Sampled Values ROCOF performance methodology breakdown

André Felipe Silva Melo
Department of Electrical Engineering
University of Seville
Seville, Spain
andre.melo@ieee.org

Jose Miguel Riquelme-Dominguez
Electrical Engineering Department
Escuela Técnica Superior de Ingenieros Industriales
Universidad Politécnica de Madrid
Madrid, Spain
jm.riquelme@upm.es

Francisco Gonzalez-Longatt
Department of Electrical Engineering
University of South-Eastern Norway
Porsgrunn, Norway
fglongatt@fglongatt.org

Jose L. Rueda and Peter Palensky
Department of Electrical Sustainable Energy
Technische Universiteit Delft
Delft, Netherlands
J.L.RuedaTorres@tudelft.nl

***Abstract*— Using Ethernet networks and communication protocols for protection applications requires protection engineers to understand different tools and technologies. This paper presents an investigation focused on clarifying the process bus-related concepts considering some relevant hardware, software, and protocol implementation aspects that may lead to misassumptions when doing Process Bus tests and studies. The authors performed real-time simulations considering 23 ROCOF scenarios under six different network background traffic environments to investigate network devices' throughput performance. In addition, the authors created a MATLAB script to subscribe and interpret the generated SV data correctly.**

Keywords—Frequency, frequency protection, IEC 61850, Sampled Values, Network Devices, Real-Time Simulation.

I. Introduction

The popularization of the IEC61850 standards and their concepts have been supporting the creation of new ways to solve the newest challenges related to the power systems reliability [1][2][3]. Part 9-2 of the standard introduced the Sampled Values (SV) protocol profile, which, joint with IEC61869 standards, creates the possibility to replace the system's analogue measurement and the conventional instrumentation with an equivalent Ethernet network with a data-stream time-coherent called Process Bus (PB).

According to the IEC61850 standard series, a typical substation is structured in three levels called Station, Bay, and Process Level connected by two networks. Station bus (SB), which interconnects the Intelligent Electronic Devices (IED) at the bay level to station-level and Process bus (PB), which connects the IEDs at primary equipment level to other IEDs [4]. The PB is the main characteristic to consider a substation digital. In this scenario, the hardwire connections between the switchyard equipment and the bay devices is replaced by a high availability communication network where the process data is published in real-time [5].

The research visit of J. M. Riquelme-Dominguez to the DIgEnSys-Lab has been supported by the research project funded by the Spanish National Research Agency/Agencia Estatal de Investigacion, grant number PID2019-108966RB-I00/AEI/10.13039/501100011033. Prof F Gonzalez-Longatt acknowledges the technical support provided by the teams of Typhoon HIL.

In addition, the PB has a high data flow load, the majority of SV for voltage and currents, and Generic Oriented-Object System Event (GOOSE) for process indications, trips, and automation. The SV stream is multicast communication published in the network in real-time. For this reason, to guarantee high-speed performance, its publisher/subscriber mechanism does not consider data receiving confirmation or retransmission [6].

Thus, to ensure the performance of the critical functions and the system reliability, the complete understanding of the SV protocol fundamentals and implementation aspects of network and protection devices is essential to testing and investigating the SV devices behaviour in non-ideal situations and interpreting them correctly. In addition, ensuring the network performance becomes a critical matter since an eventual delivery delay or a loss of packets can force the relay to disable the protection functions to avoid a miss operation [7][8][9].

This main paper contributes to clarifying how to correctly interpret PB-based applications applying a correct test methodology considering the relevant hardware, software, and protocol implementation aspects that may lead to missing assumptions when doing academic research with IEC 61850 Sampled Values. The authors performed real-time simulations considering 23 Rate Of Change Of Frequency (ROCOF) scenarios under six different network background traffic environments to investigate network devices delivery performance. In addition, a MATLAB model was created to correctly subscribe and interpret the generated data and investigate the effect of a packet loss over the ROCOF measurement.

II. Sampled Values Application and Real-Time Simulation

A. Sampled Values

The Sampled Values (SV) transport the digitized voltages and currents from the process instrument transformers via a communication network. The SV transmission concept is that the publisher device periodically sends messages in a frequency defined by the standard. The SV protocol data profile is defined by the IEC61850-9-2. It includes the complete mapping of the sampled value model [10].

Regarding the digital interface of the SV devices, the IEC 61869-9 defines samples and publish rates to be applied according to the application. The F4000S1I4U4 notation describes the variant for protection application compatible with legacy SV standard 9-2LE for 50Hz systems [11][12]. Fig. 1 indicates a protection SV packet, the application service data unit (ASDU) contains one sample with a dataset composed of four voltages and four currents called *PhsMeas1*. The *smpCnt* parameter is used to the subscriber organize the samples inside of a one-second period.

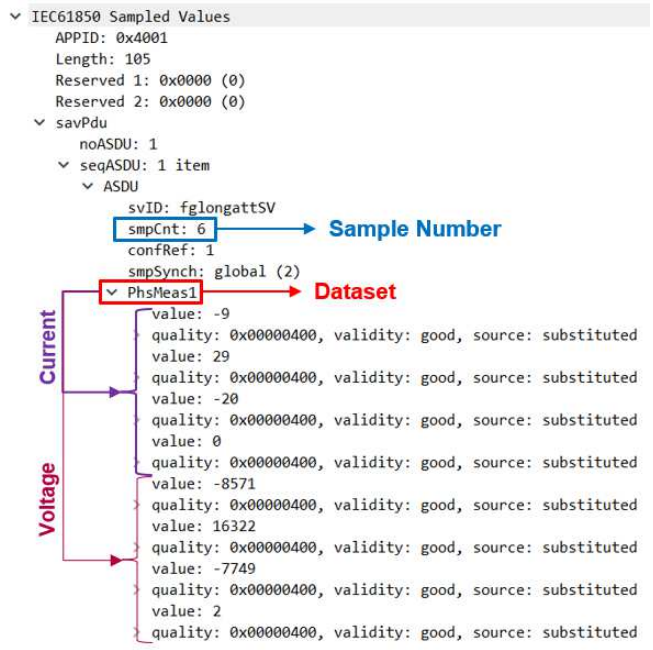

Fig. 1. Example IEC 61850 sampled values structure.

B. Rate Of Change Of Frequency

The ROCOF is an extremely important indicator of the frequency response of low rotational inertia power systems. To assess the performance of the frequency relay protection based on the ROCOF element synthetic signal has been created to assess properties. The test signal is based on frequency change between two limits using a straight line that represented a constant ROCOF (Hz/sec) -see Fig. 2.

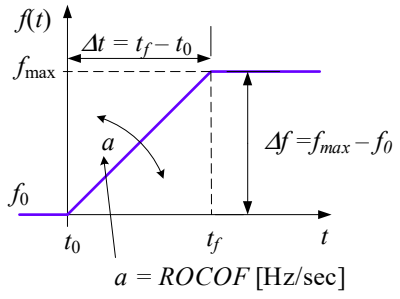

Fig. 2. Time dependant frequency signal used for testing purposes of constant ROCOF.

The test signal in this paper is a time-dependent signal $f(t)$ is calculated using the following mathematical expression:

$$\begin{cases} f(t) = f_0 & t < t_0 \\ f(t) = f_0 + ROCOFt & t_f \le t \le t_0 \\ f(t) = f_n & t > t_f \end{cases} \quad (1)$$

A constant ROCOF is enforced in $t \in [t_0, t_f]$ is reached by modifying the slope of the straight line (a), $ROCOF = a$. The authors have created a MATLAB script to produce a data file for the tests used in this paper.

C. Real-Time Simulation

The real-time simulation framework provides a magnificent tool to test IEC61850 based applications in real-life applications. This scientific paper uses the Typhoon HIL digital real-time simulation framework to produce the time-dependant frequency signal as a data stream of the IEC61850 sampled values. The data stream generated by the real-time simulator emulates the merging unit, and it is injected into the ethernet communication network. The Typhoon HIL toolchain read the test file, and it produces an F4000S1I4U4 SV stream.

III. Methodology and Testing

A. Test Setup Architecture

The used test setup is an adaptation of the test setup for verification test, proposed by the IEC61850-90-4 technical report, which presents network engineering guidelines [13]. Fig. 3 presents the test setup diagram. The real-time simulator and the traffic generators send the packets through the network. Since the test cases last 60 seconds, it is not possible to use the IED subscriber disturbance recording for the analysis. For this reason, the raw traffic data is captured by a network analyzer to be used in MATLAB for further analysis.

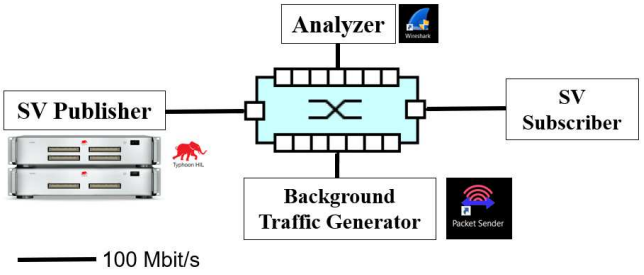

Fig. 3. Schematic representation of the test setup architecture.

B. ROCOF Test Cases

The SV stream performance is assessed using a test method based upon an under and over frequency constant frequency slope according to the IEC 60255-181 [14]. All the tests consider the system frequency consider in steady data (f_0 = 50 Hz), the under-frequency events are designed to reach the minimum frequency (f_{min} = 45 Hz) considering constant ROCOF and a similar situation for the over-frequency event (f_{max} = 55 Hz). A total of 13 under-frequency test signals are created considering $ROCOF$ = 0.25, 0.5, 0.75, 1, 2, … 10 Hz/sec. Similar conditions were followed for the over-frequency test signals.

C. Background Traffic Injection Test

External background traffic is injected into the network using Packet Sender and CMC 256. The Packet Sender is used for sending low priority messages to specified addresses. At the same time, the CMC256 is used to send high priority SV streams to increase the network bandwidth consumption.

Six test cases are proposed to test the SV propagation performance.

- No extra network traffics.

- 5 Mbps additional low priority traffic.
- 25 Mbps additional low priority traffic.
- 25 Mbps additional low priority traffic and 4.3 Mbps high priority traffic.
- 30 Mbps additional low priority traffic and 8.6 Mbps high priority traffic.
- 40 Mbps additional low priority traffic and 12.9 Mbps high priority traffic.

D. Sampled Values Ethernet packet inspection.

Wireshark network analyzer is a network sniffer tool; it makes it possible to capture the network traffic in the host network interface card (NIC). However, to correctly perform the SV data analyses, some considerations shall be taken into account using Wireshark in Windows environments. The Wireshark does not register timestamps. In a Windows computer, the Wireshark gets the timestamps from the WinPcap library. The WinPcap consists of a driver that provides low-level network access and a library that is used to access low-level network layers [15]. Allowing applications like Wireshark to capture and transmit network packets bypassing the protocol stack.

The *WinPcap* library is synchronized to the computer's clock only at the beginning of the packet capture. Consequently, the capture timestamps may have a few milliseconds of inaccuracy. Since the time between samples is 250 µs in the F4000S1I4U4 variant and the ASDU data does not carry sample origin timestamp, an µs accuracy is required for time delay analyses.

Thus, using the Wireshark capture files timestamp for time delay analyses may lead to erroneous results. Nevertheless, since the Wireshark is capable of decoding the SV protocol data and the correctly SV subscription does not rely on the timestamp, the captured data was used to rebuild the waveform and track packet loss by looking at the *smpCnt*.

E. Sampled Values Data decoding using MATLAB

The *smpCnt* parameter is the sample numerical indexing a one-second period, its value is incremented each time a new sampled value is taken, and it is set to zero when the synchronization occurs every second. The IEC 61869-9 defines the use of the *smpCnt* for time alignment. After receiving the SV packet, the subscriber allocates the samples in their respective places regardless of the arrival order. As a result, the signal can be accurately processed in a time-coherent way.

Although the protection relays available cannot record a 60-second disturbance, the data captures were analyzed using a MATLAB script that interprets the SV data in the same way as the protection relays. Fig. 4 presents an SV data capture aligned using the created MATLAB script. The upper plot shows the Voltage measurement aligned according to the Wireshark timestamp. The bottom plot shows the same measurement aligned according to the *smpCnt*.

The first voltage measurement presented in Fig. 4 is an example of a wrong data analysis caused by the Wireshark timestamp inaccuracy; the signal presents a waveform distortion caused by a false network jitter. In addition, the time alignment according to the sample index works as a jitter buffer filter. Since the sample order and sample rate are known, a possible real jitter shall not affect the waveform, as presented in Fig. 4 second measurement.

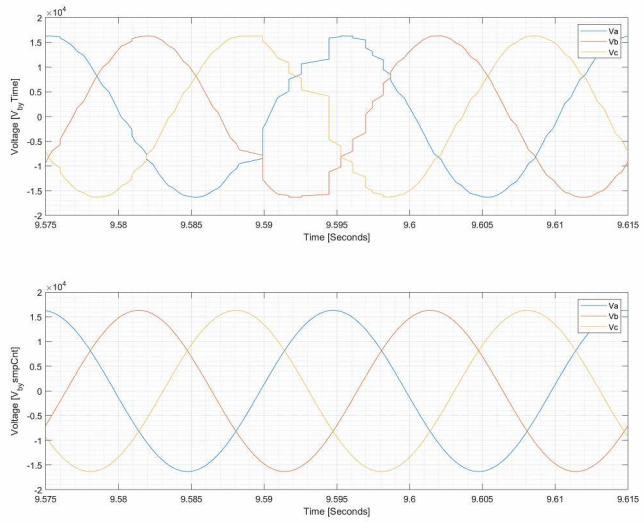

Fig. 4. SV voltage stream aligned by time arrival and smpCnt index.

F. Network Packet Delivery Reliability

The background traffic injection test was performed to verify the network reliability in terms of packets delivery. Table 1 presents the packets data loss under the three worst background traffic scenarios. The left column presents the background traffic load injected for the analysis. The right column presents the maximum continuous packets loss in a second period.

The presented values consider 138 data capture of 60 seconds. Eventual packet losses were detected during the tests. However, since it represents less than 1 per cent of the test cases, it can not be considered a conclusive result. Therefore, the ten best and the ten worst results were discarded. Fig. 5 shows the *smpCnt* count of an SV stream captured under the worst load scenario; no conclusive packet loss was detected.

TABLE I. BACKGROUND TRAFFIC TEST

Background Traffic Injection	
Brackground Traffic	***Maximum Pakcet Loss/s***
25 Mbps low-priority & 4.3 Mbps high priority	No loss
30 Mbps low-priority & 8.6 Mbps high priority	No loss
40 Mbps low-priority & 12.9 Mbps high priority	No loss

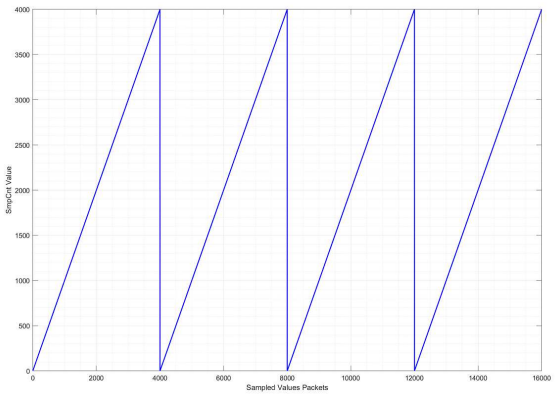

Fig. 5. Plot of the *smpCnt* Values.

Although the maximum load injected was not enough to force a packet loss, this result was already expected since the architecture uses high-performance network devices. Furthermore, when using external background traffic for network reliability tests, the bandwidth is not the unique parameter to be considered. The packet's priority and the switch's throughput performance are the key points for analysis; an industrial switch can process and forward more than 30 million packets per second.

Thus, to force a continuous packet loss due to background traffic, a high-priority external traffic load of about 90 per cent of the link bandwidth shall be used. Otherwise, the test may lead to wrong conclusions.

G. ROCOF Measurement

Fig. 6 presents the positive ROCOF slopes test scenarios using the MATLAB subscription to process the SV stream captured under the worst load scenario. Since the SV used variant uses a high sample rate and there is no packet loss, the ROCOF detection was very accurate and sensitive for all scenarios.

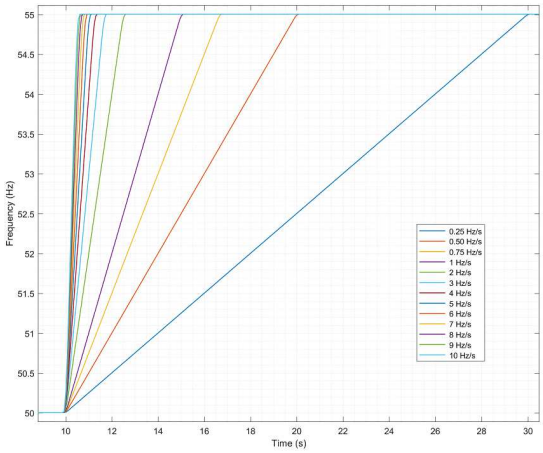

Fig. 6. Plot of the Time dependant frequency signal used for testing purposes of constant ROCOF in this paper.

In addition, to investigate the effect of the SV packet loss over the ROCOF measurement, additional test data were created by removing manually 3 SV data packets from the simulation file captures. The packets were strategically removed along the first second of the ROCOF to investigate its effects inside of the test slopes.

Fig. 7 presents the raw data analysis of the first second of the test slopes. The upper side image shows the ROCOF in a packet loss condition. The bottom image shows the same signals in normal conditions, respectively. By analyzing the raw data, the packet loss creates a sharp false change in the instantaneous frequency. However, to investigate a possible effect over a protection device, some implementation aspects shall be considered.

Different manufacturers may use different measurement methods, protection algorithms, and error compensation filters regarding measurement implementation. The IEC 60255-181 describes the general requirements on frequency measurement for protection IEDs; the packet loss may have a different signal response depending on the applied method. For instance, a missing sample value at the sinewave's peak may not affect a zero-crossing frequency measurement.

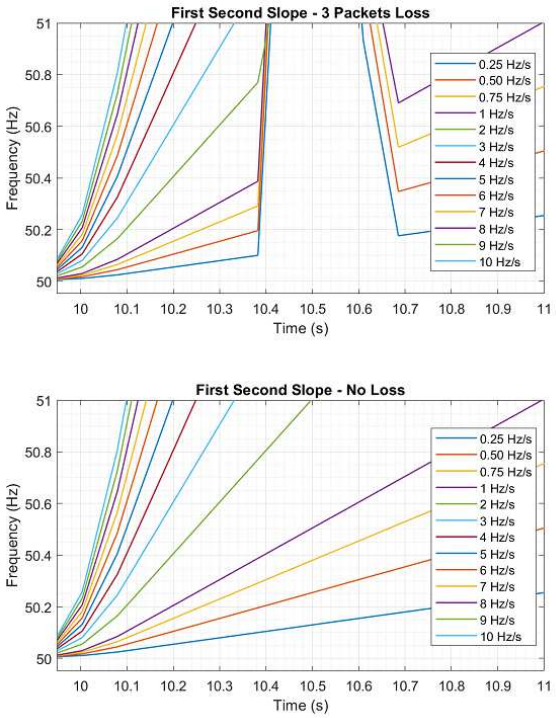

Fig. 7. Plot of the first 1 second window of the ROCOF slopes.

Although the raw data values present an instantaneous frequency change, it shall not affect the protection relay operation. The PB protection devices are designed with packet loss detection mechanisms; when a packets loss is detected for a certain number of consecutive packets (usually 3), the IED disables the dependent protection function to avoid a miss operation. In addition, some IEDs algorithms are capable of doing a signal interpolation to compensate the packet loss. Fig. 8 presents the signal interpolation implemented in the MATLAB subscriber script. The green square marks the interpolation of the three removed packets.

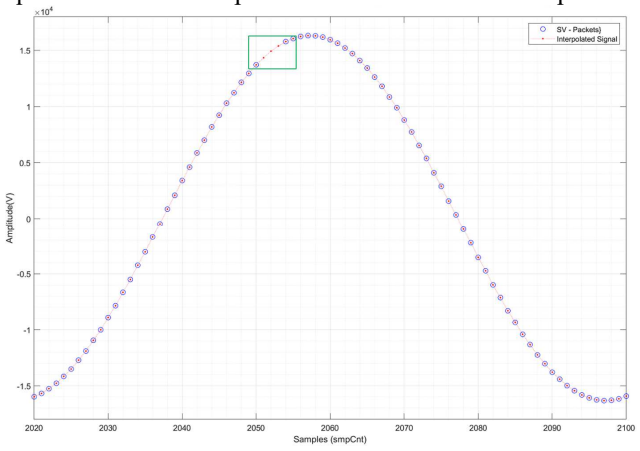

Fig. 8. Plot of the voltage amplitude depicting SV packets and interpolated signal

IV. CONCLUSION

This paper presented preliminary investigation results that aim to clarify how to apply a correct test methodology considering the relevant hardware, software, and protocol implementation aspects that may lead to false results when doing academic research with IEC 61850 Sampled Values. The presented results are mainly about the network devices

packet throughput performance, testing tools considerations, and IED implementations aspects that guarantee the reliability under an SV packet loss scenario. From the discussion presented in Subsections III.D-III.E, it is possible to determine that the Wireshark is a powerful tool for data protocol analysis. However, it is not adequate for network time-critical conformance analyses in a Microsoft Windows environment, and its Ethernet time stamps may lead to a false latency and jitter analysis. According to the discussion presented in Subsection III.F, a typical industrial Ethernet switch has a proven throughput high-performance capability, and the background traffic required to compromise its performance in a single bus architecture eventually is beyond the used traffic injection tools capabilities. As a result, no considerable packets loss rate was found during the testing.

Regarding frequency measurement, depending on the method, a possible SV data loss may have an impact on the instantaneous ROCOF measurement. However, in a real protection IED, this false ROCOF change shall not affect the protection performance since the protection devices are capable of monitoring the missing samples and disabling the protections functions after a number of consecutive losses. Moreover, some devices are capable of interpolating the missing samples until the complete data subscription reestablishment, as presented in Subsection III.G.

Furthermore, the SV applications have been proving to be operationally reliable over the years. The presented discussion can contribute to a clear understanding of its work principles and related technologies for further investigations and discussions.

REFERENCES

[1] A. Alvarez de Sotomayor, D. Della Giustina, G. Massa, A. Dedè, F. Ramos, and A. Barbato, "IEC 61850-based adaptive protection system for the MV distribution smart grid," *Sustain. Energy, Grids Networks*, vol. 15, pp. 26–33, 2018, doi: 10.1016/j.segan.2017.09.003.

[2] M. G. Kanabar and T. S. Sidhu, "Performance of IEC 61850-9-2 process bus and corrective measure for digital relaying," *IEEE Trans. Power Deliv.*, vol. 26, no. 2, pp. 725–735, 2011, doi: 10.1109/TPWRD.2009.2038702.

[3] A. Apostolov, F. Auperrin, R. Passet, M. Guenego, and F. Gilles, "IEC 61850 process bus based distributed waveform recording," *2006 IEEE Power Eng. Soc. Gen. Meet. PES*, pp. 1–6, 2006, doi: 10.1109/pes.2006.1709631.

[4] IEC TR 61850-1 Ed. 2.0, *Communication networks and systems for power utility automation – Part 1: Introduction and overview*. 2013.

[5] A. F. Silva Melo, U. C. Netto, J. C. C. da Silva, and U. J. Dreyer, "Influence of process bus on performance of power system protection," *Electr. Power Syst. Res.*, vol. 200, no. March, 2021, doi: 10.1016/j.epsr.2021.107491.

[6] S. M. Blair, A. J. Roscoe, and J. Irvine, "Real-time compression of IEC 61869-9 sampled value data," *2016 IEEE Int. Work. Appl. Meas. Power Syst. AMPS 2016 - Proc.*, 2016, doi: 10.1109/AMPS.2016.7602854.

[7] D. Bogdanov, G. Dimitrov, and F. Gonzalez-Longatt, "Improving the reliability of busbar protection system with IEC 61850 GOOSE based communication," in *Advances in Intelligent Systems and Computing*, 2018, vol. 680, pp. 459–467, doi: 10.1007/978-3-319-68324-9_50.

[8] S. Chase, E. Jessup, M. Silveira, J. Dong, and Q. Yang, "Protection and testing considerations for IEC 61850 Sampled Values-based distance and line current differential schemes," in *72nd Annual Conference for Protective Relay Engineers*, 2019, pp. 1–10, [Online]. Available: http://prorelay.tamu.edu/wp-content/uploads/sites/3/2019/03/ProtectionAndTesting_6898_20190307.pdf.

[9] I. Ali, M. S. Thomas, and S. Gupta, "Sampled values packet loss impact on IEC 61850 distance relay performance," *2013 IEEE Innov. Smart Grid Technol. - Asia, ISGT Asia 2013*, pp. 1–6, 2013, doi: 10.1109/ISGT-Asia.2013.6698767.

[10] IEC 61850-9-2 Standard ed2.1, "Communication networks and systems for power utility automation – Part 9-2: Specific communication service mapping (SCSM) – Sampled values over ISO/IEC 8802-3," 2020.

[11] IEC 61869-9 Ed. 1.0, "IEC 61869-9 Instrument transformers – Part 9: Digital interface for instrument transformers," 2016.

[12] UCA International Users Group, "Implementation Guideline for Digital Interface to Instrument Transformers Using IEC 61850-9-2," 2004.

[13] IEC TR 61850-90-4 Ed. 2.0, "Communication networks and systems for power utility automation – Part 90-4: Network engineering guidelines," 2020.

[14] IEC 60255-181 Ed. 1.0, *Measuring relays and protection equipment – Part 181: Functional requirements for frequency protection*. 2019.

[15] H. Wang and R. Ma, "Design of network protocol analyzers using WinPcap," *Open Cybern. Syst. J.*, vol. 8, pp. 779–783, 2014, doi: 10.2174/1874110x01408010779.