THANOS: Teleprotection Holistic Application for ONOS Controller

Juan Lucas Vieira, Vinicius C. Ferreira, Ian Vilar Bastos, Silvio Ereno Quincozes, Wilker de Oliveira Delfino, Yago de Rezende dos Santos, Yona Lopes, Diego Passos, Célio V. N. Albuquerque, Igor M. Moraes, Luiz C. Schara Magalhães, Natalia C. Fernandes, and Débora C. Muchaluat-Saade
MídiaCom Lab, Universidade Federal Fluminense, Niterói, Brazil
{juanlucasvieira, viniciusferreira, ianvilar, sequincozes, yagorezende, yonalopes}@id.uff.br,
{wilkerrj, schara, natalia, debora}@midiacom.uff.br, {dpassos, celio, igor}@ic.uff.br

***Abstract*—Supervisory and control systems should provide reliable and autonomic functionalities for real-time communication. The new generation of communication-based energy applications relies on networks to exchange messages between devices in the substation. Therefore, the underlying communication network must satisfy strict temporal constraints imposed by these complex electrical power systems. In this work, we present a practical description of THANOS: an SDN-based application built on top of ONOS that facilitates discovery, communication configuration, and monitoring of intelligent devices in IEC 61850 compliant substations. THANOS enables automatic configuration of IEC 61850 protocols with failure recovery support. THANOS also supports multiple backup instances to improve control resiliency. We first present an overview of THANOS architecture. Then, we highlight the challenges and lessons learned during the development of THANOS. Finally, we present experiments that evaluate THANOS' functionalities.**

***Index Terms*—IEC 61850, SDN, Smart Grids, Teleprotection**

I. Introduction

Electric power systems are crucial to infrastructural and economic development of all countries. The supply of electricity is an essential service that must be provided in an appropriate, efficient, and continuous manner to the population. Therefore, the development and implementation of complex transmission and distribution systems are continuously evolving to deal with the challenges and requirements of Smart Grids (SG).

Communication in SG scenarios is based on international standards such as IEC 61850 [1], which relies on timely delivery of messages to support critical services — such as teleprotection — and imposes temporal constraints up to 3 ms. Consequently, high performance and resiliency must be achieved by the underlying communication infrastructure.

Teleprotection schemes speed up the process of eliminating both external and internal faults in transmission lines. Several protection devices are integrated to prevent problems such as overcurrents, overvoltages, and disturbances from causing damage to equipment and operators. Nevertheless, the safety of these schemes depends on the assurance of a proper communication network, including configuration and monitoring.

This work is supported by CAPES, CNPq, FAPESP, FAPERJ, TAESA and P&D ANEEL (PD-07130-0053/2018).

In recent years, the Software Defined Network (SDN) paradigm has been used to satisfy those requirements [2]–[5]. In this context, the Autonomic and Resilient Communication Framework for Smart grids (ARES) [6] provides autonomic and flexible communication network configuration to support power grid services that depend on the provision and maintenance of a secure, highly available and adaptive communication channel. ARES is based on IEC 61850 and SDN, and is suitable for a variety of SG scenarios, including electric vehicles and power transmission networks.

In this paper, we present the practical experience of developing THANOS (Teleprotection Holistic Application for ONOS), a realization of the ARES conceptual framework for teleprotection scenarios, created to deploy, configure, and manage substation automation and control communication systems, following the IEC 61850 standard. THANOS is implemented on top of the ONOS SDN controller [7], a stable controller platform with distributed controller support for automatic fault response based on the widely used OpenFlow protocol [8].

THANOS simplifies the provision of the communication flows for substation and teleprotection schemes using the IEC 61850 substation configuration file to configure a robust and efficient communication network autonomically and provides the required tools to manage the communication in teleprotection schemes. It offers a management interface for the electrical operation manager, which displays all THANOS autonomous configuration processes while enabling the monitoring and manual operation of the communication network.

We present an architecture overview and highlight the challenges and lessons learned during the deployment of THANOS. We also present experiments to validate and test THANOS in a realistic scenario, with IEDs, industrial SEL-2740S SDN switches, and typical teleprotection traffic using GOOSE and SV messages [9]. The validation comprises the discovery of switches in the telecommunication network, the authorization and commissioning processes and the provisioning of primary and backup communication paths.

The remaining of this work is organized as follows. Section II reviews protocols and requirements of the IEC 61850 standard. Section III presents related work. Section IV presents an overview of THANOS architecture. Section V discusses experiments to demonstrate THANOS suitability for telepro-

tection scenarios. Finally, Section VI concludes the paper.

II. Background

To standardize communication in power substations, Technical Committee 57 developed the IEC 61850 standard [10], a global, vendor-independent standard for control, automation, and protection of substation systems [11]. Such substation systems based on IEC 61850 rely on packet-switching networks for message exchange between electric devices.

A. Configuration and Protocols

The IEC 61850 standard utilizes an XML-based definition called Substation Configuration Language (SCL). The SCL-based specification consists of an IED Capability Description (ICD), which contains features and functionalities of an IED; a System Specification Description (SSD), which contains the complete specification of a substation automation system, including the single-line diagram for the substation, their logical nodes and the required data types; and the Substation Configuration Description (SCD) file, composed of ICD and SSD information, describing the substation in detail.

The IEC 61850 standard also defines communication protocols with different goals for exchanging command and data messages between devices in a substation. The Manufacturing Message Specification (MMS) protocol [12] is used by the Supervisory Control and Data Acquisition (SCADA) to control and supervise functions of electrical system devices. The Generic Object Oriented Substation Event (GOOSE) protocol [9] allows the exchange of commands and critical alarms between IEDs. The Sampled Values (SV) protocol [9] is used to send voltage and current measurements to IEDs of a substation. These data can be sent by current and potential transformers or by Merging Units (MU), which receive analog values from transformers and convert them to digital samples.

B. Communication Requirements

Since the IEC 61850 standard relies on packet-switching networks for monitoring, control, and protection tasks, several requirements that must be met by the electric devices and the communication infrastructure are defined.

The standard defines two communication models: Two Party Application Association (TPAA) or Multicast Application Association (MCAA) [13]. The TPAA communication model consists on a bidirectional, reliable and connection-oriented message exchange between two devices, in a client-server manner. The MCAA model consists of unidirectional transmissions between a publisher and several subscribers. These subscribers must detect lost and duplicated packets. The MMS protocol follows the TPAA model, while GOOSE and SV follow the MCAA model.

Timely delivery of messages is crucial for the proper operation of the services in a substation. Failure to delivery teleprotection related messages (*e.g.*, circuit break trip commands) can cause equipment damage and even loss of life. Therefore, both TPAA and MCAA communication models have to meet temporal communication constraints established by IEC 61850. The most stringent requirements are for GOOSE Trip messages and SV current and voltage samples, both with 3 ms maximum allowable delay [10].

III. Related Work

This section provides an overview of several works in the literature that rely on the SDN paradigm to deal with the complexity and requirements of IEC 61850 based systems.

Maziku and Shetty [2] propose an SDN framework that incorporates a security risk model and mitigation policies for IEC 61850-based substation communication networks. Their work considers the susceptibility of IEDs to each threat and calculates the threat score and the impact of each IED over the entire substation network. The controller's resource monitor and the threat detector constantly observe the network resources and inform the threat mitigator that deploys a mitigation technique based on the network's security score. Although this framework addresses the security risk assessment, it does not provide automatic topology mapping, resource management, and failure resilience.

In [3], the authors propose an autonomous framework to improve the resilience of inter-substation communication after disaster events. Their solution uses SDN to reconfigure the network after detecting link failures and relies on wireless communication as a redundancy for the wired network that connects the substations. The SDN controller configures OpenFlow [14] fast-failover rules that enable switches to change the port to which traffic is sent in case of failure of the default port. Upon detecting a wired link failure, a switch forwards data through the wireless port. The authors evaluate the proposal's performance against strict delivery time requirements of critical GOOSE messages by using Mininet and NS-3.

Molina et al. [4] propose a framework to control IEC 61850 communication in SDN networks. The framework supports: network configuration based on the SCD file parsing; traffic filtering; Quality of Service (QoS); flow and queue priorities configuration; load balancing; tunneling to exchange messages with the WAN; and security features that uses network slicing, VLAN IDs, firewall, Access Control Lists (ACL) and an anomaly detection system. A functional test is performed using Mininet to validate the network configuration, control and monitoring. This proposal share similarities with THANOS, however, THANOS offers the robustness desired for critical environments with fast recovery on link's failure, and support for backup instances.

Lopes et al. [5] propose SMARTFlow, an SDN-based architecture for autonomic management and control of communication networks for substations based on IEC 61850. SMARTFlow proactively calculates layer-2 multicast trees to forward GOOSE and SV messages and reconfigures all flow entries in case of network failures. Also, the proposed system monitors the network and defines the configuration of client-server flows on-demand. The proposal was implemented and tested using Mininet.

IV. THANOS Overview

THANOS is a practical implementation of the ARES framework [6] applied to teleprotection. THANOS follows several ARES modules definitions and interfaces and also provides a Graphical User Interface (GUI) to facilitate configuration and management for teleprotection communication networks.

ARES comprises five planes, as shown in Figure 1. At the bottom, the Energy Plane consists of the actual electrical devices. On top of that lies the Data Plane, representing the communication network devices and connections, following the SDN plane separation paradigm. The Control Plane consists of the SDN core, which is instantiated by ONOS in our implementation. ONOS adds stability for the teleprotection scenario [8] and provides distributed controller support that mirrors the network configuration state into backup instances that assume the control plane if the master instance fails.

THANOS consists of implementing the main modules of ARES Control Plane: Discovery, Management and Path Configuration. The Discovery Module detects and exports the network topology, including switches and devices, while the Path Configuration Module calculates unicast and multicast paths, as well as backups for dealing with switch or link faults. The Management Module receives all user requests and orchestrates them among other modules, automating resource provisioning. THANOS also adds a Security Module that was not originally part of ARES, to support access control. The Management Interface represents a graphical tool to ease network control and monitoring to the substation operator.

A. Discovery Module

The Discovery Module is responsible for identifying and mapping hosts (*e.g.*, IEDs, merging units, workstations), switches, and links to support communication provisioning.

The *Host Discovery* process interacts with the ONOS core to discover new devices in the network. Also, this process interacts with the Security Module API to verify the access privileges of the host. Specifically, the Discovery Module retrieves information about IEDs from the Security Module, including manufacturer, device name, operating status, operating mode and unicast and multicast addresses. *Unknown hosts* are devices that are not included nor described in the SCD file. Therefore, *unknown hosts* are reported to the Security Module to allow proper actions to be taken. These actions range from blocking to requesting a flow provision to the Path Configuration Module.

The *Topology Discovery* process interacts with the core of ONOS controller through the *Topology Service*, which provides network topology information. It implements a listener that captures new switches added to the network, previously authorized by the security module. It listens to LLDP packets of proprietary switches and notifies the GUI and the Security Module to start the adoption process.

B. Management Module

The Management Module is responsible for managing provisions and monitoring network events. In THANOS, this module comprises three main components: *Resource Manager*, *Provisioning Manager*, and *Monitoring Manager*.

The *Resource Manager* serves as a hub within the module, gathering the data needed by the *Provisioning Service* and receiving network events from the *Monitoring Service*. It also receives IED communication demands from the *Discovery Module* and resolves which IEDs are publishers or subscribers in MCAA-based communications.

The *Provisioning Manager* is responsible for creating, removing, and checking the status of provisions. A provision object represents a communication service in the substation. It is comprised of the following: i) Source: the source node of the communication; ii) Destination: the destination of the communication, which can be one node or multiple according to the communication model (TPAA or MCAA); iii) Priority: the priority of the communication service; iv) Ethertype and source/destination port: indicate which communication protocol is used by the service (*e.g.*, MMS, GOOSE, SV, ICMP).

To install a provision, the *Provision Manager* forwards the required information to the Path Configuration Module and stores the primary and backup paths used to install the communication in the SDN data plane. Paths are kept to verify whether active provisions are affected by link or device failures. If both main and backup paths fails, the provision is considered as affected. In this case, an alert is sent to the GUI to inform the provision failure.

The *Monitoring Manager* uses ONOS listeners to monitor relevant switch, host, and link events. For example, link down events that trigger provisioning checks at the *Provisioning Manager* or switch port activation events that are forwarded to the Discovery Module to trigger host discovery.

C. Path Configuration Module

The Path Configuration Module is responsible for configuring TPAA and MCAA communication paths with failure recovery support. To perform its functionalities, as installing communication paths in switches, and enabling failure recovery, the management of flows, OpenFlow groups, and the network topology graph is necessary. Therefore, we subdivide the Path Configuration Module into four components to manage the installation complexity: *Flow Manager*, *Group Manager*, *Topology Manager*, and *Path Manager*.

The *Flow Manager* creates, removes, and installs flow rules in switches to enable end-to-end communication, considering MAC and IP addresses, Ethertype, VLAN IDs, queue priority for QoS requirements, and TCP/UDP ports. The component interacts with the ONOS controller core that translates the set of instructions to the corresponding switches.

To support fault recovery and the installation of multicast trees for MCAA communication, the *Group Manager* component creates, removes, and installs OpenFlow groups, which consist of a list of action buckets that the switch triggers depending on the characteristics of the group. Each action bucket points to a switch interface or to another group. THANOS uses both fast-failover and *All* groups in the backup implementations. Fast-failover groups trigger only

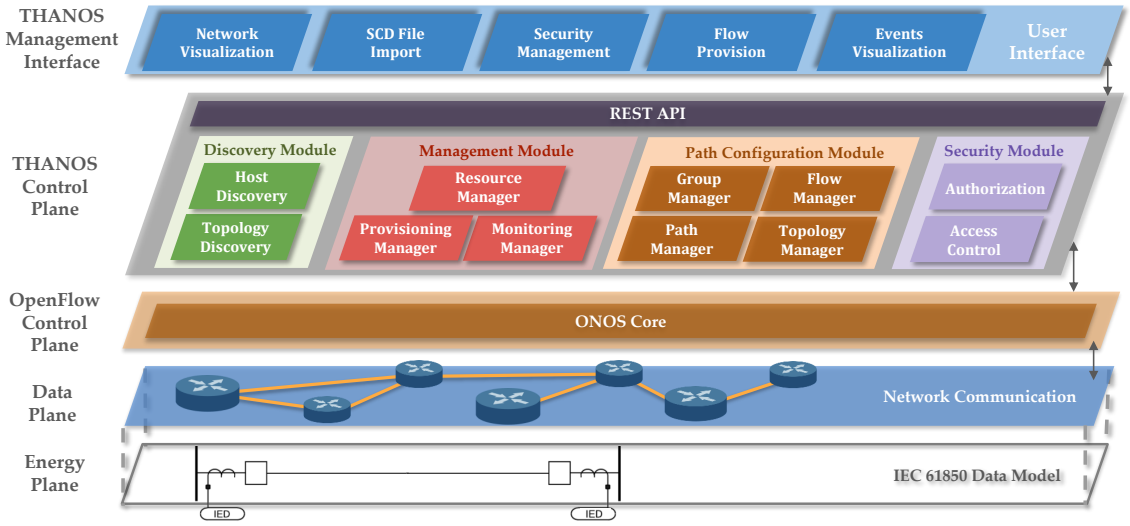

Fig. 1. Overview of THANOS architecture which provides features to automate communication provision for substation and teleprotection schemes.

the first alive bucket of the list, allowing primary and backup interfaces. *All* groups trigger all action buckets at each packet reception, allowing a packet to be simultaneously transmitted through different interfaces. The component interacts with the ONOS core that translates the set of instructions to the corresponding switches.

The *Topology Manager* builds the adjacency matrix and calculates shortest paths, based on Dijkstra's Algorithm, and multicast trees, based on Prim's Algorithm, interacting with the Discovery Module to retrieve switches, links and hosts in the network.

Finally, the *Path Manager* component has two sub-components: *Unicast Manager* and *Multicast Manager*. The former establishes TPAA communication with a primary path and a disjoint backup path. In contrast, the latter establishes MCAA communication with a primary multicast tree and pre-configures one backup multicast tree for each possible link failure in the primary multicast tree. The component interacts with the Management Module through a common interface.

D. Security Module

The Security Module is responsible for performing *Authentication* and *Access Control* of network devices. The *Authentication* component authenticates SDN switches through an adoption process involving digital certificates and key exchange. The *Access Control* component authorizes IEDs whose address is contained in the SCD file. SCD-specified communications are forwarded for pre-provisioning. Other types of hosts are temporarily blocked until they are authorized by the network administrator using the Management Interface.

E. THANOS Northbound API

The THANOS backend implements a REST API to support information retrieval and requests from the Management Application, such as a provision request, and the Northbound API is also used to notify the Management Interface relevant events, as link-down events, provision failures, or detection of new switches and hosts.

F. Backup Support

The support for backup instances of THANOS is built using ONOS distributed API, a set of primitives that ONOS offers to easily maintain the distributed state of objects [7]. This functionality is specially desired by applications that run in critical environments such as electric power systems, and provides fault-tolerance in case of controller failures.

G. THANOS Management Interface

The THANOS Management Interface gives the operator a simple GUI comprising five components, as shown in Figure 1, organized into the Dashboard View, and the Security View. The Dashboard View holds the Network Visualization and the Events Visualization panes, as shown in Figure 2, while the Security View contains the Security Manager component.

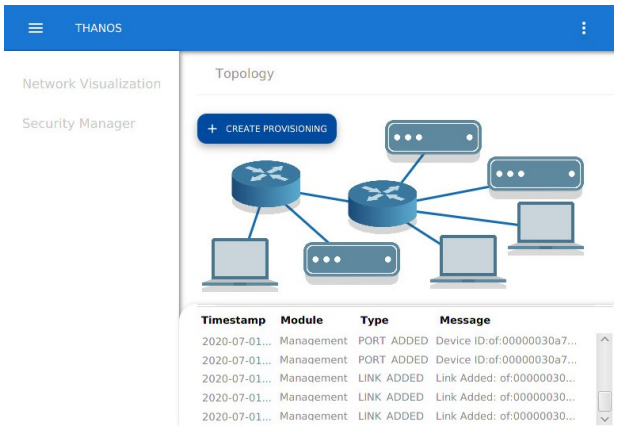

Fig. 2. THANOS Management Interface Dashboard View

The *Network Visualization* shows the network graph containing switches, IEDs, and hosts. The operator can configure the IP address, netmask, and gateway of switches, prior the adoption process, and visualize device information (*e.g.*, name, IP and MAC addresses, manufacturer, software version) and its

provisions. It gives the operator a powerful tool to anticipate potential hazards, by looking at a switch and its provisions, it is possible to infer the consequences of a failure in the communication traffic.

The *SCD File Import* allows the user to upload the SCD file that will be sent to the Security Module. After the processing of the SCD data, a message is sent to the frontend, triggering a topology update with the IEDs information. The *Security Manager* displays unauthorized devices and flows detected in the network, allowing the operator to authorize hosts and unknown flows. The provision of an unknown flow can only occur if the involved devices are authorized, either by the SCD file or manually by the operator.

The *Flow Provision* component gives the operator a tool to create provisioning requests. THANOS allows each provision to be labeled, providing semantic information to ease provision organization and maintainability. Finally, the *Events Visualization* component displays logs and events, such as failures and incoming devices.

H. Teleprotection Requirements Support and Lessons Learned

Reliability is essential for the teleprotection scenario, where packet loss can cause equipment and life loss. Therefore, in addition to the redundant communication paths functionality, it was necessary to support the backup instances of THANOS. This feature can be challenging considering the complexity of different modules and the consistency that must be maintained between the multiple instances.

Communication monitoring and priorization are also important for the teleprotection scenario. To that end, THANOS monitors network links and generates UI alerts for failed paths and absence of backup paths in the network. THANOS also uses OpenFlow switch queues to prioritize critical traffic and support temporal constraints of teleprotection messages.

The operator must easily interact with the system without having extensive knowledge of SDN communication networks. Therefore, we identified the need for a GUI that exposes relevant data to the teleprotection scenario, identifying electrical equipment, and reduces network management complexity. THANOS' management interface offers a hub for several important features. The SCD import facilitates the configuration of communication between IEDs since paths are automatically pre-configured and can be installed with just one click. It also displays alerts for failed provisions, absence of backup paths in the network, and unauthorized transmission attempts.

The OpenFlow protocol provides a standardized communication between the control and data planes. However, some switches may present limited OpenFlow support, especially those usable for teleprotection because of the substations' safety policies. For instance, in our deployment, we needed to adapt THANOS because of limitations such as limited group chaining, unsupported flow instructions, and the need for an adoption procedure using vendor proprietary software, which was solved by implementing an equivalent procedure in THANOS.

V. Experimentation and Results

We evaluated THANOS in a real SDN testbed composed by two physical SEL-421-1 IEDs, four Raspberry Pi 3 Model B, and a THANOS Controller (Intel Core i7-8700). These devices were connected by two SDN switches, model SEL-2740S. In particular, two Raspberries were assumed to be regular hosts (not listed in the SCD), while two were configured in the SCD as the destination to IEC 61850 messages sent by the IEDs.

The first experiment considers two real switches that already have certificates to authenticate with the control plane. Both switches are connected simultaneously to the controller. The time for each switch event is measured until the switch is added to the control plane structures. The measured time of each event is displayed in Figure 3. The total time from the new switch connection to the final switch availability event for switches 1 and 2 was 597 ms and 457 ms respectively. This result demonstrates that a network switch may become available in about half a second.

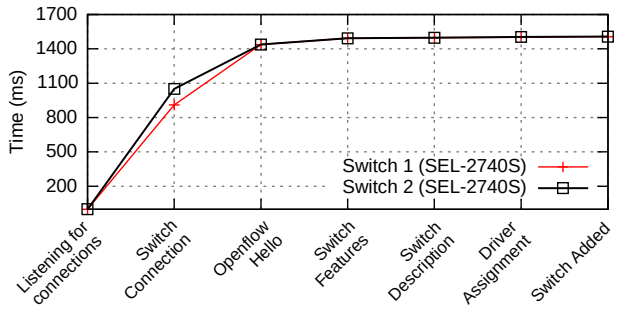

Fig. 3. Time until switch availability.

An additional experiment reveals that the average time for importing an SCD file containing 52,884 lines (2 MB) was 314 ms. This includes the total time from selecting the upload button on the GUI to receiving the response from the access control. Additional requests, such as host and switch authentication, took 31 ms, on average. The aforementioned results were extracted from 10 experiment runs.

Once THANOS discovers the network topology, ARP probes are sent over each port of the discovered switches to identify the hosts connected to the network. Host responses allow the ONOS core to discover them. However, they will not be able to communicate through the SDN network until the authorization and provisioning processes are concluded. Therefore, the ARP probing procedure triggers HTTP requests to the Security Module API for each discovered host. These requests can be observed in the first peak in Figure 4. The SCD file import and the corresponding HTTP requests can be identified at the second peak in Figure 4. Finally, the last peak illustrates the moment THANOS enters operation mode, after the corresponding Management Interface event.

In fact, some requests trigger secondary ones. For example, when a host is not authorized by the Security Module, it generates a new request for manual authorization in the GUI. Cascading messages related to host authentication and the corresponding UI updates are illustrated in Figure 5, at the second

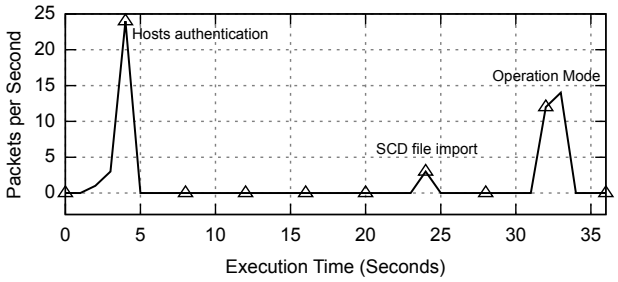

Fig. 4. Event timeline (HTTP requests).

peak. Similarly, it is possible to identify a correlation between topology requests and the corresponding switch authentication at the third peak. Note that these peaks result from the events illustrated in Figure 4.

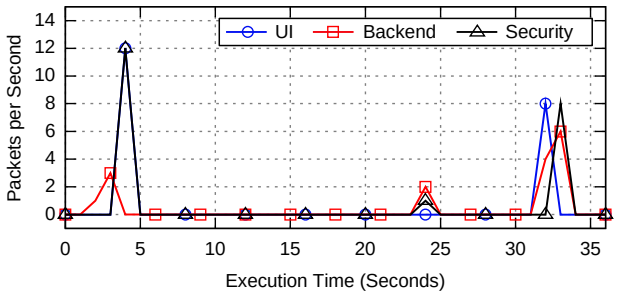

Fig. 5. Event timeline (HTTP requests per service).

This experiment illustrates the proper function of THANOS, as well as its consistency with the Management Module and Network Visualization, without significant overheads caused by security operations.

VI. Final Remarks

This work presented the pratical experience of developing THANOS, an instantiation of the ARES framework for teleprotection systems based on SDN and IEC 61850. THANOS was designed and implemented using the ONOS SDN controller and provides a high-level GUI for substation communication network management.

Our experience revealed a series of challenges in implementing a comprehensive framework such as ARES in the critical infrastructure of a substation. The strong security requirements expected from such a system coupled with the need to interact with specialized types of hosts, such as IEDs, proved to be particularly difficult, triggering a number of non-trivial design choices. Those choices were also affected by the high-availability requirements of the power sector, resulting, for example, in the need for a backup controller. We identified the need for a resourceful and user-friendly GUI as an important cornerstone of THANOS, as it must interface with personnel without expertise in computer networks — and SDN, in particular. We also identified particularities of data plane equipment that required software adjustments in THANOS.

Another challenge was coping with the stringent temporal requirements imposed by IEC 61850. To that end, we made the decision of proactively installing all time-critical flows — and their backups — by inspecting SCD files on initialization. Thus, the controller introduces no delay overhead, allowing the time requirements to be met. However, we were further concerned with the efficiency and overhead of THANOS' interactions. Therefore, we conducted an evaluation with industrial switches and real IEDs. Practical experiments demonstrated THANOS' ability to set up and manage a real teleprotection communication infrastructure in a timely manner and without incurring in excessive overhead.

For future work, we intend to perform further evaluations of THANOS. We are currently developing packet generators for the main communication protocols of IEC 61850, which will allow us to test THANOS in larger-scale deployments. We also plan to evaluate the usability of the GUI by non-specialized personnel.

References

[1] Technical Committee on Power systems management and associated information exchange, "IEC 61850 - communication networks and systems in substations," International Electrotechnical Commission (IEC), Tech. Rep., 2002- 2013.

[2] H. Maziku and S. Shetty, "Software Defined Networking enabled resilience for IEC 61850-based substation communication systems," in *2017 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 2017, pp. 690–694.

[3] A. Aydeger, N. Saputro, K. Akkaya, and S. Uluagac, "SDN-enabled recovery for Smart Grid teleprotection applications in post-disaster scenarios," *Journal of Network and Computer Applications*, vol. 138, pp. 39 – 50, 2019.

[4] E. Molina, E. Jacob, J. Matias, N. Moreira, and A. Astarloa, "Using software defined networking to manage and control IEC 61850-based systems," *Computers & Electrical Eng.*, vol. 43, pp. 142–154, 2015.

[5] Y. Lopes, N. C. Fernandes, C. A. M. Bastos, and D. C. Muchaluat-Saade, "SMARTFlow: A Solution for Autonomic Management and Control of Communication Networks for Smart Grids." 30th ACM SAC, 2015, pp. 2212–2217.

[6] Y. Lopes, N. C. Fernandes, D. C. Muchaluat-Saade, and K. Obraczka, "ARES: An autonomic and resilient framework for smart grids," in *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*. IEEE, 2017, pp. 222–229.

[7] P. Berde, M. Gerola, J. Hart, Y. Higuchi, M. Kobayashi, T. Koide, B. Lantz, B. O'Connor, P. Radoslavov, and W. Snow, "ONOS: towards an open, distributed SDN OS," in *Proceedings of the third workshop on Hot topics in software defined networking*. ACM, 2014, pp. 1–6.

[8] A. A. Zopellaro Soares, J. L. Vieira, S. E. Quincozes, V. C. Ferreira, L. M. Uchôa, Y. Lopes, D. Passos, N. C. Fernandes, I. Monteiro Moraes, D. Muchaluat-Saade *et al.*, "SDN-based teleprotection and control power systems: A study of available controllers and their suitability," *International Journal of Network Management*, p. e2112, 2020.

[9] P. Code, "Communication networks and systems in substations–part 8-1: Specific communication service mapping (scsm)–mappings to mms (iso 9506-1 and iso 9506-2)," 2004.

[10] IEC-61850-5, "IEC 61850-5: Communication requirements for functions and device models," *Technical Report, IEC*, 2003.

[11] Y. Rangelov, N. Nikolaev, and M. Ivanova, "The IEC 61850 standard—Communication networks and automation systems from an electrical engineering point of view," in *19th International Symposium on Electrical Apparatus and Technologies (SIELA)*. IEEE, 2016, pp. 1–4.

[12] ISO-9506-1, "Manufacturing Message Specification (MMS):part 1: Service definition," *International Organization for Standardization*, 2003.

[13] IEC-61850-7-1, "IEC 61850-7-1: Communication Network and Systems for Power Utility Automation. Basic Communication Structure-Principles and Models," *Technical Report, IEC*, 2011.

[14] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "OpenFlow: enabling innovation in campus networks," *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 2, pp. 69–74, 2008.