined by SCD files) to flow efficiently through the network.

4.4.3. QoS pushing

Taking into account the bandwidth-sharing techniques in IEEE 802.3, latency reduction can be achieved by logical traffic separation and prioritization; therefore, it is recommended in [8] that IEC 61850 networks use the IEEE 802.1Q standard.

Moreover, rate limiting or policing mechanisms adjust the incurred frame latency in a switch. In [17], the authors verify experimentally the latency in an IEC 61850 substation, where the network resources are shared among data with different priorities (SV, GOOSE and SNMP), and they suggest that "port ingress rate limiting is one way of protecting against failures related to network flooding, but this also complicates network design and configuration".

For implementing QoS mechanisms, our platform allows network designers to establish traffic shaping policies that distinguish flow types in an easily centralized manner. In particular, we use the QoS Floodlight module (Fig. 2(b)), which pushes flow rules that redirect specific traffic to different queues, which must be previously created and configured on the particular switch[1]; in our case, we use the OVSDB protocol (via ovsdb-client software). As a result, the OpenFlow actions are populated together with QoS policies, which can be exploited by all flow types including those whose data rate can be known a priori, such

[1] OpenFlow supports [5] setting the network type of service bits and enqueuing packets and, in fact, the used module offers not only rate limiting based on queues but also Type of Service (ToS) or Differentiated Services Code Point (DSCP) policies, even though these functions may or not be supported by OpenFlow switches.

Please cite this article in press as: Molina E et al. Using Software Defined Networking to manage and control IEC 61850-based systems. Comput Electr Eng (2014), http://dx.doi.org/10.1016/j.compeleceng.2014.10.016

as SV (*SmpRate* field indicated during the engineering stage in the SCL files parsed). Thus, the C&M planes take into consideration the QoS requirements of GOOSE or SV over other services, such as MMS, HTTP, FTP or video data.

4.4.4. Load balancing

The platform has a load balancer module (Fig. 2(b)) that allows the distribution of the traffic load in a set of members determined through the REST API. The module offers load distribution for several protocols (UDP, TCP, or ICMP flows) to different servers. This functionality may be used in redundant systems, where data concentrators or gateways are balanced.

4.4.5. Layer 2 tunneling

Unless IEDs and MUs implement R-GOOSE and R-SV (IEC 61850-90-5) to carry GOOSE and SV between substations, it is necessary to encapsulate the exchange of layer 2 messages over the wide area network (WAN). The platform allows us to create and manage different types of tunnels in a centralized and common way, which is achieved through OVSDB commands (this cannot be provisioned by OpenFlow messages). In particular, it is possible to forward Ethernet frames over a point-to-point Generic Routing Encapsulation (GRE, IETF RFC 2784) tunnel, which is one of the techniques adopted by the technical report IEC 61850-90-1 to connect substation networks over a WAN.

4.5. Monitoring

Varying communication conditions, such as bandwidth or network load, may affect the IEC 61850 message transfer performance. Therefore, in the following sections we detail the deployed monitoring methods.

4.5.1. Resource and failure visibility

Our proposal includes real-time passive monitoring to know the status of network resources, such as the throughput and to detect network stress events during which delays may increase, allowing the system to act accordingly. This is possible because sFlow provides information about flows, communication interfaces and a number of other signals describing the status of the device. Moreover, this can be used for link dimensioning for network planning purposes.

Considering the risk of failures, another important parameter taken into account is the recovery time (from links, nodes, network element failures), which allows us to evaluate the quality of a network. Regarding network failure detection, it is essential to maintain the performance. In our case, the platform has enabled the Port Down Reconciliation module (Fig. 2(b)) that is responsible for "reconciling flows across a network when a port or link goes down" [13]. However, the analysis of the recovery time after failure is out of scope for this work.

4.6. Security

Standardization bodies prioritize the promotion of Smart Grid cyber security strategies. IEC 62351-6 [18] includes security methods for IEC 61850 communication profiles, such as cryptographic algorithms or authentication certificates. Nevertheless, because of the stringent latency requirements of SV and GOOSE (they mainly require transfer times below 3 milliseconds) "encryption is not recommended" and is also ambiguous regarding the need for ensuring data integrity and source authenticity. "Instead, the communication path selection process (e.g., the fact that GOOSE and SV are supposed to be restricted to a logical substation LAN) shall be used to provide confidentiality for information exchanges" [18]. Therefore, the generation of network policies should be appropriate to mitigate different vulnerabilities. Below, we propose different cyber security controls, such as access control, network isolation or monitoring.

4.6.1. Traffic isolation

As previously mentioned, traffic isolation by network virtualization may be necessary to separate types of data in a substation. VLAN (IEEE 802.1Q) is a traditional technology to limit broadcast domains and its use is recommended in [8]. Moreover, it helps improve the network security and availability. Ref. [17] analyzes the use of VLAN according to Multiple Spanning Trees (IEEE 802.1s), and it indicates that network segmentation may help to manage those networks whose resources are shared by process and station buses.

The platform makes network virtualization easier by using the Virtual Network Filter module (Fig. 2(b)) that allows us to create logical networks based on MAC addresses without using VLAN; although at the same time, if we use VLAN, this feature enables VLAN IDs of each logical network can overlap each other. Therefore, the proposed layer 2 segmentation is oriented to create a better isolation among electrical circuit functions, and is an effective complement to the VLAN-based traffic segregation proposed by [8]. Furthermore, taking into account that OpenFlow emerged for achieving network isolation to enable researchers to run experiments on production networks, the authors of [19] propose using OpenFlow to test new technologies for Smart Grid development.

In Fig. 4, a diagram outlines an example where a network is sliced into logical networks based on different data flows: for example, every MAC address of MUs in a process bus or a whole substation can be assigned to the same logical network and, at the same time, allocate each GOOSE or SV to a unique VLAN.

Please cite this article in press as: Molina E et al. Using Software Defined Networking to manage and control IEC 61850-based systems. Comput Electr Eng (2014), http://dx.doi.org/10.1016/j.compeleceng.2014.10.016

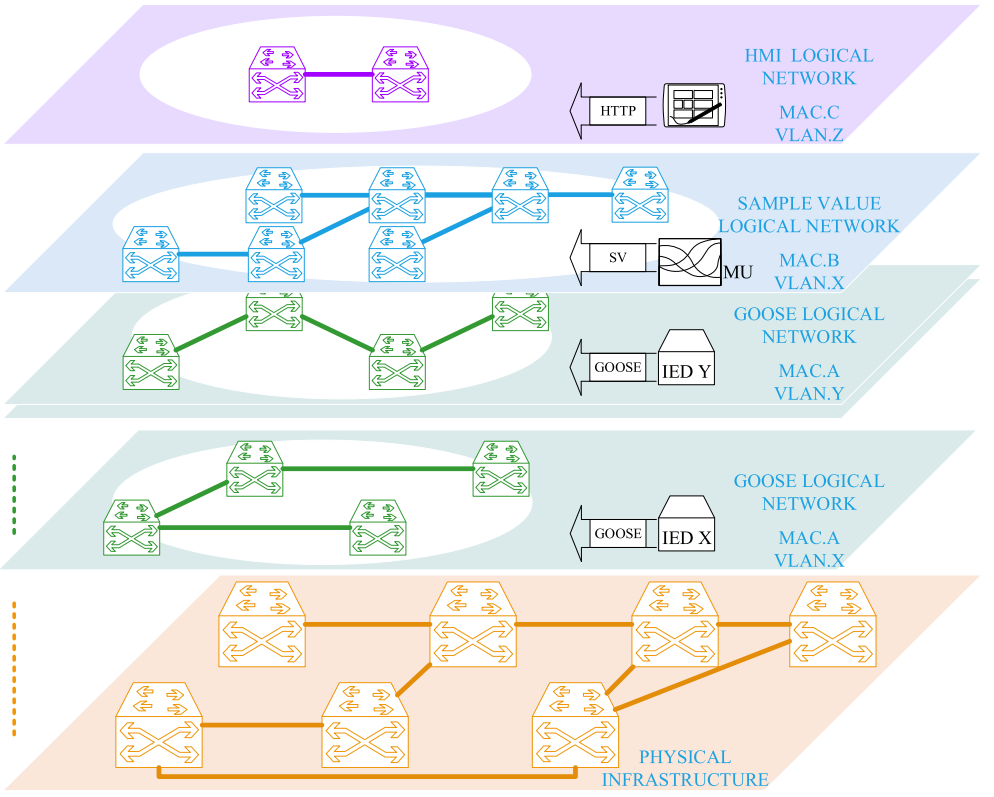


Fig. 4. Example of network virtualization based on MAC and VLAN addresses.

4.6.2. Anomaly detection

In our architecture, the sFlow collector detects when a certain threshold is exceeded and communicates it to the Floodlight controller, which inserts the appropriate OpenFlow actions. The platform allows us to insert flows (defined by MAC/IP addresses, Ethertype, VLAN, TCP/UDP ports, etcetera) and thresholds to monitor them. By default, it establishes the SV rates obtained from the SCD configuration file to detect abnormal rates in the transmission of SV to particular multicast MAC addresses.

Furthermore, with this feature, network designers can protect the connected nodes against Denial of Service (DoS) attacks. They can protect certain targets, for example, MACs of IEDs or IP addresses of MMS servers, from one or several addresses (distributed DoS). When this incoming traffic exceeds a predetermined threshold, Floodlight will be aware of this and limit these specific packets.

4.6.3. Firewall and spoofing control

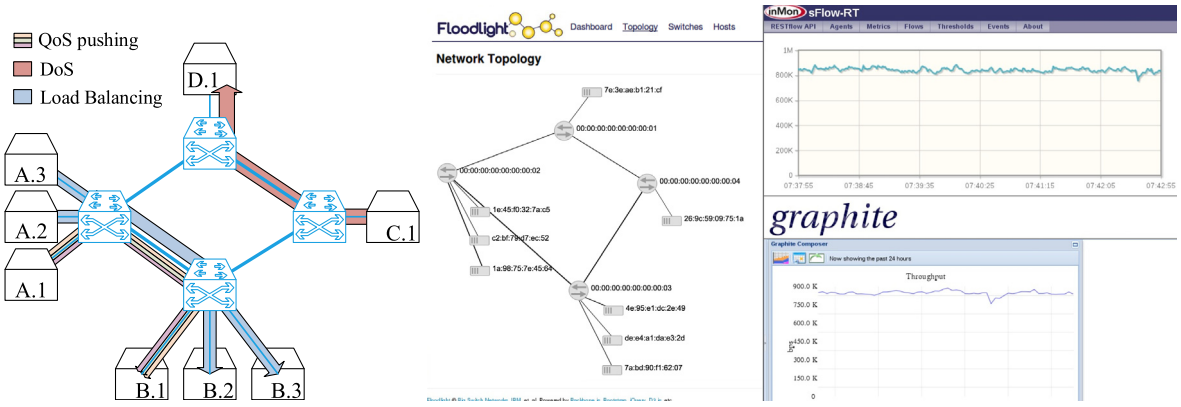
Because of the lack of need for implementing authentication and encryption mechanisms for GOOSE and SV messages, Ref. [20] demonstrates opportunities to compromise the security of an IEC 61850 system with MAC spoofing attacks. For the purpose of solving these problems, the Firewall Floodlight module (Fig. 2(b)) is used to limit ingress traffic according to the MAC source address, port and switch. Thus, the platform allows us to establish MAC Access Control Lists (ACLs) statically so that only the enabled rules will be able to transmit and receive data. Moreover, using the Device Manager module (Fig. 2(b)), the controller continuously restricts the attachment of devices to only a single MAC Address (the first connected one), helping to avoid spoofing attacks and other traditional problems that may well occur when addresses are duplicated.

Other issues related to the protection of C&M planes and SDN security challenges have not been considered in this paper.

5. Functional validation

In this section, leveraging the fact that the C&M framework is aware of the actual network status, we evaluate the capabilities of the proposal. With this aim, we employ Mininet [21], the most widespread tool for emulating SDN-based networks; it "creates virtual networks, running real kernels, on a single machine". Additionally, to build scenarios where the hosts send and receive SV and GOOSE frames, we use the open source rapid61850 project, published in [22], which processes an SCD file to generate the data model and communications code required for an IED. This code implements the communications stack that allows IEDs to send predefined messages (VLANs, Multicast addresses, etcetera), and they are able to encode and decode GOOSE and SV packets. The rapid61850 tool parses an SCD file and performs SCL schema validation,

Please cite this article in press as: Molina E et al. Using Software Defined Networking to manage and control IEC 61850-based systems. Comput Electr Eng (2014), http://dx.doi.org/10.1016/j.compeleceng.2014.10.016



(a) Network topology used in validation. (b) Screenshot of Floodlight, sFlow-RT and Graphite GUI.

Fig. 5. Testing topology and GUIs.

and then it generates C code that models each IED existing in the SCD file. This enables us to compile code for each IED and include them in the emulation process.

Mininet provides a Python API with which topologies can be defined together with multiple performance parameters. The results presented here correspond to an out-of-band configuration: Mininet uses Open vSwitch to create a set of Ethernet bridges that communicate with Floodlight, which runs on another machine through independent network resources; although it is remarkable that Mininet allows in-band configurations, where data and control planes share the same resources.

In our case, the results are performed on a ring network, where the nodes are attached by edge links (100 Mb/s) and switches are connected among themselves with trunk links (1 Gb/s). This topology is extracted from [8], and it is widely used in real substations. Additionally, despite the fact that Mininet uses the *NetEm* tool for emulating various capabilities of links, we have not included any additional synthetic delay. Fig. 5(a) shows how the use cases are handled by the network.

Fig. 5(b) shows a screenshot of the graphical user interfaces (GUI) used for displaying the network performance. To illustrate the advantages provided by the platform, some representative examples are shown below, making use of the Graphite software for real-time graphing.

5.1. Use cases

- *QoS pushing*: Fig. 6(a) shows the throughput of different flows (TCP and UDP using *iperf* and SV with rapid61850) in scenarios where rate limiting is established. As verified, there are no QoS policies during the first 25 s; afterwards, the following egress rate limits are set during the next 20 s, from 09:02:50 until 09:03:10 (flows recover their previous rate when the traffic shaping is disabled):
  - TCP flow: 20 Mb/s.
  - UDP flow: 2 Mb/s.
  - SV flow: 4.5 Mb/s.
- *DoS*: Fig. 6(b) exemplifies a situation in which DoS attacks can be detected in near real-time. Through a simple ping flood attack, where a node is overwhelmed with ICMP Echo Request packets, we can see a first phase during which DoS control is disabled and a second phase with DoS control enabled. Specifically, a threshold of 100 IP packets per second is set.
- *Load balancing*: Fig. 6(c) shows the TCP throughput from two nodes to two different IP addresses (IP.1 and IP.2) even though, in principle, the application (*iperf*) had generated traffic to one and the same IP address (IP.100).

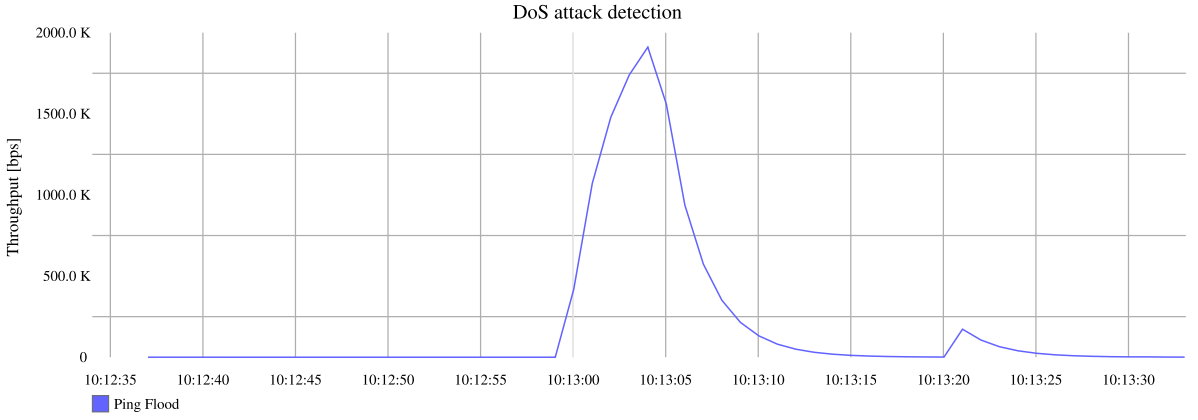
The emulation process allows us to emulate the GOOSE and SV data communications of a substation without using any real IEDs, checking the proper operation of the network design and validating the traffic engineering methods. Although there are approaches for modeling and simulating IEC 61850 networks and Smart Grid communications, as explored in [23], there are no industrial network simulators that integrate OpenFlow switches and inter-IED communication. Otherwise [24] combines network emulation with real-time software simulators. Indeed, our emulation platform raises the possibility to integrate simulation tools to recreate physical processes such as the AMICI tool [24], which has been used to analyze the security and reliability of interdependent infrastructures, such as the power grid and ICT.

6. Related and future work

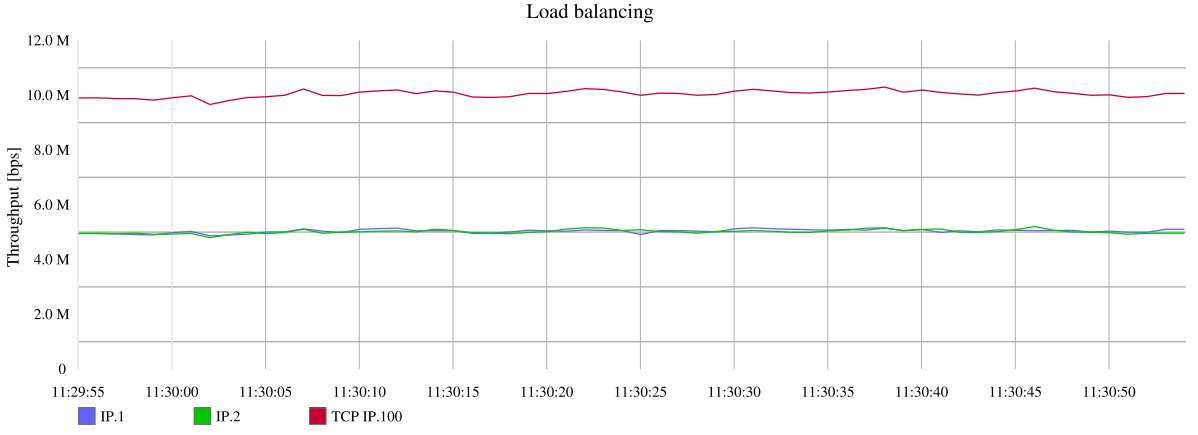
This part emphasizes our contribution to the related research. Commercial tools are available that also address the integration of network management and control of IEC 61850 substations. A representative system is Cisco's Connected Grid

Please cite this article in press as: Molina E et al. Using Software Defined Networking to manage and control IEC 61850-based systems. Comput Electr Eng (2014), http://dx.doi.org/10.1016/j.compeleceng.2014.10.016

(a) QoS effect for TCP, UDP and SV flows.



(b) Detection of exceeded thresholds.



(c) Load balancing effect over TCP traffic.

Fig. 6. Examples of platform features.

Design Suite that combines hardware and software to unify the "design, configuration, visualization and monitoring of electrical and communications networks" but without using the capabilities of SDN. Obviously, it is a proprietary system, which is a major drawback, whereas our framework facilitates the interoperability by using standard solutions, a main objective of IEC 61850.

Please cite this article in press as: Molina E et al. Using Software Defined Networking to manage and control IEC 61850-based systems. Comput Electr Eng (2014), http://dx.doi.org/10.1016/j.compeleceng.2014.10.016

Regarding the scope of OpenFlow in IEC 61850 facilities, on the one hand, [19] evaluates experimentally the modularity and flexibility offered by an OpenFlow solution to compare its performance with Multiprotocol Label Switching (MPLS) in the context of a Smart Grid application which, however, is not focused on the inter-substation environment. On the other hand, [14] is mainly oriented to automate the substation network configuration. However, with respect to maintenance of the operating network, it only contains ideas, as also identified in [25], such as the configurable packet inspection, dynamic monitoring, security policies and access control between connected IEDs, thereby enabling "the controller can easily manage traffic and curtail congestion events", or it can "open the door for control applications or recording tools driven by network events and traffic patterns". However, both papers only suggest the opportunities without implementing a solution, while our platform incorporates many mentioned capabilities, as previously detailed. In addition, despite the fact that [14] proposes to obtain network information derived from the IED device configuration, the authors do not use the IEC 61850-6 standard, while we include a thorough description of SCD parsing. Moreover, in [14], the authors analyze the possibility of exploiting the benefits of OpenFlow in IEC 61850 substations, but our framework also incorporates management and monitoring tools to handle different data traffic. Likewise, this framework has been identified in the SGAM.

Concerning the increasingly important combination of sFlow and OpenFlow, we apply some of the anomaly detection and actuation methods implemented in [7] in the context of substations.

With regard to future work, the platform works as a NOS where new functionalities can be incorporated and provide an improvement of the described capabilities, but always with a greater focus of meeting the IEC 61850 requirements. We emphasize the following:

- All Floodlight modules are network load independent; therefore, a possible future optimization is related to achieving further convergence between data path control and monitoring services. This would overcome the limitations of some modules, such as load balancing or shortest path forwarding. In the latter case, the network may have bottleneck links because the shortest path is only based on number of hops and not on link status.
- Resource provision: based on the actual network load, the platform should supply more bandwidth to deal with QoS properly.

Therefore, the consideration of network utilization could be easily integrated with resource computing and management, and it may be possible to achieve more fine-grained traffic engineering. This approach is consistent with the platform presented in [6], which relies on Floodlight and sFlow monitoring to control TCP flows and better schedule networks.

7. Conclusion

In this paper, we describe how to implement an SDN framework based on the OpenFlow, sFlow and OVSDB protocols to handle an IEC 61850-based network efficiently. Accordingly, an SGAM-based procedure is introduced for conceptualizing the development of a modular network operating system, which configures data flows by parsing standard configuration files and diagnosing network conditions. Thus, it allows us to include automation techniques for performing a flow-based resource management that enable features such as traffic filtering, QoS, load balancing or security capabilities. This has been developed on top of the open-source Floodlight controller, Open vSwitch and sFlow-RT software, and evaluated in emulated networks. This emulation enables the delivery of critical messages and the evaluation of the proposed features.

Our work provides tools that facilitate the goals of the IEC 61850 specification and are appropriate for achieving a more deterministic performance. Indeed, it shows that the flow-based modeling approach helps meet the communication demands imposed by IEC 61850 systems, such as latency or bandwidth. Furthermore, the platform provides several advantages over legacy architectures devised in previous work, including interoperability and more flexibility in the data path control. In summary, we present the improvements obtained by using SDN technologies to enable and enhance the development of IEC 61850 networks.

Acknowledgements

The work described in this paper was produced within the Training and Research Unit UFI11/16 funded by the University of the Basque Country (UPV/EHU). Furthermore, the authors would like to acknowledge the ZABALDUZ Program for financing the contract of Elias Molina with the UPV/EHU in collaboration with the System-on-Chip Engineering S.L. company.

References

[1] Li F, Qiao W, Sun H, Wan H, Wang J, Xia Y, et al. Smart transmission grid: vision and framework. IEEE Trans Smart Grid 2010;1(2):168–77. http://dx.doi.org/10.1109/TSG.2010.2053726.
[2] Open Networking Foundation (ONF). Software defined networking: the new norm for networks. Technical report; 2012.
[3] IEC TC57. Communication networks and systems for power utility automation – Part 6: Configuration description language for communication in electrical substations related to IEDs, IEC 61850-6, Geneva, Switzerland; 2009.
[4] Zhu L, Shi D, Wang P. IEC 61850-based information model and configuration description of communication network in substation automation. IEEE Trans Power Delivery 2014;29(1):97–107. http://dx.doi.org/10.1109/TPWRD.2013.2269770.
[5] Open Networking Foundation (ONF). OpenFlow switch specification, version 1.4.0; October 2013.
[6] Suh J, Kwon T, Dixon C, Felter W, Carter J. OpenSample: a low-latency, sampling-based measurement platform for SDN. Technical report. IBM; 2014.

Please cite this article in press as: Molina E et al. Using Software Defined Networking to manage and control IEC 61850-based systems. Comput Electr Eng (2014), http://dx.doi.org/10.1016/j.compeleceng.2014.10.016

[7] Giotis K, Argyropoulos C, Androulidakis G, Kalogeras D, Maglaris V. Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments. Comput Networks 2014;62(0):122–36. http://dx.doi.org/10.1016/j.bjp.2013.10.014.
[8] IEC TC57. Communication networks and systems in substations Part 90-4: Network engineering guidelines. IEC/TR 61850-90-4. Geneva, Switzerland; 2013.
[9] Chen T, Hu L. Internet performance monitoring. Proc IEEE 2002;90(9):1592–603. http://dx.doi.org/10.1109/JPROC.2002.802006.
[10] Argyropoulos C, Kalogeras D, Androulidakis G, Maglaris V. PaFloMon – a slice aware passive flow monitoring framework for openflow enabled experimental facilities. In: European workshop on software defined networking (EWSDN); 2012. p. 97–102. http://dx.doi.org/10.1109/EWSDN.2012.13.
[11] Pfaff B, Pettit J, Koponen T, Amidon K, Casado M, Shenker S. Extending networking into the virtualization layer. In: 8th ACM workshop on hot topics in networks (HotNets-VIII). New York; 2009.
[12] Smart Grid Coordination Group. Smart grid reference architecture, (sgcg/m490/c_smart grid reference architecture). Technical report. CEN–CENELEC–ETSI; 2012.
[13] Big Switch Networks. Floodlight openflow controller.
[14] Cahn A, Hoyos J, Hulse M, Keller E. Software-defined energy communication networks: from substation automation to future smart grids. In: IEEE international conference on smart grid communications (SmartGridComm); 2013. p. 558–63. http://dx.doi.org/10.1109/SmartGridComm.2013.6688017.
[15] Ingram D, Schaub P, Campbell D. Multicast traffic filtering for sampled value process bus networks. In: 37th Annual conference on IEEE industrial electronics society; 2011. p. 4710–5. http://dx.doi.org/10.1109/IECON.2011.6120087.
[16] Selga J, Zaballos A, Navarro J. Solutions to the computer networking challenges of the distribution smart grid. IEEE Commun Lett 2013;17(3):588–91. http://dx.doi.org/10.1109/LCOMM.2013.020413.122896.
[17] Ingram D, Schaub P, Taylor R, Campbell D. Network interactions and performance of a multifunction IEC 61850 process bus. IEEE Trans Ind Electron 2013;60(12):5933–42. http://dx.doi.org/10.1109/TIE.2012.2233701.
[18] IEC TC57. Power systems management and associated information exchange data and communications security Part 6: Security for IEC 61850, IEC TS 62351-6. Geneva, Switzerland; 2007.
[19] Sydney A, Ochs DS, Scoglio C, Gruenbacher D, Miller R. Using GENI for experimental evaluation of software defined networking in smart grids. Comput Networks 2014;63(0):5–16. http://dx.doi.org/10.1016/j.bjp.2013.12.021. Special issue on Future Internet Testbeds Part {II}.
[20] Hoyos J, Dehus M, Brown T. Exploiting the GOOSE protocol: a practical attack on cyber-infrastructure. In: Globecom workshops (GC Wkshps). IEEE; 2012. p. 1508–13. http://dx.doi.org/10.1109/GLOCOMW.2012.6477809.
[21] Lantz B, Heller B, McKeown N. A network in a laptop: rapid prototyping for software-defined networks. In: Proceedings of the 9th ACM SIGCOMM workshop on hot topics in networks (Hotnets-IX). New York: ACM; 2010. p. 19:1–6. http://dx.doi.org/10.1145/1868447.1868466.
[22] Blair S, Coffele F, Booth C, Burt G. An open platform for rapid-prototyping protection and control schemes with IEC 61850. IEEE Trans Power Delivery 2013;28(2):1103–10. http://dx.doi.org/PWRD.2012.2231099.
[23] Li W, Zhang X. Simulation of the smart grid communications: challenges, techniques, and future trends. Comput Electr Eng 2014;40(1):270–88. http://dx.doi.org/10.1016/j.compeleceng.2013.11.022.
[24] Genge B, Siaterlis C, Hohenadel M. AMICI: An assessment platform for multi-domain security experimentation on critical infrastructures. In: 7th International conference on critical information infrastructures security, Lecture Notes in Computer Science 7722; 2012. p. 228–239. http://dx.doi.org/10.1007/978-3-642-41485-5_20.
[25] Zhang J, Seet B-C, Lie T-T, Foh CH. Opportunities for software-defined networking in smart grid. In: 9th International conference on information, communications and signal processing (ICICS); 2013. p. 1–5. http://dx.doi.org/10.1109/ICICS.2013.6782793.

Elias Molina is currently a PhD student at the University of Basque Country (UPV/EHU). He received a BSc degree in Telecommunication Engineering from the University of Seville and an MSc degree in ICTs and Mobile Networks from the UPV/EHU, in 2010 and 2012, respectively. He worked from 2010 to 2012 as a trainee engineer in Tecnalia Research & Innovation.

Eduardo Jacob received his MSc in Industrial Communications and Electronics from the University of the Basque Country (UPV/EHU) in 1991. He received his PhD in ICT at the same university in 2001. He is an assistant professor at the Faculty of Engineering of Bilbao, where he is acting as the Head of the Communications Engineering Department and leads the I2T research lab.

Jon Matias received his MSc degree in Telecommunication Engineering in 2003 from the University of the Basque Country (UPV/EHU). He has been researcher at the I2T research lab since 2005 and an assistant lecturer in the Communications Engineering Department at the Faculty of Engineering of Bilbao since 2006.

Naiara Moreira received the qualification of Telecommunications Engineer and the MSc degree in Advanced Electronic Systems from the University of the Basque Country (UPV/EHU) in 2009 and 2012, respectively. From 2009 to 2011, she worked as a Research Engineer in Tecnalia Research & Innovation. She is currently pursuing a PhD degree in Advanced Electronic Systems at UPV/EHU.

Armando Astarloa received the MSc and PhD degree in Electrical Engineering from the University of the Basque Country (UPV/EHU), in 1999 and 2005, respectively. In 2001, he started working in the Telecommunications Department of the UPV/EHU as a researcher and lecturer. He is a member of the Applied Electronics Research Team and co-founder and promoter of the System-on-Chip Engineering company.

Please cite this article in press as: Molina E et al. Using Software Defined Networking to manage and control IEC 61850-based systems. Comput Electr Eng (2014), http://dx.doi.org/10.1016/j.compeleceng.2014.10.016