Modelling the IEC 61850 and DNP3 Protocol Using OPNET in an Electrical Substation Communication Network

Dion Njova
Department of Electrical and Mining Engineering
University of South Africa
Johannesburg, South Africa
53113934@mylife.unisa.ac.za

Kingsley Ogudo
Department of Electrical & Electronics Engineering, Faculty of Engineering and the Built Environment
University of Johannesburg
Johannesburg, South Africa
kingsleyo@uj.ac.za

Patrice Umenne
Department of Electrical and Mining Engineering
University of South Africa
Johannesburg, South Africa
umennpo@unisa.ac.za

Abstract— **Communication protocols are part of supervisory control and data acquisition (SCADA) and they are used by the devices connected on the SCADA network. In this paper the distributed network protocol (DNP3) and International Electrotechnical Commission IEC 61850 communication protocols were modelled in OPNET. The simulation of DNP3 and IEC 61850 communication protocol is done in different scenarios and the traffic behavior is analyzed. The DNP3 protocol is modelled as the medium protocol of communication during the maintenance of a 400kV Transformer at an Electrical Substation. Its network traffic behavior is then analyzed for this operation. The IEC 61850 protocol is then used as a medium of communication in the same Electrical Substation communication network (SCN) when a faulty backbone switch is present. In this scenario the network traffic behavior is again analyzed. The DNP3 simulation during the maintenance of the 400 kV Transformer shows that the model is working since the throughput is consistent without dropped packets at the Substation RTU end and the 400kV Transformer IED end. The IEC 61850 simulation when a faulty backbone switch is present shows that the model is working in this scenario since the throughput is again consistent. When the IEC 61850 protocol is modelled on the SCN, the time delay is 80 µs during normal operation and with a faulty switch the delay is 100 µs for this protocol. This shows that for the IEC 61850 model the time delay increases when there is a faulty backbone switch but not exceedingly since there is a backup switch in the model. The DNP3 model shows that during the maintenance of the 400kV Transformer the time delay is approximately 160 µs. The IEC 61850 protocol performs approximately twice as fast as the DNP3 protocol during normal operation in an SCN.**

Keywords— Supervisory Control and Data Acquisition (SCADA), Distributed Network Protocol (DNP3), International Electrotechnical Commission (IEC) 61850, Intelligent Electronic Devices (IED's), Remote Terminal Unit (RTU).

I. INTRODUCTION

Supervisory Control and data acquisition (SCADA) involves the control and monitoring of the running equipment to perform the functions of parameter adjustment, measurement, data acquisition and equipment control [1]. SCADA system is used at an Electrical Substation to monitor alarms, analogue messages such as voltage levels and to open and close breakers remotely. This paper analyzes the traffic characteristics in different operational scenarios when two communication protocols commonly used in SCADA systems namely IEC 61850 and DNP3 are applied over an Electrical Substation grid. DNP3 is an open source protocol used in the SCADA System [2]. DNP3 protocol defines and identifies three layers in a network (data link, application layer and physical layer). This is referred to as the Enhanced performance Architecture (EAP). DNP3 protocol function is defined by the application layer. The information format is defined by the data link layer. The physical layer consists of an ordinary fibre transceiver or RS-485 [3]. DNP3 has been modified such that it can be transported over TCP/IP. The DNP3 frame is simply encapsulated with TCP/IP headers as in [4]. DNP3 over TCP/IP consists of a four layered protocol model, these layers are data link layer, application layer, pseudo transport layer and physical layer [5]. The DNP3 application layer is a request response architecture type model. In this model the master station sends a request for status and the outstations respond to these requests. Messages can also be sent by the outstations without a request [5]. The maximum size of a DNP3 reconstructed application layer message is 2048 octets [6]. This size can however be adjusted as in [6]. The DNP3 protocol has a security mechanism referred to as a secure authentication (DNP3-SA). The DNP3-SA protocol can be applied under unicast communication as in [7]. The international electrotechnical commission proposed the IEC 61850 protocol as the common communication standard to be used in power systems. IEC 61850 can be modelled using the object-oriented approach as is done in [8]. The IEC 61850 is a communication protocol based on the Ethernet packet [9]. IEC 61850 has been used as a standard protocol of communication in smart grids and for substation automation functions. It has a System Configuration Language (SCL), abstract communication service interface and an object-oriented data model. The communication aspect of IEC 61850 enables it to be used for metering, measurement, protection and control functions in substation automation [10]. Communication models and information has been made available on the implementation of the IEC 61850 standard in power grid systems. To achieve perfect mapping between communication technologies such as IEC 61850 and power grid systems information mapping models such as Ether Passive Optical Network (EPON) are developed in [11]. IEC 61850 protocol has three hierarchical levels that it uses to group the functions of IED's. The lowest level is data objects. The second level is the logical nodes and the top level is the logical device or the physical device [12]. In the IEC 61850 protocol the status signals and analog signals are sampled by the primary

For reprint or republication permission, email to IEEE Copyrights Manager at pubs-permissions@ieee.org. All rights reserved. Copyright ©2022 by IEEE.

equipment. The digital values are transmitted to the IED's over the process bus with GOOSE and SV messages as in [13]. The maximum time delay for GOOSE messaging is 4 ms [14]. The latest technology based on the IEC 61850 can be used to link all SCN devices such as automation, protection and primary devices together as in [15]. The paper is structured in the following way section II continues with the literature of related works, section III gives the methodology used, section IV analyses the results and section V gives a conclusion.

II. RELATED WORKS

DNP3 can be used to evaluate SCADA traffic characteristic to detect cyber threats as in [16]. There the DNP3 slave runs the PLC's (Cyber energy systems) while the DNP3 master runs the SCADA network (physical part). IEC 61850 can improve the operation of substation devices, however because it uses network communication to operate these devices it opens them up to security breaches. Hence the paper in [17] discusses the method that can be used to provide security protection to the three major layers in an IEC 61850 network which are the process layer, the interval layer and the station control layer. IEC 61850 can be used to provide operational advantages when it comes to connectivity in a substation grid. During the upgrade of substation utilities there maybe complexities in connecting devices. Such complexities can be eliminated by using the IEC 61850 standard strictly as discussed in [18]. In this paper the merging unit receives signals from several primary devices, and it makes use of sampled values type messages for multicasting to the ethernet network. In a substation network several meters are connected to a data concentrator unit (DCU) during the metering process. The paper in [19] focuses on the design of IEC 61850 as a value added service for a DCU which will enable meters from different vendors to be integrated. The IEC 61850 defined Substation Configuration Description Language (SCL) can be used in the description of the Protection Intelligent Center in a substation network as is done in [20]. The paper in [21] shows how the source maintenance of data can be used to operate the whole power or substation automation network.

III. METHODOLOGY

A. Substation Communication Network Block Diagram

Figure 1 shows the Substation Communication Network (SCN) block diagram designed in this paper. It consists of the protection IED's, Switch IED, two backbone switches, a gateway switch and the Substation RTU.

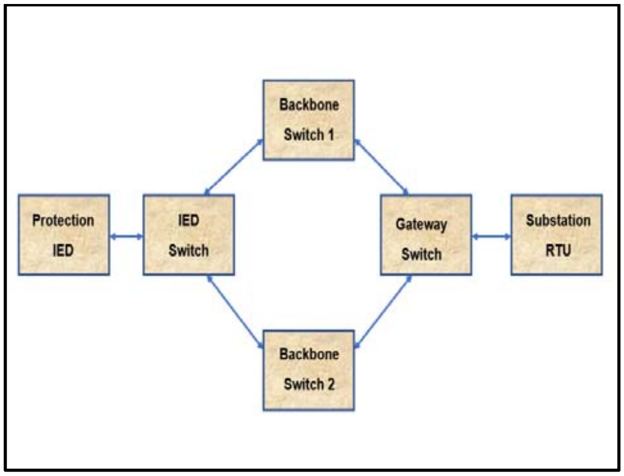


Fig. 1 Substation Communication Network (SCN) block diagram

B. Substation Communication Network OPNET Model

Figure 2 shows the same Substation Communication Network (SCN) model simulated in OPNET. The Substation Communication Network model in OPNET is modelled with a server that simulates the Substation RTU (gateway device), ten IED's that simulate protection relays and 13 switches that simulate the ten protection IED switches, two backbone switches and the gateway switch. The communication medium used between the devices is optical fiber as selected in the OPNET software [22].

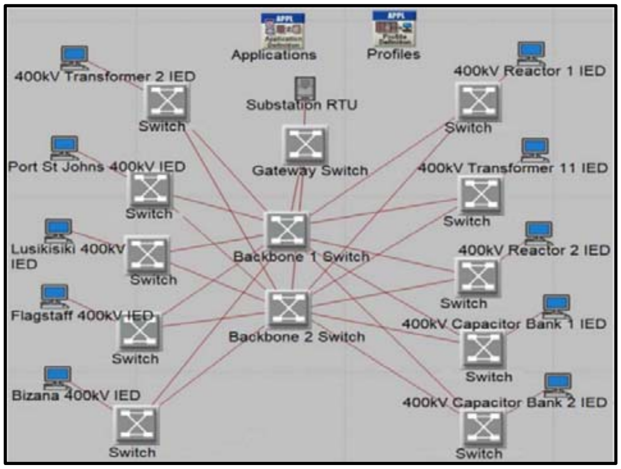


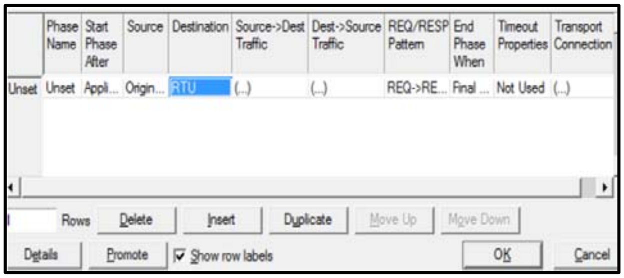
Fig. 2. OPNET Substation Communication Network (SCN) model.

C. DNP3 Simulation Configuration

The manual configuration of the DNP3 protocol in OPNET is shown in Fig.3. Basically, the DNP3 protocol is applied over the TCP/IP settings in OPNET as discussed in the literature review. The IED traffic characteristics are set as follows: the request count is set to 3 seconds, initialization time is set to 50 ms, inter request time is set to 1 second, inter packet time is set to 1 second, packet per request is set to 3222 bytes and request packet size is set to 3222 bytes [23,24]. The substation RTU traffic characteristics are configured as follows: inter packet time is set to 1 second, request

For reprint or republication permission, email to IEEE Copyrights Manager at pubs-permissions@ieee.org. All rights reserved. Copyright ©2022 by IEEE.

processing time is set to 50 ms, packet per response is set to 1024 bytes and response per packet size is 1024 bytes [22,24].

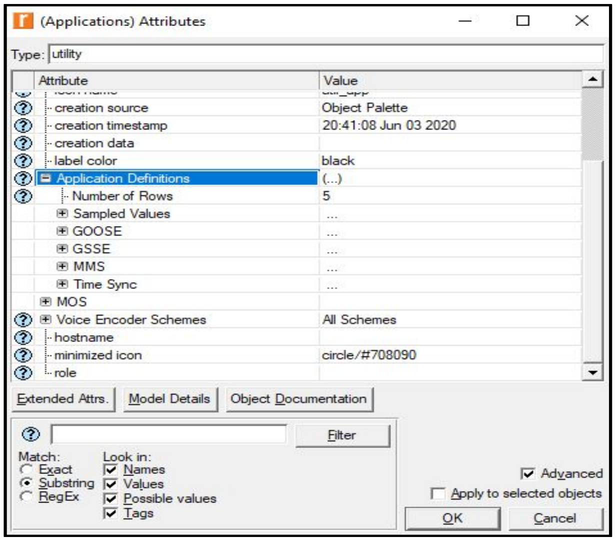


	Phase Name	Start Phase After	Source	Destination	Source->Dest Traffic	Dest->Source Traffic	REQ/RESP Pattern	End Phase When	Timeout Properties	Transport Connection
Unset	Unset	Appli...	Origin...	RTU	(...)	(...)	REQ->RE...	Final ...	Not Used	(...)

Fig. 3 DNP3 Manually configuration [23]

D. IEC 61850 Simulation Configuration

The IEC 61850 protocol stack configuration is shown in Fig.4. The data packet sizes for messaging are configured as follows. Sample values are set to 15 frames/sec [25,26], Controls/GOOSE packets are set to 204 bytes, time sync packets set to 219 bytes, Analogues/SV packets are set to 219 bytes [26,27,28], indication/GSSE packets are set to 144 bytes, Alarm/MMS packets are set to 144 bytes.



(Applications) Attributes

Type: utility

Attribute	Value
creation source	Object Palette
creation timestamp	20:41:08 Jun 03 2020
creation data	
label color	black
Application Definitions	(...)
Number of Rows	5
Sampled Values	...
GOOSE	...
GSSE	...
MMS	...
Time Sync	...
MOS	
Voice Encoder Schemes	All Schemes
hostname	
minimized icon	circle/#708090
role	

Fig. 4 IEC 61850 Protocol stack configuration [26]

IV. RESULTS AND DISCUSION

The results consist of the performance of the network when the DNP3 protocol is applied over the network during a maintenance operation. Secondly the performance of the network when the IEC 61850 protocol is applied over the same network, with one backbone switch being faulty and one backbone switch operating normally in this scenario. Therefore, results cover a maintenance operation and the possibility of a fault occurring in the network. This are normal occurrences in a power substation grid.

A. Performance of the DNP3 protocol

The performance of the DNP3 protocol is analyzed during a substation maintenance operation. The data traffic and the time delay between the 400 kV transformer II IED and the substation RTU on the model were monitored during this simulation. Fig.5 shows the received and sent traffic at the substation RTU end. The received traffic at the substation RTU end is more than the sent traffic because the Substation RTU is receiving data from all the IED devices on the SCN shown in Fig.2 at the same time. The Substation RTU only sends traffic when its requesting data from the IED's or when it is sending a control command to the IED's, in general to one device at a time. The received traffic at the substation RTU end is initially steady then at a time of two minutes and forty seconds there is a sharp increase in traffic at the RTU. This occurs because of the alarms and indications messages it receives from the 400kV Transformer II IED during the maintenance operation.

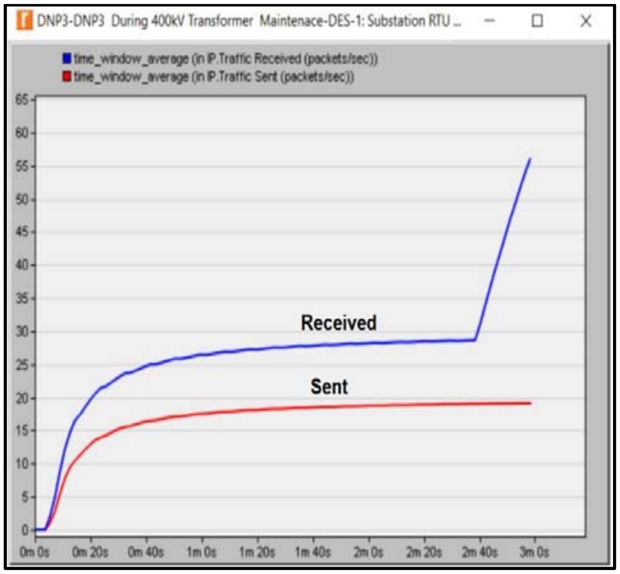


Fig. 5. Sent and Received Traffic at the Substation RTU end.

Fig.6 shows the sent and received traffic at the 400 kV Transformer II IED end. The 400 kV Transformer II IED sends more traffic to the Substation RTU and receives less traffic from the Substation RTU. The reason for this is because the Substation RTU request data from the 400 kV Transformer II IED and the transformer responds by sending all the data to the substation RTU, as a result the 400 kV transformer has more sent traffic and less received traffic on that communication line. There is a steady sent traffic for two minutes and then a sharp increase in sent traffic occurs at two minutes forty seconds. This is caused by the increase in the alarm messages sent by the 400 kV Transformer II IED to the Substation RTU during the maintenance operation indicating the need for maintenance.

For reprint or republication permission, email to IEEE Copyrights Manager at pubs-permissions@ieee.org. All rights reserved. Copyright ©2022 by IEEE.

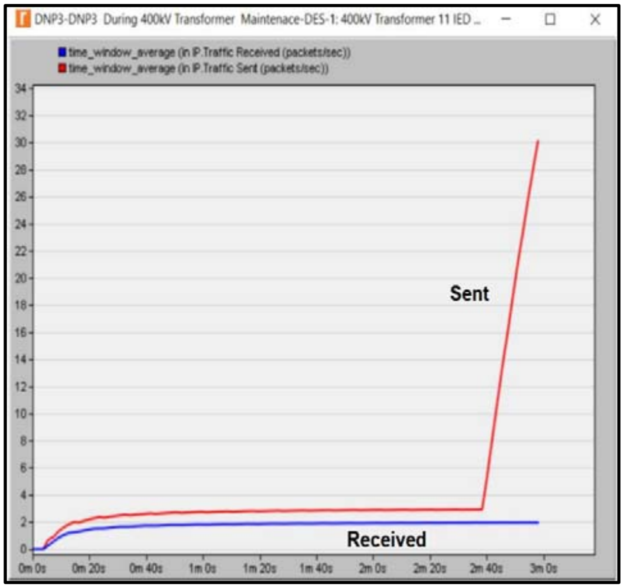


Fig. 6. Sent and Received Traffic at the Transformer II IED end.

During the maintenance operation data is received at the Substation RTU end. The time delay for the traffic of this data at the RTU end is measured. Fig.7 shows the graph of the time delay at the Substation RTU end when it is communicating with the 400 kV Transformer II IED. The average time delay at the Substation RTU end is determined to be 160 µs. This time delay is related to the volume of data received at the RTU end from several devices on the network.

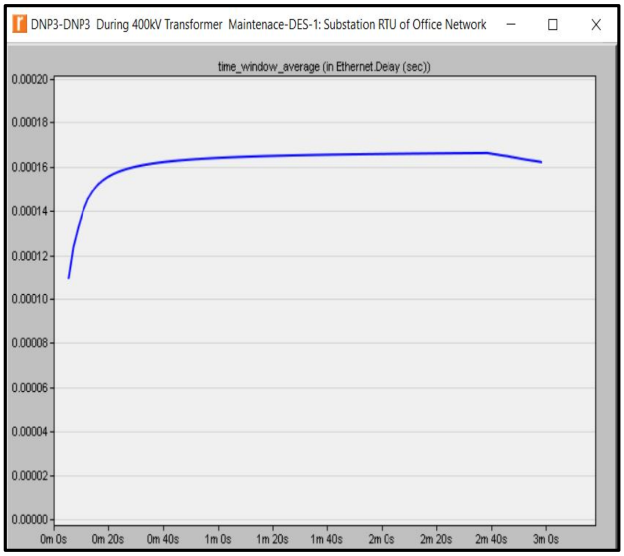


Fig. 7. Time delay at the Substation RTU end.

When the 400kV Transformer II IED is communicating with the Substation RTU, the time delay at the 400 kV Transformer II IED end due to the traffic of data at the transformer end is 17 µs. This can be seen on the graph in Fig.8 below. The time delay at the transformer end is related to the volume of traffic at this end.

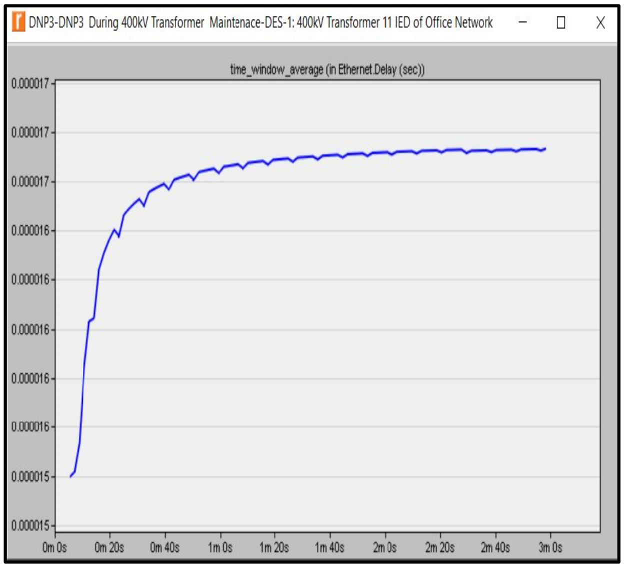


Fig. 8. Time delay at Transformer II IED end.

The received (Rx) throughput at the Substation RTU end can be seen in Fig.9. The received (Rx) throughput at the RTU end shows a steady increase with a sharp increment at a time of two minutes and forty seconds. The sharp increment occurs due to the many alarm messages coming from the transformer to the RTU during the maintenance operation. The sent (Tx) throughput at the 400 kV Transformer II IED end can be seen in Fig.10. Again, for the sent (Tx) traffic from the 400 kV Transformer II IED end there is a steady increase in traffic with a sharp increment occurring at two minutes and forty seconds. The received (Rx) traffic is almost a mirror image of the sent (Tx) traffic because the 400 kV Transformer II IED sends many alarm messages to the Substation RTU. The alarm messages account for the sharp increase in traffic. Since the received (Rx) traffic is almost a mirror image of the sent (Tx) traffic on this channel this validates the model. The throughput is consistent without dropped packets this proves the model is working. The data throughput rate for the DNP3 protocol from Fig.9 and 10 ranges between (20 – 450) kbps. The RTU received (Rx) throughput exceeds the 400 kV Transformer sent (Tx) throughput because the RTU is listening to several devices on the SCN.

For reprint or republication permission, email to IEEE Copyrights Manager at pubs-permissions@ieee.org. All rights reserved. Copyright ©2022 by IEEE.

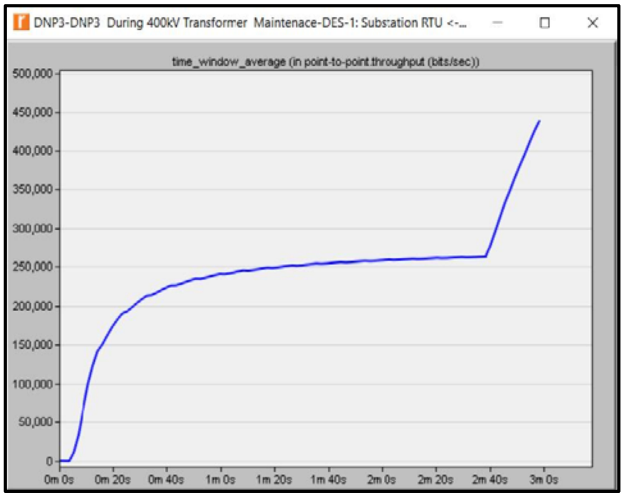


Fig. 9. Received (Rx) Throughput at the Substation RTU end .

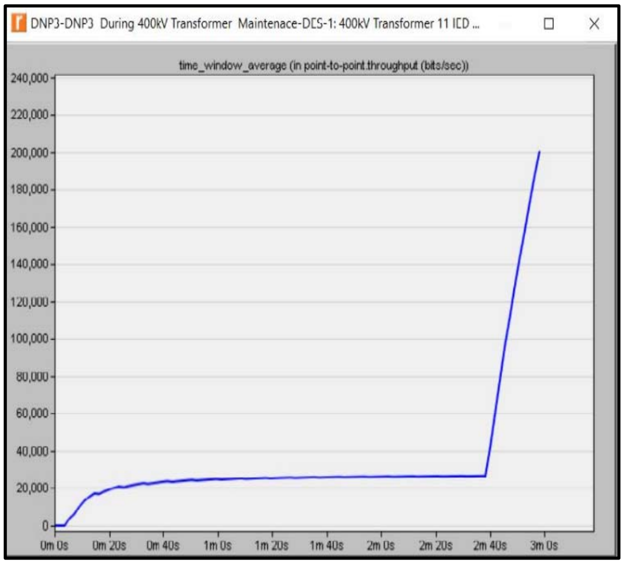


Fig. 10. Sent (Tx) Throughput at the 400kV Transformer II IED end.

Fig.11 shows the received (Rx) throughput at the 400 kV Transformer II IED end and Fig.12 shows the sent (Tx) throughput from the Substation RTU end. The sent (Tx) throughput from the RTU end exceeds the received (Rx) throughput at the 400 kV Transformer II IED end, because the Substation RTU sends traffic to several devices on the SCN. The received (Rx) traffic is a mirror image of the sent (Tx) traffic validating the model. Both the received (Rx) throughput at the Transformer end and the sent (Tx) throughput from the RTU are consistent indicating there are no dropped packets and that the model is working.

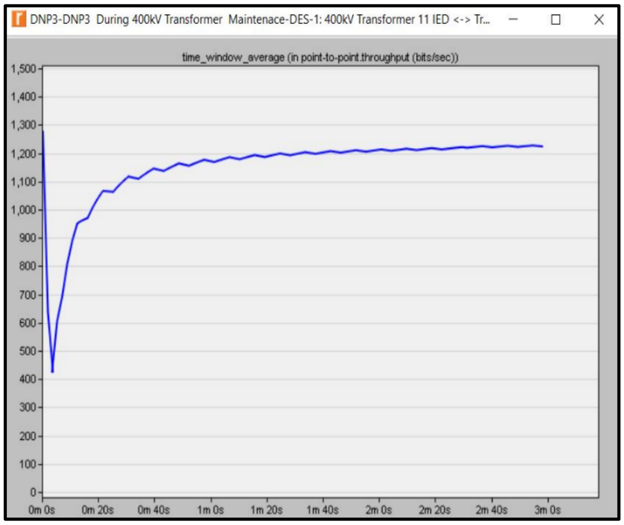


Fig. 11. Received (Rx) Throughput at the Transformer II IED end.

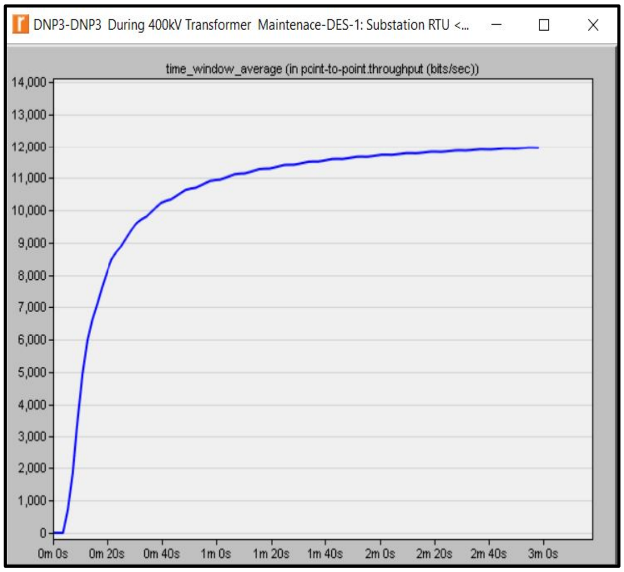


Fig. 12. Sent (Tx) Throughput from the Substation RTU end.

B. Performance of the IEC 61850 Protocol

The IEC 61850 protocol is applied over the network while modelling a scenario in which there is a faulty backbone switch. The performance of the IEC 61850 protocol is then determined and the effect of the faulty backbone switch on the network parameters of time delay and throughput is analyzed. The network time delay for normal operation is depicted by a red line and the network time delay for a faulty backbone switch operation is depicted by a blue line as can be seen in Fig.13 below. Normal operation occurs when two backbone

For reprint or republication permission, email to IEEE Copyrights Manager at pubs-permissions@ieee.org. All rights reserved. Copyright ©2022 by IEEE.

switches are operating at the same time while the faulty backbone switch operation occurs when one of the backbone switches has failed and the network is running on a single backbone switch. The time delay for the network during normal operation for the IEC 61850 protocol is 80 µs and during a faulty backbone switch operation the average time delay is 100 µs as can be seen in Fig.13.

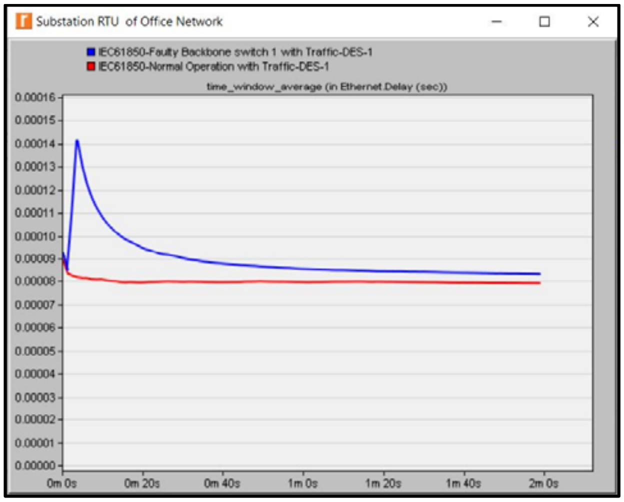


Fig. 13. Ethernet time delay for “Normal Operation” and “Faulty backbone switch” operation .

In this operation the communication is between the IED devices and the Substation RTU but through (via) the backbone switches on the model. Data is sent from all the IED devices to the Substation RTU through (via) the backbone switches on the network. Fig.14 shows the resultant sent throughput during normal operation with two healthy backbone switches and during the faulty backbone operation with one faulty backbone switch. When the network is operating with a faulty backbone switch the throughput is lower than during normal operation with two healthy backbone switches as can be seen in Fig. 14 below.

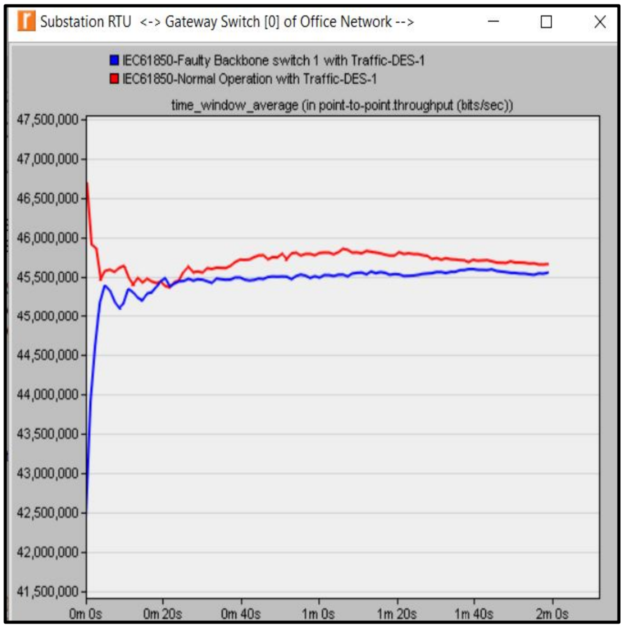


Fig. 14. Sent Throughput from IED’s to Substation RTU via the backbone switch in bps.

The received throughput at the backbone switch from the IED’s during normal operation with two healthy backbone switches and during a faulty backbone switch operation with a failed backbone switch can be seen in Fig.15. The received throughput for normal operation and the received throughput during a faulty backbone switch operation are the same and match each other. The reason for the received throughput for normal operation and faulty operation being the same is because the received throughput in this case is measured at the backbone switch point before failure occurs.

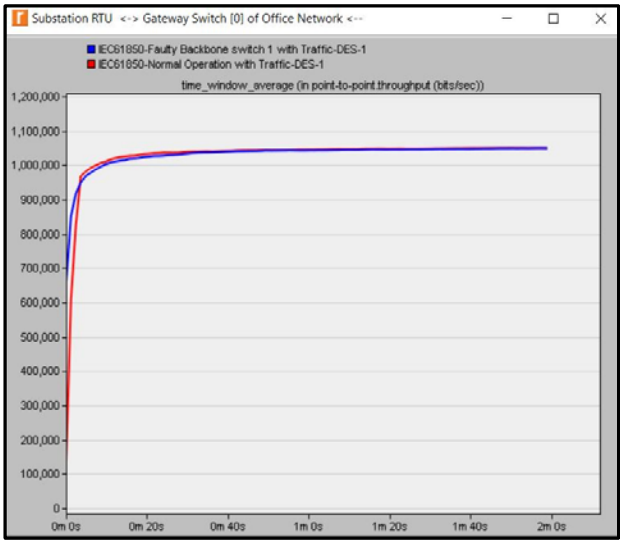


Fig. 15. Received throughput at the backbone switch in bps.

The queuing delay at the transmitting (Tx) end during normal operation and during a faulty backbone switch operation can be seen in Fig.16. The queuing delay during normal operation is 0.7 µs and during a faulty backbone switch operation is

For reprint or republication permission, email to IEEE Copyrights Manager at pubs-permissions@ieee.org. All rights reserved. Copyright ©2022 by IEEE.

1.25 µs for the IEC 61850 protocol. The queuing delay for normal operation is less than when there is a faulty switch.

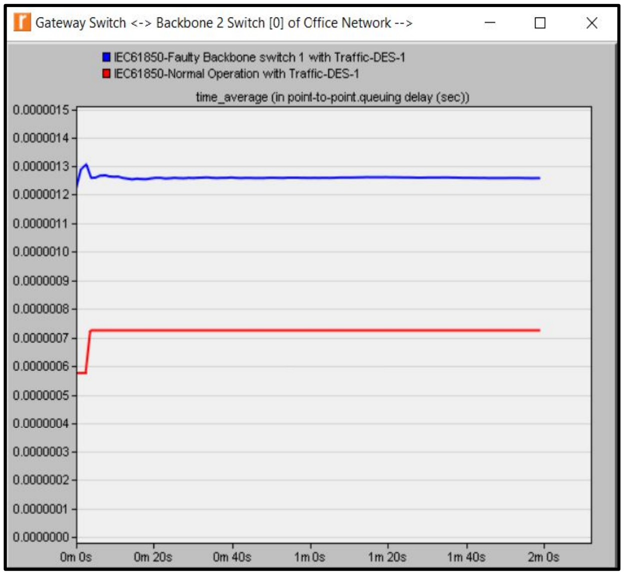


Fig. 16. Queuing delay at the Transmitting (Tx) end.

The queuing delay at the received (Rx) end for normal operation and faulty backbone switch operation can be seen in Fig.17. The delay is 0.59 µs for normal operation and 1.3 µs for a faulty backbone switch operation. Again, the queuing delay for normal operation is less than for a faulty operation at the received (Rx) end.

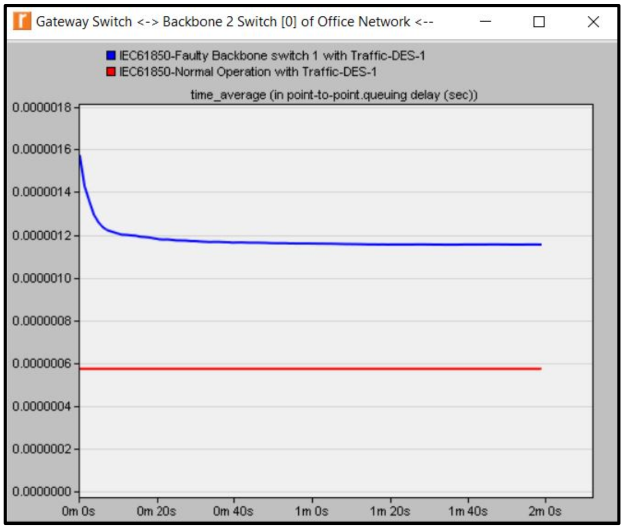


Fig. 17. Queuing delay at the Received (Rx) end.

V. CONCLUSION

The throughput when the DNP3 protocol is applied over the SCN during the maintenance of the 400 kV Transformer IED ranges between (20 – 450) kbps. The time delay when the 400 kV Transformer is communicating with the Substation RTU during maintenance at the RTU end is 160 µs for the DNP3 protocol. The time delay for the IEC 61850 protocol when applied over the network during a normal operation is 80 µs and for a faulty backbone switch scenario the delay is 100 µs in the network. The throughput when the IEC 61850 protocol is applied over the same network is in the range of (1-45) Mbps. In conclusion the IEC 61850 protocol is approximately twice as fast as the DNP3 protocol. The model can be used to show the difference in performance between the DNP3 and IEC 61850 protocol with respect to parameters such as throughput and time delay. Finally, the model can be used to show traffic behavior during operational scenarios such as maintenance and faulty devices in the network.

ACKNOWLEDGMENT

We would like to acknowledge the University of South Africa, the ESKOM South Africa TESP Grant and the University of Johannesburg for the assistance with funding towards the research and the provision of resources to enable the completion of this work.

REFERENCES

[1] L. Cheng, "Study and application of DNP3.0 in SCADA system," Proceedings of the International Conference on Electronic & Mechanical Engineering and Information Technology, Harbin, 2011, pp. 4563-4566, doi: 10.1109/EMEIT.2011.6024045.

[2] A. Ortega, A. A. Shinoda and C. M. Schweitzer, "Performance analysis of smart grid communication protocol DNP3 over TCP/IP in a heterogeneous traffic environment," IEEE Colombian Conference on Communications and Computing (COLCOM), Medellin , Colombia, 2013, pp. 1-6, doi: 10.1109/ColComCon.2013.6564828.

[3] Hao Li, Guangjie Liu, Weiwei Jiang and Yuewei Dai, "Designing snort rules to detect abnormal DNP3 network data," International Conference on Control, Automation and Information Sciences (ICCAIS), Changshu, 2015, pp. 343-348, doi: 10.1109/ICCAIS.2015.7338690.

[4] J. Nivethan and M. Papa, "A Linux-based firewall for the DNP3 protocol," 2016 IEEE Symposium on Technologies for Homeland Security (HST), Waltham, MA, 2016, pp. 1-5, doi: 10.1109/THS.2016.7568963.

[5] M. Cebe and K. Akkaya, "A Bandwidth-Efficient Secure Authentication Module for Smart Grid DNP3 Protocol," 2020 Resilience Week (RWS), Salt Lake City, UT, USA, 2020, pp. 160-166, doi: 10.1109/RWS50334.2020.9241294.

[6] J. A. Crain and S. Bratus, "Bolt-On Security Extensions for Industrial Control System Protocols: A Case Study of DNP3 SAv5," IEEE Security & Privacy, vol. 13, no. 3, pp. 74-79, May-June 2015, doi: 10.1109/MSP.2015.47.

[7] R. Amoah, S. Camtepe and E. Foo, "Securing DNP3 Broadcast Communications in SCADA Systems," IEEE Transactions on Industrial Informatics, vol. 12, no. 4, pp. 1474-1485, Aug. 2016, doi: 10.1109/TII.2016.2587883.

[8] Meiqin Mao, Fengming Mei, Peng Jin and Liuchen Chang, "Application of IEC61850 in energy management system for microgrids," 2014 IEEE 5th International Symposium on Power Electronics for Distributed Generation Systems (PEDG), Galway, 2014, pp. 1-5, doi: 10.1109/PEDG.2014.6878690.

[9] D. A. Poştovei, C. Bulac, I. Triştiu and B. Camachi, "A practical implementation of modern Distributed Control Systems in Electric Power Substations," 12th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Bucharest, Romania, 2020, pp. 1-6, doi: 10.1109/ECAI50035.2020.9223256.

[10] Y. Wang, Y. Tian, L. Yang, L. Liu, G. Yu and Z. Zhu, "IEC 61850 extensions to describe the configuration of feeder automation and metering systems," 2nd International Conference on Power and Renewable Energy (ICPRE), Chengdu, 2017, pp. 1057-1061, doi: 10.1109/ICPRE.2017.8390694.

[11] L. Xiong and K. Zhang, "IEC-61850 based EPON system information mapping scheme for energy internet," IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA), Chengdu, 2018, pp. 295-299, doi: 10.1109/ICCCBDA.2018.8386530.

For reprint or republication permission, email to IEEE Copyrights Manager at pubs-permissions@ieee.org. All rights reserved. Copyright ©2022 by IEEE.

[12] H. Albunashee and R. A. Mc Cann, "DER Coordination Strategy for Volt/VAR Control using IEC61850 GOOSE Protocol," North American Power Symposium (NAPS), Wichita, KS, USA, 2019, pp. 1-5, doi: 10.1109/NAPS46351.2019.9000302.

[13] Y. Ren et al., "Testing system for substation automation system based on IEC61850," International Conference on Advanced Power System Automation and Protection, Beijing, 2011, pp. 2396-2399, doi: 10.1109/APAP.2011.6180829.

[14] Z. Shujian, S. Ming and G. Gaofei, "The research based on IEC 61850 intelligent terminal of substation," IEEE 3rd International Conference on Communication Software and Networks, Xi'an, 2011, pp. 304-307, doi: 10.1109/ICCSN.2011.6014056.

[15] C. Chenfan and S. Xiaozhou, "The New Distributed Busbar Protection IED Based on IEC61850," International Conference on Power System Technology (POWERCON), Guangzhou, 2018, pp. 3076-3079, doi: 10.1109/POWERCON.2018.8602155.

[16] H. Yang, L. Cheng and M. C. Chuah, "Modeling DNP3 traffic characteristics of field devices in SCADA systems of the smart grid," *Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES),* Pittsburgh, PA, 2017, pp. 1-6, doi: 10.1109/MSCPES.2017.8064535.

[17] J. Zhang, X. Ji, J. Li and A. Li, "Design and Implementation of IEC61850 Communication Security Protection Scheme for Smart Substation based on Bilinear Function," *IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC),* Chongqing, China, 2020, pp. 2079-2083, doi: 10.1109/ITNEC48623.2020.9084985.

[18] X. Chen, P. A. Crossley and H. Guo, "Design, construction and validation of a next generation protection and control system based on IEC61850 standards," *12th IET International Conference on Developments in Power System Protection (DPSP 2014)*, Copenhagen, 2014, pp. 1-6, doi: 10.1049/cp.2014.0037.

[19] W. Huang, G. Chen, J. Teng and B. Liu, "Development of an IEC61850-Based DCU for AMI,*" 3rd International Conference on Green Technology and Sustainable Development (GTSD*), Kaohsiung, 2016, pp. 126-131, doi: 10.1109/GTSD.2016.38.

[20] X. Ma, Z. Bo, L. Wang, Q. Wang, L. Chen and F. Wei, "Description of protection intelligent center using IEC61850 defined SCL," *5th International Conference on Electric Utility Deregulation and Restructuring and Power Technologies (DRPT),* Changsha, 2015, pp. 938-942, doi: 10.1109/DRPT.2015.7432362.

[21] Q. Chen, G. Li and X. Tang, "Maintenance technology of substation source end based on IEC61850," *IEEE International Conference on Information Technology,Big Data and Artificial Intelligence (ICIBA*), Chongqing, 2020, pp. 371-375, doi: 10.1109/ICIBA50161.2020.9277025.

[22] A.S. Sethi and V.Y. Hnatyshin, “The Practical OPNET User Guide for Computer Network Simulation”, New York, Taylor and Francis Group, LLC, 2019, pp. 1-528. ISBN 9780367380953.

[23] D. Njova, K. Ogudo and P. Umenne, "Packet Analysis of DNP3 protocol over TCP/IP at an Electrical Substation Grid modelled in OPNET," *IEEE PES/IAS PowerAfrica*, Nairobi, Kenya, 2020, pp. 683-687, https://ieeexplore.ieee.org/document/9219968.

[24] G. Clarke, D. Reynders and E. Wright, “Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems”, IDC Technologies, England, pp.166-168, 2004.

[25] T. Amare, C. M. Adrah and B. E. Helvik, "A Method for Performability Study on Wide Area Communication Architectures for Smart Grid", 7th International Conference on Smart Grid (icSmartGrid), Newcastle, Australia, 2019, pp. 64-73, https://doi.org/10.1109/icSmartGrid48354.2019.8990736

[26] D. Njova, K. Ogudo and P. Umenne, “Analysis of the IEC 61850 protocol when used for communication during maintenance operation in an electrical substation grid” ICONIC '20: Proceedings of the 2nd International Conference on Intelligent and Innovative Computing Applications September 2020 Article No.: 45, Pages 335 -341, ISBN 978-1-4503-7558-0, https://doi.org/10.1145/3415088.3415133

[27] T. S. Ustun, M. A. Aftab, I. Ali and S. M. S. Hussain, "A Novel Scheme for Performance Evaluation of an IEC 61850-Based Active Distribution System Substation", *IEEE Access,* vol. 7, pp. 123893-123902, 2019, https://doi.org/10.1109/ACCESS.2019.2937971

[28] Z. Zhang, X. Huang, B. Keune, Y. Cao and Y. Li, "Modeling and Simulation of Data Flow for VLAN-Based Communication in Substations", *IEEE Systems Journal,* vol. 11, no. 4, pp. 2467-2478, Dec. 2017, https://doi.org/10.1109/JSYST.2015.2428058

For reprint or republication permission, email to IEEE Copyrights Manager at pubs-permissions@ieee.org. All rights reserved. Copyright ©2022 by IEEE.