Performance Evaluation of IEC 61850 GOOSE Messages over a 5G Network for Protection Coordination in Smart Grid

1st Tesfaye Amare Zerihun
SINTEF Energy Research
Trondheim, Norway
tesfaye.zerihun@sintef.no

2nd Henrik Lundkvist
SINTEF Digital
Trondheim, Norway
henrik.lundkvist@sintef.no

3rd Santiago Sanchez Acevedo
SINTEF Energy Research
Trondheim, Norway
santiago.sanchez@sintef.no

***Abstract*—With low latency communication, it is possible to improve the reliability and reduce the downtime for the electric grids with coordination of digital protection relays. 5G wireless networks are quickly getting better coverage and becoming a viable alternative for smart grid communication. Moreover, there is a significant enthusiasm within the mobile network industry for energy use cases in this context. In this paper, we evaluate the feasibility of using a commercial 5G-NR access network with 4G core for protection coordination using IEC 61850 GOOSE. This is intended to validate previous studies that have evaluated smart grid communication over experimental 5G networks and to give practical insights on how to approach the configuration of protection coordination considering the limitations of the mobile network.**

***Index Terms*—5G, IEC 61850, R-GOOSE, Protection, FLISR**

I. Introduction

One of the key features of a smart grid is its ability to self heal. Self-healing in power grids refer to automatic functionality that can increase the reliability of the power grid by detection and mitigation of faults. The functionality is often referred to as FLISR, fault localization, isolation and service restoration. Faults can be caused by for example trees falling over the power lines or equipment failure, where the affected grid section needs to be disconnected from the rest of the grid as quickly as possible, and it needs to be repaired before the section can be activated again. However, by isolating the faulty section and reconfiguring the network, the service can be restored in the surrounding parts of the grid, and the number of customers affected by the fault can be minimised if there are alternative lines that can provide energy. In the different steps of the FLISR process, there are alternative distributed and centralized solutions that can be deployed. A review of different centralized and distributed control solutions for self-healing can be found in [1], where it is noted that traditional solutions have been centralized but the number of distributed and decentralized solutions in the literature is increasing. For centralized solutions, the communication will mainly be towards the centralized control entity, while distributed or decentralized control rely on more multicast or peer-to-peer communication.

The communication requirements can be derived from IEC 61850-5. Due to some differences in the time required for circuit breakers to react, fault current detection, etc., there can be some variation in the requirements. Examples of requirements for distributed switching for isolation and service restoration are 5 ms end-to-end latency with 99.9999% service availability [2], or similarly a one-way delay of maximum 4-10 ms for teleprotection in [3]. Other sources cite more relaxed requirements, e.g. 10 ms as ideal latency and 30 ms as maximum end-to-end latency [4]. 3GPP has included the FLISR use case in the recent study on smart energy and infrastructure, and relaxed the requirement on maximum end-to-end latency to 20 ms and the service availability to 99.999% [5]. The energy use cases are highly interesting for 5G networks and the latency requirements are among the strictest identified. In this study we focus on protection coordination, where (primary and backup) protective relays are coordinated by communicating signals that indicate their state. This has somewhat lower communication requirements than the primary protection mechanism itself.

It has been frequently observed that Internet applications adapt to the service quality that the network can provide, rather than driving the development of quality of service mechanisms in the network. This has been the case for applications that are typically considered to require high quality of service, such as video streaming and phone calls. Consequently, it is intriguing to examine a comparable approach, analyze and evaluate the performance of commercial 5G networks in the context of protection coordination, and investigate if the protection coordination mechanisms can be parameterized to work within the constraints of the network.

In this paper we describe an experimental evaluation of protection coordination implemented over a commercial 5G network. The use case is very similar to the one evaluated in [4], and [6] where an experimental 5G testbed is used. However, while [4] use a test network with a 5G core and LTE

This paper has been funded by the CINELDI - Centre for intelligent electricity distribution, an 8 year Research Centre under the Research Council of Norway's FME-scheme (Centre for Environment-friendly Energy Research, 257626/E20). The authors gratefully acknowledge the financial support from the Research Council of Norway and the CINELDI partners.

radio, this paper use a commercial 5G network. A commercial network does not leave the same possibility to control network parameters but it complements the picture with measurements of the performance in an actual 5G network. The commercial 5G network uses NR, i.e. the new 5G radio interface, with an Evolved Packet Core (EPC) core network and this work will investigate and show the performance that can be expected from existing 5G non-standalone networks.

In the next section, the background for IEC 61850 and mobile communication is explained to give the context of the study. Then the methodology is described in Section III before the results are presented and discussed in Section IV. Finally the paper is concluded in Section V.

II. Background

A. IEC 61850 for wide area communication

IEC 61850 is a set of standards for substation automation, but the use of it is being extended beyond its original scope of single substations. One reason for its expansion is that it has been designed for low latency control, making it valuable for emerging functions and applications as the power system undergoes evolution. The logical nodes communicate through one of multiple communication services, that include both client-server communication and services for peer-to-peer communication. For protection coordination the Generic Object Oriented Substation Event (GOOSE) service is used for transfer of event information. It is intended for peer-to-peer multicast communication between Intelligent Electronic Devices (IEDs) to support distributed real-time solutions.

The basic GOOSE protocol is designed to work directly over Ethernet, as it was designed to be used within one substation. For the extension to wide area communication, an alternative network protocol stack is supported where the IEC 61850 communication is sent over UDP and IP, commonly reffered to as Routable-GOOSE (R-GOOSE).

Protection coordination often require wide area communication as the IEDs are located across multiple substations or geographical areas. Considering the use of IEC 61850 for protection coordination, it must be taken into consideration that R-GOOSE is not supported by many of the commercial IEDs/equipment. Moreover, IP multicast will generally not be supported on the Internet and instead requires a managed IP network. Consequently, native GOOSE despite its benefit, requires multicast Ethernet traffic to be transmitted and tunnelled through a Wide Area Network (WAN). To address this, a viable solution is to employ Generic Routing Encapsulation (GRE), a protocol designed to encapsulate and tunnel various types of payloads/packets primarily within IP networks. It is a low overhead solution that provides a minimal functionality necessary to forward data of other protocols over IP networks such as the Internet.

B. Mobile networks for smart grids

Mobile networks are among the most commonly used WAN technologies in smart grid, but effective integration of mobile networks in the smart grid context requires further considerations and customisation of the mobile network services. Several research efforts have been dedicated to exploring and addressing the specific requirements and challenges associated with integrating mobile networks into the smart grid infrastructure.

Garau et al. investigate the use of LTE for FLISR application using a co-simulation of an LTE network and distribution grid [7]. The simulations indicate that an unloaded LTE network can be used for the communication FLISR protocol, while load from other mobile network users may cause problems. An experimental evaluation of LTE for automation of smart grid has been reported in [8], the results show that LTE is useful mainly for less demanding use cases than FLISR. Similarly, statistics collected from commercial networks show that even if the mean latency is acceptable, the probability of experiencing high latencies is too high [6], [9]. There are multiple mechanisms at the radio interface that can be considered to handle limitations in LTE-based radio access networks for transport of IEC 61850 [10], the Access Class Barring mechanism in LTE can help to avoid congestion in the random access channel.

In [11] the choice of transporting L2 GOOSE directly over non-IP service of 5G is compared to using the GOOSE over IP (IEC-61850-90-5) standard and a common IP transport service of the 5G network. The conclusion is that transmission of Ethernet frames over non-IP service seems more promising once the 5G core network (5GC) is deployed. Hence, GOOSE tunnelled over GRE for transport over an emulated mobile network has been demonstrated in [12]. A 5G test network in Finland has been used to get a first indication on the feasibility of an experimental 5G URLLC implementation for differential protection, with latencies in the order of 2 ms each in uplink and downlink [6]. Routable GOOSE has been used for self-healing in [13] with network slicing to isolate GOOSE traffic and reach low latency.

C. Mobile core network

The mobile networks are divided into a Radio Access Network (RAN) and a core network. The 4th generation core, known as EPC may be distributed in a similar way to the 5GC, but the 5GC is better designed for it. For example, there is a single mobility anchor point per UE in the EPC, while it can be differentiated between multiple services running on the same UE in 5G. From a practical point of view, it has been common to have a centralized core network in EPC so that all traffic needs to pass through a central gateway, which may change in 5G. One point to notice is that mobile networks are typically designed with Internet connection as the main service. Hence, traffic will be sent over a default bearer that routes the packets out of the mobile core network to the Internet. Only for specific services such as IMS (Internet Protocol Multimedia System) based VoLTE (Voice over LTE) will a dedicated bearer be used, and the packets may be routed to a dedicated IP network. Hence, unless the MNO offers a special service to the grid operator, the packets will not only be routed to a centralized core network node, it will actually need to be routed to the Internet and then back in to the core network. For common Internet services this is a reasonable policy, which has advantages from a security point of view. However, for latency critical services it will be important to keep the routing internal to the core network, and an appropriate configuration of the network service is needed. The measurements made in this paper have been made with SIM cards that have been enabled to be routed directly in the core network. However, the EPC in this case is centralized in Oslo, at a distance of around 500 km from Trondheim where the tests have been made.

III. Methodology

A. System Considered

The paper looks into protection coordination in smart grid where digital relays/IEDs coordinate with each other to isolate, locate and clear faults. We consider a solution where the IEDs communicate with blocking signals, to create a distributed solution that can handle complex topologies thanks to the real-time communication between the IEDs. The principle of the solution can be understood from the following steps, considering a typical radial grid in smart distribution grids, as shown in Figure 1.

- A short circuit fault occurs.
- All IEDs that detect the fault downstream send blocking signal to all IEDs upstream.
- IEDs receiving block signal (from downstream IEDs) stop sending block signal upstream, since they can conclude that the fault can be isolated further downstream.
- After some delay, the IED which is closest to the fault location trips its circuit breaker.
- The IED that tripped its breaker stops sending block signal.
- IEDs upstream continues operating (no tripping), as the fault has been isolated by the downstream IED closest to the fault point.

In the context of a radial grid, the IEDs are assumed to employ time grading coordination. Each IED is programmed to initiate a trip sequence after a specified duration upon detecting a fault, unless a block signal is received. The upstream IEDs are used as a backup protection measure and they are configured with a longer reaction time, as they are intended to come into play only if the downstream IED fails. The optimal configuration of the tripping time is crucial. On one hand, a lengthier configured time implies that the fault current, if persist for a longer period, can potentially damage the grid and the propagation of the fault to other parts of the network. On the other hand, a shorter configured time raises the risk of unnecessary tripping, resulting in the shutdown of larger portions of the grid.

B. System Design

The test system comprises an MV power distribution network and an ICT support system for exchanging information between the substations in the power system network. A hardware in the loop test-bed incorporating real time simulator, commercial 5G network, communication emulator and hardware IEDs is used. A real time simulator (OPAL-RT) is used as a simulation tool for modelling the power system and some ICT components such as the virtual IEDs and virtual merging units (MU). A commercial 5G network is used for the wide area communication while mininet is used to emulate some communication network functions.

Power system: The power system considered is a 22 KV MV power distribution network with a radial topology. All substations are assumed to be equipped with advanced digital relays (IEDs). A simple schematic diagram of the power system topology is shown in Figure 1.

ICT system: The ICT support system comprises the digital relays (both virtual and hardware protection IEDs), virtual merging units (MUs) and the communication network connecting them. All the communication inside a substation and between substations is assumed to be based on the IEC 61850 protocol.

The IEDs in the first three substations (Substation 1, 2 and 3) are modelled as virtual IEDs inside OPAL-RT and the IED in Substation 4 is a hardware IED - SIEMENS 7SJ85. Each of the four IED equipped substations has virtual merging units for collecting the current and voltage measurements. For intra-substation communication, a physical Gigabit LAN/Ethernet network with Planet switch IGS-6325-16P4S is used for exchanging IEC 61850 GOOSE and sampled values (SVs) between MUs, protection IEDs and circuit breakers. Where as, for Inter-substation communication between the IEDs (exchange of blocking GOOSE messages), a commercial 5G network connected to the National Smart Grid Laboratory (NSGL) is used. In order to synchronise the Opal-RT real-time simulator and the virtual IEDs with the hardware IED , an IRIG-B led precision time protocol (PTP) is employed.

As conventional IEC 61850 GOOSE messages can not be routed outside a substation premise, an encapsulation technique named GRE, is employed at the gateways of the substations. The virtual gateways (5G Gateway switches in Figure 2) are emulated using Mininet on two different linux servers (Intel(R) Xeon(R) Silver 4110 CPU @ 2.10GHz and Intel(R) Core(TM) i7-8665U CPU @ 1.90GHz 2.11 GHz). These gateways perform functions such as the GRE encapsulation and filtering the traffic. The gateways are used to encapsulate the conventional GOOSE packets with an IP header so that the packets can be routed through the wide area network (5G). They also perform filtering of the traffic. i.e., any other traffic such as sampled values from MUs will be discarded at the gateway and only blocking GOOSE messages will be forwarded to the other substations. The virtual 5G gateways are then connected to the commercial 5G network through Huawei and Zyxel antennas.

IV. Results

This section presents the end-to-end (E2E) performance analysis of the system. The primary focus is on the E2E path, which comprises the 5G network and the IEDs, for

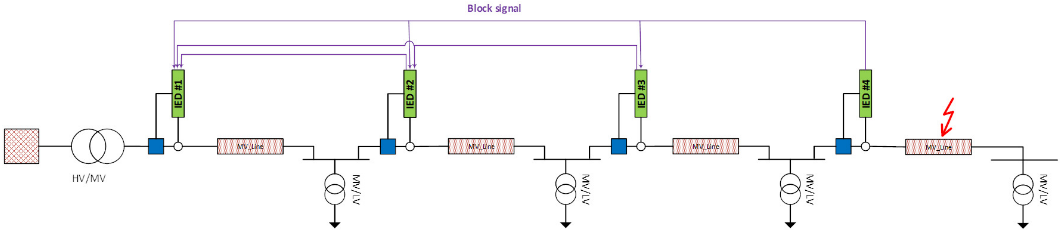

Fig. 1. Power system network.

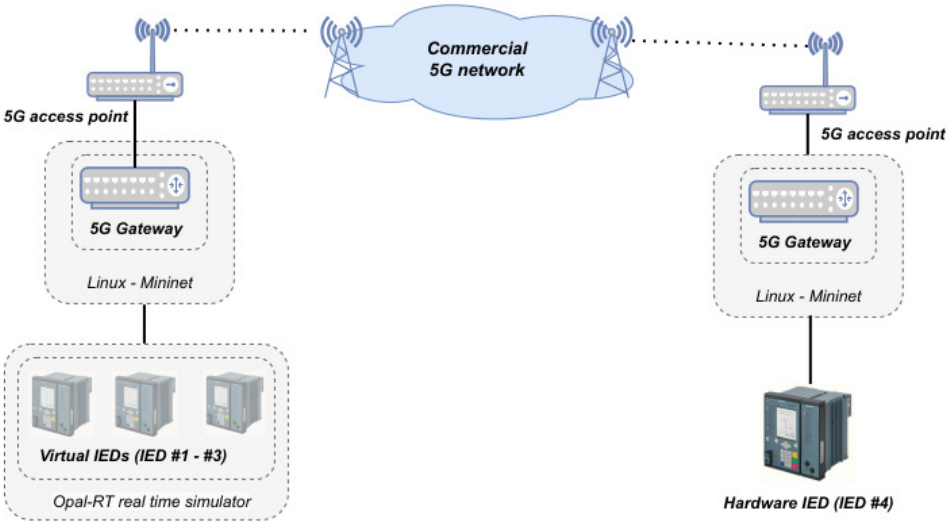

Fig. 2. Communication network architecture.

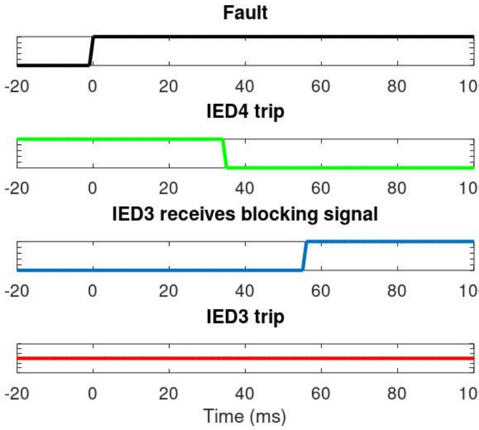

Fig. 3. Blocking signal arrive in time, IED does not trip.

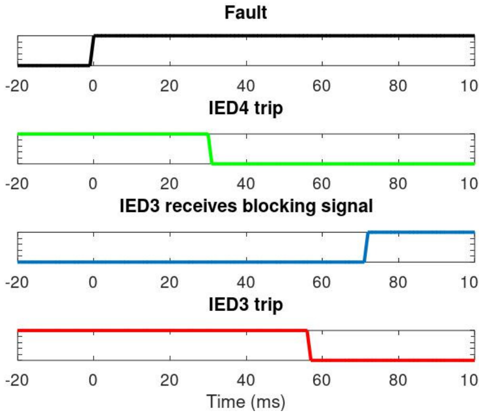

Fig. 4. Blocking signal does not arrive in time, IED3 trips.

the evaluation of the actual reaction time of the protection coordination mechanism. In addition, the insights gained and lessons learned from the use of a commercial 5G network are also discussed.

A. Grid Protection Performance

Figure 3 and Figure 4 show the timelines of events after the occurrence of a fault. The fault occurs at the end of the radial line at time 0, as shown in the top time line. The fault is then detected by IED 4 which is closest to the fault location after around 35 ms, as can be seen in the second time line. IED 4 will send a blocking signal, and the third time line shows when the blocking signal is received by the next IED (IED 3) upstream of IED 4. This depends on the random delay of the communication network. The fourth time line shows the trip status of IED 3. As long as the blocking signal arrives before the pre-configured tripping time of IED 3, the IED will not trip and the power will continue to flow. This is illustrated in Figure 3 where the tripping time at IED 3 has been set to around 60ms and the blocking signal arrived before the tripping time of IED 3. However, if the tripping delay in the IED 3 is configured to a value shorter than the time it takes for the blocking signal to arrive, IED 3 will trip. This is illustrated in Figure 4 where IED 3 trips in the fourth time line, because the blocking signal does not arrive in time.

The protection coordination scheme is therefore dependent on the latency of the transmission of the blocking signal from IED 4 to upstream IEDs such as IED 3 when a fault has been detected. This has been measured, with the blocking signal sent using GOOSE over a live commercial 5G network. The measured latencies can be seen in Figure 6 where the mean latency is 26 ms and the standard deviation is 6.2 ms.

We have also measured if the blocking signal arrives in time at IED 3. This depends on how long IED 3 is configured to wait before it trips as a backup relay. Hundreds of experiments were carried out involving various trip time setting of backup relays ranging from 20 ms to 50 ms. The results, as can be seen in Figure 5, show that with a configured trip time above 45 - 50 ms, the probability of the IED 3 tripping unnecessarily is close to zero. In fact, when trip time is set to greater than 50 ms, IED3 never tripped unnecessarilyy in our experiments, while it tripped with probability 0.2 with 30 ms setting and always tripped unnecessarily with 20 ms. This is well aligned with the observed network delays in the CDF where most packets had a delay below 40 ms. This confirms that configuring the trip time of the backup relay/IED with some margin to the average network delay is recommended.

To put the measured delays into context, we may compare this with a larger set of measurements from the open data set[1] provided by RTR (Austrian Regulatory Authority for Broadcasting and Telecommunications). These are denoted with nationwide in Figure 6, while the measurements from our experiments are denoted with single position. The nationwide data set consists of measurements taken from 5G NR networks from UEs within Austria during May of 2023, the average measured round trip time is also 26 ms. It is worth pointing out that while the measurements in Austria are round trip time measurements, we technically consider one-way end-to-end measurements between two different IEDs in our experiment setup. However, it should also be noted that both the end-points on the path we consider are located on the same mobile network, albeit in different cells. Hence, it is fully comparable to the round trip delay.

The standard deviation from the measurements in Austria is around 26 ms, i.e. significantly higher than for the measurements of the GOOSE traffic. This could be expected since the measurements in Austria are taken from different locations on different mobile networks, while the measurements in our experiments are taken from a single location in a single network. Another important point to note is that the measurements in Austria are made towards a server on the Internet, i.e. the packets need to exit from the mobile core network through a gateway and return back again. In the measurements we have made the mobile network operator has enabled traffic between the two UEs we use to be routed directly in the mobile core network. Hence, the variation in the latency can also be expected to be reduced by avoiding to pass through an Internet exchange point. In this context it is also worth noting that most traffic in Austria will need to travel shorter distances than the distance in the Norwegian network (between Trondheim and Oslo), hence it should not be surprising that the Norwegian measurements do not show lower average latency.

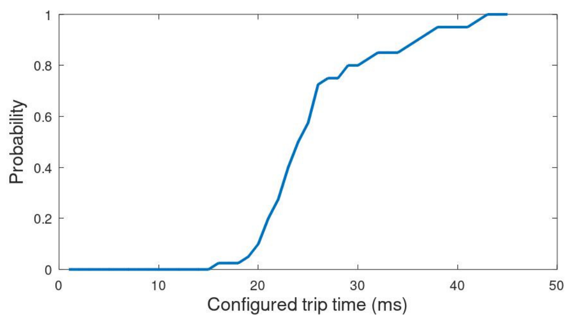

Fig. 5. The probability of blocking the backup IED (avoiding unnecessary trips) as a function of configured trip time.

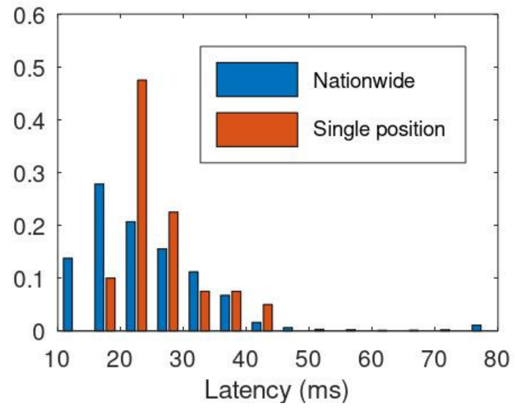

Fig. 6. Histogram of measured latency from a fault occurs until a blocking signal is received at IED 3 (red bars) and estimate of the corresponding latency histogram for the data set covering Austria.

B. Discussion

The observed network latency is generally sufficiently low to make a commercial 5G network viable for certain types of protection coordination traffic. However, the protection coordination scheme needs to be designed with the communication latency in mind so that it does not have too strict latency requirements. The principle of applications that adapt to the network performance rather than requiring strict quality of service guarantees has been widely used on the Internet. However, one aspect to consider is the time dynamics of the adaptation. While Internet applications can relatively easily

[1] https://www.netztest.at/en/Opendata

adapt and improve application performance as the network quality varies, the power grids rely on long-lived hardware that can limit what upgrades that can be implemented. In addition, the power grid as a critical infrastructure has a stringent requirement on the range of values that can be used for setting the protection coordination.

In the case of grid protection, the adaption can be made when the protection coordination scheme is configured, and possibly parameters can be updated in case of major upgrades of the communication network. The result of this study shows that the network delay for a given location has less variation than the overall delay distribution from the mobile networks in a country. Hence, by assessing the network latency when the protection coordination scheme is configured, a suitable value can be found by striking a balance between minimizing the likelihood of protection failures (such as avoiding unnecessary trips from backup IEDs) caused by network latency and minimizing the duration that grid equipment may be subjected to high currents in the event of a fault, while ensuring the safety of the grid is not compromised.

However, there are different types of grid protection and protection coordination schemes with different communication requirements. For example, some protection schemes rely on constant exchange and comparison of synchronized PMU samples which put much stricter requirements on the communication latency. Fortunately, the mobile network technology is also progressing, with new functionality for low latency and high reliability being deployed. Such network features need to be implemented by configuring policies and parameters, which should be done in cooperation between the network operator and the grid operator. For example, with the roll out of 5G core networks, it is expected that mobile networks will have a more distributed routing, which eliminates the need to send all traffic through central locations. As the mobile networks evolve, grid operators will be able to implement new advanced protection schemes, using mobile network configurations that provide sufficient quality of service.

V. Conclusion

In this paper the viability and challenges of using available commercial 5G networks for grid protection coordination have been investigated with a hardware-in-the-loop test bed. While there is limited possibilities to experiment with the parameters of a commercial network, it gives some insights into how protection coordination schemes can use available 5G networks in practice.

The first conclusion is that the parameter configuration of the protection coordination scheme should preferably be based on the measured performance of the mobile network, under the constraints of a safe grid operation. There is of course uncertainty in the measurements, but using measurements specifically from the position of the IED is more appropriate than using statistics collected over larger measurement campaigns covering wider areas. Even though this will reduce the size of the data set and therefore have less accurate results for statistical outliers, the protection coordination scheme should make a trade-off within latency values that are within the acceptable range for the application.

It should also be noted that there are significant potential for improvement of the network performance if the service can be configured to provide higher reliability and lower latency than the normal mobile broadband services. Therefore, further studies that identify suitable ways for the mobile network operator to provide services that are aligned with the requirements of the grid protection and protection coordination traffic is motivated. On the other hand, it is worth to note that there is also some room for adaptation in the protection scheme parameters, which can make it possible for the mobile network to provide a limited set of affordable services.

In future work, we plan to look into the 5G network configuration to find settings that are suitable for different protection schemes. This requires either realistic network simulation tools, or preferably control over a mobile network. Hence, as a complement to public mobile networks, we are currently building a test-bed consisting a private 5G networks that allow more room for experimentation. In addition, security is an important aspect for the protection of key infrastructure such as the power grid. This has not been considered in the scope of this paper, but needs to be addressed in future work.

References

[1] R. M. Campos, C. C. Figueroa, H. V. Oyarzún, and J. M. Baeza, "Self-healing of electric distribution networks: A review," in *2018 7th International Conference on Computers Communications and Control (ICCCC)*, 2018, pp. 63–70.

[2] 3GPP, "Study on Communication for Automation in Vertical Domains," 3rd Generation Partnership Project (3GPP), TR 22.804, Dec. 2018. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/22804.htm

[3] E. Grossman, "Deterministic Networking Use Cases," RFC 8578, May 2019. [Online]. Available: https://www.rfc-editor.org/info/rfc8578

[4] A. Aleixo, R. Paulo, R. Jorge, A. Rodrigues, C. Arantes, J. Cabaça, and P. Neves, "Resilient 5g technologies optimized for power grid protection solutions using iec 61850 time-critical communications," July 2020.

[5] 3GPP, "Study on 5G Smart Energy and Infrastructure," 3rd Generation Partnership Project (3GPP), TR 22.867, Dec. 2021. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/22867.htm

[6] P. Hovila, P. Syväluoma, H. Kokkoniemi-Tarkkanen, S. Horsmanheimo, S. Borenius, Z. Li, and M. Uusitalo, "5g networks enabling new smart grid protection solutions," 2019.

[7] M. Garau, E. Ghiani, G. Celli, F. Pilo, and S. Corti, "Co-simulation of smart distribution network fault management and reconfiguration with lte communication," *Energies*, vol. 11, no. 6, p. 1332, 2018.

[8] P. Ferrari, A. Flammini, M. Loda, S. Rinaldi, D. Pagnoncelli, and E. Ragaini, "First experimental characterization of lte for automation of smart grid," in *2015 IEEE International Workshop on Applied Measurements for Power Systems (AMPS)*. IEEE, 2015, pp. 108–113.

[9] H. Lundqvist, J. E. Håkegård, and A. Lie, "Mobile networks for smart grid revisited," in *2020 6th IEEE International Energy Conference (ENERGYCon)*. IEEE, pp. 882–887.

[10] C. Kalalas, *Cellular networks for smart grid communication*. Universitat Politècnica de Catalunya, 2018.

[11] J. Cheng, B. Kovács, and M. Darula, "Proposal for iec goose transport in 5g networks," 2018.

[12] V.-G. Nguyen, K.-J. Grinnemo, J. Taheri, and A. Brunstrom, "A deployable containerized 5g core solution for time critical communication in smart grid," in *2020 23rd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*. IEEE, 2020, pp. 153–155.

[13] 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)*, 2020, pp. 1–6.