5G Communication Infrastructure for Smart Grids: A Protection Use Case

Author(s): Saleh, Talal; Välisuo, Petri; Kauhaniemi, Kimmo; Elmusrati, Mohammed

Title: 5G Communication Infrastructure for Smart Grids: A Protection Use Case

Year: 2023

Version: Accepted Manuscript

Please cite the original version:

Saleh, T., Välisuo, P., Kauhaniemi, K. & Elmusrati, M. (2023). 5G Communication Infrastructure for Smart Grids: A Protection Use Case. In *2023 IEEE PES Innovative Smart Grid Technologies Europe (ISGT EUROPE)*, 1-5. IEEE. https://doi.org/10.1109/ISGTEUROPE56780.2023.10408607

5G Communication Infrastructure for Smart Grids: A Protection Use Case.

Talal Saleh, Petri Välisuo, Kimmo Kauhaniemi, Mohammed Elmusrati
School of Technology and Innovations
University of Vaasa
Vaasa, Finland
saleh.talal@uwasa.fi

***Abstract*—A smart grid is an advanced electricity network enabled by IoT, ICT, and advanced grid technologies. 5G and beyond networks are expected to serve as the communication infrastructure of smart grids, providing intelligence, virtualization, and connectivity for millions of devices. This paper investigates the potential of 5G communication infrastructure for smart grids, specifically in the protection of smart grids. We evaluate the communication performance of 5G SA and NSA in a protection scenario, where a UE acting as an IED simulates R-GOOSE and R-SV packets and transmits them over the 5G network. We test the 5G network latency, packet loss, and jitter to evaluate its performance. By visualizing and computing the R-GOOSE and R-SV traffic it is observed that the latency of the majority of packets was 12-15 ms in SA and 20-45 ms in NSA.**

***Index Terms*—5G, smart grid, communication infrastructure, R-GOOSE, R- SV**

I. Introduction

Fifth-generation (5G) cellular wireless technology is considered to be an enabler for digitalizing power grids by providing solutions to time-critical low-latency power quality issues and by supporting the concept of the Internet of Things (IoT) and Information and Communication Technology (ICT) in smart grids [1]–[5].

The digitalization of the power system is commonly referred to as the Smart Grid, which facilitates bi-directional power flow and two-way communication between distributed energy resources (DERs), prosumers, and other entities. The literature indicates that with increasing DER integration and bidirectional power flow the traditional protection schemes may not be suitable for future power systems [6]–[10].

To address this, 5G technology, equipped with the possibility of having virtualized functionalities, edge computation, and dedicated sliced networks, can serve as an enabler to advance protection schemes by enabling real-time monitoring, control, and coordination of power system components, thus enhancing the overall resiliency and adaptability of the Smart Grid. The incorporation of 5G technology in the Smart Grid architecture can unlock new possibilities and enhance the effectiveness of the protection schemes, paving the way for a more sustainable and efficient energy future.

Smart grid use cases are mostly related to Ultra Reliable Low Latency Communication (URLLC) and Massive Machine Type Communication (mMTC). In certain power system protection applications, it is required that communication latency should be less than 10 ms [11]. 5G aims to provide low latency of up to 1 ms along with connectivity of 100,000 devices/km2 in a single cell, and reliability of 99.999% which means 5.26 minutes of downtime per year or 25.9 seconds per month [12].

This research paper is divided into four sections. Section II and Section III present background and related research work in the application of 5G in smart grids and grid protection. Section IV explains our laboratory test setup which simulates and transfers (Routable Generic Object Oriented Substation Events) R-GOOSE and (Routable Sampled Values) R-SV packets over a 5G network. In Section V results are analyzed.

II. Background

Communication Infrastructure plays an essential role in monitoring and controlling a smart grid by enabling real-time data flow between the grid management systems and the controlled devices [13]. With the integration of 5G, it might be possible for devices to directly communicate with each other without the need of routing data to a centralized or decentralized management system.

For 5G networks to be integrated with smart grids, it is relevant to discuss the monitoring, control, and communication infrastructure of power systems. Monitoring and control play a critical role in power system protection by providing real-time data on the state of the power system and enabling fast and accurate responses to faults and disturbances.

Monitoring, protection, and control applications of an electrical grid can be categorized into three classes namely Local area, Wide area, and Remote area network [14]. Each class application has varying time constraints and latency requirements. The response time of these different classes ranges from less than 1 ms to more than 1-minute [14].

Local area class focuses on the operation of local applications or localized protection functionalities which senses disturbances and isolate faults at a local level, for example, communication of Intelligent Electronic Devices (IEDs) in a substation. Local area operations are highly time-critical in order of less than 10 ms [14]. In the case of local area applications, the communication is carried out at vertical levels between the process level, bay level, and station level.

In wide-area communication, the IEDs located in remote or far areas coordinate with each other. Wide area class operation is slightly less time critical ranging from 10-1000 ms [14]. For example, in protection application such as (loss-of-main) LOM and Logic selectivity, the IEDs located at remote distances needs to communicate with each other within the time limit of 300 ms and 100 ms respectively [14].

In this paper, our focus is to present a 5G communication infrastructure concept for protection use cases Fig. 1 and test the communication of simulated IEDs over a 5G network. Power system protection is one of the use cases of a smart grid which requires a reliable cost-effective latency-critical communication infrastructure. In this paper, we will evaluate how the latency requirements are met with our 5G test setup.

III. Related Work

Bag *et.al.* in [11] discussed 5G uses cases in power systems related to load compensation, power management, and protection in microgrids. It is essential to mention that time synchronization is needed for some protection cases, such as line-differential protection. Any time desynchronization will result in false tripping.

A software based framework using 5G communication to solve issues related to auto network reconfiguration, network function virtualization (NFV), plug-and-play of devices, and metering infrastructure is presented in [15]. In the proposed framework an energy layer connects to virtualized function layer and application layer through a telecom (5G) layer.

Author in [16] also proposes a novel architecture for virtualizing power systems by moving some control logic to the edge, communicating over a 5G network. The proposed method allows some functions near the field devices and other decision-making functions for protection IEDs to be virtualized by moving them to the edge. The work also compares 5G-based virtualized architecture and Ethernet-based IEC61850 architecture.

A novel, 5G-based architecture with a real-time test setup for sending IEC61850 GOOSE messages over a commercial non-standalone (NSA) 5G network was presented in [17]. The results show that the 5G communication was suitable for the voltage drop in an (Feeder Circuit Breaker) FCB opening scenario but not for the (Transmission System Operator) TSO fault simulation scenario. The authors also proposed to deploy some (Fault Detection Isolation and Recovery) FDIR system functionalities at the edge.

Two wireless power network management strategies were tested for power network control, and monitoring in [13]. The first approach was an LTE communication-based centralized management, and the other was 5G-based distributed network management. The performances were evaluated and compared by simulating a fault management scenario in a co-simulation framework. The result shows that 5G-based distributed network management performs better than LTE-based centralized network management in terms of latency and speed.

Authors in [18] studied 5G performance in distribution grid protection and fault location scenarios. The controlled-hardware-in-loop setup developed by the authors was used to test 5G communication in different scenarios including line differential protection, intertrip protection, and virtualized fault

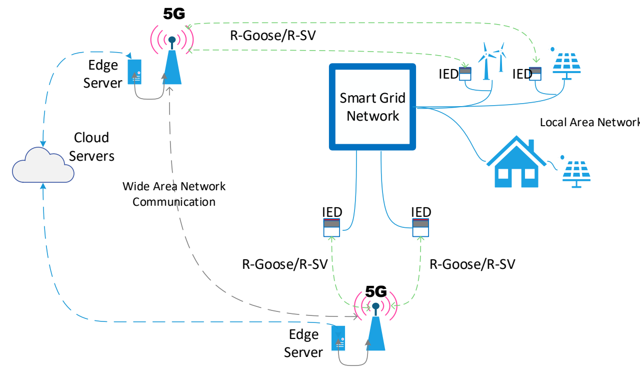

Fig. 1. 5G Communication Infrastructure for Protection Use Case.

passage indicator. They used a 5G commercial NSA network for sending RSV and R-GOOSE messages. According to the test results 5G had better performing throughput and latency as compared to 4G. Similarly, authors in [14] also investigated the performance of IEC61850-90-5 based R-Goose messages over commercial NSA 5G network. Authors performed test and statistical analysis for logic selectivity and LOM protection schemes. By comparing the latency and packet loss of both networks the authors reasoned that the reliability of the current commercial NSA 5G network is lower as compared to the reliability of commercial 4G network. Authors also performed a commercial 5G network test by encrypting R-GOOSE messages and sending over a VPN tunnel to the device which was also time synchronized.

A framework is proposed by [19] in which an AI-native based Radio Access Network (RAN) slicing framework is introduced which will help in integrating IEC61850 services in 5G and beyond network. [20] research work proposes hardware-based network slicing for isolating critical control and monitoring traffic used in smart grid self-healing applications. In the proposed prototype, the authors implemented Field Programmable Gate Array (FPGA) based 5G network and isolated R-GOOSE traffic over a 5G network by multiple network slices. The results of the proposed approach by the authors show a round trip time delay of 10.02 ms from a smart grid control center to the IEDs with a packet loss of 0.3%.

Data transmission over wireless communication could be affected by the size of the packets. Authors in [21] highlighted that packet size according to IEC 61850 may not be optimal for protection communication over a wireless channel. Transmission of smaller packet sizes over wireless communication might result in higher packet losses. To mitigate these packet losses, authors in [21] suggested aggregating multiple data packets horizontally – bundling packets from several merging units under one Ethernet header – or aggregating multiple data packets vertically which means bundling consecutive packets of a single merging unit. The results of the experiment by the authors show that packet aggregation can decrease packet loss in a wireless communication channel.

Previous work mostly focused on utilizing commercial 5G networks or simulated 5G networks. In our work, we have tested a 5G network which can be considered as a private 5G network. With this private 5G network we experimented and analyzed the performance of R-GOOSE and R-SV messages over SA and NSA 5G networks.

IV. R-GOOSE/R-SV Over 5G Test Setup

The 5G network created in the laboratory is based on Amarisoft callbox, a 3GPP release-16 compliant solution. With the callbox, the communication of R-GOOSE and R-SV messages is tested over NSA and SA architecture. NSA architecture tested in the laboratory uses LTE band b40 for control plane signaling and New Radio (NR) band n77 for data plane traffic. The core in the NSA deployment is an Evolved Packet Core (EPC), which means that this architecture does not have 5G core functionalities such as NFV and network slicing.

The 5G SA architecture consists of a gNodeB (gNB), 5G core, and control plane signaling and data traffic over the NR band carrier. In our laboratory, 5G SA services are running over NR band n77 at 3.9 GHz frequency. Table I shows the 5G network configuration in NSA and SA deployment modes.

For the user equipment (UE) to connect to band B40 and band n77, the wireless chipset should support these band connectivity. The wireless module used by the 5G HAT in this test setup is SIMCom's SIM8200EA-M2 module which is built on a Qualcomm Snapdragon X55 platform. This wireless module is 3GPP release-15 compliant and it supports connectivity in n77 and B40 bands [22].

A UE connects over-the-air to the basestation (BS) through a 5G test sim card. The sim card information is configured with the callbox to allow test sim cards to be registered and authenticated with the IMS server. Once the registration process is completed and an IP address is assigned to a UE, data traffic can be sent over a 5G network. A test sim card inserted in a 5G HAT allows the Raspberry PI (RPI) to connect with the laboratory 5G network.

In this experimental setup, communication of two simulated IEDs is tested over-the-air 5G network by sending R-GOOSE and R-SV messages Fig. 2. A 5G HAT connects with RPI through a USB 3.1 connection which allows R-GOOSE/R-SV data traffic to transfer from RPIs to 5G HAT using USB communication protocol. The USB connection between the 5G HAT and RPI is a USB 3.1 Gen 2 which can provide data rates up to 10 Gbps but it can also cause radio frequency interference in the 2.4 GHz and 5GHz frequency band regions [23]. To establish the connection between a 5G HAT and a RPI, the RPI can use NDIS or RNDIS dial-up methods. In our experiment, we used the NDIS dial-up method to connect RPI with the 5G HAT. Fig. 3 shows the protocol stack for sending R-GOOSE and R-SV data traffic in our test setup.

RPIs are configured to act as IEDs which generate, send, and read R-GOOSE/R-SV messages. An open-source application [24] compliant with IEC61850-90-5 standard protocol is used to transmit and receive R-GOOSE and R-SV messages. The application written in C++ uses UDP multicasting to send and receive R-GOOSE and R-SV data traffic. Author in [25] used the same application to evaluate the communication delay of R-GOOSE/R-SV transmitted over Ethernet.

A sender RPI generates R-GOOSE/R-SV UDP packets and sends them to a USB connected 5G HAT which converts the digital signals into radio frequency signals and sends them over the air. On the receiving side, the same process continues in the reverse order. Every second one R-GOOSE and R-SV data packet is generated. The frequency rate of packet generation can be increased by reducing the time between consecutive packets.

Wireless signals are influenced by the channel condition through which they travel. Since the test setup is located in a closed building with dense metallic infrastructure, it might affect the 5G network performance. However, these conditions are not studied in detail in this paper.

TABLE I
Deployment Configurations

Deployments	StandAlone	Non - StandAlone
Bands	n77	40 and n77
Frequencies	3.900 – 3.950 GHz	2.300 – 2.305 GHz, 3.900 – 3.950 GHz
Bandwidth	50 MHz	5 MHz (band 40), 50 MHz (n77)

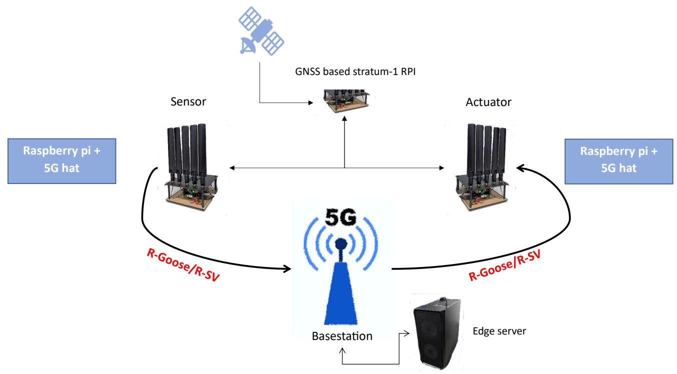

Fig. 2. R-GOOSE and R-SV over 5G Setup.

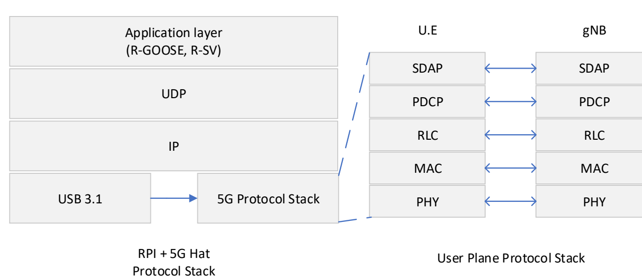

Fig. 3. Test setup data traffic protocol stack.

V. Results and Analysis

The performance of the 5G network established in the laboratory is evaluated by using the iperf3 network performance measurement tool and by measuring the latencies using one-way ping command. Parallel to these testing, the R-GOOSE and R-SV message's latency and packet loss is verified by visualizing the packets captured by Wireshark at the interfaces of sender RPI and receiver RPI.

A. *Network Perfromance Evaluation*

To validate the Quality of Service (QoS) of the 5G network, we compared the network performance of 5G SA and NSA deployments by measuring latency, jitter, and packet loss. Since the R-GOOSE and R-SV protocols are mapped over the IP layer using the UDP protocol, we tested the UDP performance of the 5G network.

In UDP mode, iperf3 sends UDP packets and measures packet loss rate and jitter. We ran the UDP test for two minutes for all deployment types and observed that when the data traffic is normal the packet loss for both deployments is zero. However, if data traffic significantly increases, packet loss also increases which might be due to RPI's inadequate processing capability or 5G network congestion. The results in Table II show that the jitter for SA and NSA was approximately 7-16 ms.

To evaluate the one-way latency in a 5G network, we used the OWAMP protocol, which is an Internet Engineering Task Force (IETF) standard protocol specified in RFC 4656 [26]. We used the one-way ping tool to measure the unidirectional latency between the two UEs.

B. *Captured R-GOOSE and R-SV messages*

The packet capturing process continued for more than 22 hours and every second R-GOOSE and R-SV packets were generated and transferred over the 5G network.

The R-GOOSE and R-SV packet information is extracted with a code written in Python. More than 80,000 R-GOOSE and 80,000 R-SV packets are processed to compute the latency of the data traffic and visualize the results. The latency of the R-GOOSE and R-SV packets is computed by taking the epoch time differences of the captured packets at the sender RPI and the receiver RPI. From the extracted data, the mean, median, mode, and standard deviation of all the latencies are computed. The visualization of the density graph of the extracted data shows that majority of the R-GOOSE and R-SV packets are located in the region of 12 ms to 45 ms (Fig. 4). In the case of NSA deployment, majority of the R-GOOSE and R-SV packets have one-way latency of approximately 30 ms with zero packet loss. On the other hand, in the SA 5G deployment, the majority of R-GOOSE and R-SV packets have a latency of 12-13 ms, shown in Table. III. Packet loss in SA is significantly higher than NSA this might also be because the signal strength in SA was noticed to be weaker than NSA.

The RPIs were initially poorly time synchronized, causing inaccurate latency measurements with even negative latency observations, as shown in Fig. 5. In this case, the receiver RPI sometimes seemed to have an arrival timestamp of milliseconds before the packet was generated and transferred over the 5G network. To solve this issue, we synchronized both RPIs with a time server RPI, developed as a GNSS-based Stratum-1 NTP server, thus leading to microsecond-level synchronization and eliminating negative latency observations.

TABLE II
QoS Performance of 5G Network

Deployment	Iperf3 (packet loss)	Iperf3 (Jitter)	OWAMP (one-way latency)	OWAMP (one-way jitter)
NSA	0.00%	8-9 ms	25-28 ms	10-17 ms
SA	0.55%	7-16 ms	9-13 ms	3-6 ms

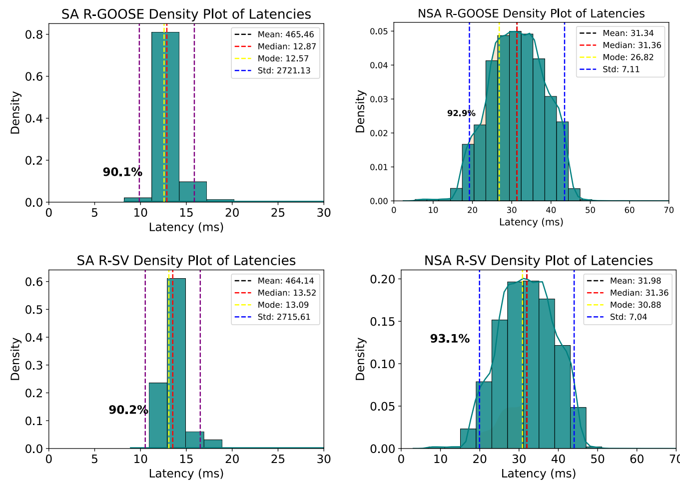

Fig. 4. Packets Density Distribution.

TABLE III
Captured Packet's One-Way Latency and Packet Loss

Test Results		Non-StandAlone	StandAlone
Avg. Latency (ms)	***R-GOOSE***	27	12.5
	R-SV	31	13
Packets Lost	***R-GOOSE***	0	12794
	R-SV	0	12808

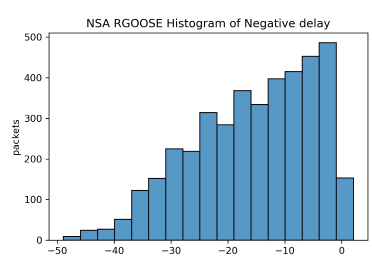

Fig. 5. Negative Latencies

CONCLUSION

In conclusion, this paper evaluated the applicability of private 5G SA and NSA communication networks for protection use cases in smart grids. To determine if the 5G network can meet stringent requirements of protection applications, the performance of the 5G network was evaluated by measuring jitter, latency, and packet loss. In addition, the performance of simulated R-GOOSE and R-SV messages transmitted over a 5G network was visualized by capturing packets and computing packet loss and latencies.

The results show that the 5G communication between simulated IEDs was able to provide low latency communication in the order of 12-40 ms depending upon the 5G deployment type. 5G SA showed a lower latency as compared to 5G NSA but had a higher packet loss. In this experimental setup, the sampling rate of both R-GOOSE and R-SV messages was 1 Hz. In the future, we plan to test the performance of the 5G network for higher sampling rates. Overall, this study demonstrates that the 5G network shows promising performance in the communication of protection applications and it can be considered as an enabler for the digitalization of smart grids.

ACKNOWLEDGMENT

We would like to acknowledge European Regional Development Fund (ERDF) and the Regional Council of Ostrobothnia for financing the 5G Hub Vaasa project. The research was conducted during the project.

REFERENCES

[1] R. K. Beniwal, M. K. Saini, A. Nayyar, B. Qureshi, and A. Aggarwal, "A Critical Analysis of Methodologies for Detection and Classification of Power Quality Events in Smart Grid," *IEEE Access*, vol. 9, pp. 83 507–83 534, 2021, conference Name: IEEE Access.

[2] E. Esenogho, K. Djouani, and A. M. Kurien, "Integrating Artificial Intelligence Internet of Things and 5G for Next-Generation Smartgrid: A Survey of Trends Challenges and Prospect," *IEEE Access*, vol. 10, pp. 4794–4831, 2022, conference Name: IEEE Access.

[3] A. Hassebo, A. A. Mohamed, R. Dorsinville, and M. A. Ali, "5G-based Converged Electric Power Grid and ICT Infrastructure," in *2018 IEEE 5G World Forum (5GWF)*, Jul. 2018, pp. 33–37.

[4] B. Hu and H. Gharavi, "A Hybrid Wired/Wireless Deterministic Network for Smart Grid," *IEEE Wireless Communications*, vol. 28, no. 3, pp. 138–143, Jun. 2021, conference Name: IEEE Wireless Communications.

[5] J. Tao, M. Umair, M. Ali, and J. Zhou, "The impact of Internet of Things supported by emerging 5G in power systems: A review," *CSEE Journal of Power and Energy Systems*, vol. 6, no. 2, pp. 344–352, Jun. 2020, conference Name: CSEE Journal of Power and Energy Systems.

[6] N. Hussain, M. Nasir, J. C. Vasquez, and J. M. Guerrero, "Recent Developments and Challenges on AC Microgrids Fault Detection and Protection Systems–A Review," *Energies*, vol. 13, no. 9, p. 2149, Jan. 2020, number: 9 Publisher: Multidisciplinary Digital Publishing Institute.

[7] B. Patnaik, M. Mishra, R. C. Bansal, and R. K. Jena, "AC microgrid protection – A review: Current and future prospective," *Applied Energy*, vol. 271, p. 115210, Aug. 2020.

[8] V. Telukunta, J. Pradhan, A. Agrawal, M. Singh, and S. G. Srivani, "Protection challenges under bulk penetration of renewable energy resources in power systems: A review," *CSEE Journal of Power and Energy Systems*, vol. 3, no. 4, pp. 365–379, Dec. 2017, conference Name: CSEE Journal of Power and Energy Systems.

[9] B. Tetteh and K. Awodele, "Power System Protection Evolutions from Traditional to Smart Grid Protection," in *2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE)*, Aug. 2019, pp. 12–16, iSSN: 2575-2693.

[10] U. Shahzad, S. Kahrobaee, and S. Asgarpoor, "Protection of Distributed Generation: Challenges and Solutions," *Energy and Power Engineering*, vol. 09, no. 10, pp. 614–653, 2017.

[11] G. Bag, L. Thrybom, and P. Hovila, "Challenges and opportunities of 5G in power grids," *CIRED - Open Access Proceedings Journal*, vol. 2017, no. 1, pp. 2145–2148, Oct. 2017.

[12] T. Doukoglou, V. Gezerlis, K. Trichias, N. Kostopoulos, N. Vrakas, M. Bougioukos, and R. Legouable, "Vertical Industries Requirements Analysis & Targeted KPIs for Advanced 5G Trials," in *2019 European Conference on Networks and Communications (EuCNC)*, Jun. 2019, pp. 95–100, iSSN: 2575-4912.

[13] M. Garau, M. Anedda, C. Desogus, E. Ghiani, M. Murroni, and G. Celli, "A 5G cellular technology for distributed monitoring and control in smart grid," in *2017 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB)*, Jun. 2017, pp. 1–6, iSSN: 2155-5052.

[14] P. Jafary, A. Supponen, and S. Repo, "Network Architecture for IEC61850-90-5 Communication: Case Study of Evaluating R-GOOSE over 5G for Communication-Based Protection," *Energies*, vol. 15, no. 11, p. 3915, Jan. 2022, number: 11 Publisher: Multidisciplinary Digital Publishing Institute.

[15] H. C. Leligou, T. Zahariadis, L. Sarakis, E. Tsampasis, A. Voulkidis, and T. E. Velivassaki, "Smart Grid: a demanding use case for 5G technologies," in *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, Mar. 2018, pp. 215–220.

[16] T. A. Zerihun and B. E. Helvik, "Dependability of Smart Distribution Grid Protection Using 5G," in *2019 3rd International Conference on Smart Grid and Smart Cities (ICSGSC)*, Jun. 2019, pp. 51–59.

[17] M. O. Nait Belaid, V. Audebert, and B. Deneuville, "DESIGNING A 5G BASED SMART DISTRIBUTION GRID PROTECTION SYSTEM," in *CIRED 2021 - The 26th International Conference and Exhibition on Electricity Distribution*, vol. 2021, Sep. 2021, pp. 1241–1245.

[18] P. Hovila, H. Kokkoniemi-Tarkkanen, S. Horsmanheimo, P. Raussi, S. Borenius, and K. Ahola, "CELLULAR NETWORKS PROVIDING DISTRIBUTION GRID COMMUNICATIONS PLATFORM," in *CIRED 2021 - The 26th International Conference and Exhibition on Electricity Distribution.* , Online Conference: Institution of Engineering and Technology, 2021, pp. 1207–1211.

[19] D. Carrillo, C. Kalalas, P. Raussi, D. S. Michalopoulos, D. Z. Rodríguez, H. Kokkoniemi-Tarkkanen, K. Ahola, P. H. J. Nardelli, G. Fraidenraich, and P. Popovski, "Boosting 5G on Smart Grid Communication: A Smart RAN Slicing Approach," *IEEE Wireless Communications*, pp. 1–8, 2022, arXiv:2208.14538 [eess].

[20] R. Ricart-Sanchez, A. C. Aleixo, Q. Wang, and J. M. Alcaraz Calero, "Hardware-Based Network Slicing for Supporting Smart Grids Self-Healing over 5G Networks," in *2020 IEEE International Conference on Communications Workshops (ICC Workshops)*, Jun. 2020, pp. 1–6, iSSN: 2474-9133.

[21] P. Raussi, H. Kokkoniemi-Tarkkanen, and K. Ahola, "Methodology to Decrease Packet Loss in IEC 61850 Substation Communication over Wireless 5G Communication."

[22] "SIM8200EA_m2." [Online]. Available: https://www.simcom.com/product/SIM8200EA_M2.html

[23] N. Srivastava, A. C. Scogna, and H. Shim, "Enabling the next generation USB 3.1 (Gen 2) in mobile devices," in *2018 IEEE International Symposium on Electromagnetic Compatibility and 2018 IEEE Asia-Pacific Symposium on Electromagnetic Compatibility (EMC/APEMC)*, May 2018, pp. 18–23.

[24] "smartgridadsc/RGOOSE_rsv." [Online]. Available: https://github.com/smartgridadsc/RGOOSE_RSV

[25] S. S. Hussain, M. M. Roomi, D. Mashima, and E.-C. Chang, "End-to-End Performance Evaluation of R-SV / R-GOOSE Messages for Wide Area Protection and Control Applications," in *2023 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, Jan. 2023, pp. 1–5, iSSN: 2472-8152.

[26] M. J. Zekauskas, A. Karp, S. Shalunov, J. W. Boote, and B. R. Teitelbaum, "A One-way Active Measurement Protocol (OWAMP)," Internet Engineering Task Force, Request for Comments RFC 4656, Sep. 2006, num Pages: 56. [Online]. Available: https://datatracker.ietf.org/doc/rfc4656