2025 33rd Southern African Universities Power Engineering Conference (SAUPEC)

A comparison study between Modbus and IEC 61850 MMS Protocols

Rayner Johnson, Senthil Krishnamurthy, Halter Mataifa, and Mohammed Esmail
Center for Substation, Automation and Energy Management Systems
Department of Electrical, Electronic, and Computer Engineering
Cape Peninsula University of Technology
Bellville, Cape Town 7530, South Africa
214240525@mycput.ac.za , krishnamurthys@cput.ac.za, mataifah@cput.ac.za and ebrahimm@cput.ac.za

2025 33rd Southern African Universities Power Engineering Conference (SAUPEC) | 979-8-3315-3516-2/25/$31.00 ©2025 IEEE | DOI: 10.1109/SAUPEC65723.2025.10944359

***Abstract*— The growing adoption of renewable energy primary plants has been seen globally. South Africa has seen a significant development in utility-scale photovoltaic (PV) farms in recent years due to the alleviated regulations stipulated in the latest Electricity Regulation Amendment Act. Connecting the PV plants to the power grid has also undergone a technical evolution by incorporating modern embedded computers known as Intelligent Electronic Devices (IEDs). The International Electrotechnical Committee (IEC) 61850 standard defines a suite of protocols used in modern power systems. This study compares the IEC 61850 Manufacturing Messaging Specification (MMS) with the well-known MODBUS protocol. The comparison is achieved by simulating a solar farm's Power Plant Controller (PPC).**

Keywords—Power Plant Controller, Industrial Protocols, photovoltaic plant

I. Introduction

The power grid consists of three primary components: generating plants, the transmission grid, and the distribution network. Traditionally, power is generated in large quantities and flows from generation through transmission before reaching consumers via distribution. With the increasing adoption of renewable energy (also known as primary plants), power is now commonly injected at various stages of the power grid, leading to distributed energy resources (DERs). In recent years, there has been a significant focus on power quality and the integration of renewable energy technology into power grids [1][2][3]. These renewable plants must contribute to a stable and healthy grid by supporting reactive power, frequency control, and voltage regulation, among other factors. Therefore, local utilities enforce grid code requirements to ensure renewable energy plants can maintain grid stability. For these plants to provide support, they must communicate effectively with the utility, responding promptly to operational commands [4].

A. SCADA Integration for DERs

Supervisory control and data acquisition (commonly referred to as SCADA) define the communication network and control implementation to achieve this interaction of the DERs to the utility. The rise of the Smart Grid enabled the refurbishing of the existing power grid infrastructure with intelligent devices. This proved a costly and efficient way of improving the power grid [1]. The deployment of IEDs enabled critical information for monitoring and control purposes to be the backbone of the power grid. A limitation was identified: each device needed seamless integration with the next. With legacy protocols such as Modbus, this proved to be an extensive task as the mapping of signals was required for each device. Each vendor had their unique method that needed to be implemented for the devices to be compatible. Therefore, the International Electrotechnical Committee published a standard for device interoperability [6]. The IEC 61850 provides the structure for messaging frames that can be applied throughout the electrical grid. The suite of protocols currently listed in IEC 61850 has proven successful in delivering faster and more reliable communication between devices [7]. Now, it is desirable for devices integrating within the power grid to be compatible with the IEC 61850. However, the gap exists in DER technologies that peripherally interact with the grid. In photovoltaic farms, the inverters convert the direct current (DC) power generated from the silicon solar panel and produce alternating current (AC) synchronized with the grid's local parameters. Modbus-compatible communication modules have only met communication requirements for reading and writing commands to the inverters. Currently, no utility-scale inverter manufacturer provides an inverter with IEC 61850 compatibility, despite the proven efficiency of the protocols listed in the IEC 61850 standard and the further development of the IEC 61850-7-420 that specifies the connection of DERs. This study compares Modbus and IEC 61850 MMS protocol in applying a power plant controller (PPC).

B. Research on Protocols

The paper thoroughly researches implementing IEC 61850 protocols in substation automation systems (SAS). These studies have shown that modeling a multi-protocol substation environment highlights the benefits of using the IEC 61850 GOOSE protocol compared to the Modbus RTU implementation. These benefits included time-synchronization, less physical layer cables, and interoperability [8]. However, there is little to no research on investigating the implementation of the IEC 61850 MMS protocol to replace Modbus for inverter communication. The IEC 61850 MMS protocol is typically used in bay-level communication in SAS environments. There is adequate research available on the mapping of Modbus to IEC 61850 MMS for SAS [9]. The IEC 61850 standard released an extension, IEC 61850-7-420, that deals explicitly with integrating distributed energy resources (DERs). This is the initial phase for allowing the expansion of the IEC 61850 standard to be implemented to the renewable energy

979-8-3315-3516-2/25/$31.00 ©2025 IEEE

Authorized licensed use limited to: Cape Peninsula University of Technology. Downloaded on November 20,2026 at 09:56:19 UTC from IEEE Xplore. Restrictions apply.

resources connected to the substations. It is noted that all inverter manufacturers to date only produce communication modules compatible with proprietary Modbus protocols.

This study incorporates a hardware-in-the-loop configuration where an SEL 3555 RTAC has been configured as the PPC and interacts with a simulation of PV inverters connecting to the grid. The simulation is compiled and processed using Real-Time Digital Simulator (RTDS) Nova Core. The functionality allows the SEL RTAC to communicate with the simulation running on the RTDS, and by capturing these packets, it is possible to create an analysis between Modbus and IEC 61850 protocol.

The structure of the paper includes a brief background of the protocols and how their message structure is composed. A description of PPC and their position in the grid-connected PV farms. These are both covered in section 2: Grid Connected PV Plants. Section 3: Lab Scale Implementation discusses the configuration of the simulation and the SEL RTAC to achieve a test bed used to extract data. The data captured is analyzed in section 4, and the comparison study of the two protocols is conducted in section 5. Finally, section 6 provides the conclusion highlighting the advantages and disadvantages of each protocol

II. Grid Connected PV Plants

A. Power Plant Controller (PPC)

In utility-scale PV farms, communication between the facility's devices and the grid is configured to the PPC. The PPC provides set points to the inverters, instructing them on how to operate. For instance, if the grid provides the command for the PV farm to provide more reactive power, the PPC relays this command to the inverters. The inverters must respond by adjusting their output to match the desired setpoint received from the grid. Grid code compliance standards outline the response time and accuracy required for the setpoint to be issued and the output to be achieved. Inverter manufacturers such as Sungrow, Huawei, and Canadian Solar only provide Modbus-compatible communication modules to interact with the inverter controllers—the following sub-section details how data is presented and transmitted using Modbus.

B. Modbus Protocol

Modbus protocol is an application layer-based protocol [10]. It is implemented using the Client-Server or Master-Slave approach. Modbus TCP/IP (transmission control protocol and internet protocol) is implemented over ethernet networks and would be used to communicate with the PPC in the case of utility solar farms. The encapsulation of a Modbus packet using TCP/IP can be seen in Figure 1. It is noted that the required bytes for the TCP/IP encapsulation are summarized by calculating the bytes used in the additional frames (total of 8 bytes) concerning the extract shown below in Figure 1.

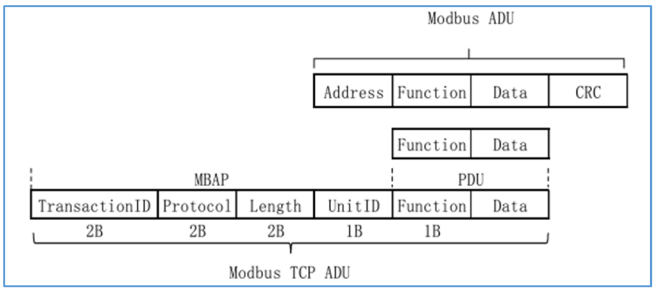

Figure 1: Modbus RTU and TCP/IP Frame [5]

Memory registers configure, control, and monitor devices in Modbus. Each vendor will have a specific register map that details the list of signals for that device. The database for Modbus is divided into four data types: Discrete Inputs, Coils, Input Registers, and Holding Registers. The Modbus Protocol Data Unit will contain a function code corresponding to the register. The order of registers and their assigned function codes may vary depending on the manufacturer. However, the most common structure of function code is to register below in Table 1 [5]. It is essential to understand these registers and their associated data type when capturing Modbus data. An example of a Modbus signal would be the position of a breaker; it could be listed under Function Code 1xx and mapped to register 10001. The data type associated with this register is a coil/Boolean. Therefore, it is essential to understand what a bit value of 0 or 1 represents in this register. Table 1 below lists the four common Modbus registers with function codes and data types.

TABLE I. Modbus Register

Function Code	Modbus Register	
	Description	***Data Type***
0xx	Read/Write Discrete Outputs Coils	Boolean
1xx	Read Discrete Inputs	Boolean
3xx	Read Input Registers	Integer/ Unassigned Integer
4xx	Read/Write Holding Registers	Integer/ Unassigned Integer

C. IEC 61850 MMS Protocol

The IEC 61850 standard defines an abstract service for communication, and part 8.1 describes the ‘mapping’ to Manufacturing Message Specification (MMS) [11]. In contrast to Modbus, the IEC 61850 creates common data classes and logical nodes for operations[12][13]. The standard also incorporates an XML-based Substation Configuration Language(SCL) that facilitates the ease of implementation. This SCL and file format established by the IEC 61850 standard creates an efficient method of storing data versus legacy protocols. The IEC 61850 defines more than just how bytes are transmitted; it also standardizes how the data should be arranged [12]. A physical device is composed of Logical Nodes (LN). Each LN is made up of several Data Objects (DO). Concerning the extract from IEC 61850-7-4, Table 2 below displays the XCBR Logical Node that defines the circuit breaker. The IEC 61850 standard adopted the MMS protocol from a previously defined industrial communication standard ISO 9506 [13] and [15].

Authorized licensed use limited to: Cape Peninsula University of Technology. Downloaded on November 20,2026 at 09:56:19 UTC from IEEE Xplore. Restrictions apply.

TABLE 2: XCBR LOGICAL NODE [12]

XCBR class				
Data Name	Common Data Class	Explanation	T	M/O/C
LNName		The name shall be composed of the class name, the LN-Prefix and LN-Instance-ID according to IEC 61850-7-2 clause 19		
Data				
LocKey	SPS	Local operation (local means without substation automation communication, hardwired direct control)		M
RemCtlBlk	SPC	Remote Control Blocked		O
Loc	SPS	Local Control Behavior		M
EEHealth	INS	External equipment health		O
EEName	DPL	External equipment name plate		O
OpCnt	INS	Operation counter		M
Controls				
Pos	DPC	Switch position		M
BlkOpn	SPC	Block opening		M
BlkCls	SPC	Block closing		M
ChaMotEna	SPC	Charger motor enabled		O
Metered Values				
SumSwARs	BCR	Sum of Switched Amperes, resetable		O
Status Information				
CBOpCap	INS	Circuit breaker operating capability		O
POWCap	INS	Point On Wave switching capability		O
MaxOpCap	INS	Circuit breaker operating capability when fully charged		O

Concerning Table 2, the DO of the XCBR LN can be noted with their Common Data Class (CDC). Taking the 'Loc' DO from the table, we see it is assigned to a CDC of SPS. SPS stands for single-point status and refers to controlling a single bit. This is similar to the Modbus registers with Boolean data type, as expressed previously. However, it must be noted that the range in CDC in IEC 61850 versus the range of data types defined for a typical Modbus configuration.

Diving one step deeper into understanding the IEC 61850 XCBR LN, an extract of DO 'Loc' can further be expanded to display the Data Attributes associated with this DO. The CDC of an SPS is further defined by the IEC 61850-7-3 [14]. In particular interest are the additional DAs defined as quality and time, represented by 'q' or 't' in Table 3 below. These Das are interesting because they provide further information regarding the "Loc" DO. The quality attribute signifies that data transferring is 'live' and healthy. If data associated with the DO is unavailable, the quality attribute will reflect 'false.' The time attribute signifies the time related to that event. This is often paired with a simple network time protocol (SNTP) using a GPS clock for accurate readings. Understanding the exact time of events can be very useful in diagnostics as it clearly states a sequence of events.

TABLE 3: SPS Common Data Class [14]

SPS class					
Attribute Name	Attribute Type	FC	TrgOp	Value/Value Range	M/O/C
DataName	Inherited from Data Class (see IEC 61850-7-2)				
DataAttribute					
status					
stVal	BOOLEAN	ST	dchg	TRUE | FALSE	M
q	Quality	ST	qchg		M
t	TimeStamp	ST			M
substitution					
subEna	BOOLEAN	SV			PICS_SUBST
subVal	BOOLEAN	SV		TRUE | FALSE	PICS_SUBST
subQ	Quality	SV			PICS_SUBST
subID	VISIBLE STRING64	SV			PICS_SUBST
configuration, description and extension					
d	VISIBLE STRING255	DC		Text	O
dU	UNICODE STRING255	DC			O
cdcNs	VISIBLE STRING255	EX			AC_DLNDA_M
cdcName	VISIBLE STRING255	EX			AC_DLNDA_M
dataNs	VISIBLE STRING255	EX			AC_DLN_M
Services					
As defined in Table 13					

III. Lab Scale Implementation

To compare the two protocols, a single simulation needs to be modified to have one simulation running using Modbus and the second simulation using MMS. Capturing the packets transmitted and received between the devices can be analysed using Wireshark. The Real-Time Digital Simulator (RTDS) Nova Core was selected to run the simulations as it can execute hardware-in-the-loop testing. Thus, an external IED can communicate with the simulation in real-time. The base example used for this simulation involves a complex configuration between two solar systems connected to the grid via a transformer. Concerning Figure 2 below, the configuration of the solar systems is summarised in the respective green boxes labelled "PV System 1" and "PV System 2". This example case was compiled by the RTDS team and utilized a Modbus GTNETx2 configuration for communicating with an SEL 3555 RTAC acting as the PPC. Therefore, modifying this base example by adjusting the GTNETx2 configuration to use the IEC 61850 GSE-7 MMS configuration is possible.

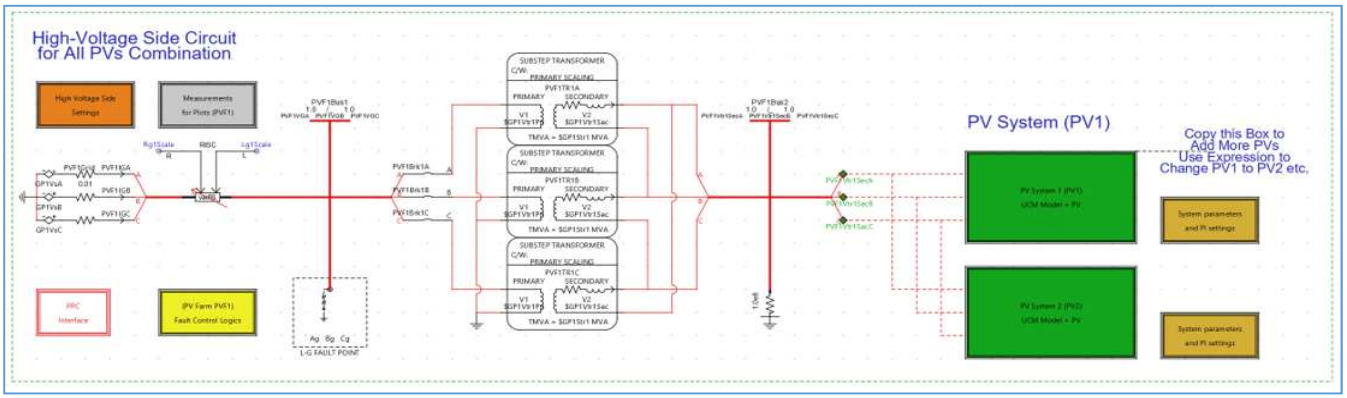

Figure 2: PV System Simulation Draft

Configuring the GTNETx2 GSE-7 communication module is required using the RTDS IED Configuration Tool (ICT) software. Developing the IED file involves selecting LN and using the data binding tab to assign the signals to and from the simulation. Within the ICT software, data sets are also created to monitor the status of the circuit breakers in simulation. This IED file is exported as a Configured IED Description file (CID). Using the CID file exported from the RTDS ICT software and importing it into the SEL AcSELerator Architect software to build a project that will house both the SEL RTAC and the GTNETx2 IED configuration. This project is then saved and loaded into the AcSELerator RTAC software to be compiled by the SEL 3555 RTAC.

Interfacing with the simulation can be done via the buttons defined in the Runtime. Visual displays of the position of

Authorized licensed use limited to: Cape Peninsula University of Technology. Downloaded on November 20,2026 at 09:56:19 UTC from IEEE Xplore. Restrictions apply.

circuit breakers are also displayed in the Runtime panel, as well as charts displaying numerical values relating to the behaviour of the solar farms. Therefore, it is possible to compare the data captured via the SEL RTAC comms monitoring function and validate it via the data displayed in the Runtime window. The SEL RTAC also displays tags, and once a project is 'live,' it is possible to monitor these tags within the SEL RTAC software. It is essential to validate the data across multiple platforms to ensure consistency.

The testing purpose of this simulation is to evaluate the effectiveness of each protocol in the application of PPC monitoring the output of solar farms connected to the grid. This is achieved by running each simulation and capturing the ethernet packets between the SEL 355 RTAC and the Nova Core GTNETx2 communication module. Wireshark software is then used to analyze network protocol. In using Wireshark to investigate the network traffic, it is essential to establish the IP addresses assigned to each device. The IP addresses are listed as follows:

SEL 3555 RTAC - 192.168.1.170

Operator PC - 192.168.1.199

RTDS GTNETx2 - 192.168.1.206

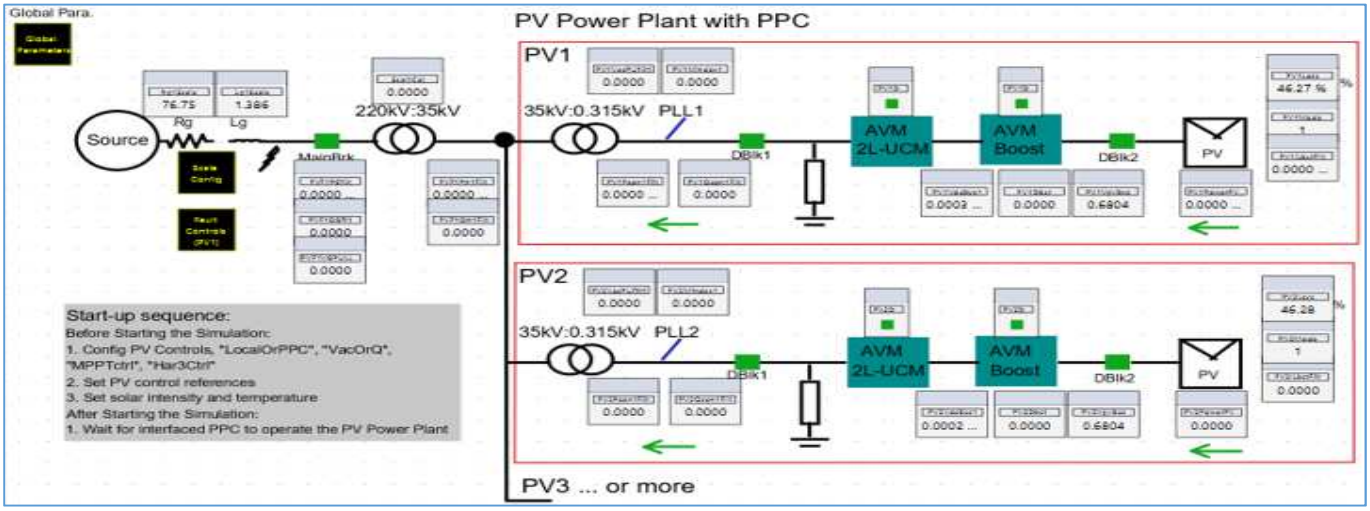

Figure 3: PV System Simulation Monitoring

IV. Simulation Results

Simulating while changing breaker positions and capturing packets results in exchanging packets between the RTDS simulation and the SEL RTAC, which contain data relevant to the breaker statuses.

A. Modbus Data

Understanding the data types associated with the registers assigned to the signal names will provide a base for interpreting the state of breakers. The data is validated by cross-checking the data from the RTDS runtime panel to the SEL RTAC tags, and the packet analysis is done on Wireshark. The main breaker is closed to monitor the state of breakers, and the PV1DBlk1, PV1DBlk2, PV2DBlk1, and PV2DBlk2 are left open. This is confirmed that in RSCAD FX, only the main breaker is closed, and the state of the tag is RTAC, which reads 'TRUE.' The packet captured in Wireshark can be analyzed below. The query comes from source IP address 192.168.1.170 (SEL 3555 RTAC) to Read Coils. The response o the query comes from IP Address 192.168.1.206 (GTNETx2 card of the RTDS Nova Core). Looking at the response, we can expand the Modbus data and see the four-bit values it has stored, each with a bit value of '0' except for bit 1, which has a bit value of '1'. Bit 1 is mapped to the primary breaker coil in the GTNETx2 Modbus configuration. A block diagram displaying the equipment connection is detailed in Figure 4 below, which is taken from the RTDS manual for the Modbus GTNETx2.

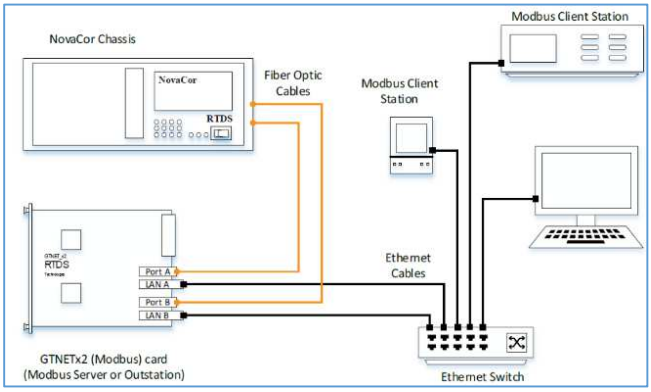

Figure 4: Modbus HIL Lab Scale Implementation

Time can also be recorded to determine the communication speed from the request query. It can be noted that looking at the query request from line 304, the time lapsed was recorded as 3.760800 seconds. The response transaction listed in line 308 was recorded at 3.761282 seconds. Therefore, the delta from the query to the response is 0.000482 seconds. These responses are recorded using the 'comms capture' function in the SEL RTAC software. A snippet of these packet capture is displayed below in Figure 5

Authorized licensed use limited to: Cape Peninsula University of Technology. Downloaded on November 20,2026 at 09:56:19 UTC from IEEE Xplore. Restrictions apply.

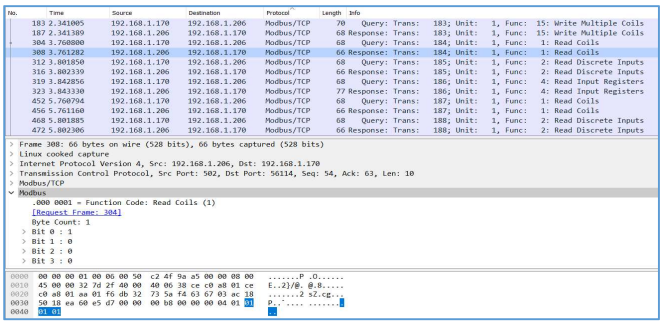

Figure 5: Wireshark Capture Analysis for Modbus Packets

B. MMS Data

The exercise is then repeated using the MMS configuration of the GTNETx2 card and SEL 3555 RTAC. Firstly, it is essential to understand that data sets are created. The data sets are used to group logical nodes related to a specific area of focus, such as breaker status. The MMS protocol creates a poll or report based on the datasets. When a data bit changes value, it can be triggered to send a report. Multiple third-party software programs can be used to confirm the communication and status of each data attribute. In this experiment, IED Explorer was used to poll the state of the GTNETx2 IED. This is then confirmed with both the SEL RTAC and the RTDS MMS Voyager. In SEL RTAC, the 'validity' data attribute goes from 'invalid' to 'valid' once successful communication is achieved. A packet can be intercepted and analysed in Wireshark for a further breakdown. In the below packet analysis, the source is IP address 192.168.1.206 (RTDS GTNETx2) and confirms a request to read from 192.168.1.170 (SEL RTAC). The device is stated as IED1NewDevice, the name of the IED provided for the GTNETx2 communication from the ICT software. The dataset that the request to read is stated as the "BreakerSt," which was defined to provide a list of data attributes regarding the breaker status positions. There are five results, and each reading provides a successful communication. The modifications available for MMS Lab Scale Implementation are taken from the RTDS manual and presented below in Figure 6. It is noted that the lab scale implementation uses a GPS satellite clock for time synchronisation.

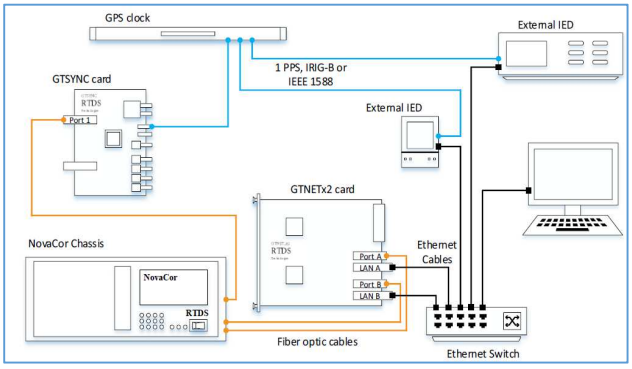

Figure 6: IEC 61850 MMS HIL Lab Scale Implementation

The time can also be recorded to determine the communication speed from the request query. It can be noted that, in Figure 7, Wireshar query request from line 3254, the time lapsed was recorded as 34.011657 seconds. The response transaction listed in line 3258 was recorded at 34.012177 seconds. Therefore, the data from the query to the response is 0.0005 seconds

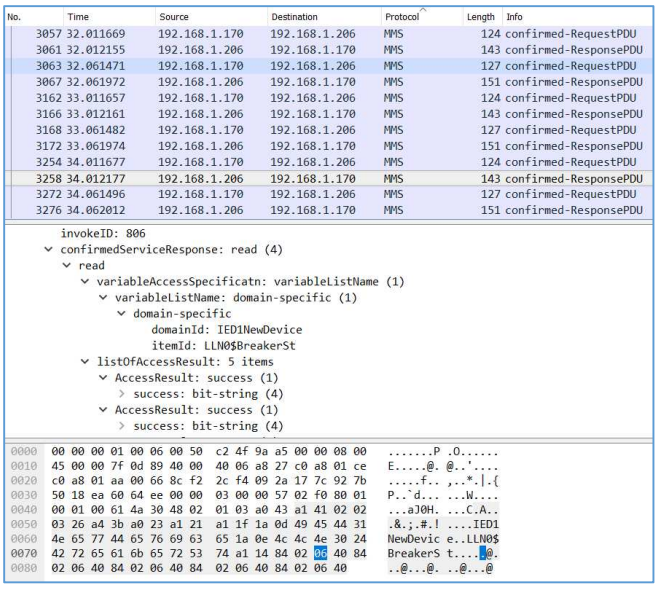

Figure 7: Wireshark Capture Packet Analysis for MMS

V. INDUSTRIAL PROTOCOL SIMULATION RESULTS COMPARISON

The comparison of the two protocols can be analyzed by looking at their capabilities, restrictions, implementation, and longevity in the future. While both protocols can achieve the same outcome, they differ in the message structure and data available. Modbus provides an exceptionally lightweight protocol that can be seen as an advantage as it will require less bandwidth in the communication network. However, Modbus lacks a few critical data points achieved in the IEC 61850 MMS protocol [16]. Firstly, MMS uses a quality data attribute that indicates successful communication between the two devices. Secondly, MMS incorporates a timestamp linked to an event that can be used for diagnostic purposes. Not only does MMS contain additional data that Modbus does not provide, but the IEC 61850 [17] has also created a comprehensive platform for interoperability. Not only can devices from different vendors communicate efficiently, but it has also established a file-sharing structure that can be compatible with any device.

Furthermore, unlike Modbus, the IEC 61850 MMS protocol can create reports triggered upon an event and provide real-time data, which works off a poll rate. Comparing the two protocols, developing and implementing the IEC 61850 protocols have gained popularity within the SAS; however, the adoption of distributed renewable energy resources has been slower.

Interestingly, the query response times from the Modbus and MMS were very similar, with a difference of only 18µs. Further research could be conducted to determine the applicability of the IEC 61850 Generic Object-Oriented Substation Event (GOOSE) protocol, as its quick responsiveness has proven successful in protection environments.

VI. CONCLUSION

The IEC 61850 MMS protocol provides quality data attributes, time-stamped, and real-time data exchange functionality. However, although Modbus is a lighter data-intensive protocol, it lacks the functionality that can be

Authorized licensed use limited to: Cape Peninsula University of Technology. Downloaded on November 20,2026 at 09:56:19 UTC from IEEE Xplore. Restrictions apply.

achieved by adopting the IEC 61850 MMS. However, to this day, no inverter manufacturer has provided an inverter used in utility-scale PV farms that is IEC 61850 compatible. This could be due to the familiarity with using Modbus in a tried and tested solution, and moving away from this could cause undesirable problems. However, the IEC 61850 standard provides an excellent option for communication in renewable energy and will likely become more prevalent soon.

Communication in the energy sector has received significant attention, and this paper creates a real-time simulation that interacts with a PPC. Further development of this simulation could evaluate the effectiveness of IEC 61850 protocols for applying the PPC. If the research continues to promote the advantages of implementing the IEC 61850 protocols, equipment manufacturers will be encouraged to develop compatible inverters.

ACKNOWLEDGEMENT

The authors acknowledge Cape Peninsula University of Technology for offering the facilities to conduct this research at the Center for Substation, Automation, and Energy Management Systems and the Center for Intelligence Systems and Emerging Technologies (CISET). This research was partly funded by the NRF Thuthuka Grant, Number 138177, Eskom Tertiary Education Support Programme (TESP) funding.

REFERENCES

[1] Kumar, Amit & Kumar, Pradeep. (2021). “Power Quality Improvement for Grid-connected PV System Based on Distribution Static Compensator with Fuzzy Logic Controller and UVT/ADALINE-based Least Mean Square Controller.” Journal of Modern Power Systems and Clean Energy. 9. 1289-1299. 10.35833/MPCE.2021.00028

[2] Yang, Can & Pan, Yun & Zhao, Xun & Xu, Qing. (2024). “Research on Power Quality Analysis System Based on IEC 61850”. 2024 IEEE 7th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), pp. 1207-1210. 10.1109/IAEAC59436.2024.10503664.

[3] Kumar, S.; Abu-Siada, A.; Das, N.; Islam, S. Review of the Legacy and Future of IEC 61850 Protocols Encompassing Substation Automation System. Electronics 2023, 12, 3345. https://doi.org/10.3390/electronics12153345

[4] M. Ourahou, W. Ayrir, B. EL Hassouni, A. Haddi, (2020). Review on smart grid control and reliability in presence of renewable energies: Challenges and prospects, Mathematics and Computers in Simulation, Volume 167, Pages 19-31,ISSN 0378

[5] Xuan, Luo & Yongzhong, Li. (2019). Research and Implementation of Modbus TCP Security Enhancement Protocol. Journal of Physics: Conference Series. 1213. 052058. 10.1088/1742-6596/1213/5/052058.

[6] Jácome-Barrionuevo, M. Quizhpi-Cuesta and F. Quizhpi-Palomeque, "Implementation of SCADA for IEC 61850 communication in the IEEE 14-Bus System," 2024 6th Global Power, Energy and Communication Conference (GPECOM), Budapest, Hungary, 2024, pp. 577-583

[7] Kumar, Amit & Kumar, Pradeep. (2021). “Power Quality Improvement for Grid-connected PV System Based on Distribution Static Compensator with Fuzzy Logic Controller and UVT/ADALINE-based Least Mean Square Controller”. Journal of Modern Power Systems and Clean Energy. 9. 1289-1299. 10.35833/MPCE.2021.00028

[8] N. Barry. (2018).Consideration of the IEC 61850 Protocol and Implications for Substation Engineering. University of Kwazulu-Natal, hdl.handle.net/10413/16183

[9] Wang, D. & Yan, C. & Bi, J. & Yuan, S.. (2012). An approach to mapping between Modbus and IEC 61850 for condition monitoring communication gateway in substations. 36. 78-84. 10.3969/j.issn.1000-1026.2012.19.014.

[10] S. Sharma, V. Kumar, P. Sharma, S. Gupta and A. Shukla, "SCADA Communication Protocols: Modbus & IEC 60870 – 5," 2022 1st International Conference on Sustainable Technology for Power and Energy Systems (STPES), SRINAGAR, India, 2022, pp. 1-6

[11] Jae-Duck Lee, Seong-Joon Lee, Jeong-Hyo Bae and Dae-Yun Kwon, "The PMU interface using IEC 61850," 2013 International Conference on ICT Convergence (ICTC), Jeju, 2013, pp. 1125-1128

[12] Poushideh, M. & Haddadnia, Javad. (2012). A Proposed Method for Increase Security in SCADA Systems. International Journal of Computer and Electrical Engineering. 912-915. 10.7763/IJCEE.2012.V4.634.

[13] Adamiak, Mark & Baigent, D. & Mackiewicz, R. (2009). IEC 61850 communication networks and systems in substations: An overview for users. The Protection & Control Journal. 61-68.

[14] Schwarz, Karlheinz. (2014). The Standard Message Specification for Industrial Automation Systems ISO 9506 (MMS). Industrial Communication Technology Handbook, Second Edition. 10.1201/b17365-29.

[15] IEC, “IEC 61850: Communication networks and systems in substations, Part 7-4 ‘Power systems management and associated information exchange’, Eidtion 2.0,” 2007

[16] C. Ruland, N. Kang and J. Sassmannshausen, "Rejuvenation of the IEC 61850 protocol stack for MMS," 2016 IEEE International Conference on Smart Grid Communications (SmartGridComm), Sydney, NSW, Australia, 2016, pp. 625-630

[17] IEC, “IEC 61850: Communication networks and systems in substations, Part 7-3 ‘Common data classes,’ Eidtion 1.0,” 2005

BIOGRAPHY

Mr Rayner Johnson completed B.Tech in Mechatronics Engineering from Cape Peninsula University of Technology (CPUT), Cape Town, South Africa in 2018. He recently completed his MENG in the Smart Grid division of the Department of Electrical, Electronics, and Computer Engineering (DEECE) at Cape Peninsula University of Technology (CPUT), Cape Town, South Africa, in 2024. Rayner Johnson has worked as a supervisory control and data acquisition (SCADA) engineer at a South African Independent Power Producer, SOLA Group, designing and commissioning utility-scale photovoltaic systems since 2021.

Prof. Senthil Krishnamurthy completed MENG in Power Systems Suma Cum-laude and a Doctorate in Electrical Engineering. He is an Associate Professor of Power systems in the Department of Electrical, Electronics, and Computer Engineering (DEECE) at Cape Peninsula University of Technology. He is the Centre Head for Intelligent Systems and Emerging Technologies (CISET) & Deputy Head for the Center for Substation, Automation and Energy Management Systems (CSAEMS). Prof Krishnamurthy is a registered Professional Engineer with ECSA, a Senior Member of SAIEE, and a Member of IEEE. He is an NRF-rated researcher (C2). His research interests include Power Systems, AI-based Optimization Methods, Protective Relaying Systems, Substation Automation, Renewable Energy, Energy Management Systems, Smart Grids, and Parallel Computing.

Dr. H. Mataifa received B.Tech, M. Tech, and Doctorate of Engineering degrees in electrical engineering from Cape Peninsula University of Technology (CPUT), Cape Town, South Africa, in 2011, 2016, and 2023, respectively, and holds a BSc. I obtained a degree in applied mathematics and computer science from the University of South Africa (UNISA) in 2020. He is a senior lecturer at the Research Centre for Intelligent Systems and Emerging Technologies (CSIET), CPUT. His research interests encompass the optimization of power system operation and the efficient grid integration of distributed energy resource technologies.

Dr. Mohammed Esmail received a B.Sc. degree (Hons.) in electronics engineering technology from the University of Gezira (UoG), Wad Madani, Sudan, in 2001, the M.Sc. degree in biomedical engineering from the University of Cape Town (UCT), Cape Town, South Africa, in 2013, and the Ph.D. degree in electrical engineering from the Cape Peninsula University of Technology (CPUT), in December 2023., From 2017 to 2021, he was a part-time lecturer and Focus area Leader at the Centre for Intelligent Systems and Emerging Technologies (CISET), CPUT. His research interests include intelligent grid optimization and control, integrated distributed energy resource technologies, conventional interconnected power systems, dynamical modeling of complex interconnected power systems, and point-to-point positioning applications.

Authorized licensed use limited to: Cape Peninsula University of Technology. Downloaded on November 20,2026 at 09:56:19 UTC from IEEE Xplore. Restrictions apply.