22rd International Conference on Renewable Energies and Power Quality (ICREPQ'24)
Bilbao (Spain), 26th to 28th June 2024
Renewable Energy and Power Quality Journal (RE&PQJ)
ISSN 2172-038 X, Volume No.22, September 2024

A practical implementation of virtualized protection system with IEC61850 under Docker

E. Torres, N. Escobar, P. Eguia, O. Abarrategi, D.M. Larruskain, V. Valverde and G. Buigues

Department of Electrical Engineering, School of Engineering of Bilbao, University of the Basque Country UPV/EHU
Plaza Ingeniero Torres Quevedo, nº 1, 48013 Bilbao (Spain)
Phone/Fax number: +0034 94 601 7332

Abstract. Substation Automation Systems (SAS) are currently designed and operated based on IEC 61850 standard. This standard along with the evolution of the information processing technology brings the possibility of developing new centralized SAS architectures based on virtualized protection and control. However, communication latency must be evaluated as it can limit the scalability of virtualized SAS. This paper explores via a practical simulation case the effects of the number of virtual IEDs in the data traffic of a virtualized IEC61850 SAS based on Docker. Simulation results have shown that the increase in the network traffic due to a higher number of virtual IEDs produces a longer delay in tripping operation under a fault condition.

Key words. IEC 61850, virtualization, protection, digital substation.

1. Introduction

The Substation Automation System (SAS) plays an important role in substations as it performs essential functions such as protection, automation and control. Earlier SAS used a centralized approach, although finally a distributed architecture was adopted due to limitations in available technology in those days. In a typical distributed SAS, Intelligent Electronic Devices (IEDs) are linked to a local processor, which controls one or more bays and is connected to a Human Machine Interface (HMI) or to a SCADA system for overall control. The design of SAS is currently based on the functional requirements of the IEC 61850 international standard to enable greater integration of protection, control, measurement and supervisory functions in the substation and easier interoperability between devices from different manufacturers. The standard establishes the following levels in the architecture of SAS:

- Process level: It contains substation primary equipment (power transformers, current and voltage transformers, switching equipment), and merging units (MU) which merge voltage and current signals from instrument transformers and transform them into digital signals.
- Bay level: It contains intelligent electronic devices (IEDs) for protection and control.
- Station level: It contains the Human Interface Unit (HMI) and SCADA systems for monitoring and operation of the substation, as well as gateways for the communication with the remote control center.

In an IEC 61850 substation, horizontal communication (e.g. between IEDs in the bay level) and vertical communication (e.g. between bay and station level) between IEDs is Ethernet based, by means of the process bus and the station bus, respectively.

As an alternative to the typical distributed architecture, the centralized approach has gained renewed interest in recent years due to the development of high-performance computing platforms. A CPC (Centralized Protection and Control) system consists of a high-performance computing platform capable of providing protection, control, monitoring, communication and asset management functions. It uses a lower number of devices, which improves operational safety and interoperability, and provides enhanced cybersecurity, due to the limited number of access points for cyber threats [1]. Also, the potential of the application of virtualization technologies in substations has recently started to be explored, in order to develop more flexible substations to manage the growing variability in the operation conditions of future electric systems [2, 3]. A virtualized SAS means a paradigm shift and the evolution to fully digital substations, where substation functionalities will be provided by software applications running autonomously in the same computing platform. As a result, hardware dependency will be reduced, as well as the time required for the commissioning of new substations and the deployment of new functionalities in existent substations.

Both approaches allow centralization of protection functions, typically carried out by multiple conventional relays, in a single computing platform and so, a reduction in the number of devices with regard to the traditional approach. However, as stated in [4], there is a difference regarding communication between different protection functions: in a centralized approach it is device internal and not necessarily visible over the IEC 61850, whereas in a virtualized approach it develops over a virtualized communication network. As a result, in a virtualized approach, some extension is required to represent the computer running the virtual IEDs in IEC 61850 SCL

(Substation Configuration Language) and latency issues derived from virtual communication should be carefully examined. On this way, the application of virtualization in substations poses several challenges that have to be further investigated, in order to guarantee correct real-time operation of the most critical SAS functionalities, as those related to protection and control.

In this paper, communication performance requirements of IEDs according to IEC 61850 standard are introduced in Section 2, and latency and scalability issues of virtualization of protection IEDs are discussed in Section 3. A practical simulation case study that analyzes the influence of the number of virtual IEDs in the data traffic of an IEC 61850 substation is described in Section 4. From this study, conclusions are extracted regarding the influence of the number of IEDs in the scalability of real virtualized SAS implementations.

2. IEC 61850 standard

IEC 61850 is the international Standard applicable to substation protection, automation and control systems. It provides the engineering definitions and processes for configuration and parameterization of the functions required for digital communication between IEDs in the substation. The main purpose of the standard is the interoperability between devices from different manufacturers. With that purpose, an XML-based Substation Configuration Language (SCL) is specified in the standard to create a set of files for the configuration of an IEC 61850 substation, which facilitates the engineering process and the integration of equipment from different vendors. One of those files is the Substation Configuration Description (SCD) file, which contains a description of the switchyard equipment and the topology of the one-line diagram, the capabilities of all protection and control IEDs used in the substation, as well as the subnetworks, access points and communication connections between IEDs.

An IEC 61850 IED is represented by means of a hierarchical data model, which is depicted in Figure 1. In this model, a physical device (PD) defined by its network IP address enables to identify the IED within the system. It contains a logical device (LD) with one or more logical nodes (LN) which represent the different functions performed by the IED.

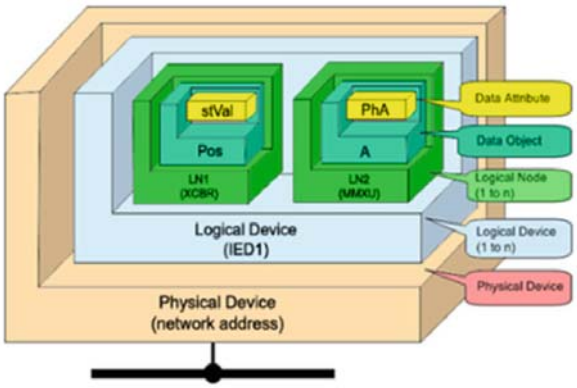

Fig.1. IEC 61850 data model [5]

The following protocols are specified in the IEC 61850 for communication between IEDs:

- MMS (Manufacturing Message Specification): It is used for application, configuration and monitoring data exchange.
- SMV (Sampled Measured Values): It is applied for communication of measurement values.
- GOOSE (Generic Object Oriented Substation Events): It allows fast and reliable communication of critical events and states.

MMS protocol is intended for communications between IEDs and higher level entities, such as a SCADA or a gateway. It applies a client-server approach, where a client requests data from a server. In contrast, GOOSE and SMV are protocols for the operation of protection systems, which are based on a publisher-subscriber mechanism, where a subscriber receives all messages but filters those messages is subscribed to. SMV messages are used in continuous real-time monitoring and control for the transmission of voltage and current signal measurements to protection and control equipment, and data are sent as high speed streams of data set samples. GOOSE messages are used for communication of real-time event-driven situations between IEDs. In GOOSE communication, the publisher sends messages periodically but when an event happens, it sends a burst of messages to minimize the chance of message loss (Figure 2).

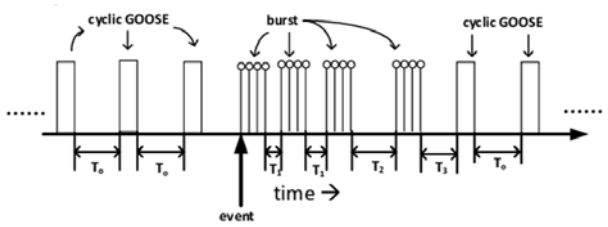

Fig.2. GOOSE transmission [5]

Operation of protection and control functions requires fast reliable communication of different type of messages. According to IEC 61850, the transfer time involved in the transmission of information between two devices includes the processing time within publisher, the transmission time from publisher to subscriber, and the processing time within subscriber to decode the received message (Figure 3). Also, different transfer time classes are defined depending on the application (Table I). In the case of protection functions, a transfer time class TT6 is established, with a transfer time below 3 ms.

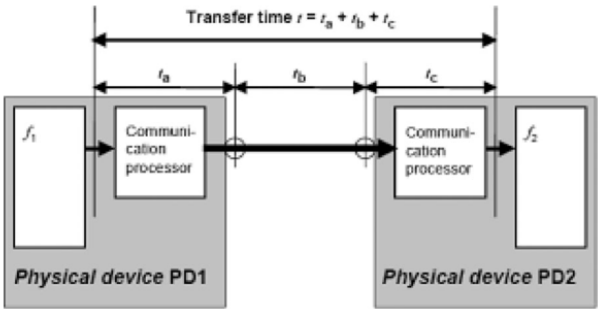

Fig.3. Overall transmission time between devices [6]

Table I. – Classes for transfer times (IEC 61850-5)

Transfer time class	Transfer time (ms)	Application examples: Transfer of
TT0	>1000	Files, events, log contents
TT1	1000	Events, alarms
TT2	500	Operator commands
TT3	100	Slow automatic interactions
TT4	20	Fast automatic interactions
TT5	10	Releases, status changes
TT6	3	Trips, blockings

3. Virtualization issues of protection and control functions

Virtualization consists on the creation of a software-based or virtual representation of a physical IT resource. It is widely applied in the IT sector and it is the basis of cloud computing. It improves the scalability and flexibility of systems, which reduces capital and operating costs, so its application in electric substations is being evaluated. There are two main virtualization approaches: hardware-level virtualization and operating system (OS) level virtualization (Figure 4). Hardware virtualization involves virtualizing the hardware on a server and creating virtual machines that provide the abstraction of a physical machine. It uses a hypervisor, which emulates virtual hardware (CPU, memory, etc.) for each virtual machine, which in turn runs its own operating system and applications. In contrast, OS virtualization encapsulates standard OS processes and their dependencies to create containers that share the underlying OS kernel [7].

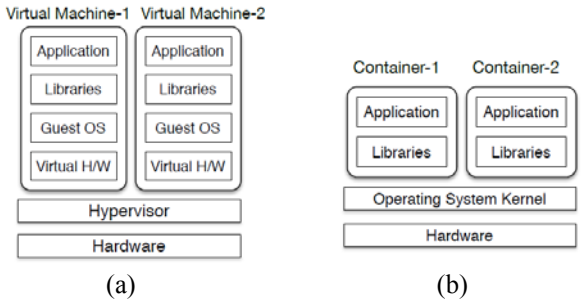

Fig.4. Hardware (a) and operating system (b) virtualization [7]

Virtual machines are typically more resource-intensive than containers, but also provide a high level of isolation, which is important in substation environments for security and compliance reasons. In contrast, containers are gaining a great popularity as they are more portable and can isolate application environments from other applications as well as from the host and, which facilitates the deployment of applications, and will enable the development of more agile and flexible substations. Virtualization of substation protection functionalities is analyzed in [8], where various possible approaches to develop virtual protection relays are identified, such as a straightforward approach based on directly porting a complete IED into a VM, or an alternative approach where common modules are consolidated to a separate VM. Container technology may be also applied to differentiate between protection functions in the virtual IED and take advantage of its scaling and portability characteristics. However, when applied in substation automation, virtualization faces new challenges in comparison to cloud environments, such as limited compute, storage and network resources, mixed criticality of applications, as well as real-time and high availability requirements of protection and control functions [9]. A critical challenge in virtualization of protection is guaranteeing real-time performance, which can be affected by different factors and is directly related to the scalability of virtualized protection and control solutions, i.e. the maximum number of IEDs that can be virtualized on the same computing platform, without affecting correct operation. In [8], results of preliminary tests of virtualized protection in VMs show a variation in the response time of overcurrent protection under different hardware allocation to VMs and fault magnitude. In addition, real-time performance of a protection and control application running in virtual machines and containers is evaluated in [10], being concluded that primary causes of timing errors were poor resource isolation and virtual network delays.

In a virtualized protection and control system, communication between virtualized applications relies on a virtual network. The influence of networking across Docker containers in real-time automation systems is investigated in [11] to determine whether communication between Docker containers, running on the same or different hosts, can be achieved within deadlines required by real time applications. The tests carried out using several Docker-supported software networking solutions (Host, Bridge and MACvlan) and a hardware-assisted solution (SR-IOV) under various workloads revealed some differences between them in terms of network latency and missed packets.

In the literature, different approaches are considered to emulate the network traffic in virtualized substation applications. A first approach is the use of an application that generates the different types of messages in a substation. This approach was applied in [6], where a laboratory virtual environment with 13 virtual machines to analyze the performance of virtualization of power system protection is described. Authors used Triangle MicroWorks 61850 Test Suite for running multiple IEC 61850 servers and clients on a single physical server, as well as for the generation and traffic simulation of GOOSE and SV packets. The research was later extended in [12] to consider 171 virtual machines running on three physical servers under Windows and Linux operating systems using the libIEC-61850 open source library. The developed platform was also tested with a physical merging unit sending sampled values to a virtualized overcurrent protection with the GOOSE publisher service implemented. In [13], authors emulate a virtual centralized protection and control system workload, using MGEN network test tool for the simulation of multicast packets with size and arrival rate similar to GOOSE and SV messaging. A different approach to these studies is used in [14], where authors consider the coupling of power grid simulation and virtualization of network infrastructure. A reduced circuit is simulated using HYPERSIM real-time simulation system, and a virtualized network including a simplified overvoltage

protection (PTOV) is set up via Containernet, using open source library libIEC61850 as interface. An advantage of this approach is the connection between energy and communication systems, which enables mapping the dependencies between them, providing online data for the development and testing of substation process-level analysis algorithms.

4. A case study of virtualization of protection and control IEDs

In this section, a simple case study of substation virtualization under Docker is described, that considers the coupling between the power and the communication systems to analyze the influence of the number of virtual IEDs in the data traffic of an IEC 61850 substation. The case study is based on an application available in a public repository [15], which simulates the operation of a simple substation with various IEDs using the open library libIEC61850. Although the application is not designed to run in real time, it provides some insight about the behavior of virtual IEDs in an IEC 61850 substation. A simplified one-line diagram of the substation is shown in Figure 5.

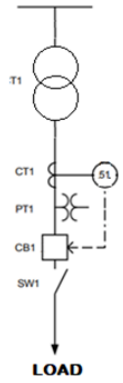

Fig.5.Simplified one line diagram

An SCD configuration file of the substation includes the information of substation primary equipment, IEDs and communication network. There are four IEDs in the substation: a circuit breaker (IED1_XCBR), a temporary overcurrent protection (IED2_PTOC) and two merging units (IED3_SMV, IED4_SMV) at the low and high voltage sides of the power transformer. The overcurrent protection is fed with sampled values from the merging unit and activates a protection trip conditioning (PTRC) logical node at the same logical device, publishing a GOOSE message with a trip command. The logical node XCBR is subscribed to GOOSE messaging from PTRC and updates its state after receiving a trip command. The application uses Docker, a tool for the automation and deployment of applications in lightweight containers, to create and run six Docker containers corresponding to the four IEDs, to the IEC61850 python based client and to the primary process simulator for the circuit simulation. Container networking refers to the ability for containers to connect and communicate with each other, and is configured in the application as "bridge", which lets containers connected to the same bridge network communicate, while providing isolation from containers that are not connected to that bridge network [16]. In addition, the application includes a graphical interface to browse the model and control the simulation. It has been used to modify a resistive load in order to create an overcurrent condition and cause the operation of the overcurrent protection, as shown in Figure 6, where current signals at both sides of transformer T1 are represented.

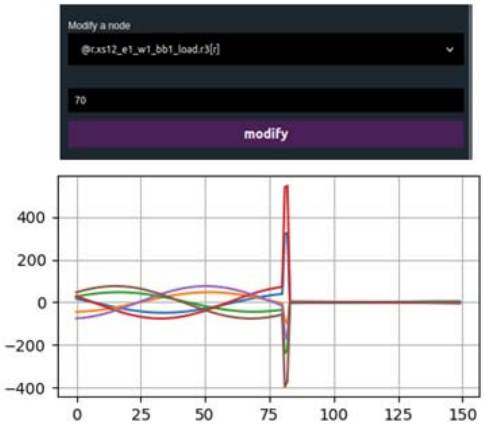

Fig.6. Transformer HV and LV current signals

The effect of virtualization on network traffic has been analyzed by means of Wireshark software, which required to modify the application to include a new Docker container in order to execute Wireshark in the same virtual environment (Figures 7 and 8).

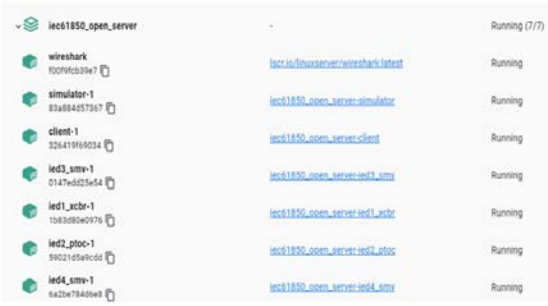

Fig.7. Docker containers

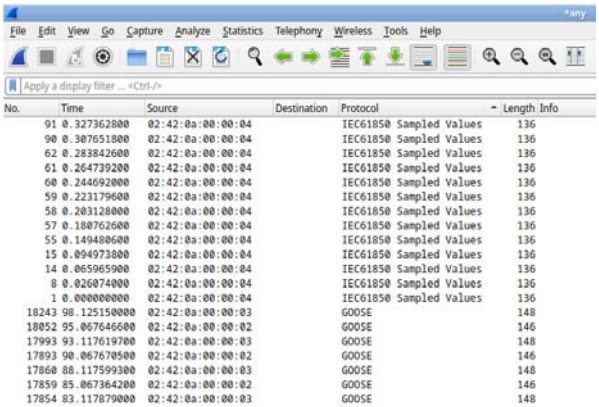

Fig.8. Capture of GOOSE and SMV messages with Wireshark

Figures 9 and 10 show periodic GOOSE messaging from IED1_XCBR and SMV messaging from IED3_SMV, respectively, in the base case under normal condition, as captured by Wireshark.

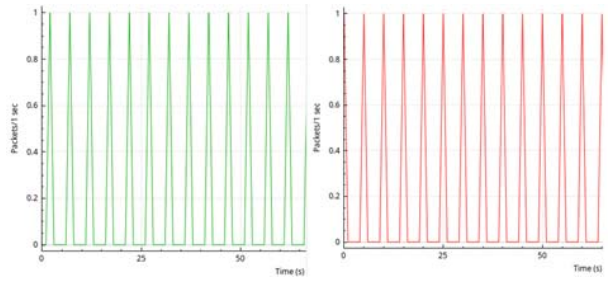

Fig.9.GOOSE messages from IED1_XCBR and IED2_PTOC in the base case, under normal condition

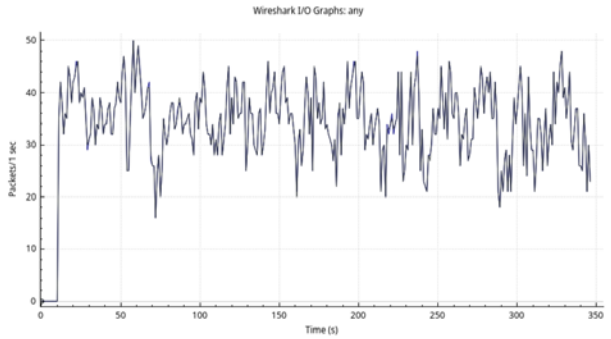

Fig.10.SMV messages from IED3_SMV in the base case, under normal condition

A case study was developed to evaluate the influence of virtualization scalability in an IEC 61850 substation. With this purpose, the IEC 61850 SCD configuration file of the substation was modified to include a higher number of IEDs. In particular, the number of IEDs publishing SMV messages was increased to boost the network traffic and the consumption of hardware resources by virtualization (Figure 11). Figure 12 shows an example of the network traffic obtained using Wireshark, when 1 and 7 new additional IEDs sending SMV were included, under normal operation condition. As it is shown, when the number of SMV publishers increases the network traffic rises significantly, in comparison to the base case.

CONTAINER ID	NAME	CPU %	MEM USAGE / LIMIT	MEM %	NET I/O
a30033db4b68	wireshark	0.25%	121MiB / 1.918GiB	6.16%	932kB / 0B
146c24fdac53	iec61850_open_server_ied2_ptoc_1	2.06%	1.148MiB / 1.910GiB	0.06%	951kB / 72.7kB
4aeab4de2652	iec61850_open_server_ied5_smv_1	2.03%	968KiB / 1.918GiB	0.05%	1.52MB / 444kB
12cd97b803fe	iec61850_open_server_ied3_smv_1	1.95%	960KiB / 1.918GiB	0.05%	1.68MB / 532kB
c2f970b84e9b	iec61850_open_server_ied9_smv_1	2.05%	912KiB / 1.918GiB	0.05%	1.32MB / 346kB
1fbbda00f672	iec61850_open_server_ied1_xcbr_1	2.16%	1.117MiB / 1.918GiB	0.06%	1.57MB / 493kB
abad4a550267	iec61850_open_server_ied4_smv_1	2.18%	1.305MiB / 1.918GiB	0.07%	1.62MB / 331kB
6dcc6cc16926	iec61850_open_server_ied11_smv_1	2.06%	924KiB / 1.918GiB	0.05%	1.33MB / 346kB
e23522b78087	iec61850_open_server_ied6_smv_1	2.16%	1.25MiB / 1.918GiB	0.06%	1.33MB / 346kB
fe1748b07a7d	iec61850_open_server_ied7_smv_1	2.22%	1.176MiB / 1.918GiB	0.06%	1.34MB / 346kB
cd9a5d966290	iec61850_open_server_ied8_smv_1	1.94%	1.098MiB / 1.918GiB	0.06%	1.33MB / 346kB
78089f2152b3	iec61850_open_server_simulator_1	0.01%	98.18MiB / 1.918GiB	5.00%	3.42MB / 5.88MB
d5ebde787952	iec61850_open_server_client_1	0.03%	43.37MiB / 1.918GiB	2.21%	1.97MB / 1.42MB
319c82b90571	iec61850_open_server_ied10_smv_1	2.04%	976KiB / 1.918GiB	0.05%	1.32MB / 346kB

Fig.11. Resource usage by Docker containers

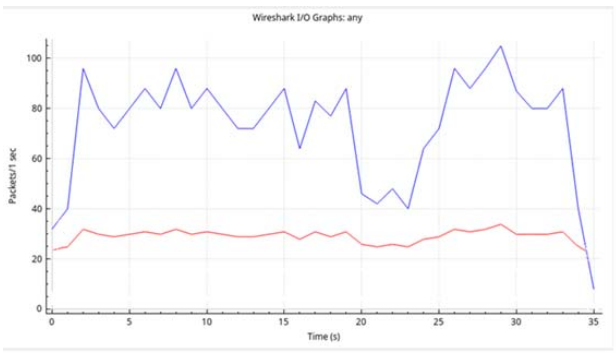

Fig.12.Increase in SMV network traffic in the base case (red) and in the case study (blue), under normal operation condition

The occurrence of an overcurrent event produces the activation of the overcurrent protection (IED2_PTOC) and the operation of the circuit-breaker (IED1_XCBR). IED1_XCBR is subscribed to GOOSE messages published by the PTRC logical node of IED2_PTOC when temporary overcurrent function of PTOC logical node is activated, and GOOSE communication between both IEDs was analyzed with Wireshark to evaluate the time operation after a fault. The value of parameters sqNum (sequence number) and stNum (state number) was monitored, as for every GOOSE message published, sqNum is incremented by one, while stNum is updated with an event. Figure 13 shows two captures of Wireshark corresponding to two consecutive GOOSE packets from IED2_PTOC. As it is shown, stNum changes from 1 to 2, while sqNum is initialized to 0, which means the operation of protection and the publication of the corresponding trip message The delay due to communication can be calculated as the difference between the instants of operation of the protection and of opening of the circuit breaker.

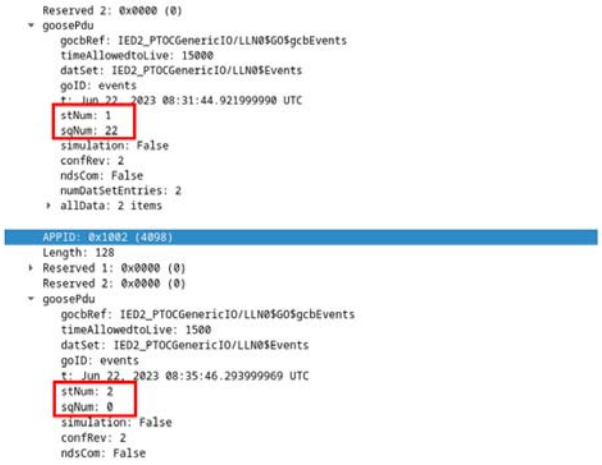

Fig.13.Identification of operation time with Wireshark

The communication delay was calculated in three scenarios with different number of IEDs (A: base case with 4 IEDs, B: case study with 1 additional IED, C: case study with 7 additional IEDs) for different overcurrent conditions. Results obtained in different tests are shown in Figure 14, where a significant increase is observed in the scenario C with 11 IEDs. In scenario A, an average communication delay of 37 ms was obtained, which increased around 3 ms in scenario B and 44 ms in scenario C. As a result, performance requirements of the most critical transfer time classes TT4, TT5 and TT6 of IEC 61850 would not be fulfilled when increasing the number of virtualized devices.

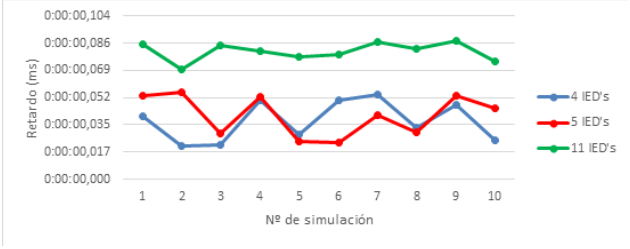

Fig.14.Operation time in scenarios A, B and C

In addition, the use of Wireshark tool allowed to identify an increase in the amount of SMV messages in network traffic (Figures 15 to 17) in scenarios B and C, in comparison to scenario A, but also a decrease in the frequency of SMV publishing.

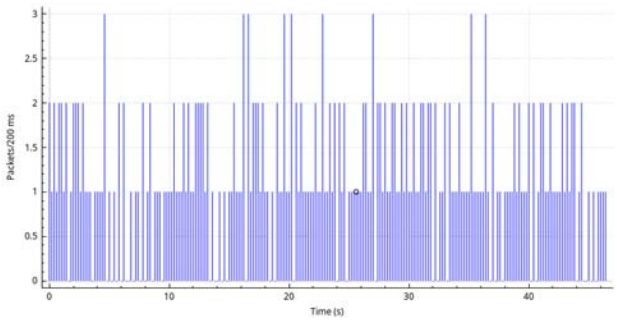

Fig.15. SMV messages in scenario A

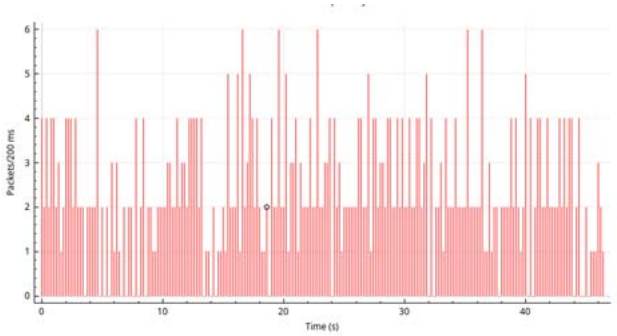

Fig.16. SMV messages in scenario B

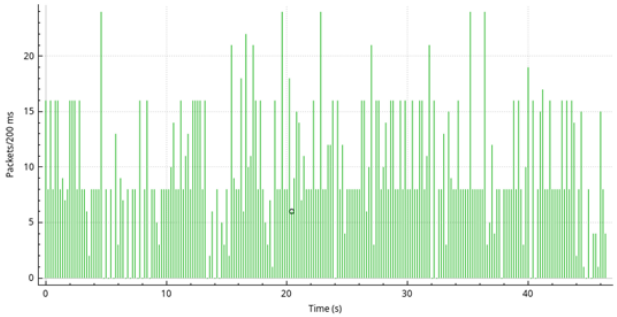

Fig.17. SMV messages in scenario C

5. Conclusion

Virtualization of protection and control functions means a paradigm shift in SAS. Performance of virtualization of IEDs is analyzed through the evaluation of network traffic. In this paper, the effect on network traffic of virtualization has been analyzed using a public application for the simulation of a simplified IEC 61850 substation. A case study with different number of virtual IEDs publishing SMV messages to modify network traffic was used to evaluate the effect on the tripping time under fault. Simulation results showed a higher delay in the publication of SMV and a higher latency in the tripping time when more virtual IEDs were included in the case study. Although the application is not developed for real-time simulation, it has allowed identifying latency issues due to virtualization of IEDs that can affect scalability in real substations.

Acknowledgement

This work was supported by the Basque Government under GISEL Research Group grant "IT1522-22" and Elkartek VIRTGRID "KK-2022-00069".

References

[1] M. Adamiak et al., Centralized Substation Protection and Control, IEEE PES Power System Relaying Committee, Report of Working Group K15 of the Substation Protection Subcommittee, 2015.

[2] S. Dayabhai, J. Prestwich, A substation automation solution that uses virtualization to reduce cost while ensuring redundancy and security compliance, Power and Energy Automation Conference, Washington (USA), March 2018.

[3] R. Hunt, B. Flynn, T. Smith, The substation of the future: Moving toward a digital solution, IEEE Power & Energy Magazine, Vol. 17, nº 4, pp. 47-55, 2019.

[4] C. Brunner, IEC 61850 and Virtualized Protection, PacWorld, nº 66, December 2023.

[5] P. Bishop, N.K.C. Nair, IEC 61850 Principles and applications to electric power systems, 2nd Edition, Springer, 2022.

[6] R. Wójtowicz, R. Kowalik, D. Rasolomampionona, Next generation of power system protection automation – Virtualization of protection systems, IEEE Transactions on power Delivery. Vol. 33(4), pp. 2002-2010, 2018.

[7] P. Sharma, L. Chaufournier, P. Shenoy, Y.C. Tay, Containers and Virtual Machines at Scale: A Comparative Study, 17th International Middleware Conference, Trento (Italy), December 2016.

[8] D. Samara, G. McKenzie, P. Khajuria, R. Ariya, P. Gopalakrishnan, V. Ravindran, Virtual protection relay – A paradigm shift in power system protection, INTEL-Kalkitech White paper. (Available at: www.intel.com/)

[9] S. Schönborn, T. Sivanthi, A. Kulmala, H. Nivery, R. Birke, The virtues of -virtualization, ABB Review, nº 2, pp. 118 – 123, 2023.

[10] S. Schönborn, R. Birke, D. Kozhaya, T. Sivanthi, Real-time performance of virtualised protection and control software, 27th International Conference on Electricity Distribution (CIRED), Paper nº 10702, Rome (Italy), June 2023.

[11] G. Albanese, R. Birke, G. Giannopoulou, S. Schönborn, T. Sivanhi, Evaluation of networking options for containerized deployment of real-time applications, 26th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Vasteras (Sweden), 2021.

[12] R. Wójtowicz, R. Kowalik, D. Rasolomampionona, Virtualization of protection systems – Test performed on a large environment base don data center solutions, IEEE Transactions on Power Delivery, Vol. 37(4), pp. 3401-3411, 2022.

[13] R. Carvalho, M. Antunes, J.P. Barraca, D. Gomes, R.L. Aguiar, Design and evaluation of a low-latency CPC environment for virtual IEDs, IEEE 11th International Conference on Cloud Networking (CloudNet), Paris, 7-10 November 2022.

[14] D. Rösch, S.Nicolai, P. Bretschneider, Combined simulation and virtualization approach for interconnected substation automation, 6th International Conference on Smart and Sustainable Technologies (SpliTech), Bol and Split (Croatia), 2021.

[15] R. Massink, ied_61850_open_server, An open source implementation of an IEC 61850 IED using lib61850. Available at: https://github.com/robidev?tab=repositories

[16] Docker Manuals, https://docs.docker.com/manuals/