# Cyber Security Architecture in Smart Grids Using Software Defined Networks

Fábio Antonio Ferreira
Electronics Engineering Division
Technological Institute of Aeronautics - ITA
Sao Jose dos Campos, Brazil
fantonios@gmail.com

Osamu Saotome
Electronics Engineering Division
Technological Institute of Aeronautics - ITA
Sao Jose dos Campos, Brazil
osaotome@gmail.com

***Abstract*—The constant use of connected industrial equipment in an intelligent network demonstrates the opportunities that can be generated with data capture and configuration changes. Content trafficked in these networks may be caught by malicious attacks to cause interference and disruption to the service. The present paper presents a proposal for the analysis of the protocol header, the network packets transmitted in an openflow switch, using Software Defined Network (SDN). And apply information recognition in data streams in a real-time intrusion detection system.**

***Keywords—Smart Grids; SDN; Cyber Security; Openflow;***

## I. INTRODUCTION

Smart grids allow for the modernization and automation of the Electric Power System (SEP). These modifications are only possible by standardizing the IEC-61850 standard. Which according to Gurjão, the IEC-61850 is a standardized data model totally focused on the concepts of object orientation. This concept has become essential for the implementation of monitoring and validation of communication status between the control center and all other interconnected points. Knowing the traffic of information that transports in this network is essential, for a classification and rapid response to incidents. Analyzing the behavior of a network infrastructure using the current architecture takes a long time and the response may be late. In the midst of all these changes, we do not observe the exploitation of security holes in our environment, in this context, software-defined networks allow automation and the separation of the control plane from the data plane of the switches. This change determines that any communication flow of any request, which go through the equipment with these characteristics will be forwarded its intelligence settings to a server. This server is termed as a controller that applies rules of flows to network assets according to its systems signature analysis validation.

## II. SOFTWARE DEFINED NETWORK (SDN)

Computer networks have reached a stage of disruption, emerging new concepts and different ways to orchestrate the diverse equipment of a network infrastructure. In our current structure of computer networks, we have big problems like complexity to scale a network and add more devices, lack of interoperability between proprietary software, proprietary protocols and the impossibility of testing new ideas on switches and routers. To add more resources and a programming interface to the network components, a software-defined network architecture was created that allows the abstraction of the network infrastructure, thus separating the data plane from the data plane. By separating these two functions, the network asset allows the control of the network to be directly programmable and the basic infrastructure is abstracted from the point of view of application and service. From this step the switches can share the same control plane, which holds the global view of the network. This creates the opportunity to redefine the routes of multiple switch streams by configuring the application on the controller. The flow control rules are defined by the OpenFlow protocol that is responsible for the communication between the controller and the writing of the flows in the routers and interconnected switches on software defined networks.

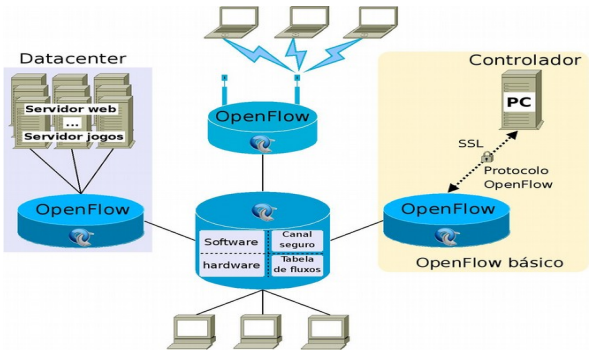


Figure 1. Openflow division of the control plan and data plan.

## III. SMART GRID

According to [1], Smart Grid or smart grids, it is a comprehensive concept that can become a fundamental element of transformation. This network can transform the electrical system we know into a modern network that will

allow power utilities and consumers to change the way they make and consume power. With the introduction of new electronic meters, it is apparent the evolution and possibilities that the insertion of Telecommunication, sensing, information systems and computing will generate combined with our current infrastructure. The deployment of this architecture is a shift in the paradigm of the electric sector, taking into account the need to make the delivery system more interactive for reasons that differ in each country or region. The need to incorporate different sources of energy into the grid, in particular decentralized, renewable and intermittent generating sources and to introduce new consumers as electric vehicles, as well as the importance of improving efficiency and the proper design of the grid are among the reasons article to justify the increasing application of intelligence in the electrical systems in the world.

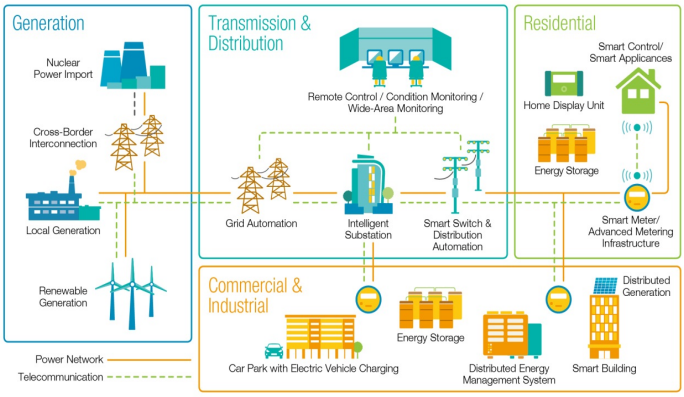


Figure 2. Structure of a Smart Grid

## IV. Cyber Security

Borders are created in physical environments to delimit locales and create authentication patterns to accredit anyone who wishes to pass through this means of access. In this context physical security shows us that we need large retaining walls to protect a property, when we fail something forgetting a part of this open protection we consider a vulnerability. Such security applied in a cyberspace (or cyberspace) that is considered the digital space created by computer networks, is not limited to borders but applies in the definitions of data packet flows, configurations of network devices such as firewall, routers, switches and the perimeter protection of the data center infrastructure.

## V. Intelligent Electronic Device

As we can see for [9] IED is the acronym for Intelligent Electronic Device, which relates to microprocessed equipment that can be used in various applications within a substation automation system, also called SAS, such as protection, control, automation , measurement and monitoring of electrical systems, allowing the design of interlocking and blocking logic. For these devices to be considered as intelligent it is necessary some actions among them the connection with an ethernet network to exchange frames using Layer 2 of the OSI model. Such a discussion is only possible by the intervention of a standard to which [10] gives us the definition that the IEC-61850 is a standardized data model totally focused on the concepts of object orientation. For this, it uses functions and attributes of physical devices (IEDs) found in a substation or power plant. The functions and their respective instances form what is called the "Logical Node", and a set of "logical nodes" forms a "logical device", which in turn resides internally in an IED. Knowing that to have a communication between IEDs the substations or power plants must apply the standard IEC-61850. It is necessary to understand how the exchange of information between these intelligent devices occurs. To answer this question we will describe the use of one of the protocols used to establish communication between IEDs. One of the protocols used is the so-called Generic Object Oriented Substation Event (GOOSE), which for [10] is responsible only for the traffic of information messages of any protection or digital signal. Such messages can be faster than the actual physical actuation of a relay from one relay to another. All this for using the UDP standard in its design, ie does not check to see if there was an error in the transmission of the message. In this way, even if a packet of data is lost, another packet identical to the one that was lost has already been sent again until an acknowledgment of receipt is received, thus ensuring that the message is received. Below is a figure that demonstrates the topology of an IEC-61850 network.

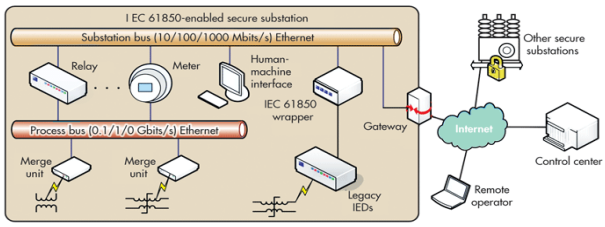


Figure 3. Network Topology IEC-61820

## VI. Proposed Architecture

This article proposes the creation of a cyber security architecture in smart grids using the concept of software-defined networks to identify the existing flows in a grid. It is intended to create an algorithm in the programming language Python using the pcapy library a module for capture and analysis of packages. This step will have a client machine that will be carried out the creation of the program and specifications of how the GOOSE protocol behaves used to exchange frames between IEDs. Along with this data will be created OpenFlow servers using Floodlight software to perform the information flow control operation coming from the switches (SDN), which received the connections of the IEDs. The development of this part will be accomplished by the creation of a virtual network using Mininet software, and the installation of Linux servers with the Debian 9 distribution and the software required to run software applications. In the

aid of the capture of packages will be installed wireshark software that will also be used to understand the signature patterns of each header of the packages. The data that will be validated when developing this experiment is the exchange of GOOSE messages. To simulate the capture and reading of the packets it will be necessary to generate the content of messages according to the standards of the standard IEC-61820, for this function will be used the packetH software an ethernet packet generator. Knowing that the standard communication between the IEDs is performed by data link second layer in the OSI model, so the need to send ethernet packets. All this network traffic will pass through the openflows switches and forwarded to the controller taking the appropriate actions of the predefined flows within their settings. After capturing the packets, a classification will be performed to identify the signature patterns contained in each package that will pass through the openflow controller, thus creating a standardization of signatures. With prior traffic classification, we will have sufficient content to know and identify false positives of system signatures. The demand for data flow will be treated as specific and unique bringing exclusivity to each packet trafficked but classifying one by one to create a knowledge base on the infrastructure of smart grids. As the Openflow controller learns about intelligent networks, it will be enabled with algorithms to control the data flows processed by the IEC 61850 standard that models the systems and the network communication for automation in the Electrical Power System (SEP). Next we can observe the proposed architecture.

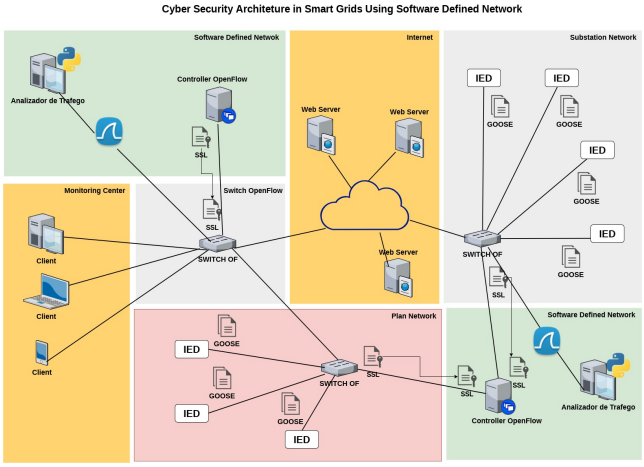


Figure 4. Architecture Proposed

## VII. Conclusion

This paper presents the concepts of networks defined by software and smart grids, presenting the proposal to create a GOOSE packet analysis architecture in a network standardized by IEC 61850. It was described the possibility of creating software using pcap to capture and interpret each packet that interacts with the openflow controller. This work will collaborate with possible projects of cyber security implementations in intelligent electrical networks, being possible to create catalogs of patterns of package signatures, classifying as passive or level of intrusion.

## References

[1] CPQD, “SmartGrid” 2017. [Available at http://www.cpqd.com.br/mercado/smart-grid; accessed on 9 may 2017].

[2] CGEE, “Management and Strategic Studies Center” 2017. [Available at http://seer.cgee.org.br; acessed on 10 may 2017].

[3] UFRJ, “Information Provider Financial Economics the Electric Energy Sector” 2017. [Available at http://www.provedor.nuca.ie.ufrj.br accessed on 1 may 2017]

[4] CPQD, “OpenFlow 1.3 Software Switch” 2017. [Available at https://github.com/CpqD/ofsoftswitch13; accessed on 10 may 2017].

[5] Mininet, “Mininet” 2017. [Available at http://mininet.org; accessed on 2 may 2017].

[6] McKeown et al. 2008] McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Pe-terson, L., Rexford, J., Shenker, S., and Turner, J. (2008). OpenFlow: in campus networksenabling innovation in campus networks. ACM SIGCOMM Computer Com- munication Review.

[7] B. Nunes, M. Mendonca, X.-N. Nguyen, K. Obraczka, and T. Turletti,“A survey of software-defined networking: Past, present, and future of programmable networks,” IEEE Communications Surveys & Tutorials,vol. 16, no. 3, pp. 1617–1634, 2014.

[8] [Xing et al. 2013] Xing, T., Huang, D., Xu, L., Chung, C.-J., and Khatkar, P. (2013). Snort-flow: A openflow-based intrusion prevention system in cloud environment. In Rese-arch and Educational Experiment Workshop (GREE), 2013 Second GENI, pages 89–92. IEEE.

[9] PLC and SCADA, “What is an IED” 2017. [Available at http://plcescada.com/eletrica/voce-sabe-o-que-e-um-ied/; accessed on 15 october 2017].

[10] Network IEC-61850, “Protocol Study” 2017. [Available at https://www.automacaoindustrial.info/redes-iec-61850-estudo-de-protocolo-e-exemplo-de-aplicacao; accessed on 15 october 2017];

[11] Industry Expert Assess Power’s Frontiers. Octuber 2017. Disponibilize in: <http://www.electronicdesign.com/power/industry-experts-assess-power-s-frontiers>

[12] Project Floodlight, “Project Floodlight,” 2017. [Available at http://www.projectfloodlight.org/floodlight/; accessed on 9 June 2015].

[13] F. Hu, Q. Hao, and K. Bao, “A survey on software defined networking (sdn) and openflow: From concept to implementation,” Communications Surveys Tutorials, IEEE, vol. PP, no. 99, pp. 1–1, 2014.

[14] A. Cahn, J. Hoyos, M. Hulse, and E. Keller, “Software-defined energy communication networks: From substation automation to future smart grids,” in Smart Grid Communications (SmartGridComm), 2013 IEEE International Conference on. IEEE, 2013, pp. 558–563.

[15] T. S. Ustun , C. R. Ozansoy and A. Zayegh,“Implementing Vehicle- to-Grid (V2G) Technology With IEC 61850-7-420,”IEEE Trans. Smart Grid, vol. 4, pp. 1180-1187, 2013.

[16] W. Xia, Y. Wen, C. H. Foh and D. Niyato ,“ A Survey on Software-Defined Networking,” IEEE Communications Surveys & Tutorials, vol.17, pp. 27-51, 2014.

[17] Jianchao Zhang et al.,“Opportunities for Software-Defined Networking in Smart Grid,” Information, Communications and Signal Processing (ICICS),pp.1-5, 2013.