

Software-Defined Energy Communication Networks: From Substation Automation to Future Smart Grids

Adam Cahn, Juan Hoyos, Matthew Hulse, Eric Keller
University of Colorado, Boulder

Abstract—Energy communication networks (ECNs) play an integral role in electrical substations. Substations host many Intelligent Electronic Devices (IEDs) that monitor the state of the electricity infrastructure. This critical data is packaged and transmitted between multiple IEDs for proper system monitoring and control. The modern network that interconnects IEDs, while a significant improvement over the historic serial interconnection, has many challenges which have yet to be addressed – ranging from setup complexity to security policies. In this paper we propose that software-defined networking can alleviate many of today’s problems and create a network which can evolve with changing technologies and needs. We demonstrate an auto-configuring substation network which eliminates many substation network management issues. Our prototype is built using a Ryu-based, software-defined network controller and tested with actual IEDs used in substations. We also discuss how our software-defined energy communication network (SDECN) architecture not only solves problems of today, but enables substation networks to easily evolve with the rapid evolution of the smart grid.

I. INTRODUCTION

Our society has become highly dependent on energy – without it, everything from the light and heat in our homes to the massive datacenters that support the Internet would not be possible. The electrical grid is the complex energy infrastructure that moves electricity from its sources of production (power plants) to its sources of consumption (load centers). The Grid is comprised of the network of electrical transmission lines and substations that move energy from one source to another as well as data communication networks that transmit information *about* energy. These energy communication networks (ECNs) are pervasive and are the essential component in management of the Grid.

For more than 20 years almost all communication between devices inside and outside of power substations has been implemented using copper wires and legacy communication protocols [1]. There were many disadvantages to this approach, including long implementation schedules, the high cost of copper wiring, the lack of monitoring, and the difficulty in performing maintenance. More recently, Ethernet-based systems have been introduced to overcome some of these problems [2]. While the transition to Ethernet is certainly an improvement, it still leaves many problems – namely, the long and arduous process to standardize each individual solution when introducing a new technology (stifling the ability to evolve as needs change) as well as the difficult and error-prone process to manage the network infrastructure [3].

We argue that what ECNs require is an underlying technology which allows for (i) rapid innovation that *enables the evolution of both the specialization within each infrastructure as well as integration between them* and (ii) is simpler to

manage and verify the correctness of the network operation. Software-defined networking (SDN) is a recent innovation in computer networking that builds intelligence into a network through software control. An SDN-based network can make high-level decisions that impact detailed network functionality, optimizing the network’s performance in a manner not (easily) possible with traditional network management techniques. SDN is versatile, powerful and practical. SDN concepts and technologies are available today and have already been implemented on existing network infrastructures such as Google’s backbone network [4]. Even more, solutions to verify network behavior statically [5] and during run-time [6] become possible.

In this paper we propose a Software-Defined Energy Communication Network (SDECN), which applies SDN technology to the Grid. As a first step, we demonstrate this application within the context of substation automation to create a self-configuring substation network, thus alleviating telecom and power engineers from the burdensome and often overwhelming challenge of managing the complexity of substation networks. Additionally, we also discuss how SDECN will enable greater levels of automation of the distributed power management as well as new models for multi-tenant substations. Our SDECN prototype is built with the Ryu [7] open source SDN network controller platform and tested within a network containing real IEDs.

II. MODERN SUBSTATION IS ALREADY OUTDATED

The Grid is composed of power generation facilities, high-voltage transmission lines, lower-voltage distribution lines and load centers (residential and commercial buildings). Transmission lines carry electricity at high voltages over large distances, while distribution lines carry electricity at lower voltages to our residential and commercial load centers over shorter distances. Transmission and distribution lines are connected by intermediate physical facilities called substations. A substation transforms voltages up and down and has the added, critical responsibilities to constantly measure, monitor, protect and control its section of the Grid.

Within a substation, many of the devices used for protection, monitoring and control were (and still are) proprietary, closed and inflexible [8]. As networking technologies have advanced, the desire to have devices interoperate by communicating with one another, enabling distributed intelligence, has become the goal. This is especially the case with newer, network-enabled IEDs. In the mid-1990s, there were different protocols in the industry, however no one fulfilled all the requirements. The TC 57 working group began the development of a new standard called IEC 61850. This standard defines

not only different protocols but also standardizes the names and functions of the substations elements. In 2003, IEC 61850 was released with the goal of substation automation [9]. The standard uses *abstraction* to shield services, communications protocols and power management devices from each other to enable easier device interoperability. As an example, in IEC 61850 devices are assigned meaningful names for reference rather than using cryptic number and letter sequences [9]. The internal, cryptic device names have been abstracted so they can be referenced using human-friendly names.

While IEC 61850 is a forward-thinking standard, not all future requirements were predicted and technologies quickly changed. The rapid advance of technology and the lengthy standardization process (especially one requiring international agreement) creates a large gap in unmet needs. For example, the standard was originally designed for intra-substation communication on a LAN (most of the communication involves layer 2 multicast and flooding). However, the need was quickly recognized for IEDs to communicate *between* substations. An amended standard (IEC 61850-90-1) was released about 5 years later to allow for *inter-substation* communication. However, the technical details to achieve such communication was unspecified and therefore has required workarounds or ‘hacks’ to achieve [10]. In addition, little attention was given to the security of the substation’s network. As an example, it has been demonstrated that a computer can connect to a substation’s network and, without any authentication, inject traffic masquerading as a legitimate substation event. Such a security breach in a substation can have far-reaching effects, including the loss of power to major sections of the Grid [11].

III. ENTER SDN

Advances in datacenter network technologies have exploded in part due to open standards, falling equipment prices and embracing of new technologies. Ironically the Grid requires, but has not implemented, many of the innovations in important areas such as security, performance, reliability/self-healing, simplified management and automation. As our demand for electricity continues to rise and the trend to cover this extra demand with renewable, clean energy resources creates scenarios where the volatility of these resources will require new Information Technology (IT) to avoid blackouts. Incorporation of modern technologies such as SDN will be vital for the Grid’s transformation into a “smart grid”.

SDN is a relatively new network architecture which decouples the *network intelligence from the network devices*, as shown in Figure 1. Traditionally, network devices run distributed routing protocols and provide an interface to configure the various parameters of those routing protocols on each device. With SDN, software running on a logically central controller¹ provides the network intelligence and directly manages a collection of ‘dumb’ forwarding devices through a standard interface. SDN was proposed to overcome the mis-match between what network operators wanted and what network devices provided [13], [14] – *e.g.*, for traffic engineering, operators wanted to calculate paths to avoid congestion, whereas

¹Logically centralized simply relates to the programming abstraction, whereas the actual implementation can be implemented with a distributed system to provide extra processing or fault tolerance [12].

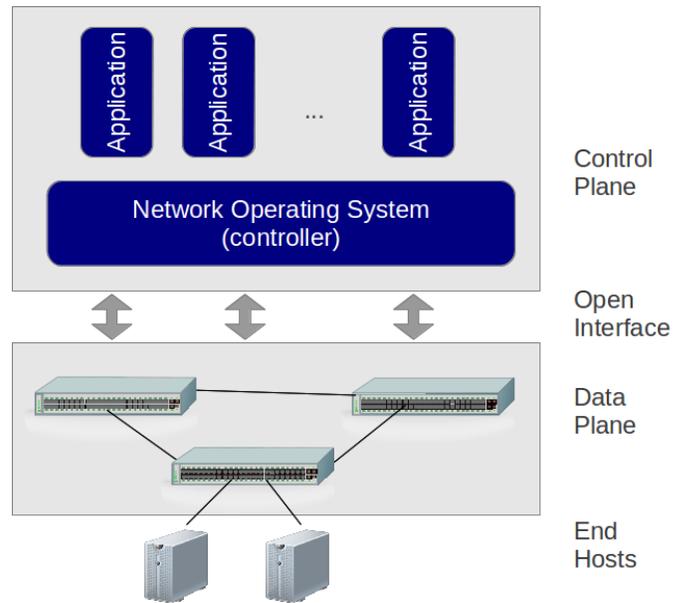


Fig. 1. Overview of SDN architecture

with a protocol such as OSPF, they had to determine what link weights would result in OSPF deciding on the desired paths.

The current embodiment of SDN is the OpenFlow [15] specification which specifies the communication between each switch and the controller and is supported by many commercially available Ethernet switches. With OpenFlow, each switch maintains a flow table that is used in the forwarding decision to determine how packets are processed. At a simplified level, the headers of packets are used for a lookup in this table, and the value stored determines the action the switch will take – *e.g.*, forwarded out a given port, drop the packet, or send it to the controller to make the determination. The OpenFlow specification opens access to this table through a communication protocol with an external controller.

Of significant importance, SDN allows for innovation by providing the ability to write software and deploy it. With this key capability, not only do operators have better control over their networks, but new capabilities can be introduced rapidly – leading to an evolvable network.

In the remainder of this paper we present our software-defined energy communication network (SDECN). We will present the design and implementation of a network controller which solves many of the security and management issues of modern substations and discuss future possibilities for a virtualized substation that are enabled with our SDECN.

IV. EASING SUBSTATION NETWORK MANAGEMENT WITH SDN

Network management within a substation is a complexity headache for substation operators. The transition from hard-wired connections to an Ethernet-based network introduced new functionalities to utilities and the power sector, such as the ability to have distributed data acquisition with distributed intelligence. A substation may contain over a hundred different IEDs, each generating and/or consuming information about the

status of some aspect of the substation. Proper configuration and maintenance of IED communication requires significant effort due to the complex message grouping mechanisms, archaic traffic control schemes through VLANs and the overhead of synchronizing configurations across all publishers, subscribers, and interconnection devices. The network complexity skyrockets when one considers the variety of protocols that are being used – such as IEC 61850 Sample Measure Value (SMV), Generic Object Oriented Substation Event (GOOSE), Manufacturing Message Specification (MMS), Precision Time Protocols (PTP), Distributed Network Protocol (DNP 3.0), and proprietary management protocols [1].

A key challenge in managing networks using these protocols is that they rely heavily on layer-2 multicast. To segregate this multicast traffic and ensure reliable communication (*e.g.*, avoiding congestion), network devices must be configured with a variety of layer 2 and layer 3 networking techniques – *e.g.*, virtual LANs (VLAN), multicast filtering, GARP Multi Registration Protocol (GRMRP), and Multiple MAC (or VLAN) Registration Protocol (MMRP or MMVP) [16]. A recent discussion between engineers on a LinkedIn discussion board demonstrates that this is a significant and unquestionable challenge [17]. Efficient, reliable, and safe operation of substation networks is further constrained by traffic complexity, security and congestion issues.

We utilized SDN to design a self-managed substation network based on our SDECN architecture which addresses the following capabilities:

Auto-configured: Each new application, protocol, and device adds an extra level of complexity to the network design and maintenance [16]. This task traditionally falls to the power engineers and telecommunication engineers to configure the network devices to meet these requirements – a laborious and error-prone task [3]. Furthermore, each individual IED must be configured to match the network configuration (*e.g.*, which multicast address to use, which port to use, etc.). A single IED can be part of multiple message groups and, as is usually the case, the many IEDs in an operational substation evolve into a complex logical mesh of message groups. The first requirement is that we support these already-configured IEDs and improve upon the scenario by adding isolation of traffic so that information goes only to where it is meant to go. Our software-enabled networking controller removes the need for maintaining the configuration of multiple VLANs for traffic isolation purposes. This complex networking configuration traditionally needed to be replicated across all IEDs and inter-network devices. An SDN-controller reduces the overhead of configuring layer-2 and layer-3 switches by using configurable software to dynamically create message groups and instantiate new IEDs onto the substation network.

Configurable packet inspection: By implementing a software-defined network controller we introduce the possibility of advanced packet management capabilities which can assist in handling some of the complex traffic profiles seen on substation communication networks. Traffic monitors can be dynamically added as subscribers to existing message groups where they can record and potentially take action upon detecting anomalous events such as a circuit breaker closure or cascading sensor failure. Our SDN-controller for

substations will support the creation and custom configuration of monitoring nodes which can, in the future, be enabled to dynamically adjust message group traffic policies, subscriber lists, or other control functions at the controller level.

Security: Link isolation is a critical requirement of the substation network not only for superfluous traffic congestion on IED network interfaces, but also for security and access issues within the operating environment. IED configuration is commonly carried out ‘live’ when other devices on the substation network are performing monitoring and control of the substation. The risk of a malicious attack, masked as a live-reconfiguration event, is an attack vector that could be mitigated with a higher degree of network-level security. The SDN-enabled substation network controller has the capacity to support more security at the controller level. The nature of the software-defined controller also allows for greater flexibility in security policies and access control between connected IEDs. A group of devices that are linked through a message group can be enabled for one-way communication and only allow the authorized publisher to send traffic into the network. This addresses a common hole in substation network security [11].

Latency-aware, Congestion avoidance: Message data on IED networks has an upper-bound of 4ms latency tolerance as an operational requirement [18]. This window ensures timely delivery of event notifications to subscribers and substation controllers. Violations to these time windows has been linked to substation failure or critical malfunction. As such, the risk of link saturation is dangerous. IED substation networks deployed in the field frequently operate near bandwidth capacity. The multi-layered VLAN configurations carry complex traffic loads between unique message groups which risks congestion across the logical layers of the substation network. Avoidance of traffic saturation is difficult to implement in the layer-2 switches traditionally deployed in operational substations, due to the use of minimum-spanning trees which do not provide traffic engineering capability and, even worse, do not utilize the full capacity of the network. In contrast, the software-enabled network controller can easily manage traffic and curtail congestion events (*e.g.*, redirecting some traffic along alternate paths).

In summary, IED communication requires tedious setup due to the complex message grouping mechanisms, VLANs for traffic isolation and the mundane repetition of setup across publishers, subscribers and interconnection devices. These requirements outline the improvements that SDN-based substation networks should target.

V. PROTOTYPE AND EVALUATION

In order to evaluate the operational performance, features and configuration enhancements that SDN can bring to a complexity-burdened electrical substation IED network, we built a prototype of the SDECN system as an SDN network controller. While many SDN controller platforms exist, the differentiator is mostly programming language, in which case we prefer Python. As such, our prototype was built on top of the python-based Ryu [7] open-sourced network controller which, through support of a large telecom provider in Japan (NTT), is building towards high-quality network control services in large production environments.

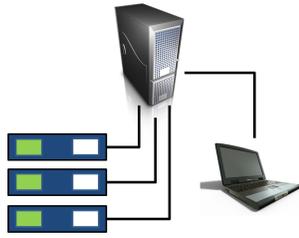


Fig. 2. Prototype lab setup with three real IEDs, a server emulating a network, and a laptop with software to emulate additional IEDs.

A. Test Setup

Our laboratory contains three IEDs which we used for testing – two Schweitzer Engineering Laboratories (SEL) 2411 and one SEL 351 devices. We emulated an OpenFlow network topology on a Dell PowerEdge R710 server with four network interface cards using Mininet [19] to emulate a topology of SDN switches. As shown in Figure 2, each of the IEDs are connected to one of the network interface cards of the Dell PowerEdge R710, and an additional laptop was connected with software to simulate additional IEDs and run monitoring software.

The laboratory setup serves as a testbed for an electrical substation IED network under a software controller that can parse and read configuration files of IEDs, dynamically allocate and setup network channels, guarantee efficient and automated networking and easily support event or traffic monitoring.

B. System Details

Operator Management Interface

The software controller takes advantage of out-of-the-box support in Ryu for providing a REST API. The Configuration Loader component implements an asynchronous node creation, discovery and flow entry method based on data derived from IED device configuration files. The following are commands operators can use to interact with our network controller:

- `Add_IED(file)`: A function for adding an IED based on the IED’s configuration file containing information relevant to the IED’s communication requirements. This function enables the network controller to determine how to configure the network.
- `Add_Monitor(file)`: A function for adding a virtual node based on a configuration from a text file containing monitor node information. The controller changes the configuration of the network so the monitor can receive the stream of data. If no subscriber list is specified, the monitor will subscribe to *all* current subscription schemes on the controller.
- `Del_IED(Node_ID)`: A function for removing and unloading an IED configuration based on its `Node_ID` in the controller’s runtime configuration.
- `Del_Monitor(Node_ID)`: A function for removing and unloading a virtual monitor node based on its `Node_ID` in the controller’s runtime configuration.

- `Run_Monitor(Node_ID)`: Instantiate the `call_prog` logging tool linked to the corresponding `Node_ID` of a monitor node. If the program is located on the system call path, it will begin executing in parallel with the OpenFlow controller and receive message traffic based on its subscriptions.

All of these functions run on-demand when executed on the local controller. The Configuration Loader module serves as an API template for addressing the complex needs of a substation IED network, serving as a bridge between complex IED configuration files and distilling only their relevant traffic broadcast and subscription information.

Auto-Configure Network based on IED Configurations

To address the needs of a smarter, software-enabled controller for substation networks, our prototype must support network management needs. This includes the ability to address secure switching, complex monitoring of network events and traffic as well as device discovery by the controller. The capacity to launch an independent monitoring node with a specific traffic or event-logging routine is also supported. Both physical IEDs and virtual monitoring nodes are placed into the network by a Configuration Loader module which parses an IED configuration to extract information and determine a network configuration to enable the specified communication.

An important consideration to take into account is that in order to configure the network, the controller must know where the IED is connected in the network (what port of which switch). To automatically determine this, the network controller attempts discovery of the port location of the device by sending a ping to the device IP address and looking for a *packet-in* event triggered from the IED’s response². Upon receiving the *packet-in*, the controller creates an entry in its runtime configuration of the device and in the message groups that it is subscribed to.

Secure switching is built off of the Ryu controller link isolation module. Packets are first identified by the switch port and the MAC address of the sender is subsequently derived. This also facilitates the building of flow entries into the switching table which is used during IED discovery. In the default Ryu implementation, multicast destinations are treated as broadcast destinations. This is an undesirable behavior for the substation IED network and so multicast addresses are instead checked against the ‘subscribers’ list and a specific dispatch is created for all matched entries.

We currently rely on shortest path selection which we found to result in paths within the latency requirements of the target substation environment, but we will be expanding to enable bandwidth and latency guarantees. This ensures isolation of non-subscribers from the message traffic and allows the multicast addressing scheme function on the same logical network without broadcasting. In classical implementations, isolation of broadcast of messages was accomplished using VLANs which added significant complexity to the logical network configuration.

²Packet-in is an OpenFlow message type where a switch sends a message to the network controller, typically when it receives a packet for which it does not have a table entry. Packet-in messages include the port number on which the packet was received.

Dynamic Monitoring

To meet the needs of traffic monitoring outside of substation IEDs, the OpenFlow controller must be designed to support development of advanced monitoring programs that can be plugged into a running network. We therefore open the door for control applications or recording tools driven by network events and traffic patterns. We incorporated the ability to mirror any traffic of interest on a dedicated logging machine called a Monitor. Monitors can be added as network nodes and their configuration sets are specified as follows:

The current ‘bird-on-the-wire’ implementation of monitoring nodes supports the instantiation of logging applications which can be extended beyond simply running an external program. System calls, or more complex software monitors, can feed configuration changes and traffic policy back into the controller and are a first step towards the creation of a program/controller API. Such an extension enables integration of third-party software.

C. Results

As our SDECN architecture is targeted at network management and evolvability, evaluation is based more on the qualitative arguments made previously and verification that the network behaves as expected and within required bounds. That said, scalability and reliability are concerns. The scalability of SDECN has been proven out with SDN deployments and studies, such as Google’s inter-datacenter network [4]. The reliability of SDECN relates to the reliability of the centralized controller, for which it is fairly trivial to implement a backup hot-swappable controller (e.g., as has been demonstrated commercially [20]). Where SDECN is most applicable is in network management – by eliminating human error, which has been shown to be the majority of network problems [3], we are providing a more reliable network.

In the laboratory environment, the OpenFlow controller successfully replicated the existing statically-configured, non-software-enabled networks. The OpenFlow controller consistently provided message delivery under the latency bounds of 4ms. In fact, latency was on the order of 10s of microseconds and matched the latency we observed when we replicated the topology with legacy Ethernet switches. This type of extra slack could be used by the controller to perform extra packet processing. Three IED devices with four message groups were configured and run for over ninety minutes with a variety of events.

Link isolation was verified by adding an extra switch to one of the IEDs. Then, using port mirroring and Wireshark we corroborate that only the message configured for that IED was the one who was arriving

In summary, the behavior of our experiments using the SDECN prototype matched the behavior of a traditional setup consisting of legacy Ethernet switches. The difference was that we did not have to configure the network in the SDECN prototype, whereas we had to set up the Ethernet switches with mechanisms such as multicast filtering. Even more, as we innovate new features, such as better traffic engineering, we do not need to modify the hardware or firmware of any of the switches, we simply update the software running on the controller.

VI. LOOKING AHEAD - SDECN VIRTUALIZATION OF THE GRID

Our current prototype dramatically simplifies network management by using SDN to provide an auto-configuring network which is secure and efficient. With a programmable and evolveable network based on SDN, we envision transforming the electric grid into a powerful, virtualized environment.

A. Virtual IEDs

Modern intelligent electronic devices contain microprocessors that allow the substation operator to control specific, high-level monitoring, protection and/or control functions through a rudimentary, vendor-specific user interface. They are expensive, inflexible, have limited programmability and, many times serve a single purpose.

Traditionally, the IEDs contained analog inputs which were used to determine the state of the attached sensor(s). Recently, Merging Unit (MU) devices have been introduced which simply packetize analog readings in a sample measured value (SMV) over Ethernet. Given the difficulty in network management without this extra traffic, the SMV traffic does not traverse the substation network but is instead connected directly to one of the IEDs in the substation.

With SDN, we have the opportunity to introduce an elegant solution to this suboptimal design. Rather than employing the current solution that requires a proprietary physical device, we propose that the software running in an IED be moved to run within a virtual machine on a commodity computer. As shown in Figure 3, the substation architecture then becomes a series of sensors which measure such attributes as current and voltage, devices that packetize these measurements, a collection of servers which can process the measurements and a self-configuring (software-defined) network interconnecting all of these devices.

To fully realize the benefits of these virtual IEDs, their configuration must be automated through centralized control. This vision is within our grasp. It leverages technology already widely used in datacenters to provide great amounts of automation – a primary goal in substations. Imagine the daunting and labor-intensive task for an organization such as The Electric Reliability Council of Texas (ERCOT) [21] to manage tens or even hundreds of thousands of IEDs within its 3,600 substation network. The large amount of manual labor required is time-consuming, costly and likely to introduce many errors. However, with datacenter-style automation, if a group of *SDN-IEDs* required a new configuration or system update, the substation engineer would simply push this information out to that group from a *single interface* within his virtual substation. Such an architecture would eliminate errors and save a substantial amount of time and money.

While large organizations like ERCOT may be large enough to add manpower to manage the network infrastructure, this is not the case for everyone – less than half of the 48,000 distribution substations and 14,000 transmission substations perform even some automation [22]. With a highly-automated and virtualized infrastructure, we will make the technology *accessible to all*.

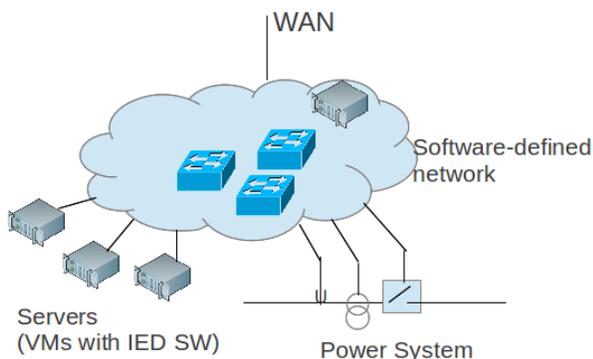


Fig. 3. Future substation with virtualized IEDs.

B. Virtual, Multi-tenant Substation

One of the early use cases for SDN has been providing network virtualization [23]. That is, network resources are partitioned among multiple parties and each is given full control over its slice of the network (whether it be multiple companies or multiple business units within the same company). Coupling this with virtualized IEDs and other control software, each substation could be virtualized into a multi-tenant environment.

Virtual substations could be created from physical substations that could be dedicated to a particular customer or utility, a type of energy source (e.g., wind), specific geographic regions or any other logical grouping to meet the changing demands of the energy industry. Doing so allows for a more cost-effective use of infrastructure. Grid infrastructure is expensive to build and resources such as transmission lines are often shared among utilities. The owner of the lines derives revenue from multiple utilities that use their lines to transmit electricity. This idea of infrastructure sharing could be extended much further with a virtualized Grid that partitions resources and provides independent control over each slice.

This is analogous to today's data centers that provide an Infrastructure as a service (IaaS) cloud computing model. While the financial model does not yet exist for Grid-IaaS, a virtualized power grid would open up new avenues for revenue generation as well as utilize computing and network resources more efficiently across the entire power grid. In addition, this virtualized Grid would provide increased stability of the physical grid as a whole with its abilities to isolate problems more quickly, provide compute redundancy in an emergency, even out CPU processing and balance network traffic.

VII. CONCLUSION

As the Grid is updated and transformed into a smart grid, the challenges of network management continue to increase. In this paper, we designed and deployed a substation network architecture which provides an auto-configuring, secure, and reliable network through the use of software-defined networking technology. This also serves as a first step toward virtualizing the Grid by enabling the incorporation of technology that is widely used in datacenters today to automate many different types of services. By introducing SDN into substations we have not only demonstrated solutions for today's problems, but we have also opened the door for substation network functionality to evolve at speeds far exceeding those achieved via standards.

REFERENCES

- [1] R. E. Mackiewicz, "Overview of 61850 benefits," in *Transmission and Distribution Conference and Exhibition*, May 2006.
- [2] G. Scheer and D. Dolezilek, "Comparing the reliability of ethernet network topologies in substation control and monitoring networks," <https://www.selinc.com/WorkArea/DownloadAsset.aspx?id=2584>, 2000.
- [3] Z. Kerravala, "Configuration management delivers business resiliency," Nov. 2002, the Yankee Group.
- [4] U. Hölzle, "Openflow @ google," Presentation at OpenNetworking Summit: <http://www.opennetsummit.org/archives/apr12/hoelzle-tue-openflow.pdf>, 2012.
- [5] P. Kazemian, G. Varghese, and N. McKeown, "Header space analysis: static checking for networks," in *Proc. USENIX conference on Networked Systems Design and Implementation (NSDI)*, 2012.
- [6] A. Khurshid, X. Zou, W. Zhou, M. Caesar, and P. B. Godfrey, "VeriFlow: verifying network-wide invariants in real time," in *Proc. USENIX conference on Networked Systems Design and Implementation (NSDI)*, 2013.
- [7] "Ryu," <http://osrg.github.com/ryu/>.
- [8] M. Qureshi, A. Raza, D. Kumar, S.-S. Kim, U.-S. Song, M.-W. Park, H.-S. Jang, H.-S. Yang, and B.-S. Park, "A survey of communication network paradigms for substation automation," in *IEEE International Symposium on Power Line Communications and Its Applications (ISPLC)*, Apr. 2008.
- [9] IEC, "Communication networks and systems in substation – Specific communication service mapping, IEC 61850."
- [10] J. Wen, C. Hammond, and E. Udren, "Wide-area ethernet network configuration for system protection messaging," in *Conference for Protective Relay Engineers*, 2012.
- [11] J. Hoyos, M. Dehus, and T. Brown, "Exploiting the GOOSE protocol: A practical attack on cyber-infrastructure," in *IEEE Globecom Workshops (GC Wkshps)*, 2012.
- [12] T. Koponen, M. Casado, N. Gude, J. Stribling, L. Poutievski, M. Zhu, R. Ramanathan, Y. Iwata, H. Inoue, T. Hama, and S. Shenker, "Onix: a distributed control platform for large-scale production networks," in *Proc. USENIX conference on Operating systems design and implementation (OSDI)*, 2010.
- [13] A. Greenberg, G. Hjalmtysson, D. A. Maltz, A. Myers, J. Rexford, G. Xie, H. Yan, J. Zhan, and H. Zhang, "A clean slate 4d approach to network control and management," *SIGCOMM Comput. Commun. Rev. (CCR)*, vol. 35, no. 5, pp. 41–54, Oct. 2005.
- [14] M. Casado, M. J. Freedman, J. Pettit, J. Luo, N. McKeown, and S. Shenker, "Ethane: taking control of the enterprise," in *Proc. SIGCOMM*, 2007.
- [15] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "OpenFlow: Enabling innovation in campus networks," *SIGCOMM Comput. Commun. Rev. (CCR)*, vol. 38, no. 2, 2008.
- [16] D. M. E. Ingram, P. Schaub, and D. A. Campbell, "Multicast traffic filtering for sampled value process bus networks," in *Conference on IEEE Industrial Electronics Society (IECON)*, 2011.
- [17] "Linkedin discussion: A question on ethernet multicast filtering," <http://lnkd.in/D2u3PV>, 2013.
- [18] IEC, "Communication networks and systems in substation – Specific communication service mapping. IEC 61850.5 part 5 Clause 13.4."
- [19] "Mininet," <http://mininet.github.com/>.
- [20] "Big network controller," <http://www.bigswitch.com>.
- [21] D. Yeomans, "ERCOT opens its doors to the public. offers tours of its taylor control center," <http://www.kxan.com/dpp/news/local/austin/ercot-opens-its-doors-to-the-public>, Oct. 2012.
- [22] G. Zeiss, "Distributech utility university: Substation automation and enterprise data management," <http://geospatial.blogs.com/geospatial/2012/01/distributech-utility-university-substation-automation-and-enterprise-data-management.html>, Jan. 2012.
- [23] R. Sherwood, G. Gibb, K.-K. Yap, G. Appenzeller, M. Casado, N. McKeown, and G. Parulkar, "Can the production network be the testbed?" in *Proc. USENIX conference on Operating systems design and implementation (OSDI)*, 2010.